ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ
ՀԱՄԱԼՍԱՐԱՆ

ՅՈՒՐԻ ՄՈՎՍԻՍՅԱՆ

ԲԱՐՁՐԱԳՈՒՅՆ ՀԱՆՐԱՀԱՇԻՎ ԵՎ ԹՎԵՐԻ ՏԵՍՈՒԹՅՈՒՆ

Yerevan State University

Yu. M. Movsisyan

HIGHER ALGEBRA & NUMBER THEORY

Yerevan
Yerevan State University Press
2015

Ереванский Государственный Университет

Ю. М. Мовсисян

ВЫСШАЯ АЛГЕБРА И ТЕОРИЯ ЧИСЕЛ

Ереван
Издательство Ереванского госуниверситета
2015

ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Յու. Մ. Մովսիսյան

ԲԱՐՁՐԱԳՈՒՅՆ ՀԱՆՐԱՀԱՇԻՎ ԵՎ ԹՎԵՐԻ ՏԵՍՈՒԹՅՈՒՆ

Երրորդ հրատարակություն

Թույլատրված է ՀՀ Կրթության և գիտության նախարարության կողմից որպես դասագիրք համալսարանների ուսանողների համար

ԵՐԵՎԱՆ
ԵՊՀ ՀՐԱՏԱՐԱԿՉՈՒԹՅՈՒՆ
2015

ՀՏԴ 512:511(075.8)
ԳՄԴ 22.14+22.13 ց73
Մ 917

Նվիրում եմ ծնողներիս հիշատակին

Մովսիսյան Յու. Մ.
Մ 917 Բարձրագույն հանրահաշիվ և թվերի տեսություն: Բուհական դասագիրք/ Յու. Մ. Մովսիսյան.- Երրորդ հրատարակություն.- Եր.: ԵՊՀ հրատ., 2015, 944 էջ:

«Բարձրագույն հանրահաշիվ և թվերի տեսություն» դասագիրքը հեղինակի «Բարձրագույն հանրահաշիվ», 1983 թ. ուսումնական ձեռնարկի վերամշակված և ընդլայնված տարբերակն է: Այն կազմված է երեք մասից, որոնք համապատասխանաբար կոչվում են՝ Մաս Ա. «Թվերի տեսություն», Մաս Բ. «Դասական և գծային հանրահաշիվ», Մաս Գ. «Հանրահաշվական կառուցվածքներ»: Դասագիրքը սկսվում է «Նախնական (ընդհանուր) հասկացություններ և արդյունքներ» բաժնից:

Դասագրքում բացի թվերի տեսության դասական գաղափարներից, հարցերից և արդյունքներից դիտարկվում են նաև թվերի աքսիոմային տեսության, ինչպես նաև կիրառություններին վերաբերող հարցեր: Հատուկ ուշադրություն է դարձվում թվերի տեսության հանրահաշվական բնույթի արդյունքներին և ընդհանրացումներին, որոնք բնական հենք են հանդիսանում նաև հանրահաշվի և թվերի տեսության դասընթացի հետագա զարգացումների համար և վերաբերում են խմբերին, օղակներին, դաշտերին, կավարներին, բուլյան հանրահաշիվներին:

Նախատեսվում է համալսարանների մաթեմատիկայի և մեխանիկայի, կիրառական մաթեմատիկայի և ինֆորմատիկայի, տնտեսագիտության, ֆիզիկայի և ռադիոֆիզիկայի ֆակուլտետների, ինչպես նաև հարակից մասնագիտությունների ուսանողների, ասպիրանտների, դասախոսների, ՈԲՖ-ի ունկնդիրների և գիտաշխատողների համար:

ՀՏԴ 512:511(075.8)
ԳՄԴ 22.14+22.13 ց73

ISBN 978-5-8084-1980-3

Բ ո վ ա ն դ ա կ ու թ յ ու ն

Երկու խոսք . . . 15

Նախնական (ընդհանուր) հասկացություններ և արդյունքներ . . . 17

Գ լ ու խ 0 ՏԵՍԱ-ԲԱԶՄԱՅԻՆ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐ: ԲԱԶՄՈՒԹՅՈՒՆՆԵՐԻ ՕՂԱԿ, ՀԱՆՐԱՀԱՇԻՎ ԵՎ σ-ՀԱՆՐԱՀԱՇԻՎ: ՀԱՐԱԲԵՐՈՒԹՅՈՒՆՆԵՐ ԵՎ ՀԱՄԱՐԺԵՔՈՒԹՅՈՒՆՆԵՐ: ՎԵՐՀԱՆԳՈՒՄ: ԱՐՏԱՊԱՏԿԵՐՈՒՄՆԵՐ ԵՎ ՁԵՎԱՓՈԽՈՒԹՅՈՒՆՆԵՐ: ՄԱՍՆԱԿԻ ԵՎ ԿԱՎԱՐԱՁԵՎ ԿԱՐԳԱՎՈՐՎԱԾ ԲԱԶՄՈՒԹՅՈՒՆՆԵՐ: ՏՈՊՈԼՈԳԻԱԿԱՆ ՏԱՐԱԾՈՒԹՅՈՒՆՆԵՐ: ՈՉ ՀՍՏԱԿ ԲԱԶՄՈՒԹՅՈՒՆՆԵՐ . . . 19

0.1. Գործողություններ բազմությունների հետ: Հարաբերություն և համարժեքություն . . . 19

0.2. Վերհանգում . . . 34

0.3. Արտապատկերումներ (ֆունկցիաներ) . . . 38

0.4. Մասնակի կարգ, մասնակի և կավարաձև կարգավորված բազմություններ . . . 56

0.5. Անշարժ կետի վերաբերյալ Քնաստեր-Տարսկիի և Բիրկհոֆ-Տարսկիի թեորեմները: Բանախի և Կանտոր-Շրյոդեր-Բեռնշտայնի թեորեմները . . . 64

0.6. Հարաբերությունների արտադրյալ և հակադարձ հարաբերություն . . . 70

0.7. Մասնակի կարգավորված բազմությունների իզոմորֆիզմը . . . 72

0.8. Տոպոլոգիա, տոպոլոգիական տարածություն . . . 76

0.9. Ոչ հստակ (fuzzy) ենթաբազմություններ . . . 83

Վարժություններ և խնդիրներ . . . 89

Մ ա ս Ա. Թվերի տեսություն . . . 97

Գ լ ու խ 1 ԱՄԲՈՂՋ ԹՎԵՐԻ ՄՆԱՑՈՐԴՈՎ ԲԱԺԱՆՄԱՆ ԷՎԿԼԻԴԵՍԻ (ԷՎԿԼԻԴԻ) ԿԱՆՈՆԸ (ԱԼԳՈՐԻԹՄԸ): ԲԱՂԴԱՏՈՒՄՆԵՐ, ՄՆԱՑՔՆԵՐԻ ԴԱՍԵՐ, ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐ ՄՆԱՑՔՆԵՐԻ ԴԱՍԵՐԻ ՀԵՏ: ԶՈՒԳՈՐԴԱԿԱՆ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐ . . . 99

1.1. Բաժանում և մնացորդով բաժանում . . . 99

1.2. Բաղդատումներ: Մնացքային տոպոլոգիա 107
1.3. Գործողություններ մնացքների դասերի հետ 114
1.4. Զուգորդական գործողություն և ընդհանրացված զուգորդականություն 117
Վարժություններ և խնդիրներ 123

Գ լ ու խ 2 ԵՐԿՈՒ ԱՄԲՈՂՋ ԹՎԵՐԻ ԱՄԵՆԱՄԵԾ ԸՆԴՀԱՆՈՒՐ ԲԱԺԱՆԱՐԱՐԸ: ԷՎԿԼԻԴԵՍԻ ԱԼԳՈՐԻԹՄԸ: ՖԻԲՈՆԱՉԻԻ ՀԱՋՈՐԴԱԿԱՆՈՒԹՅՈՒՆԸ 127
Վարժություններ և խնդիրներ 139

Գ լ ու խ 3 ՓՈԽԱԴԱՐՁԱԲԱՐ ՊԱՐԶ ԱՄԲՈՂՋ ԹՎԵՐ: ՉԻՆԱԿԱՆ ԹԵՈՐԵՄԸ ԲԱՂԴԱՏՈՒՄՆԵՐԻ (ՄՆԱՑՈՐԴՆԵՐԻ) ՎԵՐԱԲԵՐՅԱԼ ..143
3.1. Փոխադարձաբար պարզ ամբողջ թվերի հատկությունները ...143
3.2. Բաղդատումներով հավասարումներ և համակարգեր 150
Վարժություններ և խնդիրներ 156

Գ լ ու խ 4 ԵՐԿՈՒ ԱՄԲՈՂՋ ԹՎԵՐԻ ԱՄԵՆԱՓՈՔՐ ԸՆԴՀԱՆՈՒՐ ԲԱԶՄԱՊԱՏԻԿԸ 161
Վարժություններ և խնդիրներ 167

Գ լ ու խ 5 ՄԻ ՔԱՆԻ ԱՄԲՈՂՋ ԹՎԵՐԻ ԱՄԵՆԱՄԵԾ ԸՆԴՀԱՆՈՒՐ ԲԱԺԱՆԱՐԱՐԸ ԵՎ ԱՄԵՆԱՓՈՔՐ ԸՆԴՀԱՆՈՒՐ ԲԱԶՄԱՊԱՏԻԿԸ ..169
Վարժություններ և խնդիրներ 176

Գ լ ու խ 6 ՊԱՐԶ ԹՎԵՐ: ՎԻԼՍՈՆԻ ԹԵՈՐԵՄԸ: ԹՎԱԲԱՆՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԹԵՈՐԵՄԸ: ՄՅՈԲԻՈՒՍԻ ՖՈՒՆԿՑԻԱՆ: ՀԱՆՐԱՀԱՇՎԻ ՀԻՄՆԱԿԱՆ ԹԵՈՐԵՄԸ ՊԱՐԶ ՀԵՆՔՈՎ ԲԱՂԴԱՏՈՒՄՆԵՐԻ ՎԵՐԱԲԵՐՅԱԼ 179
6.1. Թվի պարզության Վիլսոնի հայտանիշը 179
6.2. Բնական թվի վերլուծությունը պարզ արտադրիչների: Մյոբիուսի ֆունկցիան 182
6.3. Հանրահաշվական բաղդատումներ 191
Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ 194

Գ լ ու խ 7 ՊԱՐԶ ԹՎԵՐԻ ԲԱՇԽՈՒՄԸ: ԷՎԿԼԻԴԵՍԻ, ԷՅԼԵՐԻ, ԲԵՐԹՐԱՆԻ, ՊՈՅԱՅԻ, ԴԻՐԻԽԼԵԻ, ԳՈԼԴԲԱԽԻ ԹԵՈՐԵՄՆԵՐԸ .. 199
Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ 217

Գ լ ու խ 8 ԻՐԱԿԱՆ ԹՎԻ ԱՄԲՈՂՋ ՄԱՍ: ԼԵԺԱՆԴՐԻ ԹԵՈՐԵՄԸ 221
Վարժություններ և խնդիրներ 228

Գ լ ու խ 9 ԷՅԼԵՐԻ ՖՈՒՆԿՑԻԱՆ: ԷՅԼԵՐԻ, ՖԵՐՄԱՅԻ, ԼՈՒԿԱՍԻ, ԳԱՈՒՍԻ, ՄՅՈԲԻՈՒՍԻ ԹԵՈՐԵՄՆԵՐԸ: ՊՍԵՎԴՈՊԱՐԶ ԹՎԵՐ: ԹՎԱԿԵՐՊ ԲԱԶՄՈՒԹՅՈՒՆՆԵՐ ԵՎ ԱՐՏԱԴՐՅԱԼԱՅԻՆ ՖՈՒՆԿՑԻԱՆԵՐ: ԿԱՏԱՐՅԱԼ ԵՎ p-ԱԴԻԿ ԹՎԵՐ 233
9.1. Էյլերի ֆունկցիայի սահմանումը, Էյլերի և Ֆերմայի թեորեմները: Պսևդոպարզ և լիովին պսևդոպարզ (Քարմայքլի) թվեր 233
9.2. Ամբողջ թվի կարգ ըստ տրված հենքի: Լուկասի թեորեմը 239
9.3. Էյլերի ֆունկցիայի հատկությունները 243
9.4. Թվակերպ բազմություններ և արտադրյալային ֆունկցիաներ: τ և σ ֆունկցիաները: Կատարյալ թվեր 252
9.5. Ֆունկցիաների Դիրիխլեի արտադրյալ: Մյոբիուսի թեորեմը շրջման վերաբերյալ 262
9.6. Ամբողջ p-ադիկ թվեր 267
9.7. p-ադիկ թվեր 276
Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ 278

Գ լ ու խ 10 ԵՐԿՐՈՐԴ ԱՍՏԻՃԱՆԻ ԲԱՂԴԱՏՈՒՄՆԵՐ: ՔԱՌԱԿՈՒՍԱՅԻՆ ՄՆԱՑՔ ԵՎ ՈՉ-ՄՆԱՑՔ: ԼԵԺԱՆԴՐԻ ՊԱՅՄԱՆԱՆՇԱՆ 285
10.1. Քառակուսային մնացք և ոչ-մնացք 285
10.2. Լեժանդրի պայմանանշանը 288
Վարժություններ և խնդիրներ 301

Գ լ ու խ 11 ԹՎԵՐԻ ՏԵՍՈՒԹՅԱՆ ԿԻՐԱՌՈՒԹՅՈՒՆԸ ԳԱՂՏՆԱԳՐՈՒԹՅԱՆ ՄԵՋ (ԿՐԻՊՏՈԳՐԱՖԻԱՅՈՒՄ).........................305
Վարժություններ և խնդիրներ 310

Գ լ ու խ 12 ԳԱՂԱՓԱՐ ԹՎԵՐԻ ՏԵՍԱ-ԲԱԶՄԱՅԻՆ ԵՎ ԱՔՍԻՈՄԱՅԻՆ ԿԱՌՈՒՑՈՒՄՆԵՐԻ ՎԵՐԱԲԵՐՅԱԼ 311

12.1. Տեսա-բազմային մոտեցում 311
12.2. Աքսիոմային մոտեցում 314
Վարժություններ և խնդիրներ 324

Մ ա ս Բ. Դասական և գծային հանրահաշիվ 327

Գ լ ու խ 13 ՏԵՂԱԴՐՈՒԹՅՈՒՆՆԵՐ ԵՎ ՏԵՂԱՓՈԽՈՒԹՅՈՒՆՆԵՐ 329
13.1. Զույգ և կենտ տեղադրություններ 329
13.2. Տեղափոխություններ, դրանց արտադրյալը 337
13.3. Շրջուն (ցիկլային) տեղադրություններ 339
Վարժություններ և խնդիրներ 346

Գ լ ու խ 14 ՄԱՏՐԻՑՆԵՐ ԵՎ ՈՐՈՇԻՉՆԵՐ 347
14.1. Մատրիցի գաղափարը: Գործողություններ մատրիցների հետ 347
14.2. Հակադարձելի մատրիցներ 356
14.3. Աջից կամ ձախից հակադարձելի ուղղանկյուն մատրիցներ . . . 370
14.4. Մատրիցի որոշիչը 375
14.5. Որոշիչի վերլուծությունը ըստ մատրիցի տողի (սյան) տարրերի 385
14.6. Իրական գործակիցներով գծային հավասարումների համակարգեր: Կրամերի և Գաուսի եղանակները 390
14.7. Օղակի և դաշտի հասկացությունները: Դաշտի բնութագրիչը: Օղակների և դաշտերի իզոմորֆիզմը 401
14.8. Օղակների և դաշտերի վրա որոշված մատրիցներ, որոշիչներ և գծային հավասարումների համակարգեր 412
Վարժություններ և խնդիրներ 418

Գ լ ու խ 15 ԿՈՄՊԼԵՔՍ ԹՎԵՐ 423
15.1. Սահմանումը և գործողություններ կոմպլեքս թվերի հետ 423
15.2. Կոմպլեքս թվի սովորական տեսքը, մոդուլը, համալուծը, նորմը, արգումենտը և եռանկյունաչափական տեսքը: Կոմպլեքս թվից n-րդ աստիճանի արմատ հանելը 428
15.3. Մեկից n-րդ աստիճանի արմատներ և նախնական արմատներ 436

15.4. Գաուսյան և ամբողջ գաուսյան թվեր: Մնացորդով բաժանման ալգորիթմը . . . 441
Վարժություններ և խնդիրներ . . . 445

Գ լ ու խ 16 ԲԱԶՄԱՆԴԱՄՆԵՐ . . . 447
16.1. Ներածություն . . . 447
16.2. Բազմանդամի սահմանումը: Գործողություններ բազմանդամների հետ: Մնացորդով բաժանման ալգորիթմը . . . 449
16.3. Բազմանդամների ամենամեծ ընդհանուր բաժանարար . . . 462
16.4. Փոխադարձաբար պարզ բազմանդամներ . . . 468
16.5. Չբերվող (պարզ) բազմանդամներ . . . 472
16.6. Բազմանդամի բազմապատիկ արմատներ և ածանցյալ: Թեյլորի բանաձևը զրո բնութագրիչով դաշտի դեպքում . . . 479
16.7. Ռացիոնալ կոտորակներ (ֆունկցիաներ) . . . 490
16.8. Մնացքների օղակ և մնացքների դաշտ ըստ տրված բազմանդամի . . . 502
16.9. Դաշտի պարզ ընդլայնումներ . . . 507
16.10. Բազմանդամի վերլուծության դաշտը: Կրոնեկերի և Գալուայի թեորեմները . . . 510
Վարժություններ և խնդիրներ . . . 517

Գ լ ու խ 17 ԳԾԱՅԻՆ (ՎԵԿՏՈՐԱԿԱՆ) ՏԱՐԱԾՈՒԹՅՈՒՆՆԵՐ . . . 521
17.1. Գծային (վեկտորական) տարածության գաղափարը: Գծային կախվածություն և անկախություն: Գծային կախվածության հիմնական թեորեմը . . . 521
17.2. Համակարգի (հաջորդականության) հենք և ռանգ . . . 530
17.3. Մատրիցի ռանգ . . . 533
17.4. Արտադրյալ մատրիցի ռանգը: Ուղղանկյուն մատրիցի աջից (կամ ձախից) հակադարձելիության հայտանիշը . . . 539
17.5. Կրոնեկեր-Կապելլիի թեորեմը . . . 543
17.6. Հենքային ենթամատրից և մատրիցի ռանգ . . . 544
17.7. Գծային (վեկտորական) տարածության հենք և չափողականություն: Ենթատարածություն . . . 548

17.8. Գծային հավասարումների համատեղելի համակարգի ընդհանուր լուծում 555
17.9. Վեկտորի կոորդինատներ և կոորդինատների ձևափոխությունը հենքի փոփոխության դեպքում 562
17.10. Ենթատարածությունների հատում, գումար և ուղիղ գումար 566
17.11. Գծային տարածությունների իզոմորֆիզմը (նույնաձևությունը) 575
17.12. Գծային ձևեր (ֆունկցիաներ)։ Համալուծ տարածություն . . . 578
17.13. Քանորդ (կամ ֆակտոր) -տարածություններ 584
17.14. Գծային արտապատկերումներ։ Գծային արտապատկերման միջուկի և պատկերի կապը 588
17.15. Գծային արտապատկերումների գծային տարածություն։ Գծային արտապատկերման մատրից։ Գծային ձևափոխության որոշիչ և հետք 596
17.16. Գծային հանրահաշիվներ։ Գծային հանրահաշիվների իզոմորֆիզմը։ Քելիի թեորեմը զուգորդական և միավորով գծային հանրահաշիվների համար 604
17.17. Երկգծային ձևեր։ Երկգծային ձևի մատրից և ռանգ 612
17.18. Սիմետրիկ և շեղսիմետրիկ երկգծային ձևեր։ Երկգծային ձևի միջուկ։ Ենթատարածության օրթոգոնալ լրացում 620
17.19. Քառակուսային ձևեր։ Իներցիայի օրենքը։ Սիլվեստրի հայտանիշը։ Քառակուսային ձևի բերումը կանոնական տեսքի 627
17.20. Էվկլիդյան (էվկլիդեսյան) տարածություններ։ Պյութագորասի թեորեմը, Կոշի-Բունյակովսկու անհավասարությունը։ Օրթոգոնալացման ընթացքը։ Էվկլիդյան տարածությունների իզոմորֆիզմը 641
17.21. Գծային ձևափոխության ինվարիանտ ենթատարածություն, սեփական արժեք, սեփական վեկտոր, բացասող բազմանդամ, բնութագրիչ բազմանդամ։ Համիլտոն-Քելիի թեորեմը 656
17.22. Անկյունագծային մատրիցով գծային ձևափոխություններ։ Գծային տարածության վերլուծումը ինվարիանտ ենթատարածությունների ուղիղ գումարի։ Արմատային ենթատարածություններ։ Ժորդանյան մատրիցներ։ Ժորդանյան հենք 669
Վարժություններ և խնդիրներ 682

Մ ա ս Գ. Հանրահաշվական կառուցվածքներ 685

Գ լ ու խ 18 ԽՄԲԵՐ 687

18.1. Կիսախմբի, քվազիխմբի, խմբի և աբելյան խմբի գաղափարները 687

18.2. Ենթակիսախմբեր և ենթախմբեր 703

18.3. Խմբերի և կիսախմբերի իզոմորֆիզմը: Քելիի թեորեմը և դրա հակադարձումը 715

18.4. Խմբի տարրի ամբողջ աստիճան և կարգ: Միածին ենթախմբեր և միածին խմբեր: Լագրանժի թեորեմը վերջավոր միածին խմբերում 721

18.5. Ձախ և աջ հարակից դասեր: Ենթախմբի նշիչ: Լագրանժի և Ֆերմայի թեորեմները վերջավոր խմբերում: Ինվարիանտ ենթախմբեր, քանորդ-խմբեր: Կոշու թեորեմը վերջավոր աբելյան խմբերում 738

18.6. Խմբային հոմոմորֆիզմներ, խմբային հոմոմորֆիզմի միջուկ և պատկեր: Քելիի ընդհանրացված թեորեմը: Հոմոմորֆիզմների և իզոմորֆիզմների թեորեմները խմբերում 751

18.7. Խմբերի ավտոմորֆիզմներ և ներքին ավտոմորֆիզմներ 763

18.8. Խմբերի ուղիղ և կիսաուղիղ արտադրյալներ 767

18.9. Խմբի ազդեցությունը բազմության վրա: Ուղեծիր, կայունացնող ենթախումբ և դասերի հավասարում: Բեռնսայդի լեմմը . . . 776

18.10. Կոշու թեորեմը կամայական վերջավոր խմբի համար: Վերջավոր p-խմբի կենտրոնը 783

18.11. Սիլովի թեորեմները (P.L.M. Sylow, 1832-1918) 787

18.12. Խմբերի ծնիչների բազմություն: Խմբի ածանցյալ 792

18.13. Դիսկրետ լոգարիթմներ 800

18.14. Կիսախմբային հոմոմորֆիզմներ, կիսախմբային հոմոմորֆիզմի միջուկ և կոնգրուենցիա, քանորդ-կիսախումբ: Կիսախմբային հոմոմորֆիզմների թեորեմները 801

Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ 806

Գ լ ու խ 19 ՕՂԱԿՆԵՐ ԵՎ ԴԱՇՏԵՐ 813
19.1. Օղակի, մարմնի, դաշտի, կիսաօղակի, քվազիօղակի գաղափարները: Վերջավոր դաշտեր: Վան դեր Վարդենի թեորեմը 813
19.2. Ենթաօղակի, իդեալի և քանորդ-օղակի գաղափարները 825
19.3. Գլխավոր իդեալներով օղակներ: Ամենամեծ ընդհանուր բաժանարարը, ամենափոքր ընդհանուր բազմապատիկը և թվաբանության հիմնական թեորեմի ընդհանրացումը գլխավոր իդեալներով օղակներում: Փոխադարձաբար պարզ տարրեր . 829
19.4. Էվկլիդյան օղակներ 846
19.5. Թվաբանական օղակներ: Ֆերմայի և Էյլերի ֆունկցիաները թվաբանական օղակներում: Օղակների վրա որոշված արտադրյալային ֆունկցիաներ 852
19.6. Օղակային հոմոմորֆիզմներ: Օղակային հոմոմորֆիզմի միջուկ: Հոմոմորֆիզմների և իզոմորֆիզմների թեորեմները օղակներում 861
19.7. Քելիի թեորեմը զուգորդական և միավորով օղակների համար 867
19.8. Պարզ և մաքսիմալ իդեալներ 868
Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ 873

Գ լ ու խ 20 ԿԱՎԱՐՆԵՐ, ԲԱՇԽԱԿԱՆ ԵՎ ՄՈԴՈՒԼՅԱՐ (ԴԵԴԵԿԻՆԴՅԱՆ) ԿԱՎԱՐՆԵՐ, ԲՈՒԼՅԱՆ ԵՎ ԴԵ ՄՈՐԳԱՆԻ ՀԱՆՐԱՀԱՇԻՎՆԵՐ 879
20.1. Կավարի գաղափարը 879
20.2. Մոդուլյար (Դեդեկինդյան) կավարներ 883
20.3. Բաշխական կավարներ 887
20.4. Բուլյան հանրահաշվի գաղափարը 892
20.5. Կավարների իզոմորֆիզմը 898
20.6. Բուլյան հանրահաշիվների իզոմորֆիզմը 901
20.7. Կավարի իդեալներ և ֆիլտրներ: Պարզ և մաքսիմալ իդեալներ 906
20.8. Բաշխական կավարի և բուլյան հանրահաշվի ներկայացումը ենթաբազմություններով: Բուլյան հանրահաշվի ներկայացումը տոպոլոգիական տարածության բաց-փակ բազմություններով . 909
20.9. Դե Մորգանի հանրահաշիվներ 915

20.10. σ-կավարներ և բուլյան σ-հանրահաշիվներ 920
20.11. Կոնգրուենցիաներ: Հոմոմորֆիզմների թեորեմը կավարներում 920
Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ 927
Չլուծված խնդիրներ 931
Առարկայական ցանկ 935
Լրացուցիչ գրականություն 941

Երկու խոսք

«Բարձրագույն հանրահաշիվ և թվերի տեսություն» դասագիրքը հանդիսանում է հեղինակի «Բարձրագույն հանրահաշիվ», 1983 թ. ուսումնական ձեռնարկի վերամշակված և ընդլայնված տարբերակը: Դասագիրքը կազմված է երեք մասից, որոնք համապատասխանաբար կոչվում են՝

Մաս Ա. «Թվերի տեսություն»,

Մաս Բ. «Դասական և գծային հանրահաշիվ»,

Մաս Գ. «Հանրահաշվական կառուցվածքներ»:

Այս երեք մասերը օրգանապես կապված են: Դասագիրքը սկսվում է «Նախնական (ընդհանուր) հասկացություններ և արդյունքներ» բաժնից, որի որոշ գաղափարներ և արդյունքներ ունեն նաև ինքնուրույն հետաքրքրություն (օրինակ, անշարժ կետի վերաբերյալ Քնաստեր-Տարսկիի թեորեմը հաճախ կիրառվում է նաև տրամաբանական ծրագրավորման սեմանտիկայի հարցերում): Այս բաժնին կարելի է անդրադառնալ ըստ անհրաժեշտության: Մաս Ա-ն նվիրված է թվերի տեսությանը, որտեղ թվերի տեսության դասական հասկացությունների, հարցերի և արդյունքների հետ մեկտեղ քննարկվում են նաև թվերի աքսիոմային տեսության, ինչպես նաև կիրառություններին վերաբերող հարցեր, որոնք արդիական են: Հատուկ ուշադրություն է դարձվում թվերի տեսության հանրահաշվական բնույթի արդյունքներին, ինչպես նաև հանրահաշվական բնույթի ընդհանրացումներին, որոնք բնական հենք են հանդիսանում նաև հանրահաշվի և թվերի տեսության դասընթացի հետագա զարգացումների համար և վերաբերում են խմբերին, օղակներին, դաշտերին, կավարներին, բուլյան հանրահաշիվներին: Դասընթացի ծրագրի սահմանափակ լինելու պատճառով ալգորիթմների բարդություններին վերաբերող հարցերը հիմնականում դուրս են մնացել մեր դիտարկումներից: Նույն պատճառով որոշ արդյունքներ բերվում են առանց ապացուցումների կամ վարժությունների և խնդիրների տեսքով: Ըստ որում, վարժությունների և խնդիրների մի զգալի մասն ուղեկցվում է հանգամանալից ցուցումներով, որոնց ուսումնասիրությունը կլինի օգտակար ընթերցողների համար: Սակայն դասագիրքը պարունակում է նաև նոր մոտեցումներ, նոր հասկացություններ (դրանք մատուցվող նյութը դարձնում են մատչելի, իսկ ընդհանրացումների տեսանկյունից՝ ավելի դյուրին և գրավիչ) և չլուծված խնդիրների ձևակերպումներ, որոնց մի մասը դասական է: Ճշտվում են նաև մինչ այժմ հրապարակված մի շարք արդյունքներ և ապացուցումներ:

Ապացուցման վերջը կամ նրա բացակայությունը դասագրքում նշանակվում է □ նշանով:

Նշենք նաև, որ խմբերի և օղակների տեսության (կամ խմբի ու օղակի գաղափարների) տեսանկյունից թվերի տեսության շատ արդյունքներ և գաղափարներ դառնում են ավելի պարզ, մատչելի և ընդհանուր, ինչպես ձևակերպումների, այնպես էլ ապացույցների տեսանկյունից: Սակայն այստեղ, հաշվի առնելով խմբի և օղակի գաղափարների անսովոր լինելը սկսնակ ուսանողների համար, մենք խուսափել ենք թվերի տեսության ավանդական հարցերում խմբի և օղակի գաղափարների կիրառություններից՝ թողնելով այն դասագրքի վերջում (Մաս Գ), որտեղ խմբերի և օղակների տեսության տեսանկյունից ներկայացվում են նաև տեսա-թվային բնույթի մի շարք ընդհանուր արդյունքներ, որոնք ունեն նաև հանրահաշվական նշանակություն և հետաքրքրություն: Մասնավորապես, խմբերի և օղակների տեսության ընդհանուր դիրքերից հասկանալի են դառնում մի շարք դասական տեսա-թվային արդյունքների իրական պատճառները: Օրինակ, պարզ թվերի քանակն անվերջ է (Էվկլիդես), որովհետև ամբողջ թվերի օղակի հակադարձելի տարրերի խումբը վերջավոր է: Մինչդեռ, թվային համակարգերի տեսա-քվազիխմբային հետազոտություններ մինչ այժմ չեն կատարված:

Վերջին տասնամյակներում հանրահաշվի և թվերի տեսության նկատմամբ աճող գիտական հետաքրքրությունը պայմանավորված է նաև դրանց կիրառություններով՝ կոմպյուտերային (համակարգչային) գիտության մեջ (տես՝ D.E. Knuth, The Art of Computer Programming, Vol. 2, Seminumeric Algorithms, 3rd ed., Addison-Wesley, Reading, Mass., 1998):

Դասագիրքը նաև հող է նախապատրաստում ուսանողների հետագա կուրսային, ավարտական և հետազոտական աշխատանքների համար:

Հեղինակ

Դասագրքի երրորդ հրատարակության առթիվ ճշտվել են նախորդ հրատարակության մեջ տեղ գտած վրիպակները:

Հեղինակ

Նախնական (ընդհանուր) հասկացություններ – արդյունքներ

Գ լ ու խ 0

ՏԵՍԱ-ԲԱԶՄԱՅԻՆ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐ: ԲԱԶՄՈՒԹՅՈՒՆՆԵՐԻ ՕՂԱԿ, ՀԱՆՐԱՀԱՇԻՎ ԵՎ σ-ՀԱՆՐԱՀԱՇԻՎ: ՀԱՐԱԲԵՐՈՒԹՅՈՒՆՆԵՐ ԵՎ ՀԱՄԱՐԺԵՔՈՒԹՅՈՒՆՆԵՐ: ՎԵՐՀԱՆԳՈՒՄ: ԱՐՏԱՊԱՏԿԵՐՈՒՄՆԵՐ ԵՎ ՁԵՎԱՓՈԽՈՒԹՅՈՒՆՆԵՐ: ՄԱՍՆԱԿԻ ԵՎ ԿԱՎԱՐԱՁԵՎ ԿԱՐԳԱՎՈՐՎԱԾ ԲԱԶՄՈՒԹՅՈՒՆՆԵՐ: ՏՈՊՈԼՈԳԻԱԿԱՆ ՏԱՐԱԾՈՒԹՅՈՒՆՆԵՐ: ՈՉ ՀՍՏԱԿ ԲԱԶՄՈՒԹՅՈՒՆՆԵՐ

0.1. Գործողություններ բազմությունների հետ: Հարաբերություն և համարժեքություն

0.1.1. Բազմություն, ենթաբազմություն: Բազմություն ասելով հասկացվում է կամայական ընդակների (օբյեկտների) կամայական համախմբություն (համախումբ), դաս: Այն ընդակները (տառերը, նշանները, առարկաները կամ գաղափարները), որոնցից կազմված է տրված (տված) բազմությունը, կոչվում են դրա տարրեր:

Այն փաստը, որ a-ն A բազմության տարր է, համառոտ գրվում է $a \in A$ կամ $A \ni a$ տեսքով, հակառակ դեպքում գրվում է՝ $a \notin A$ կամ $a \bar{\in} A$: Եթե $a_1 \in A, \ldots, a_n \in A$, ապա համառոտ գրվում է՝ $a_1, \ldots, a_n \in A$:

Վերջավոր թվով $a_1, \ldots, a_n$ տարրերից կազմված բազմությունը սովորաբար նշանակվում է հետևյալ կերպ՝ $\{a_1, \ldots, a_n\}$: Ընդ որում, մեկ տարրանի $\{a\}$ բազմությունը և ինքը a տարրը ընդունվում են որպես տարբեր մաթեմատիկական ընդակներ (օբյեկտներ):

Եթե $P(x)$-ով նշանակենք այն փաստը, որ x-ը օժտված է P հատկությամբ, ապա $\{x|\ \ P(x)\}$ ձևով կնշանակվի բոլոր այն x ընդակների (օբյեկտների) բազմությունը, որոնք օժտված են P հատկությամբ, իսկ $\{x \in A|\ P(x)\}$ ձևով կնշանակվի A բազմության բոլոր այն տարրերի բազմությունը, որոնք օժտված են P հատկությամբ:

Բազմության տարրերը ևս կարող են լինել բազմություններ: Դիտարկվում է նաև այնպիսի բազմություն, որը չի օժտված և ոչ մի տարրով: Այդպիսի բազմությունը կոչվում է **դատարկ բազմություն**:

Բազմությունը կոչվում է **վերջավոր**, եթե այն կազմված է վերջավոր թվով տարրերից կամ դատարկ է: Հակառակ դեպքում բազմությունը կոչվում է **անվերջ**:

Վերջավոր բազմությունների տեսությունը կոչվում է նաև **կոմբինատորիկա**:

A բազմությունը կոչվում է B բազմության **ենթաբազմություն** և գրվում է $A \subseteq B$ կամ $B \supseteq A$, եթե դրա յուրաքանչյուր տարր պատկանում է նաև B բազմությանը: Ըստ սահմանման, յուրաքանչյուր բազմություն հանդիսանում է իր ենթաբազմությունը՝ $A \subseteq A$ և դատարկ բազմությունը ցանկացած բազմության ենթաբազմություն է: Մյուս կողմից, եթե $A \subseteq B$ և $B \subseteq C$, ապա ակնհայտ է, որ $A \subseteq C$: Այլ կերպ ասած, ենթաբազմության գաղափարը օժտված է առինքնության և փոխանցական հատկություններով: Եթե $A \subseteq B$, ապա B-ն կոչվում է A-ի **վրաբազմություն** կամ **ընդլայնում**:

Երկու A և B բազմություններ կոչվում են **հավասար** և գրում են $A = B$, եթե $A \subseteq B$ և $B \subseteq A$: Հակառակ դեպքում A, B բազմությունները կոչվում են **ոչ հավասար** (տարբեր) և գրվում է՝ $A \neq B$: Երկու բազմությունների հավասարությունը երբեմն կոչվում է նաև դրանց տեսա-բազմային հավասարություն:

Դատարկ բազմությունը որոշվում է միարժեքորեն և այն սովորաբար նշանակվում է $\emptyset$ նշանով: Սակայն $\{\emptyset\}$ բազմությունն արդեն դատարկ չէ: Միևնույն A բազմության բոլոր ենթաբազմությունների բազմությունը նշանակվում է 2^A-ով կամ $pow(A)$-ով:

Վերջավոր A բազմության միմյանցից տարբեր տարրերի թիվը կոչվում է այդ բազմության կարգ և նշանակվում է $|A|$-ով: Եթե $|A| = n$, ապա վերջավոր A բազմությունը կոչվում է նաև n-տարրանի: Մասնավորապես, դատարկ բազմության կարգը կլինի զրո:

A բազմության x, y տարրերի **կարգավորված զույգը** ընդունված է նշանակել (x, y)-ով, որոնց հավասարությունը հասկացվում է հետևյալ կերպ՝

$$(x, y) = (x', y') \Longleftrightarrow x = x' \text{ և } y = y',$$

որտեղ «$\Longleftrightarrow$» կամ «$\longleftrightarrow$» նշանն ունի «այն և միայն այն դեպքում» իմաստը: Հաճախ օգտագործվում են նաև հետևյալ տրամաբանական նշանները՝ $\Longrightarrow$ կամ $\longrightarrow$ («բխում է», «հետևում է»), $\forall$ («ցանկացած», «կամայական»), $\exists$ («գոյություն ունի», «որևէ»), $\exists!$ («գոյություն ունի միակ»), $\vee$ («կամ»), $\wedge$ («և»):

Սովորաբար, բոլոր բնական[1] թվերի, բոլոր ամբողջ թվերի, բոլոր ռացիոնալ թվերի և բոլոր իրական թվերի բազմությունները

[1]Զրոն երբեմն համարվում է բնական թիվ, երբեմն՝ ոչ:

համապատասխանաբար նշանակվում են $\mathbb{N}$-ով, $\mathbb{Z}$-ով, $\mathbb{Q}$-ով և $\mathbb{R}$-ով: Մասնավորապես,

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$$

և այն օժտված է հետևյալ հանրահաշվական հատկություններով, որոնք համարվում են հայտնի.

1) Եթե $a, b \in \mathbb{Z}$, ապա $a + b \in \mathbb{Z}$ և $a \cdot b \in \mathbb{Z}$ (փակությունը գումարման և բազմապատկման (արտադրյալի) նկատմամբ);

2) Եթե $a, b \in \mathbb{Z}$, ապա $a + b = b + a$ և $a \cdot b = b \cdot a$ (գումարման և բազմապատկման գործողությունների տեղափոխական հատկություն կամ նույնություն);

3) Եթե $a, b, c \in \mathbb{Z}$, ապա $a + (b + c) = (a + b) + c$ և $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (գումարման և բազմապատկման գործողությունների զուգորդական հատկություն կամ նույնություն);

4) Եթե $a, b, c \in \mathbb{Z}$, ապա $a(b + c) = ab + ac$ (բաշխական հատկություն կամ նույնություն);

5) Եթե $a \in \mathbb{Z}$, ապա $a + 0 = 0 + a = a$ և $a \cdot 1 = 1 \cdot a = a$ (միավորի գոյությունը գումարման և բազմապատկման գործողությունների համար);

6) Եթե $a \in \mathbb{Z}$, ապա $a + (-a) = (-a) + a = 0$ (հակադիրի (հակադարձի) գոյությունը գումարման գործողության համար);

7) Եթե $a \in \mathbb{Z}$, ապա $a \cdot 0 = 0 \cdot a = 0$ (զրոյի հատկություն բազմապատկման գործողության նկատմամբ);

8) Եթե $a, b, c \in \mathbb{Z}$, $a \neq 0$ և $ab = ac$, ապա $b = c$ (արտադրյալ գործողության կրճատման հատկություն);

9) Եթե $a, b \in \mathbb{Z}$ և $a \cdot b = 0$, ապա $a = 0$ կամ $b = 0$ (զրոյի բաժանարարների բացակայության հատկություն):

Բազմությունը կոչվում է **հաշվելի**, եթե դրա տարրերը կարելի է համարակալել բոլոր բնական թվերով:

0.1.2. Բազմությունների միավորում: Դպրոցական դասընթացից հայտնի են բազմությունների միջև սահմանվող մի շարք հիմնական գործողություններ, որոնք կոչվում են նաև տեսա-բազմային գործողություններ: Խոսքը բազմությունների միավորման, հատման, հանման (տարբերության), սիմետրիկ տարբերության (գումարի) և դեկարտյան արտադրյալի մասին է:

A և B բազմությունների **միավորում** է կոչվում այն C բազմությունը, որը կազմված է բոլոր այն տարրերից, որոնք պատկանում են կամ A բազմությանը, կամ B բազմությանը (չի բացառվում նաև տարրի պատկանելը երկու բազմություններին), այսինքն՝ A և B բազմություններից գոնե մեկին: A և B բազմությունների միավորումը սովորաբար նշանակվում է $A \cup B$ ձևով՝

$$A \cup B = \{x \mid x \in A \text{ կամ } x \in B\} :$$

Բազմությունների միավորման սահմանումից անմիջապես բխում են նրա հետևյալ հատկությունները (նույնությունները)՝

$$A \cup \emptyset = A, \quad \text{(միավորի գոյության օրենք)}$$

$$A \cup A = A, \quad \text{(ինքնահամընկնման օրենք)}$$

$$A \cup B = B \cup A, \quad \text{(տեղափոխական օրենք)}$$

$$A \cup (B \cup C) = (A \cup B) \cup C \quad \text{(զուգորդական օրենք)}$$

կամայական A, B, C բազմությունների համար:

Վերջավոր թվով $A_1, \ldots, A_n$ բազմությունների միավորում է կոչվում այն C բազմությունը, որը կազմված է բոլոր այն տարրերից, որոնք պատկանում են $A_1, \ldots, A_n$ բազմություններից գոնե մեկին: Նշանակումը՝

$$C = A_1 \cup \cdots \cup A_n = \bigcup_{i=1}^{n} A_i;$$

Համանման եղանակով սահմանվում է կամայական թվով A_i, $i \in I$ բազմությունների միավորման գաղափարը (նշանակումը՝ $\bigcup\limits_{i \in I} A_i$)՝

$$\bigcup_{i \in I} A_i = \{x \mid \exists i_0 \in I,\, x \in A_{i_0}\} :$$

Եթե $I = \mathbb{N} = \{1, 2, \ldots\}$, ապա գործածվում է նաև հետևյալ նշանակումը՝ $\bigcup\limits_{i=1}^{\infty} A_i$:

Բազմությունների միավորման գաղափարն ունի նաև հետևյալ իմաստը. A և B բազմությունների միավորումն այն «ամենափոքր» C բազմությունն է, որն օժտված է A և B ենթաբազմություններով: Ավելի ճիշտ, C բազմությունը կոչվում է A և B բազմությունների միավորում, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա) $A \subseteq C$, $B \subseteq C$;

բ) եթե D բազմությունն այնպիսին է, որ $A \subseteq D$ և $B \subseteq D$, ապա $C \subseteq D$;

Հաջորդ տեսա-բազմային գործողությունը բազմությունների հատումն է:

0.1.3. Բազմությունների հատում: A և B բազմությունների **հատում** է կոչվում այն C բազմությունը, որը կազմված է բոլոր այն տարրերից, որոնք միաժամանակ պատկանում են և՛ A բազմությանը, և՛ B բազմությանը ու նշանակվում է $C = A \cap B$ ձևով՝

$$A \cap B = \{x \,|\, x \in A \text{ և } x \in B\} :$$

Եթե A և B բազմությունները չունեն ընդհանուր տարրեր, ապա $A \cap B = \emptyset$: Երկու A և B բազմություններ կոչվում են **հատվող**, եթե $A \cap B \neq \emptyset$: Հակառակ դեպքում, A և B բազմությունները կոչվում են **չհատվող**: Բազմությունների հատման սահմանումից անմիջապես բխում են նրա հետևյալ հատկությունները՝

$$A \cap \emptyset = \emptyset, \quad \text{(զրոյական տարրի օրենք)}$$

$$A \cap A = A, \quad \text{(ինքնահամընկնման օրենք)}$$

$$A \cap B = B \cap A, \quad \text{(տեղափոխական օրենք)}$$

$$A \cap (B \cap C) = (A \cap B) \cap C \quad \text{(զուգորդական օրենք)}$$

կամայական A, B, C բազմությունների համար:

Վերջավոր թվով $A_1, \ldots, A_n$ բազմությունների հատում է կոչվում այն C բազմությունը, որը կազմված է բոլոր այն տարրերից, որոնք միաժամանակ պատկանում են բոլոր $A_1, \ldots, A_n$ բազմություններին: Նշանակումը՝

$$C = A_1 \cap \cdots \cap A_n = \bigcap_{i=1}^{n} A_i;$$

Եթե $A_1, \ldots, A_n$ բազմությունները չունեն ընդհանուր տարրեր, ապա $A_1 \cap \cdots \cap A_n = \emptyset$: Եթե $A_1 \cap \cdots \cap A_n \neq \emptyset$, ապա տրված բազմությունները կոչվում են **հատվող**: Հակառակ դեպքում դրանք կոչվում են **չհատվող**:

Համանման եղանակով սահմանվում է նաև կամայական թվով A_i, $i \in I$ բազմությունների հատումը (նշանակումը՝ $\bigcap\limits_{i\in I} A_i$)՝

$$\bigcap_{i\in I} A_i = \{x \mid \forall i \in I,\, x \in A_i\}:$$

Եթե $I = \mathbb{N} = \{1, 2, \ldots\}$, ապա գործածվում է նաև հետևյալ նշանակումը՝ $\bigcap\limits_{i=1}^{\infty} A_i$;

Բազմությունների հատումն ունի նաև հետևյալ իմաստը. A և B բազմությունների հատումն այն «ամենամեծ» C բազմությունն է, որը միաժամանակ A և B բազմությունների ենթաբազմություն է: Ավելի ճիշտ C բազմությունը կոչվում է A և B բազմությունների հատում, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա’) $C \subseteq A$, $C \subseteq B$;

բ’) եթե D բազմությունն այնպիսին է, որ $D \subseteq A$ և $D \subseteq B$, ապա $D \subseteq C$;

Այսպիսով, բազմությունների միավորումը և հատումը դառնում են երկակի գաղափարներ, այն իմաստով, որ դրանց սահմանումներից մեկը ստացվում է մյուսից՝ ենթաբազմության «$\subseteq$» նշանը փոխարինելով ընդգրկման «$\supseteq$» նշանով:

Բազմությունների միավորումը և հատումը կապված են հետևյալ օրենքներով (նույնություններով)՝

$$\left.\begin{array}{l} A \cap (A \cup B) = A, \\ A \cup (A \cap B) = A, \end{array}\right\} \quad \text{(կլանման օրենքներ)}$$

$$\left.\begin{array}{l} A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \end{array}\right\} \quad \text{(բաշխական օրենքներ)}$$

կամայական A, B, C բազմությունների համար:

Կլանման օրենքների իրավացիությունն ակնհայտ է, իսկ բաշխական օրենքները ստուգվում են հեշտությամբ:

Կասենք, որ A բազմության ենթաբազմությունների $\mathcal{L} = \{A_i \subseteq A | i \in I\}$ դասը կազմում է A-ի **տրոհում**, եթե յուրաքանչյուր $x \in A$ տարրի համար գոյություն ունի միարժեքորեն որոշվող այնպիսի $A_i \in \mathcal{L}$, որ $x \in A_i$, այսինքն՝ $A = \bigcup\limits_{i \in I} A_i$ և $A_i \cap A_j = \emptyset$, եթե $i \neq j$, $i, j \in I$:

0.1.4. Բազմությունների տարբերություն: A և B բազմությունների **տարբերություն** է կոչվում այն C բազմությունը, որը կազմված է A բազմության բոլոր այն տարրերից, որոնք չեն պատկանում B բազմությանը ու նշանակվում է $C = A \setminus B$ ձևով՝

$$A \setminus B = \{x \in A \mid \ x \notin B\} :$$

Ակնհայտ է, որ

$$A \setminus B = A \setminus (A \cap B),$$

$$A \setminus A = \emptyset,$$

$$A \setminus \emptyset = A,$$

$$\emptyset \setminus A = \emptyset;$$

Եթե $A \subseteq B$, ապա $B \setminus A$ տարբերությունը կոչվում է A բազմության **լրացում** B բազմության նկատմամբ (մեջ) և հաճախ նշանակվում է $\bar{A}$-ով կամ A'-ով, եթե B-ն հայտնի է կամ սևեռած:

Բազմությունների միավորումը, հատումը և տարբերությունը ևս կապված են մի շարք օրենքներով (նույնություններով)՝

$$\left.\begin{array}{l} A \cap (B \setminus C) = (A \cap B) \setminus C, \\ A \setminus (B \cup C) = (A \setminus B) \setminus C, \end{array}\right\} \quad \text{(զուգորդական օրենքներ)}$$

$$\left.\begin{array}{l} A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C), \\ A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C), \\ (A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C), \\ A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C), \\ A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C), \\ (A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C) \end{array}\right\} \quad \text{(բաշխական օրենքներ)}$$

(ստուգումները թողնվում են որպես վարժություններ): Մասնավորապես,

$$\left.\begin{aligned}\overline{B\cap C} &= \overline{B}\cup\overline{C}\,,\\ \overline{B\cup C} &= \overline{B}\cap\overline{C}\ :\end{aligned}\right\}\ \text{(Դե Մորգանի օրենքներ)}$$

Անցնենք երկու բազմությունների սիմետրիկ տարբերության գաղափարին:

0.1.5. Բազմությունների սիմետրիկ տարբերություն: A և B բազմությունների **սիմետրիկ տարբերությունը** նշանակվում է $A\ominus B$ ձևով և սահմանվում է հետևյալ կերպ՝

$$A\ominus B=(A\cup B)\setminus(A\cap B)=(A\setminus B)\cup(B\setminus A);$$

Բազմությունների սիմետրիկ տարբերությունը երբեմն անվանվում է նաև սիմետրիկ գումար՝ օգտագործելով $A\oplus B$ նշանակումը:

Համապատասխան հիմնական հատկություններն են՝

$$A\ominus\emptyset=A,\quad \text{(միավորի գոյության օրենք)}$$

$$A\ominus B=B\ominus A,\quad \text{(տեղափոխական օրենք)}$$

$$A\ominus(B\ominus C)=(A\ominus B)\ominus C,\quad \text{(զուգորդական օրենք)}$$

$$A\ominus A=\emptyset,\quad \text{(նիլպոտենտության օրենք)}$$

$$A\cap(B\ominus C)=(A\cap B)\ominus(A\cap C);\quad \text{(բաշխական օրենք)}$$

Սակայն $A\cup(B\ominus C)\neq(A\cup B)\ominus(A\cup C)$; Օրինակ, $A\cup(A\ominus A)=A$, իսկ $(A\cup A)\ominus(A\cup A)=\emptyset$;

Ցանկացած A և B բազմությունների համար գոյություն ունի միարժեքորեն որոշվող այնպիսի X բազմություն, որ $A\ominus X=B$: Իրոք, $X=A\ominus B$ բազմությունը բավարարում է նշված հավասարմանը՝

$$A\ominus X=A\ominus(A\ominus B)=(A\ominus A)\ominus B=\emptyset\ominus B=B;$$

Եվ հակառակը, եթե $A\ominus X=B$, ապա

$$A\ominus(A\ominus X)=A\ominus B,$$

$$(A\ominus A)\ominus X=A\ominus B,$$

$$\emptyset \ominus X = A \ominus B,$$

$$X = A \ominus B:$$

0.1.6. Բազմությունների օղակ, կիսաօղակ, հանրահաշիվ և σ-հանրահաշիվ: Դիցուք X-ը կամայական ոչ դատարկ բազմություն է: X-ի ենթաբազմությունների $\mathfrak{R}$ ոչ դատարկ բազմությունը կոչվում է **բազմությունների օղակ**՝ որոշված X-ի վրա, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա) $A, B \in \mathfrak{R} \longrightarrow A \cup B \in \mathfrak{R}$,

բ) $A, B \in \mathfrak{R} \longrightarrow A \setminus B \in \mathfrak{R}$:

Բազմությունների յուրաքանչյուր $\mathfrak{R}$ օղակի համար՝

գ) $\emptyset = A \setminus A \in \mathfrak{R}$, որտեղ $A \in \mathfrak{R}$;

դ) $A \cap B = A \setminus (A \setminus B) \in \mathfrak{R}$, որտեղ $A, B \in \mathfrak{R}$;

ե) $A \ominus B = (A \setminus B) \cup (B \setminus A) \in \mathfrak{R}$, որտեղ $A, B \in \mathfrak{R}$:

X բազմության ենթաբազմությունների S ոչ դատարկ բազմությունը կոչվում է **բազմությունների հանրահաշիվ**՝ որոշված X-ի վրա, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա') $A, B \in S \longrightarrow A \cap B \in S$,

բ') $A \in S \longrightarrow A' = X \setminus A \in S$:

Քանի որ S-ը դատարկ չէ, ապա գոյություն ունի $A \in S$: Հետևաբար, $A' \in S$ և

գ') $\emptyset = A \cap A' \in S$, $X = \emptyset' \in S$;

դ') $A \cup B = (A' \cap B')' \in S$, եթե $A, B \in S$;

ե') $A \setminus B = A \cap B' \in S$, եթե $A, B \in S$:

Այսպիսով, բազմությունների յուրաքանչյուր հանրահաշիվ նաև բազմությունների օղակ է:

X-ի վրա որոշված բազմությունների S հանրահաշիվը կոչվում է **բազմությունների σ-հանրահաշիվ**՝ որոշված X-ի վրա, եթե S-ը բավարարում է նաև հետևյալ պայմանին՝

ա") $A_i \in S$, $i = 1, 2, \ldots \longrightarrow \bigcup\limits_{i=1}^{\infty} A_i \in S$

(այսինքն՝ S-ը փակ է իր հաշվելի թվով տարրերի միավորման նկատմամբ): Ակնհայտ է, որ բազմությունների յուրաքանչյուր S σ-հանրահաշիվ բավարարում է նաև հետևյալ պայմանին՝

$$\bigcap_{i=1}^{\infty} A_i = \left(\bigcup_{i=1}^{\infty} A_i'\right)' \in S, \quad \text{եթե } A_i \in S, i = 1, 2, \ldots$$

(այսինքն՝ S-ը փակ է նաև իր հաշվելի թվով տարրերի հատման նկատմամբ):

Միևնույն X բազմության վրա որոշված ցանկացած թվով σ-հանրահաշիվների հատումը նորից σ-հանրահաշիվ է՝ որոշված X-ի վրա: X բազմության ցանկացած թվով ենթաբազմությունների S_0 բազմությունը պարունակող բոլոր σ-հանրահաշիվների հատումը կոչվում է **S_0-ով ծնված σ-հանրահաշիվ**:

X բազմության ենթաբազմությունների $\mathcal{K}$ բազմությունը կոչվում է **բազմությունների կիսաօղակ**՝ որոշված X-ի վրա, եթե տեղի ունեն հետևյալ երեք պայմանները՝

ա°) $\emptyset \in \mathcal{K}$,

բ°) $A, B \in \mathcal{K} \longrightarrow A \cap B \in \mathcal{K}$,

գ°) Կամայական $A, B \in \mathcal{K}$ բազմությունների համար գոյություն ունեն վերջավոր թվով այնպիսի $C_1, \ldots, C_n \in \mathcal{K}$ բազմություններ, որ $C_i \cap C_j = \emptyset$, եթե $i \neq j$, և $A \setminus B = \bigcup\limits_{i=1}^{n} C_i$:

Օրինակ,

$$\mathcal{K} = \{[a, b) \mid \ a, b \in \mathbb{R}\}$$

բազմությունը կլինի բազմությունների կիսաօղակ՝ որոշված բոլոր իրական թվերի $\mathbb{R}$ բազմության վրա, եթե $a \geqslant b$ դեպքում ընդունենք՝ $[a, b) = \emptyset$: Ըստ որում, այս կիսաօղակը օղակ չէ, որովհետև $[0, 1) \cup [2, 3) \notin \mathcal{K}$:

0.1.7. Բազմությունների դեկարտյան արտադրյալ: Հարաբերություն և համարժեքություն: Դիցուք A-ն և B-ն երկու կամայական ոչ դատարկ բազմություններ են, $a \in A$, $b \in B$: a և b

տարրերի կարգավորված զույգը, ինչպես հայտնի է, նշանակվում է (a,b)-ով, որոնց $(a,b) = (a',b')$ հավասարությունը հասկացվում է որպես համապատասխան տարրերի հավասարություն: a-ն կոչվում է (a,b) կարգավորված զույգի առաջին բաղադրիչ (կոորդինատ) կամ սկզբնատարր, իսկ b-ն՝ նրա երկրորդ բաղադրիչ (կոորդինատ) կամ վերջնատարր:

Իհարկե, այս ընդակը (գաղափարը) կարելի է սահմանել նաև բազմության գաղափարի հիման վրա, ընդունելով՝

$$(a,b) = \{\{a\},\{a,b\}\}\,;$$

Կարգավորված զույգերի հավասարության $(a,b) = (a',b')$ պայմանն, այդ դեպքում հեշտությամբ բխեցվում է բազմությունների հավասարության հասկացությունից, երկու դեպքով՝

$a' = b'$, $\quad a' \neq b'$:

A և B բազմությունների **դեկարտյան (կամ ուղիղ) արտադրյալը** նշանակվում է $A \times B$ ձևով և սահմանվում է որպես (a,b) տեսքի բոլոր կարգավորված զույգերի բազմություն, որտեղ $a \in A$, $b \in B$՝

$$A \times B = \{(a,b) \mid \; a \in A, b \in B\}\;:$$

Օրինակ, $\mathbb{R} \times \mathbb{R}$-ը հարթությունն է: $\emptyset \times B = A \times \emptyset = \emptyset$:

Ակնհայտ է, որ եթե $A \neq B$, ապա $A \times B \neq B \times A$;

Բազմությունների դեկարտյան արտադրյալը բազմությունների միավորման, հատման և հանման հետ կապված են հետևյալ բաշխական օրենքներով (նույնություններով)՝

$$A \times (B \cup C) = (A \times B) \cup (A \times C),$$

$$(B \cup C) \times A = (B \times A) \cup (C \times A),$$

$$A \times (B \cap C) = (A \times B) \cap (A \times C),$$

$$(B \cap C) \times A = (B \times A) \cap (C \times A),$$

$$A \times (B \setminus C) = (A \times B) \setminus (A \times C),$$

$$(B \setminus C) \times A = (B \times A) \setminus (C \times A)\;:$$

ցանկացած A, B, C բազմությունների համար: Հետևյալ հավասարությունը կոչվում է բազմությունների **երկհամաչափության** (բիսիմետրիայի) կամ **միջինացման** (մեդիալության) նույնություն՝

$$(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)\;:$$

A_1 և A_2 ոչ դատարկ բազմությունների $A_1 \times A_2$ դեկարտյան արտադրյալի յուրաքանչյուր $\alpha \subseteq A_1 \times A_2$ ենթաբազմություն կոչվում է **հարաբերություն** որոշված A_1 և A_2 բազմությունների վրա: Եթե $A_1 = A_2 = A$, ապա նշանակվում է՝ $A \times A = A^2$, իսկ $\alpha \subseteq A \times A$ հարաբերությունը կոչվում է որոշված A բազմության վրա (մեջ):

Երկու $\alpha \subseteq A \times B$ և $\beta \subseteq C \times D$ հարաբերություններ կոչվում են **հավասար** և գրվում են $\alpha = \beta$, եթե $A = C$, $B = D$ և

$$(x, y) \in \alpha \longleftrightarrow (x, y) \in \beta\,,$$

որտեղ $x \in A$, $y \in B$.

$\alpha \subseteq A \times B$ հարաբերությունը կոչվում է **արտապատկերում** (ֆունկցիա)՝ A բազմությունից B բազմության մեջ և գրվում է $\alpha : A \to B$, եթե յուրաքանչյուր $x \in A$ տարրի համար գոյություն ունի միարժեքորեն որոշվող այնպիսի $y \in B$ տարր, որ $(x, y) \in \alpha$: Այսինքն՝ $\alpha \subseteq A \times B$ հարաբերությունը կոչվում է արտապատկերում, եթե տեղի ունեն հետևյալ երկու պայմանները.

1 *(Գոյության պայման)*: Յուրաքանչյուր $x \in A$ տարրի համար գոյություն ունի այնպիսի $y \in B$ տարր, որ $(x, y) \in \alpha$;

2 *(Միակության պայման)*: Եթե $(x, y_1) \in \alpha$ և $(x, y_2) \in \alpha$, ապա $y_1 = y_2$, որտեղ $x \in A$, $y_1, y_2 \in B$:

Եթե այս դեպքում $(x, y) \in \alpha$, ապա միարժեքորեն որոշվող y տարրը նշանակվում է $y = \alpha(x)$ տեսքով և y-ը կոչվում է x-ի պատկեր, իսկ x-ը՝ y-ի նախապատկեր:

Ցանկացած $B \subseteq A$, $B \neq \emptyset$, ենթաբազմության և $\alpha \subseteq A \times A$ հարաբերության համար

$$\alpha \cap (B \times B) = \beta \subseteq B \times B$$

հարաբերությունը կոչվում է α-ի **մակածված հարաբերություն**՝ $B \subseteq A$ ենթաբազմության վրա:

$\alpha \subseteq A \times A$ հարաբերությունը կոչվում է **համարժեքության հարաբերություն** կամ համառոտ՝ **համարժեքություն**՝ որոշված A բազմության վրա, եթե այն բավարարում է հետևյալ երեք պայմաններին.

ա) $(x, x) \in \alpha$ ցանկացած $x \in A$ տարրի համար; (առինքնություն կամ ռեֆլեքսիվություն) բ) $(x,y) \in \alpha \to (y,x) \in \alpha$; (համաչափություն կամ սիմետրիկություն)

գ) $(x,y) \in \alpha$, $(y,z) \in \alpha \to (x,z) \in \alpha$: (փոխանցականություն կամ տրանզիտիվություն)

Օրինակ, $\alpha = \{(x,x) | x \in A\}$ և $\alpha = A \times A$ հարաբերությունները համարժեքություններ են որոշված A-ի վրա, որոնցից առաջինը կոչվում է **զրոյական համարժեքություն**, իսկ երկրորդը՝ **միավոր համարժեքություն**:

Սովորաբար, α-ի փոխարեն գործածվում է «$\sim$» նշանը, իսկ $(x,y) \in \alpha$ պայմանն, այդ դեպքում, գրվում է $x \sim y$ տեսքով և կարդացվում է «x-ը համարժեք է y-ին», իսկ համարժեքության պայմանները ստանում են ավելի պարզ տեսք.

ա) $x \sim x$;

բ) $x \sim y \to y \sim x$;

գ) $x \sim y$, $y \sim z \to x \sim z$:

Լեմմ 0.1: *Միևնույն A բազմության վրա որոշված ցանկացած թվով համարժեքությունների հատումը նորից համարժեքություն է:* □

Եթե «$\sim$»-ը համարժեքություն է որոշված $A \neq \emptyset$ բազմության վրա, իսկ $a \in A$, ապա a տարրի **համարժեքության դասը** (շերտը) ըստ «$\sim$» համարժեքության նշանակվում է $[a]$-ով և սահմանվում է հետևյալ կերպ՝

$$[a] = \{x \in A \mid \ x \sim a\} \subseteq A :$$

Ակնհայտ է, որ $[a] \neq \emptyset$, որովհետև $a \sim a$ և, հետևաբար, $a \in [a]$: Յուրաքանչյուր $b \in [a]$ տարր կոչվում է $[a]$ համարժեքության դասի ներկայացուցիչ:

Լեմմ 0.2: *1) $[a] = [b]$ այն և միայն այն դեպքում, երբ $a \sim b$: 2) Եթե «$\sim$» համարժեքության երկու համարժեքության դասեր հատվում են, ապա դրանք համընկնում են: 3) $\{[a] \mid \ a \in A\}$ բազմությունը կազմում է A-ի տրոհում, որը նշանակվում է $A/_\sim$ -ով և կոչվում է A բազմության քանորդ-բազմություն կամ ֆակտոր-բազմություն ըստ «$\sim$» համարժեքության: Այսինքն՝ A-ի յուրաքանչյուր տարր պարունակվում է միարժեքորեն որոշվող որևէ համարժեքության դասում: 4) Եվ* *հակառակը, եթե $\mathcal{L} = \{A_i \subseteq A \mid i \in I\}$ համախմբությունը կազմում է A-ի տրոհում, ապա գոյություն ունի A-ի վրա որոշված այնպիսի «$\sim$» համարժեքություն, որի համապատասխան քանորդ-բազմությունը համընկնում է $\mathcal{L}$-ի հետ:*

Ապացուցում: 1) Նախ ապացուցենք համարժեքության դասերի հավասարության հայտանիշը՝

$$[a] = [b] \longleftrightarrow a \sim b :$$

Իրոք, եթե $[a] = [b]$, ապա $a \in [a]$ պայմանից կբխի՝ $a \in [b]$, այսինքն՝ $a \sim b$: Եվ հակառակը, եթե $a \sim b$, ապա $[a] \subseteq [b]$ և $[b] \subseteq [a]$: Ապացուցենք $[a] \subseteq [b]$ ներդրումը. եթե $x \in [a]$, ապա $x \sim a$ և քանի որ $a \sim b$, ապա փոխանցականության համաձայն՝ $x \sim b$, այսինքն՝ $x \in [b]$:

2) Դիցուք $[a] \cap [b] \neq \emptyset$ և $x \in [a] \cap [b]$: Ուստի $x \in [a]$ և $x \in [b]$, այսինքն՝ $x \sim a$, $x \sim b$: Համաչափության պայմանի համաձայն՝ $a \sim x$, $x \sim b$ և $a \sim b$, հետևաբար, $[a] = [b]$:

3)-ը դառնում է ակնհայտ: Իրոք, $a \in [a]$ և եթե $a \in X$ և $a \in Y$, որտեղ $X, Y \in A/_{\sim}$, ապա $a \in X \cap Y$, որտեղից՝ $X \cap Y \neq \emptyset$ և, հետևաբար, $X = Y$:

4) Սահմանելով

$$x \sim y \longleftrightarrow \exists A_i \in \mathcal{L}, \quad x, y \in A_i$$

հարաբերությունը, ստանում ենք համարժեքություն, որի համարժեքության դասերը ճիշտ համընկնում են $A_i \subseteq A$, $i \in I$ ենթաբազմությունների հետ: $\square$

Լեմմ 0.3: *Ցանկացած $B \subseteq A$, $B \neq \emptyset$, ենթաբազմության և $\alpha \subseteq A \times A$ համարժեքության համար*

$$\alpha \cap (B \times B) = \beta \subseteq B \times B$$

հարաբերությունը կլինի համարժեքություն որոշված B-ի վրա, այսինքն՝ $B \subseteq A$ ենթաբազմության վրա α-ի մակածված հարաբերությունը ևս համարժեքության հարաբերություն է: $\square$

0.1.8. Քանակական առնչություններ: Վերջավոր թվով զույգ առ զույգ միմյանց հետ չհատվող $A_1, \ldots, A_n$ վերջավոր բազմությունների միավորման կարգը որոշվում է հետևյալ բանաձևով՝

$$|A_1 \cup \cdots \cup A_n| = |A_1| + \cdots + |A_n| : \quad \text{(Գումարման աքսիոմ)}$$

Կամայական A և B բազմությունների համար $A \setminus B$ և $A \cap B$ բազմությունները չեն հատվում և

$$A = (A \setminus B) \cup (A \cap B) :$$

Հետևաբար, եթե A և B բազմությունները վերջավոր են, ապա համաձայն գումարման աքսիոմի՝

$$|A| = |A \setminus B| + |A \cap B|,$$

որտեղից՝

$$|A \setminus B| = |A| - |A \cap B|;$$

Մասնավորապես, եթե $B \subseteq A$, ապա $A \cap B = B$ և կունենանք՝

$$|A \setminus B| = |A| - |B|;$$

Քանի որ $A \setminus B$ և $B \setminus A$ բազմությունները չեն հատվում և

$$A \ominus B = (A \setminus B) \cup (B \setminus A),$$

ապա վերջավոր A և B բազմությունների դեպքում՝

$$|A \ominus B| = |A \setminus B| + |B \setminus A| =$$

$$= |A| - |A \cap B| + |B| - |B \cap A| = |A| + |B| - 2|A \cap B| :$$

Ցանկացած A և B բազմությունների համար A և $B \setminus A$ բազմությունները չեն հատվում և

$$A \cup B = A \cup (B \setminus A);$$

Հետևաբար, եթե A և B բազմությունները վերջավոր են, ապա նորից գումարման աքսիոմի համաձայն՝

$$|A \cup B| = |A| + |B \setminus A| = |A| + |B| - |A \cap B| :$$

Կամայական n-տարրանի վերջավոր $A = \{x_1, \ldots, x_n\}$ բազմության և կամայական վերջավոր $B_1, \ldots, B_n$ բազմությունների համար, $\{x_1\} \times B_1, \ldots, \{x_n\} \times B_n$ բազմությունները զույգ առ զույգ միմյանց հետ չեն հատվում և հետևաբար

$$|(\{x_1\} \times B_1) \cup \cdots \cup (\{x_n\} \times B_n)| =$$

$$= |\{x_1\} \times B_1| + \cdots + |\{x_n\} \times B_n| = |B_1| + \cdots + |B_n| :$$

Մասնավորապես, եթե բոլոր վերջավոր $B_1, \ldots, B_n$ բազմությունները m -տարրանի են, ապա՝

$$|(\{x_1\} \times B_1) \cup \cdots \cup (\{x_n\} \times B_n)| = n \cdot m,$$

որտեղից $B_1 = \cdots = B_n = B$ դեպքում կունենանք՝

$$|A \times B| = |(\{x_1\} \times B) \cup \cdots \cup (\{x_n\} \times B)| = n \cdot m = |A| \cdot |B| :$$

0.2. Վերինանգում

Եթե փոփոխականի փոփոխման տիրույթը համընկնում է բոլոր բնական թվերի $\mathbb{N}$ բազմության հետ, ապա այն կոչվում է բնական փոփոխական կամ բնական պարամետր:

n բնական պարամետրից կախված $P(n)$ պնդման իրավացիության ստուգումը n-ի բոլոր բնական արժեքների դեպքում կատարվում է վերինանգման (ինդուկցիայի, մաթեմատիկական ինդուկցիայի) եղանակով:

Վերինանգման (ինդուկցիայի) սկզբունքը (եղանակը): *n-ից կախված $P(n)$ պնդումը ճիշտ է n-ի բոլոր բնական արժեքների համար, եթե տեղի ունեն հետևյալ երկու պայմանները.*

ա) $P(n)$ պնդումը ճիշտ է $n = 1$ դեպքում, այսինքն՝ $P(1)$-ը ճիշտ է (այս պայմանը կոչվում է վերինանգման հենք);

բ) Ցանկացած $n \in \mathbb{N}$ բնական թվի համար, $P(n)$ պնդման ճիշտ լինելուց բխում է $P(n+1)$ պնդման ճիշտ լինելը (այս պայմանը կոչվում է վերինանգման կամ վերինանգային ենթադրություն կամ քայլ):

Իրոք, ենթադրելով հակառակը, որ գոյություն ունի այնպիսի $m \in \mathbb{N}$ բնական թիվ, որ $P(m)$-ը ճիշտ չէ, ստանում ենք՝

$$\mathcal{K} = \{m \in \mathbb{N} \,|\, P(m)\text{-ը ճիշտ չէ}\} \subseteq \mathbb{N}$$

ոչ դատարկ բազմությունը, որն ունի փոքրագույն տարր: Դիցուք $n_0 + 1$ թիվը $\mathcal{K}$-ի փոքրագույն տարրն է: Այդ դեպքում $P(n_0 + 1)$-ը ճիշտ չէ, իսկ $P(n_0)$-ն ճիշտ է ($n_0 \geqslant 1$, քանի որ $n_0 + 1 \neq 1$, համաձայն ա) պայմանի), որը հակասում է բ) պայմանին: $\square$

Ակնհայտ է, որ վերհանգման սկզբունքում բ) պայմանը կարելի է փոխարինել հետևյալ բ’) պայմանով.

բ’) *Ցանկացած* $n \in \mathbb{N}$ *բնական թվի համար,* $P(1), P(2), \ldots, P(n)$ *պնդումների ճիշտ լինելուց բխում է* $P(n+1)$ *պնդման ճիշտ լինելը, այսինքն, եթե* $P(k)$*-ն ճիշտ է բոլոր* $k \leqslant n$ *բնական թվերի համար, ապա* $P(n+1)$*-ը ևս ճիշտ է:*

Օրինակ, վերհանգման եղանակով ապացուցենք, որ k-տարրանի A բազմության բոլոր ենթաբազմությունների 2^A բազմության կարգը հավասար է 2^k-ի:

Իրոք, $k = 1$ դեպքում պնդումը ճիշտ է: Ենթադրելով պնդումը ճիշտ $k = n$ դեպքում, ապացուցենք, որ այն ճիշտ է $k = n + 1$ դեպքում: Եթե $A = \{x_1, \ldots, x_n, x_{n+1}\}$, ապա, համաձայն վերհանգման ենթադրության, x_{n+1}-ը չպարունակող A-ի բոլոր ենթաբազմությունների թիվը հավասար է 2^n-ի: Այդ ենթաբազմությունների կազմում ավելացնելով x_{n+1}-ը, կստանանք A-ի բոլոր այն ենթաբազմությունները, որոնք պարունակում են x_{n+1}-ը, որոնց քանակը նույնպես կլինի հավասար 2^n-ի: Հետևաբար, A-ի բոլոր ենթաբազմությունների թիվը կլինի հավասար՝

$$2^n + 2^n = 2 \cdot 2^n = 2^{n+1} : \qquad \square$$

Այստեղ և հետագայում $\mathbb{N}$-ի համար կարևոր դեր է խաղում այսպես կոչված «փոքրագույն տարրի սկզբունքը», ըստ որի բնական թվերի $\mathbb{N}$ բազմության յուրաքանչյուր ոչ դատարկ $\mathcal{K} \subseteq \mathbb{N}$ ենթաբազմություն ունի փոքրագույն տարր, այսինքն՝ այնպիսի $n_0 \in \mathcal{K}$ տարր, որը փոքր է կամ հավասար $\mathcal{K}$-ի բոլոր տարրերից: Քանի որ «փոքրագույն տարրի սկզբունքը» տեղի ունի (ճիշտ է) նաև անբողջ թվերի ներքևից սահմանափակ յուրաքանչյուր $S \subseteq \mathbb{Z}$ ենթաբազմության համար, ապա վերհանգման սկզբունքը ակնհայտորեն տարածվում է նաև այդպիսի S բազմությունների վրա որոշված $P(x)$ պնդումների համար (x-ը փոփոխվում է S-ում):

Վերհանգման սկզբունքը հստակորեն ձևակերպվել և գործածվում է Գալիլեի, Պասկալի և դե Մորգանի ժամանակներից:

Հաճախ անհրաժեշտ է լինում վերհանգման սկզբունքը կիրառել այնպիսի պնդումների (հատկությունների) համար, որոնք կախված են մի քանի բնական պարամետրերից: Օրինակ, եթե $P(n, m)$-ով նշանակենք դպրոցական դասընթացից հայտնի

$$a^n \cdot a^m = a^{n+m}, \qquad n, m \in \mathbb{N},$$

հատկությունը, ապա $P(n,m)$ պնդումը կլինի ճիշտ բոլոր n, m բնական թվերի դեպքում, եթե տեղի ունեն հետևյալ երեք պայմանները.

1) $P(1,1)$-ը ճիշտ է;

2) $P(r,s)$ պնդման ճիշտ լինելուց բխում է $P(r+1,s)$ պնդման ճիշտ լինելը, $r,s \in \mathbb{N}$;

3) $P(r,s)$ պնդման ճիշտ լինելուց բխում է $P(r,s+1)$ պնդման ճիշտ լինելը, $r,s \in \mathbb{N}$:

Ավելի ընդհանուր է վերհանգման սկզբունքի հետևյալ մեկնաբանությունը կամ ձևակերպումը: Դիցուք $P(t)$ հատկությունը կախված է t փոփոխականից, որը փոփոխվում է կամայական T բազմության վրա, ընդ որում տրված են $T_n \subseteq T$, $n = 1,2,\ldots$, ենթաբազմություններն այնպես, որ T բազմության յուրաքանչյուր $t \in T$ տարր ընկած է որևէ T_n բազմության մեջ, այսինքն՝ $T = \bigcup_{n\in\mathbb{N}} T_n$, բացի այդ՝

$$T_1 \subseteq T_2 \subseteq T_3 \subseteq \cdots \subseteq T_n \subseteq \cdots :$$

Այդ դեպքում, $P(t)$ պնդումը կլինի ճիշտ բոլոր $t \in T$ արժեքների դեպքում, եթե տեղի ունեն հետևյալ երկու պայմանները.

a) $P(t)$-ն ճիշտ է բոլոր $t \in T_1$ արժեքների համար;

b) եթե $P(t)$-ն ճիշտ է բոլոր $t \in T_k$ արժեքների համար, ապա այն ճիշտ է նաև բոլոր $t \in T_{k+1}$ արժեքների համար, $k \in \mathbb{N}$:

Օրինակ, երկու բնական պարամետրից կախված վերոհիշյալ $P(n,m)$ պնդման դեպքում կարելի է ենթադրել $t = (n,m)$, $T = \{(n,m) \mid m,n \in \mathbb{N}\}$, իսկ

$$T_k = \{(n,m) \mid m,n \in \mathbb{N}, m \leqslant k\}, \quad k = 1,2,\ldots,$$

կամ՝

$$T_k = \{(n,m) \mid m,n \in \mathbb{N}, m \leqslant k, n \leqslant k\}, \quad k = 1,2,\ldots :$$

Հաճախ վերհանգման սկզբունքը կիրառվում է նաև հասկացությունների կամ ընդակների (օբյեկտների) սահմանումների ժամանակ՝ հետևյալ կերպ:

Դիցուք պահանջվում է սահմանել ընդակների (օբյեկտների) $a_1, a_2, \ldots, a_n, \ldots$ հաջորդականությունը:

Սահմանում վերհանգման եղանակով: a_n *ընդակը (օբյեկտը) կլինի սահմանված բոլոր* $n \in \mathbb{N}$ *բնական թվերի համար, եթե տեղի ունեն հետևյալ երկու պայմանները.*

i) Սահմանված է a_1*-ը;*

ii) Յանկացած $k \in \mathbb{N}$ *բնական թվի դեպքում* a_{k+1}*-ը սահմանված է* $a_1, \ldots, a_k$ *ընդակների միջոցով:*

Օրինակներ: 1) Յանկացած $n \in \mathbb{N}$ բնական թվի համար x^n-ը կլինի սահմանված, եթե ենթադրենք՝

$$x^1 = x,$$

$$x^{k+1} = x^k \cdot x, \quad k \in \mathbb{N}:$$

2) Յանկացած $n \in \mathbb{N}$ բնական թվի համար $x_1 \in A_1, \ldots, x_n \in A_n$ տարրերի կարգավորված n-յակը նշանակվում է $(x_1, \ldots, x_n)$-ով և այն սահմանվում է հետևյալ կերպ՝

$$(x_1) = x_1,$$

$$(x_1, \ldots, x_{k+1}) = ((x_1, \ldots, x_k), x_{k+1}), \quad k \in \mathbb{N}:$$

Տեղի ունի կարգավորված n-յակների հավասարության հետևյալ պայմանը՝

$$(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n) \longleftrightarrow x_1 = x'_1, \ldots, x_n = x'_n,$$

իսկ

$$A_1 \times \cdots \times A_n = \{(x_1, \ldots, x_n) \,|\, x_1 \in A_1, \ldots, x_n \in A_n\}, \quad n \geqslant 2,$$

բազմությունը կոչվում է $A_1, \ldots, A_n$ բազմությունների դեկարտյան (կամ ուղիղ) արտադրյալ: Եթե $A_1 = \ldots = A_n = A$, ապա $A_1 \times \cdots \times A_n$ դեկարտյան արտադրյալը նշանակվում է A^n-ով, իսկ $(x_1, \ldots, x_n)$ կարգավորված n-յակը այդ դեպքում կոչվում է որոշված A բազմության վրա:

Վերհանգման եղանակով դժվար չէ ապացուցել, որ $A_1, \ldots, A_n$ վերջավոր բազմությունների դեկարտյան արտադրյալի կարգը որոշվում է հետևյալ բանաձևով՝

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|, \quad n \geqslant 2:$$

0.3. Արտապատկերումներ (ֆունկցիաներ)

0.3.1. Արտապատկերումների արտադրյալ: Դիցուք A-ն և B-ն երկու կամայական ոչ դատարկ բազմություններ են: A **որոշման տիրույթով** և B **հանգման տիրույթով** α արտապատկերումը (ֆունկցիան) նշանակվում է $\alpha : A \to B$ ձևով, որը յուրաքանչյուր $x \in A$ տարրի համապատասխանության մեջ է դնում միարժեքորեն որոշվող $\alpha(x) \in B$ տարրը; $\alpha(x)$-ը երբեմն նշանակվում է նաև αx-ով կամ $(\alpha)x$-ով, իսկ $\alpha : A \to B$ նշանակման փոխարեն երբեմն գրում են՝ $A \overset{\alpha}{\to} B$ և ասում, որ α արտապատկերումը գործում է A և B բազմությունների միջև կամ՝ A-ից B: Եթե $\alpha(x) = y$, ապա գրում են $\alpha : x \mapsto y$ և y-ը կոչվում է x-ի պատկեր կամ՝ x-ի α-պատկեր, իսկ x-ը՝ y-ի նախապատկեր կամ՝ y-ի α-նախապատկեր:

Երկու արտապատկերումներ՝ $\alpha : A \to B$ և $\beta : C \to D$ կոչվում են հավասար և գրվում է $\alpha = \beta$, եթե $A = C$, $B = D$ և $\alpha(x) = \beta(x)$ ցանկացած $x \in A$ տարրի համար:

Վերջավոր որոշման տիրույթով արտապատկերումները հարմար է պատկերել աղյուսակային ձևով: Օրինակ՝ $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 \\ b_1 & b_2 & b_3 & b_4 \end{pmatrix}$ հավասարությունը նշանակում է մի $\alpha : A \to B$ արտապատկերում, որտեղ $A = \{1, 2, 3, 4\}$, $\{b_1, b_2, b_3, b_4\} \subseteq B$, իսկ $\alpha(i) = b_i$, $i = 1, 2, 3, 4$:

Եթե $|A| = n \geqslant 1$ և $|B| = m \geqslant 1$, ապա $\alpha : A \to B$ տեսքի բոլոր արտապատկերումների թիվը հավասար է m^n-ի: Իրոք, եթե $A = \{x_1, \ldots, x_n\}$ և $\alpha : A \to B$, ապա նշանակելով $\alpha(x_1) = y_1$, ..., $\alpha(x_n) = y_n$, կարող ենք ասել, որ $\alpha : A \to B$ տեսքի բոլոր արտապատկերումների թիվը կլինի հավասար $(y_1, \ldots, y_n)$ կարգավորված n-յակների թվին, որտեղ $y_1, \ldots, y_n \in B$, այսինքն՝ որոնելի թիվը կլինի հավասար՝

$$|\underbrace{B \times \cdots \times B}_{n}| = \underbrace{|B| \cdot |B| \cdots |B|}_{n} = \underbrace{m \cdot m \cdots m}_{n} = m^n :$$

Ցանկացած $\alpha : A \to B$ արտապատկերման համապատասխան սահմանվում է հետևյալ «$\sim$» հարաբերությունը.

$$x \sim y \longleftrightarrow \alpha(x) = \alpha(y), \quad x, y \in A :$$

Ակնհայտ է, որ «$\sim$»-ը համարժեքություն է և այդ համարժեքությունը կոչվում է α-ի **միջուկ** և նշանակվում է՝ $(\sim) = Ker(\alpha)$: Եվ հակառակը,

A բազմության վրա տրված ցանկացած «$\sim$» համարժեքություն հանդիսանում է որևէ $\alpha : A \to B$ արտապատկերման միջուկ: Իրոք, վերցնենք $B = {}^{A}/_{\sim}$ և սահմանենք $\alpha : A \to B$ արտապատկերումը հետևյալ կերպ՝ $\alpha(x) = [x]$, որտեղ $x \in A$: Այդ դեպքում կունենանք՝

$$(x, y) \in Ker(\alpha) \longleftrightarrow \alpha(x) = \alpha(y) \longleftrightarrow [x] = [y] \longleftrightarrow x \sim y :$$

Այսպիսով, հանգում ենք համարժեքության գաղափարի հետևյալ բնութագրմանը. որպեսզի $\theta \subseteq A \times A$ հարաբերությունը լինի համարժեքության հարաբերություն անհրաժեշտ է և բավարար, որ այն լինի որևէ α արտապատկերման միջուկ:

Եթե տրված են երկու արտապատկերումներ՝ $\alpha : A \to B$ և $\beta : B \to C$, ապա դրանց **արտադրյալ** (կամ երբեմն համադրություն, սուպերպոզիցիա) է կոչվում այն $\alpha \cdot \beta : A \to C$ արտապատկերումը, որը որոշվում է հետևյալ կերպ՝

$$(\alpha \cdot \beta)x = \beta(\alpha x),$$

որտեղ αx-ը x-ի պատկերն է α արտապատկերման ժամանակ: Իսկ եթե $\alpha : A \to B$ և $\beta : B' \to C'$, որտեղ $B \neq B'$, ապա այդպիսի α և β արտապատկերումների արտադրյալը, մեր դասընթացում, չի սահմանվում և, հետևաբար, գոյություն չունի:

Օրինակ, եթե $\alpha : A \to B$, իսկ $\varepsilon_A : A \to A$ արտապատկերումը A բազմության **նույնական արտապատկերումն է**, այսինքն՝ $\varepsilon_A(x) = x$ ցանկացած $x \in A$ տարրի համար, ապա

$$\varepsilon_A \cdot \alpha = \alpha \cdot \varepsilon_B = \alpha,$$

որի ստուգումն ակնհայտորեն կատարվում է համաձայն երկու արտապատկերումների հավասարության վերոհիշյալ սահմանման:

Հատկություն 0.1: *Արտապատկերումների արտադրյալը զուգորդական է, այսինքն՝*

$$(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$$

կամայական $\alpha : A \to B$, $\beta : B \to C$ *և* $\gamma : C \to D$ *արտապատկերումների համար:*

Ապացուցում: Հավասարության ձախ և աջ մասերում գրված արտապատկերումները գոյություն ունեն և գործում են միևնույն բազմությունների միջև՝ $A \to D$: Այնուհետև՝

$$((\alpha \cdot \beta) \cdot \gamma)\, x = \gamma\, ((\alpha \cdot \beta) x) = \gamma\, (\beta(\alpha x))\,,$$

և

$$(\alpha \cdot (\beta \cdot \gamma))\, x = (\beta \cdot \gamma)(\alpha x) = \gamma\, (\beta(\alpha x)) : \qquad \square$$

Արտապատկերումների արտադրյալի սահմանման համաձայն $\alpha : A \to B$ և $\beta : C \to D$ արտապատկերումների $\alpha \cdot \beta$ և $\beta \cdot \alpha$ արտադրյալները միաժամանակ գոյություն կունենան, եթե $B = C$ և $D = A$, այսինքն՝ $\alpha : A \to B$ և $\beta : B \to A$: Սակայն $A \neq B$ դեպքում $\alpha \cdot \beta \neq \beta \cdot \alpha$, որովհետև $\alpha \cdot \beta : A \to A$, իսկ $\beta \cdot \alpha : B \to B$: Ենթադրելով նաև $A = B$ հավասարությունը, միևնույն է չենք կարող պնդել

$$\alpha \cdot \beta = \beta \cdot \alpha$$

հավասարությունը՝ կամայական $\alpha, \beta : A \to A$ արտապատկերումների համար, այսինքն՝ արտապատկերումների արտադրյալը տեղափոխական (տեղափոխելի) չէ նաև այս դեպքում: Օրինակ, եթե A բազմությունն առնվազն երկու տարրանի է՝ $a, b \in A$, $a \neq b$, ապա սահմանելով $\alpha(x) = a$ և $\beta(x) = b$ ցանկացած $x \in A$ տարրի համար, կունենանք՝

$$(\alpha \cdot \beta)x = \beta(\alpha x) = \beta(a) = b,$$

$$(\beta \cdot \alpha)x = \alpha(\beta x) = \alpha(b) = a :$$

Վերջավոր թվով $\alpha_1 : A_1 \to A_2$, $\alpha_2 : A_2 \to A_3$, ..., $\alpha_n : A_n \to A_{n+1}$ արտապատկերումների արտադրյալը սահմանվում է վերհանգման եղանակով, հետևյալ կերպ՝

$$\alpha_1 \cdot \alpha_2 \cdots \alpha_n = (\alpha_1 \cdots \alpha_{n-1}) \cdot \alpha_n, \quad n \geqslant 3 :$$

Մասնավորապես, $\alpha : A \to A$ արտապատկերման համար ընդունվում է $\alpha^2 = \alpha \cdot \alpha$, իսկ $\alpha^n = \alpha^{n-1} \cdot \alpha$:

0.3.2. Ներդրող կամ ինյեկտիվ արտապատկերումներ: $\alpha : A \to B$ արտապատկերումը կոչվում է **ներդրող** կամ **ինյեկտիվ**, եթե

$$\alpha(x) = \alpha(y) \longrightarrow x = y, \tag{0.1}$$

որտեղ $x, y \in A$:

Ինյեկտիվության (0.1) պայմանը կարելի է փոխարինել հետևյալ պայմանով՝

$$x \neq y \longrightarrow \alpha(x) \neq \alpha(y), \tag{0.2}$$

որտեղ $x, y \in A$: Հետևաբար, որպեսզի $\alpha : A \to B$ արտապատկերումը լինի ինյեկտիվ անհրաժեշտ է և բավարար, որ նրա $Ker(\alpha)$ միջուկը լինի զրոյական համարժեքություն:

Նշված (0.1) և (0.2) պայմանները հավասարազոր են, այսինքն՝ (0.1)$\leftrightarrow$(0.2): Ապացուցենք, օրինակ, որ (0.1) պայմանից բխում է (0.2) պայմանը: Ենթադրելով, թե $\alpha : A \to B$ արտապատկերումը բավարարում է (0.1) պայմանին, բայց չի բավարարում (0.2) պայմանին, ստանում ենք հակասություն: Իրոք, այդ դեպքում գոյություն կունենան այնպիսի $x, y \in A$ տարրեր, որ $x \neq y$, բայց $\alpha(x) = \alpha(y)$: Սակայն (0.1) պայմանի համաձայն, եթե $\alpha(x) = \alpha(y)$, ապա $x = y$, որը հակասում է $x \neq y$ պայմանին:

Հակառակ պնդումն ապացուցվում է նույն դատողություններով:

Հատկություն 0.2: *Երկու $\alpha : A \to B$ և $\beta : B \to C$ ինյեկտիվ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը նորից ինյեկտիվ արտապատկերում է:*

Ապացուցում: Դիցուք $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումները ինյեկտիվ են: Ստուգենք $\alpha \cdot \beta : A \to C$ արտապատկերման ինյեկտիվությունը՝

$$(\alpha \cdot \beta)x = (\alpha \cdot \beta)y \longrightarrow x = y\ :$$

Իրոք, եթե $(\alpha \cdot \beta)x = (\alpha \cdot \beta)y$, ապա $\beta(\alpha x) = \beta(\alpha y)$ և համաձայն β-ի ինյեկտիվության՝ $\alpha(x) = \alpha(y)$, որտեղից համաձայն α-ի ինյեկտիվության՝ $x = y$: □

Հատկություն 0.3: *Վերջավոր թվով $\alpha_1 : A_1 \to A_2$, $\alpha_2 : A_2 \to A_3, \ldots, \alpha_n : A_n \to A_{n+1}$ ինյեկտիվ արտապատկերումների $\alpha_1 \cdot \alpha_2 \cdots \alpha_n : A_1 \to A_{n+1}$ արտադրյալը նորից ինյեկտիվ արտապատկերում է:*

Ապացուցում (վերհանգման եղանակ): $n = 2$ դեպքում պնդումը ճիշտ է: Կատարելով վերհանգման ենթադրություն, ստանում ենք $\alpha_1 \cdot \alpha_2 \cdots \alpha_n = (\alpha_1 \cdots \alpha_{n-1}) \cdot \alpha_n$ արտադրյալի ինյեկտիվությունը, որպես երկու ինյեկտիվ արտապատկերումների արտադրյալ: □

Հատկություն 0.4: *Եթե* $\alpha : A \to B$ *և* $\beta : B \to C$ *արտապատկերումների* $\alpha \cdot \beta : A \to C$ *արտադրյալը ինյեկտիվ է, ապա* α*-ն ինյեկտիվ է:*

Ապացուցում: Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը ինյեկտիվ է, ապա՝

$$\alpha(x) = \alpha(y) \to \beta(\alpha x) = \beta(\alpha y) \to (\alpha \cdot \beta)x = (\alpha \cdot \beta)y \to x = y : \qquad \square$$

Կառուցենք α և β արտապատկերումների այնպիսի օրինակներ, որոնց $\alpha \cdot \beta$ արտադրյալը լինի ինյեկտիվ, բայց β-ն չլինի ինյեկտիվ: Դիցուք $\alpha : \mathbb{N} \to \mathbb{N}$ և $\beta : \mathbb{N} \to \mathbb{N}$ արտապատկերումները որոշվում են հետևյալ կերպ՝

$$\alpha(x) = 2x + 1, \quad x \in \mathbb{N},$$

$$\beta(1) = \beta(2) = 1,$$

$$\beta(x) = x, \quad x \geqslant 3, \ \ x \in \mathbb{N};$$

Այդ դեպքում $\alpha \cdot \beta : \mathbb{N} \to \mathbb{N}$ արտադրյալը կլինի ինյեկտիվ, որովհետև $\alpha \cdot \beta = \alpha$, սակայն β-ն ինյեկտիվ չէ:

$\alpha : A \to B$ արտապատկերումը կոչվում է **հակադարձելի աջից**, եթե գոյություն ունի այնպիսի $\alpha' : B \to A$ արտապատկերում, որ

$$\alpha \cdot \alpha' = \varepsilon_A;$$

Այդ դեպքում α'-ը կոչվում է α-ի աջ հակադարձ:

Եթե $\alpha : A \to B$ արտապատկերումը հակադարձելի է աջից, ապա նրա α' աջ հակադարձը, ընդհանուր դեպքում, միարժեքորեն չի որոշվում: Օրինակ, եթե $A = \{1, 2\}$, $B = \{3, 4, 5\}$, և $\alpha = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, ապա α-ն կլինի հակադարձելի աջից, ընդ որում նրա α' աջ հակադարձը որոշվում է երկու տարբեր եղանակներով՝

$$\alpha' = \begin{pmatrix} 3 & 4 & 5 \\ 1 & 2 & 1 \end{pmatrix}, \alpha' = \begin{pmatrix} 3 & 4 & 5 \\ 1 & 2 & 2 \end{pmatrix} :$$

Թեորեմ 0.1 (ինյեկտիվության հայտանիշը): *Որպեսզի* $\alpha : A \to B$ *արտապատկերումը լինի ինյեկտիվ անհրաժեշտ է և բավարար, որ այն լինի հակադարձելի աջից:*

Ապացուցում: Անհրաժեշտություն: Դիցուք

$$\alpha(A) = \{\alpha(x) \mid x \in A\} \subseteq B$$

և սևեռենք որևէ $a \in A$ տարր: Հնարավոր է երկու դեպք՝

ա) $\alpha(A) = B$, այսինքն՝ $B \setminus \alpha(A) = \emptyset$: Այս դեպքում յուրաքանչյուր $y \in B$ տարրի համար գոյություն կունենա այնպիսի $x \in A$ տարր, որ $\alpha(x) = y$, այսինքն՝ y-ն ունի նախապատկեր:

բ) $B \setminus \alpha(A) \neq \emptyset$: Այս դեպքում գոյություն ունի այնպիսի $y \in B \setminus \alpha(A)$ տարր, որի համար գոյություն չունի այնպիսի $x \in A$ տարր, որ $\alpha(x) = y$, այսինքն՝ y-ը չունի նախապատկեր:

Սահմանենք $\alpha' : B \to A$ արտապատկերումը հետևյալ կերպ՝

$$\alpha'(y) = \begin{cases} x, & \text{եթե } \alpha(x) = y, \\ a, & \text{եթե } y\text{-ը չունի նախապատկեր;} \end{cases}$$

Նախ նկատենք, որ $y \in B$ տարրին համապատասխանող $\alpha'(y)$-ը որոշվում է միարժեքորեն: Իրոք, եթե $\alpha(x_1) = y$ և $\alpha(x_2) = y$, ապա $\alpha(x_1) = \alpha(x_2)$ և համաձայն α-ի ինյեկտիվության՝ $x_1 = x_2$:

Այժմ ստուգենք $\alpha \cdot \alpha' = \varepsilon_A$ հավասարությունը.

$$(\alpha \cdot \alpha')x = \alpha'(\alpha x) = \alpha'(y) = x = \varepsilon_A(x),$$

որտեղ $y = \alpha(x)$:

α'-ի կառուցումից բխում է, որ $B \setminus \alpha(A) \neq \emptyset$ և $A \neq \{a\}$ դեպքում α'-ը չի որոշվում միարժեքորեն:

Բավարարություն: Եթե $\alpha : A \to B$ արտապատկերումը հակադարձելի է աջից, այսինքն՝ $\alpha \cdot \alpha' = \varepsilon_A$, որևէ $\alpha' : B \to A$ արտապատկերման համար, ապա համաձայն հատկություն 0.4-ի, α-ն կլինի ինյեկտիվ (որովհետև ε_A-ն ինյեկտիվ է): □

***Հետևություն 0.1**: Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումները հակադարձելի են աջից, ապա դրանց $\alpha \cdot \beta : A \to C$ արտադրյալը նույնպես կլինի հակադարձելի աջից:* □

***Հետևություն 0.2**: Եթե $\alpha_1 : A_1 \to A_2$, $\alpha_2 : A_2 \to A_3$, …, $\alpha_n : A_n \to A_{n+1}$ արտապատկերումները հակադարձելի են աջից, ապա դրանց $\alpha_1 \cdot \alpha_2 \cdots \alpha_n : A_1 \to A_{n+1}$ արտադրյալը նույնպես կլինի հակադարձելի աջից:* □

Հետևություն 0.3: Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը հակադարձելի է աջից, ապա այդպիսին կլինի նաև α-ն: □

Թեորեմ 0.1-ի ապացուցումից բխում է, որ եթե $\alpha : A \to B$ ինյեկտիվ արտապատկերմանը համապատասխան կառուցված $\alpha' : B \to A$ արտապատկերումը միակն է, ապա կամ A-ն մեկ տարրանի է, կամ $B = \alpha(A)$: Այսպիսով հանգում ենք հետևյալ գաղափարին:

0.3.3. Վերադրող կամ սյուրեկտիվ արտապատկերումներ: $\alpha : A \to B$ արտապատկերումը կոչվում է **վերադրող** (ծածկող) կամ **սյուրեկտիվ**, եթե $\alpha(A) = B$, այսինքն՝ յուրաքանչյուր $y \in B$ տարրի համար գոյություն ունի այնպիսի $x \in A$ տարր, որ $\alpha(x) = y$:

Օրինակ, եթե «$\sim$»-ը համարժեքություն է որոշված A բազմության վրա, իսկ $B = A/_\sim$, ապա սահմանելով $\pi : a \to [a]$ համապատասխանությունը ($a \in A$), ստանում ենք $\pi : A \to B$ սյուրեկտիվ արտապատկերումը, որը կոչվում է **բնական** (կամ **քանորդ**-) արտապատկերում և $Ker(\pi) = (\sim)$:

Հատկություն 0.5: *Երկու $\alpha : A \to B$ և $\beta : B \to C$ սյուրեկտիվ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը նորից կլինի սյուրեկտիվ արտապատկերում:*

Ապացուցում: Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումները սյուրեկտիվ են, ապա յուրաքանչյուր $z \in C$ տարրի համար գոյություն ունի այնպիսի $y \in B$ տարր, որ $\beta(y) = z$ և գոյություն կունենա այնպիսի $x \in A$ տարր, որ $\alpha(x) = y$: Հետևաբար, $\beta(\alpha x) = z$, այսինքն՝ $(\alpha \cdot \beta)x = z$; Այսպիսով՝ $\alpha \cdot \beta$ արտադրյալը սյուրեկտիվ է: □

Հատկություն 0.6: *Վերջավոր թվով $\alpha_1 : A_1 \to A_2$, $\alpha_2 : A_2 \to A_3, \ldots, \alpha_n : A_n \to A_{n+1}$ սյուրեկտիվ արտապատկերումների $\alpha_1 \cdot \alpha_2 \cdots \alpha_n : A_1 \to A_{n+1}$ արտադրյալը նորից սյուրեկտիվ արտապատկերում է:*

Ապացուցում (վերհանգման եղանակ): $n = 2$ դեպքում պնդումը ճիշտ է (հատկություն 0.5): Ենթադրելով պնդումը ճիշտ n-ից քիչ թվով սյուրեկտիվ արտապատկերումների համար, կստանանք՝

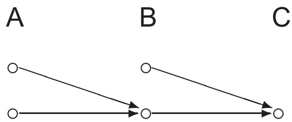
$$\alpha_1 \cdot \alpha_2 \cdots \alpha_n = (\alpha_1 \cdots \alpha_{n-1}) \cdot \alpha_n$$

արտադրյալի սյուրեկտիվությունը, որպես երկու սյուրեկտիվ արտապատկերումների արտադրյալ: □

Հատկություն 0.7: *Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը սյուրեկտիվ է, ապա β-ն սյուրեկտիվ է:*

Ապացուցում: Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը սյուրեկտիվ է, ապա յուրաքանչյուր $z \in C$ տարրի համար գոյություն կունենա այնպիսի $x \in A$ տարր, որ $(\alpha{\cdot}\beta)x = z$, այսինքն՝ $\beta(\alpha x) = z$ և հետևաբար $\beta(y) = z$, որտեղ $y = \alpha(x) \in B$: Այսպիսով, β արտապատկերումը սյուրեկտիվ է: $\square$

Դժվար չէ կառուցել α և β արտապատկերումների այնպիսի օրինակներ, որոնց $\alpha \cdot \beta$ արտադրյալը լինի սյուրեկտիվ, բայց α-ն չլինի սյուրեկտիվ: Օրինակ՝



,

այսինքն՝ $A = \{a, b\}$, $B = \{c, d\}$, $C = \{s\}$, $\alpha(a) = \alpha(b) = c$, $\beta(c) = \beta(d) = s$:

Սյուրեկտիվության հայտանիշին անցնելու համար նախ ներմուծենք հետևյալ հասկացությունը:

$\alpha : A \to B$ արտապատկերումը կոչվում է **հակադարձելի ձախից**, եթե գոյություն ունի այնպիսի $\alpha'' : B \to A$ արտապատկերում, որ

$$\alpha'' \cdot \alpha = \varepsilon_B;$$

Այդ դեպքում α''-ը կոչվում է α-ի ձախ հակադարձ:

Եթե $\alpha : A \to B$ արտապատկերումը հակադարձելի է ձախից, ապա նրա α'' ձախ հակադարձը, ընդհանուր դեպքում, միարժեքորեն չի որոշվում: Օրինակ, եթե $A = \{1, 2\}$, $B = \{3\}$ և $\alpha = \begin{pmatrix} 1 & 2 \\ 3 & 3 \end{pmatrix}$, ապա α-ն կլինի հակադարձելի ձախից, ընդ որում նրա α'' ձախ հակադարձը որոշվում է երկու տարբեր եղանակներով՝

$$\alpha'' = \begin{pmatrix} 3 \\ 1 \end{pmatrix}, \quad \alpha'' = \begin{pmatrix} 3 \\ 2 \end{pmatrix}:$$

Թեորեմ 0.2 (սյուրեկտիվության հայտանիշը): *Որպեսզի $\alpha : A \to B$ արտապատկերումը լինի սյուրեկտիվ անհրաժեշտ է և բավարար որ այն լինի հակադարձելի ձախից:*

Ապացուցում: Անհրաժեշտություն: Ըստ սյուրեկտիվության սահմանման, յուրաքանչյուր $y \in B$ տարրի համար գոյություն ունի այնպիսի $x \in A$ տարր, որ $\alpha(x) = y$: Սևեռենք այդպիսի x-երից միայն մեկը՝ նշանակելով նրան x_y-ով և սահմանենք $\alpha'' : B \to A$ արտապատկերումը հետևյալ կերպ՝

$$\alpha''(y) = x_y,$$

որտեղ $\alpha(x_y) = y$: Ստուգենք $\alpha'' \cdot \alpha = \varepsilon_B$ հավասարությունը.

$$(\alpha'' \cdot \alpha)y = \alpha(\alpha'' y) = \alpha(x_y) = y = \varepsilon_B(y) :$$

Ըստ որում, α''-ի կառուցումից բխում է, որ այն չի որոշվում միարժեքորեն, եթե α-ն ինյեկտիվ չէ:

Բավարարություն: Եթե $\alpha : A \to B$ արտապատկերման համար գոյություն ունի այնպիսի $\alpha'' : B \to A$ արտապատկերում, որ $\alpha'' \cdot \alpha = \varepsilon_B$, ապա համաձայն հատկություն 0.7-ի, α-ն կլինի սյուրեկտիվ, որովհետև ε_B-ն սյուրեկտիվ է: □

***Հետևություն 0.4**: Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումները հակադարձելի են ձախից, ապա դրանց $\alpha \cdot \beta : A \to C$ արտադրյալը նույնպես կլինի հակադարձելի ձախից:* □

***Հետևություն 0.5**: Եթե $\alpha_1 : A_1 \to A_2$, $\alpha_2 : A_2 \to A_3$, …, $\alpha_n : A_n \to A_{n+1}$ արտապատկերումները հակադարձելի են ձախից, ապա դրանց $\alpha_1 \cdot \alpha_2 \cdots \alpha_n : A_1 \to A_{n+1}$ արտադրյալը նույնպես կլինի հակադարձելի ձախից:* □

***Հետևություն 0.6**: Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը հակադարձելի է ձախից, ապա այդպիսին կլինի նաև β-ն:* □

Ինյեկտիվության և սյուրեկտիվության սահմանումներից անմիջապես չի երևում որևէ զուգահեռություն կամ նմանություն այդ երկու հասկացությունների միջև: Սակայն թեորեմ 0.1 և թեորեմ 0.2 հայտանիշներից բխում է այդ երկու գաղափարների երկակիությունը այն իմաստով, որ դրանցից մեկը կարելի է սահմանել աջ հակադարձելիության հատկությամբ, իսկ մյուսը՝ ձախ:

Թեորեմ 0.2-ի ապացուցումից բխում է նաև, որ եթե $\alpha : A \to B$ սյուրեկտիվ արտապատկերմանը համապատասխան կառուցված α'' :

$B \to A$ արտապատկերումը միակն է, ապա α-ն նաև ինյեկտիվ է: Այսպիսով, հանգում ենք հետևյալ կարևոր գաղափարին:

0.3.4. Փոխմիարժեք կամ բիեկտիվ արտապատկերումներ: $\alpha : A \to B$ արտապատկերումը կոչվում է **փոխմիարժեք** կամ **բիեկտիվ**, եթե այն միաժամանակ ինյեկտիվ է և սյուրեկտիվ:

Հատկություն 0.8: *Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումները բիեկտիվ են, ապա դրանց $\alpha \cdot \beta : A \to C$ արտադրյալը ևս կլինի բիեկտիվ:*

Ապացուցում: Բխում է 0.2 և 0.5 հատկություններից: □

Հատկություն 0.9: *Վերջավոր թվով $\alpha_1 : A_1 \to A_2$, $\alpha_2 : A_2 \to A_3, \ldots, \alpha_n : A_n \to A_{n+1}$ բիեկտիվ արտապատկերումների $\alpha_1 \cdot \alpha_2 \cdots \alpha_n : A_1 \to A_{n+1}$ արտադրյալը նորից բիեկտիվ է:*

Ապացուցում: Բխում է 0.3 և 0.6 հատկություններից: □

Հատկություն 0.10: *Եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը բիեկտիվ է, ապա α-ն կլինի ինյեկտիվ, իսկ β-ն՝ սյուրեկտիվ:*

Ապացուցում: Բխում է 0.4 և 0.7 հատկություններից: □

$\alpha : A \to B$ արտապատկերումը կոչվում է **հակադարձելի**, եթե գոյություն ունի այնպիսի $\alpha^* : B \to A$ արտապատկերում, որ տեղի ունենան հետևյալ երկու հավասարությունները՝

$$\begin{cases} \alpha \cdot \alpha^* = \varepsilon_A, \\ \alpha^* \cdot \alpha = \varepsilon_B : \end{cases}$$

Ըստ որում, նշված երկու հավասարություններով α^* արտապատկերումը որոշվում է միարժեքորեն, այն կոչվում է α-ի հակադարձ (արտապատկերում) և նշանակվում է՝ $\alpha^* = \alpha^{-1}$: Ավելին, եթե α արտապատկերումը հակադարձելի է աջից և հակադարձելի է ձախից, այսինքն՝ գոյություն ունեն այնպիսի $\alpha' : B \to A$ և $\alpha'' : B \to A$ արտապատկերումներ, որ

$$\begin{cases} \alpha \cdot \alpha' = \varepsilon_A, \\ \alpha'' \cdot \alpha = \varepsilon_B, \end{cases}$$

ապա $\alpha' = \alpha''$ և, հետևաբար, α-ն կլինի հակադարձելի: Իրոք,

$$\alpha'' = \alpha'' \cdot \varepsilon_A = \alpha'' \cdot (\alpha \cdot \alpha') = (\alpha'' \cdot \alpha) \cdot \alpha' = \varepsilon_B \cdot \alpha' = \alpha' :$$

Լեմմ 0.4: *Եթե $\alpha : A \to B$ արտապատկերումը հակադարձելի է, ապա նրա $\alpha^* = \alpha^{-1}: B \to A$ հակադարձ արտապատկերումը ևս կլինի հակադարձելի, ըստ որում՝ $\left(\alpha^{-1}\right)^{-1} = \alpha$:*

Ապացուցում: Բխում է հակադարձելի արտապատկերման սահմանումից: □

Թեորեմ 0.3 (բիեկտիվության հայտանիշը): *Որպեսզի $\alpha : A \to B$ արտապատկերումը լինի բիեկտիվ անհրաժեշտ է և բավարար, որ այն լինի հակադարձելի:*

Ապացուցում: Բավարարությունն ակնհայտ է, որովհետև $\alpha : A \to B$ արտապատկերման հակադարձելիության սահմանման առաջին հավասարությունից բխում է (թեորեմ 0.1), որ α-ն ինյեկտիվ է, իսկ երկրորդ հավասարությունից բխում է (թեորեմ 0.2), որ α-ն սյուրեկտիվ է: Հետևաբար α-ն բիեկտիվ է:

Անհրաժեշտություն: Եթե α-ն բիեկտիվ է, ապա ըստ սահմանման, α-ն կլինի ինյեկտիվ և սյուրեկտիվ: Հետևաբար (թեորեմ 0.1), գոյություն կունենա այնպիսի $\alpha' : B \to A$ արտապատկերում, որ $\alpha \cdot \alpha' = \varepsilon_A$ և (թեորեմ 0.2) գոյություն կունենա այնպիսի $\alpha'' : B \to A$ արտապատկերում, որ $\alpha'' \cdot \alpha = \varepsilon_B$: Հետևաբար, ինչպես ապացուցվեց վերևում, $\alpha' = \alpha''$ և α-ն կլինի հակադարձելի: □

Հետևություն 0.7: *1) **Եթե** $\alpha_1 : A \to B$ **և** $\alpha_2 : B \to C$ արտապատկերումները հակադարձելի են, ապա դրանց $\alpha_1 \cdot \alpha_2 : A \to C$ արտադրյալը ևս կլինի հակադարձելի ու*

$$(\alpha_1 \cdot \alpha_2)^{-1} = \alpha_2^{-1} \cdot \alpha_1^{-1};$$

*2) **Եթե** $\alpha_1 : A_1 \to A_2$, $\alpha_2 : A_2 \to A_3$, …, $\alpha_n : A_n \to A_{n+1}$ արտապատկերումները հակադարձելի են, ապա դրանց $\alpha_1 \cdot \alpha_2 \cdots \alpha_n : A_1 \to A_{n+1}$ արտադրյալը ևս կլինի հակադարձելի ու*

$$(\alpha_1 \cdot \alpha_2 \cdots \alpha_n)^{-1} = \alpha_n^{-1} \cdot \alpha_{n-1}^{-1} \cdots \alpha_1^{-1} :$$

Ապացուցում: 1) Եթե $\alpha_1 \cdot \alpha_1^* = \varepsilon_A$, $\alpha_1^* \cdot \alpha_1 = \varepsilon_B$, $\alpha_2 \cdot \alpha_2^* = \varepsilon_B$, $\alpha_2^* \cdot \alpha_2 = \varepsilon_C$, ապա

$$\alpha_1\alpha_2 \cdot \alpha_2^*\alpha_1^* = \varepsilon_A, \quad \alpha_2^*\alpha_1^* \cdot \alpha_1\alpha_2 = \varepsilon_C :$$

2) Հատկությունն ապացուցվում է վերհանգման եղանակով: □

Հատկություն 0.11: *Եթե A-ն և B-ն n-տարրանի բազմություններ են, այսինքն՝ $|A| = |B| = n \geqslant 1$, ապա $\alpha : A \to B$ տեսքի բոլոր բիեկտիվ արտապատկերումների թիվը հավասար է՝*

$$n(n-1)\cdots 2\cdot 1 = n!$$

(կարդացվում է «էն ֆակտորիալ»):

Ապացուցում (վերհանգման եղանակ): Դիցուք $A = \{x_1, \ldots, x_n\}$, իսկ $B = \{y_1, \ldots, y_n\}$: Եթե $n = 1$, ապա պնդումն ակնհայտորեն ճիշտ է: Ենթադրելով պնդումը ճիշտ n-ից փոքր բնական թվերի դեպքում, հաշվենք $\alpha : A \to B$ տեսքի բոլոր հնարավոր բիեկտիվ արտապատկերումների թիվը:

Հնարավոր են հետևյալ n դեպքերը՝

1) $\alpha(x_1) = y_1$,

2) $\alpha(x_1) = y_2$,

....

n) $\alpha(x_1) = y_n$:

Համաձայն վերհանգման ենթադրության 1) պայմանին բավարարող բոլոր $\alpha : A \to B$ տեսքի բիեկտիվ արտապատկերումների թիվը հավասար է՝ $(n-1)!$: Նույն արդյունքը տեղի ունի նաև 2), ..., n) դեպքերից յուրաքանչյուրի համար: Հետևաբար, $\alpha : A \to B$ տեսքի բոլոր բիեկտիվ արտապատկերումների թիվը կլինի հավասար՝

$$\underbrace{(n-1)! + (n-1)! + \cdots + (n-1)!}_{n} = (n-1)!n = n! \; : \qquad \square$$

$\alpha : A \to A$ տեսքի յուրաքանչյուր բիեկտիվ արտապատկերում կոչվում է A բազմության **տեղադրություն**: n-տարրանի $\{1, 2, \ldots, n\}$ բազմության յուրաքանչյուր տեղադրություն կոչվում է n -րդ աստիճանի տեղադրություն:

Հետևություն 0.8: *n-րդ աստիճանի բոլոր տեղադրությունների թիվը հավասար է $n!$-ի:*

Օրինակներ: 1) Դպրոցական դասընթացից հայտնի $\alpha(x) = \log_a x : \mathbb{R}_+ \to \mathbb{R}$ բիեկտիվ արտապատկերման հակադարձ արտապատկերումն է $\alpha^*(x) = a^x : \mathbb{R} \to \mathbb{R}_+$ արտապատկերումը, որովհետև՝

$$(\alpha \cdot \alpha^*)x = \alpha^*(\alpha x) = \alpha^*(\log_a x) = a^{\log_a x} = x = \varepsilon_{\mathbb{R}_+}(x),$$

$$(\alpha^* \cdot \alpha)x = \alpha(\alpha^* x) = \alpha(a^x) = \log_a a^x = x = \varepsilon_{\mathbb{R}}(x)\,,$$

որտեղ $a > 0$ և $a \neq 1$, իսկ $\mathbb{R}_+$-ը բոլոր դրական իրական թվերի բազմությունն է:

2) $\alpha(x) = \sin x : \left[-\dfrac{\pi}{2}\,;+\dfrac{\pi}{2}\right] \to [-1;1]$ բիեկտիվ արտապատկերման հակադարձ արտապատկերումն է $\alpha^*(x) = \arcsin(x) : [-1;1] \to \left[-\dfrac{\pi}{2}\,;+\dfrac{\pi}{2}\right]$ արտապատկերումը, որովհետև՝

$$(\alpha \cdot \alpha^*)x = \alpha^*(\alpha x) = \alpha^*(\sin x) = \arcsin(\sin x) = x = \varepsilon_{\left[-\frac{\pi}{2}\,;+\frac{\pi}{2}\right]}(x),$$

$$(\alpha^* \cdot \alpha)x = \alpha(\alpha^* x) = \alpha(\arcsin x) = \sin(\arcsin x) = x = \varepsilon_{[-1;+1]}(x)\ :$$

0.3.5. Ձևափոխություններ: $\alpha : A \to A$ տեսքի յուրաքանչյուր արտապատկերում կոչվում է A բազմության **ձևափոխություն**, այսինքն՝ ձևափոխություն է կոչվում այն արտապատկերումը, որը տրված բազմությունն արտապատկերում է իր մեջ:

A բազմության բոլոր ձևափոխությունների բազմությունը ընդունված է նշանակել $\mathcal{F}_A$-ով: Ձևափոխության առանձնահատկություններից մեկն այն է, որ ձևափոխությունը կարելի է բազմապատկել իր հետ՝ այն էլ ցանկացած վերջավոր թվով անգամ, այսինքն՝ իմաստալից է ձևափոխության բնական ցուցիչով աստիճանի հասկացությունը՝

$$\alpha^0 = \varepsilon,$$

$$\alpha^k = \underbrace{\alpha \cdots \alpha}_{k}, \quad k = 1, 2, \ldots$$

(կարդացվում է α-ի k աստիճան): Ըստ որում, վերհանգման եղանակով դժվար չէ ապացուցել, որ հավասարության աջ մասը կախված չէ փակագծերի դասավորությունից (բխում է նաև թեորեմ 1.3-ից): Այդ դեպքում, ակնհայտ է դառնում, որ յուրաքանչյուր $\alpha \in \mathcal{F}_A$ ձևափոխության համար՝

$$\alpha^m \cdot \alpha^n = \alpha^{m+n},$$

$$(\alpha^m)^n = \alpha^{m \cdot n}$$

ցանկացած m և n բնական թվերի դեպքում:

Թեորեմ 0.4: *Վերջավոր A բազմության յուրաքանչյուր $\alpha : A \to A$ ինյեկտիվ ձևափոխություն կլինի նաև սյուրեկտիվ, հետևաբար և՝ բիեկտիվ:*

Ապացուցում: Պահանջվում է ապացուցել, որ α-ն սյուրեկտիվ է, այսինքն՝ որ յուրաքանչյուր $x \in A$ տարրի համար գոյություն ունի այնպիսի $x' \in A$ տարր, որ $\alpha(x') = x$:

Դիտարկենք տարրերի՝

$$x, \alpha(x), \ldots, \alpha^k(x), \ldots$$

հաջորդականությունը: Քանի որ A բազմությունը վերջավոր է, ապա նշված (անվերջ) հաջորդականության մեջ կլինեն կրկնվող տարրեր: Դիցուք՝

$$\alpha^m(x) = \alpha^n(x), \quad \text{որտեղ} \ \ m > n;$$

Հետևաբար, $m - n > 0$ և

$$\alpha^n \left(\alpha^{m-n}(x)\right) = \alpha^n(x) :$$

Համաձայն հատկություն 0.3-ի, վերջավոր թվով ինյեկտիվ արտապատկերումների արտադրյալը նորից ինյեկտիվ է, ուստի $\alpha^n = \underbrace{\alpha \cdot \alpha \cdots \alpha}_{n}$ արտապատկերումը կլինի ինյեկտիվ և ստացված հավասարությունից կունենանք՝

$$\alpha^{m-n}(x) = x,$$

կամ

$$\alpha \left(\alpha^{m-n-1}(x)\right) = x, \quad m - n - 1 \geqslant 0,$$

$$\alpha(x') = x,$$

որտեղ $x' = \alpha^{m-n-1}(x)$: □

Թեորեմ 0.5: *Վերջավոր A բազմության յուրաքանչյուր $\alpha : A \to A$ սյուրեկտիվ ձևափոխություն կլինի նաև ինյեկտիվ, հետևաբար և՝ բիեկտիվ:*

Ապացույց: Այստեղ արդեն կօգտվենք հատկություն 0.6-ից, համաձայն որի, վերջավոր թվով սյուրեկտիվ արտապատկերումների արտադրյալը նորից սյուրեկտիվ է: Քանի որ վերջավոր բազմության բոլոր ձևափոխությունների դասը վերջավոր է, ապա՝

$$\alpha^0 = \varepsilon_A,\ \alpha,\ \ldots,\ \alpha^k,\ \ldots$$

անվերջ հաջորդականության մեջ կլինեն կրկնություններ, այսինքն՝ որևէ $m \neq n$ բնական թվերի համար կունենանք՝

$$\alpha^m = \alpha^n, \quad \text{որտեղ } m > n;$$

Հետևաբար,

$$\alpha^m(a) = \alpha^n(a) \quad \text{բոլոր } a \in A \text{ տարրերի համար և}$$

$$\alpha^{m-n}\left(\alpha^n(a)\right) = \alpha^n(a):$$

Քանի որ α^n-ը սյուրեկտիվ է, ապա յուրաքանչյուր $x \in A$ տարրի համար գոյություն կունենա այնպիսի $a \in A$ տարր, որ $\alpha^n(a) = x$; Հետևաբար,

$$\alpha^{m-n}(x) = x$$

յուրաքանչյուր $x \in A$ տարրի համար, այսինքն՝ $\alpha^{m-n} = \varepsilon_A$:

Այժմ կարելի է ապացուցել տրված $\alpha : A \to A$ ձևափոխության ինյեկտիվությունը. իրոք, եթե $\alpha(x) = \alpha(y)$, ապա $\alpha^2(x) = \alpha^2(y), \ldots, \alpha^{m-n}(x) = \alpha^{m-n}(y)$, այսինքն՝ $\varepsilon_A(x) = \varepsilon_A(y)$ և $x = y$: $\square$

Եթե $\alpha : A \to A$ ձևափոխության համար՝ $\alpha^2 = \varepsilon_A$, ապա ակնհայտ է, որ α-ն կլինի բիեկտիվ (փոխմիարժեք) արտապատկերում:

Կասենք, որ $\alpha : A \to A$ ձևափոխությունն ունի անշարժ կետ, եթե գոյություն ունի այնպիսի $a \in A$ տարր, որ $\alpha(a) = a$: Այդ դեպքում, $a \in A$ տարրը կոչվում է α-ի անշարժ կետ:

Տեղի ունի տեսա-բազմային բնույթի հետևյալ թեորեմը, որն ունի նաև օգտակար կիրառություններ:

Թեորեմ 0.6: *Եթե վերջավոր A բազմության տարրերի քանակը կենտ է և $\alpha : A \to A$ ձևափոխության համար՝ $\alpha^2 = \varepsilon_A$, ապա α ձևափոխությունն ունի անշարժ կետ:*

Ապացույց: Ենթադրենք հակառակը, որ α ձևափոխությունը չունի անշարժ կետ, այսինքն $\alpha(x) \neq x$ ցանկացած $x \in A$ տարրի համար: Դիտարկենք $\{x, \alpha(x)\}$ տեսքի զույգերի բազմությունը, որտեղ $x \in A$: Նկատենք, որ եթե $\{x, \alpha(x)\} \cap \{y, \alpha(y)\} \neq \emptyset$, ապա $\{x, \alpha(x)\} = \{y, \alpha(y)\}$: Ուստի, A բազմությունը տրոհվում է չհատվող զույգերի: Հետևաբար, $\{x, \alpha(x)\}$ տեսքի զույգերի թիվը կլինի հավասար $\frac{n}{2}$-ի, որտեղ n-ը A բազմության տարրերի քանակն է՝ $n = |A|$: Դիցուք $\frac{n}{2} = k$: Հետևաբար, $n = 2k$, որը հակասում է տրված պայմանին: □

Նշված թեորեմի ապացույցից բխում է նաև հետևյալ արդյունքը:

Հետևություն 0.9: *Եթե վերջավոր A բազմության $\alpha : A \to A$ ձևափոխության համար՝ $\alpha^2 = \varepsilon_A$ և α-ն ունի կենտ (զույգ) թվով անշարժ կետեր, ապա A բազմության տարրերի քանակը կենտ (զույգ) թիվ է:* □

Ենթավերնագիրը եզրափակենք Գ. Կանտորին (G. Cantor) պատկանող հետևյալ սահմանումներով:

Երկու A և B բազմություններ կոչվում են **հավասարազոր** կամ հավասար քանակի տարրեր պարունակող (ունեցող) և գրվում է $A \sim B$, եթե գոյություն ունի որևէ $\alpha : A \to B$ բիեկտիվ արտապատկերում: Սահմանված «$\sim$» հարաբերությունը համարժեքության հարաբերություն է, որոշված բազմությունների դասի վրա: Եթե A-ն որևէ բազմություն է, ապա նրան համապատասխանող $[A]$ համարժեքության դասը (ըստ այս «$\sim$» համարժեքության) կոչվում է A **բազմության հզորություն**: Լեմմ 0.2-ից բխում է, որ միայն հավասարազոր բազմություններն են օժտված միևնույն հզորությամբ և, հետևաբար, կարելի է ասել, որ հզորությունը այն ընդհանուր հատկությունն է, որով միաժամանակ օժտված են բոլոր հավասարազոր բազմությունները:

Բազմությունը կոչվում է հաշվելի, եթե այն հավասարազոր է բոլոր բնական թվերի բազմությանը: Կարելի է ապացուցել, որ վերջավոր կամ հաշվելի թվով հաշվելի բազմությունների միավորումը նորից հաշվելի բազմություն է:

Բոլոր իրական թվերի բազմության հզորությունը կոչվում է **կոնտինում** (continum - լատ.):

Թեորեմ 0.7 (Կանտոր): *Գոյություն ունի ինյեկտիվ արտապատկերում կամայական $A \neq \emptyset$ բազմությունից 2^A բազմության մեջ, սակայն A և 2^A բազմությունները հավասարազոր չեն:*

Ապացուցում: Յուրաքանչյուր $a \in A$ տարրի համապատասխանեցնելով $\{a\} \subseteq A$ ենթաբազմությունը, կստանանք մի $A \to 2^A$ ինյեկտիվ արտապատկերում:

Դիցուք գոյություն ունի որևէ $\varphi : A \to 2^A$ բիեկտիվ արտապատկերում: Ներմուծելով

$$M = \{a \in A \,|\, a \notin \varphi(a)\} \subseteq A$$

ենթաբազմությունը, կարող ենք ասել, որ գոյություն կունենա այնպիսի $a_0 \in A$ տարր, որ $\varphi(a_0) = M$: Եթե $a_0 \in M$, ապա ըստ M-ի սահմանման՝ $a_0 \notin \varphi(a_0) = M$, իսկ եթե $a_0 \notin M$, ապա $a_0 \in \varphi(a_0) = M$: Հակասություն:

□

0.3.6. Արտապատկերման միջուկի և պատկերի կապը և ընդհանրացված կապը: Տրված $\alpha : A \to B$ արտապատկերման համար՝

$$Im(\alpha) = \{\alpha(x) | \, x \in A\} = \alpha(A) \subseteq B$$

ենթաբազմությունը կոչվում է α-ի **պատկեր** կամ A-ի պատկեր α-ի նկատմամբ: Հետևյալ երկու արդյունքներից բխում է, որ գոյություն ունի սերտ կապ $Im(\alpha)$-ի և $Ker(\alpha)$-ի միջև:

Թեորեմ 0.8: *Եթե $\alpha : A \to B$ արտապատկերումը վերադրող (սյուրեկտիվ) է և $Ker(\alpha) = (\sim)$, ապա B և $A/_\sim$ բազմությունները հավասարազոր են: Ավելի ճշգրիտ, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\mu : B \to A/_\sim$ փոխմիարժեք (բիեկտիվ) արտապատկերում, որ $\pi = \alpha \cdot \mu$, այսինքն՝ տեղափոխական է արտապատկերումների հետևյալ եռանկյունը (դիագրամը)՝*

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[dr, "\pi"'] & B \arrow[d, "\mu"] \\ & A/_\sim \end{tikzcd} \quad ,$$

որտեղ π-ն բնական արտապատկերումն է, այսինքն՝ $\pi(x) = [x]$:

Ապացուցում: Քանի որ $\alpha : A \to B$ արտապատկերումը վերադրող (սյուրեկտիվ) է, ապա յուրաքանչյուր $y \in B$ տարրի համար գոյություն ունի այնպիսի $x \in A$ տարր, որ $\alpha(x) = y$: Սահմանենք $\mu(y) = [x]$, որտեղ $\alpha(x) = y$: Նախ համոզվենք, որ $\mu(y)$-ը կախված չէ $\alpha(x) = y$ պայմանին բավարարող x-ի ընտրությունից: Իրոք, եթե նաև $\alpha(x') = y$, ապա $\alpha(x) = \alpha(x')$ և $x \sim x'$, հետևաբար, $[x] = [x']$: Ակնհայտ է, որ սահմանված $\mu : B \to A/_{\sim}$ արտապատկերումը վերադրող (սյուրեկտիվ) է: Ապացուցենք μ արտապատկերման ներդրող (ինյեկտիվ) լինելը.

$$\mu(y_1) = \mu(y_2),\ y_1 = \alpha(x_1),\ y_2 = \alpha(x_2) \longrightarrow [x_1] = [x_2] \longrightarrow$$

$$x_1 \sim x_2 \longrightarrow \alpha(x_1) = \alpha(x_2) \longrightarrow y_1 = y_2 \ :$$

Ի վերջո, քանի որ $\mu(y) = [x]$, որտեղ $\alpha(x) = y$, ապա $\mu(\alpha(x)) = [x]$, հետևաբար, $(\alpha \cdot \mu)x = \pi(x)$ և $\alpha \cdot \mu = \pi$, որտեղից էլ բխում է μ-ի միակությունը.

$$\alpha \cdot \mu = \pi,\ \alpha \cdot \mu' = \pi \longrightarrow \alpha \cdot \mu = \alpha \cdot \mu' \longrightarrow (\alpha \cdot \mu)x = (\alpha \cdot \mu')x$$

$$\longrightarrow \mu(\alpha x) = \mu'(\alpha x) \longrightarrow \mu(y) = \mu'(y)$$

ցանկացած $y \in B$ տարրի համար: □

Թեորեմ 0.9 (ընդհանրացված կապը): *Կամայական $\alpha_1 : A \to B$ և $\alpha_2 : A \to B'$ վերադրող (սյուրեկտիվ) արտապատկերումների համար, որտեղ $Ker(\alpha_1) \subseteq Ker(\alpha_2)$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\alpha_3 : B \to B'$ վերադրող արտապատկերում, որ $\alpha_1 \cdot \alpha_3 = \alpha_2$, այսինքն՝ տեղափոխական է արտապատկերումների հետևյալ եռանկյունը.*

$$\begin{tikzcd} A \arrow[r, "\alpha_1"] \arrow[dr, "\alpha_2"'] & B \arrow[d, "\alpha_3"] \\ & B' \end{tikzcd} \quad :$$

Ըստ որում, α_3-ը կլինի փոխմիարժեք (բիեկտիվ) այն և միայն այն դեպքում, երբ $Ker(\alpha_1) = Ker(\alpha_2)$:

Ապացուցում: Քանի որ $\alpha_1 : A \to B$ արտապատկերումը վերադրող (սյուրեկտիվ) է, ապա յուրաքանչյուր $y \in B$ տարրի համար գոյություն ունի այնպիսի $x \in A$ տարր, որ $\alpha_1(x) = y$: Սահմանենք $\alpha_3(y) = \alpha_2(x)$: Նախ համոզվենք, որ $\alpha_3(y)$-ը կախված չէ $\alpha_1(x) = y$ պայմանին բավարարող x-ի ընտրությունից: Իրոք, եթե նաև $\alpha_1(x') = y$, ապա $\alpha_1(x) = \alpha_1(x')$ և $(x, x') = Ker(\alpha_1) \subseteq Ker(\alpha_2)$, հետևաբար, $(x, x') \in Ker(\alpha_2)$, այսինքն՝ $\alpha_2(x) = \alpha_2(x')$: Այնուհետև, սահմանված $\alpha_3 : B \to B'$ արտապատկերման վերադրող լինելն ակնհայտ է, որովհետև, եթե $z \in B'$ և $z = \alpha_2(x)$, $x \in A$, ապա նշանակելով $y = \alpha_1(x)$, կստանանք՝ $\alpha_3(y) = z$, որտեղ $y \in B$: Այժմ ապացուցենք, որ $\alpha_2 = \alpha_1 \cdot \alpha_3$: Քանի որ $\alpha_3(y) = \alpha_2(x)$, որտեղ $\alpha_1(x) = y$, ապա $\alpha_3(\alpha_1(x)) = \alpha_2(x)$, այսինքն՝ $(\alpha_1 \cdot \alpha_3)\, x = \alpha_2(x)$ և $\alpha_1 \cdot \alpha_3 = \alpha_2$: Այստեղից էլ բխում է α_3-ի միակությունը.

$$\alpha_1 \cdot \alpha_3 = \alpha_2,\ \alpha_1 \cdot \alpha_3' = \alpha_2 \longrightarrow \alpha_1 \cdot \alpha_3 = \alpha_1 \cdot \alpha_3' \longrightarrow$$

$$(\alpha_1 \cdot \alpha_3)\, x = (\alpha_1 \cdot \alpha_3')\, x \longrightarrow \alpha_3(\alpha_1(x)) = \alpha_3'(\alpha_1(x)) \longrightarrow \alpha_3(y) = \alpha_3'(y)$$

ցանկացած $y \in B$ տարրի համար:

Մնում է ստանալ α_3-ի փոխմիարժեքության պայմանը: Դիցուք $Ker(\alpha_1) = Ker(\alpha_2)$: Այդ դեպքում,

$$\alpha_3(y_1) = \alpha_3(y_2),\ y_1 = \alpha_1(x_1),\ y_2 = \alpha_1(x_2) \longrightarrow \alpha_2(x_1) = \alpha_2(x_2)$$

$$\longrightarrow \alpha_1(x_1) = \alpha_1(x_2) \longrightarrow y_1 = y_2\,,$$

հետևաբար, α_3-ը նաև ներդրող (ինյեկտիվ) է, այսինքն՝ α_3-ը փոխմիարժեք (բիեկտիվ) է:

Եվ հակառակը, եթե α_3-ը նաև ներդրող է, ապա

$$(x_1, x_2) \in Ker(\alpha_2) \longrightarrow \alpha_2(x_1) = \alpha_2(x_2) \longrightarrow$$

$$\alpha_3(\alpha_1(x_1)) = \alpha_3(\alpha_1(x_2)) \longrightarrow \alpha_1(x_1) = \alpha_1(x_2) \longrightarrow (x_1, x_2) \in Ker(\alpha_1)\,,$$

այսինքն՝ $Ker(\alpha_1) \subseteq Ker(\alpha_2)$ և $Ker(\alpha_1) = Ker(\alpha_2)$: □

Նկատենք նաև, որ առաջին թեորեմը բխում է երկրորդ թեորեմից:

0.4. Մասնակի կարգ, մասնակի և կավարածև կարգավորված բազմություններ

$\alpha \subseteq A \times A$ հարաբերությունը կոչվում է **մասնակի կարգ** կամ պարզապես **կարգ**՝ որոշված A բազմության վրա, եթե α-ն բավարարում է առինքնության, փոխանցականության և բ′) $(x, y) \in \alpha$, $(y, x) \in \alpha \to x = y$ (հակահամաչափություն կամ հակասիմետրիկություն)

պայմաններին:

Առինքնության և փոխանցականության պայմաններին բավարարող ցանկացած $\alpha \subseteq A \times A$ հարաբերություն կոչվում է **քվազիկարգ**, իսկ առինքնության և հակահամաչափության պայմաններին բավարարող ցանկացած $\alpha \subseteq A \times A$ հարաբերություն կոչվում է **պսևդոկարգ**:

Եթե α-ն մասնակի կարգ է, ապա սովորաբար α-ի փոխարեն օգտագործվում է «$\leqslant$» նշանը, իսկ $(x, y) \in \alpha$ պայմանն, այդ դեպքում, գրվում է $x \leqslant y$ կամ $y \geqslant x$ և կարդացվում է «x-ը փոքր է կամ հավասար y-ից» կամ «y-ը մեծ կամ հավասար է x-ից», իսկ մասնակի կարգի պայմանները ստանում են ավելի պարզ տեսք.

ա′) $x \leqslant x$; (առինքնություն կամ ռեֆլեքսիվություն)

բ′) $x \leqslant y,\ y \leqslant x \to x = y$; (հակահամաչափություն կամ հակասիմետրիկություն)

գ′) $x \leqslant y,\ y \leqslant z \to x \leqslant z$: (փոխանցականություն կամ տրանզիտիվություն)

Եթե $x \leqslant y$ առնչությունը տեղի չունի, ապա այդ դեպքում գրվում է $x \nleqslant y$ կամ $y \ngeqslant x$:

Լեմմ 0.5: *Միևնույն A բազմության վրա որոշված ցանկացած թվով մասնակի կարգերի հատումը նորից մասնակի կարգ է:* □

Եթե $x_1 \leqslant x_2$, $x_2 \leqslant x_3$, $\ldots$, $x_{n-1} \leqslant x_n$, ապա համառոտ գրվում է՝ $x_1 \leqslant x_2 \leqslant \cdots \leqslant x_{n-1} \leqslant x_n$:

A բազմությունն իր վրա որոշված «$\leqslant$» մասնակի կարգի հետ մեկտեղ կոչվում է **մասնակի կարգավորված բազմություն** և նշանակվում է՝ $A(\leqslant)$ կամ համառոտ A-ով: Եթե $x \leqslant y$ և $x \neq y$, ապա գրվում է $x < y$ կամ $y > x$ և կարդացվում է «x-ը խիստ փոքր է y-ից» կամ «y-ը խիստ մեծ է x-ից»: Ոչ դատարկ $H \subseteq A$ ենթաբազմությունը կոչվում է **ուռուցիկ** A-ում, եթե $a, b \in H$, $x \in A$ և $a \leqslant x \leqslant b$ պայմաններից բխում է՝ $x \in H$: $A(\leqslant)$ մասնակի կարգավորված բազմության $B \subseteq A$ ոչ դատարկ ենթաբազմությունը ևս կլինի մասնակի կարգավորված բազմություն՝ նույն մասնակի կարգի նկատմամբ, այսինքն՝ B-ում $x \leqslant y$ այն և միայն այն դեպքում, երբ A-ում $x \leqslant y$, որտեղ $x, y \in B$: Ավելի ճիշտ տեղի ունի հետևյալ պնդումը:

Լեմմ 0.6: *Ցանկացած $B \subseteq A$, $B \neq \emptyset$, ենթաբազմության և $\alpha \subseteq A \times A$ մասնակի կարգի համար*

$$\alpha \cap (B \times B) = \beta \subseteq B \times B$$

հարաբերությունը կլինի մասնակի կարգ որոշված B-ի վրա, այսինքն՝ $B \subseteq A$ ենթաբազմության վրա α-ի մակածված հարաբերությունը ևս մասնակի կարգ է: □

Դիցուք $A(\leqslant)$ զույգը մասնակի կարգավորված բազմություն է, $X \subseteq A$, $X \neq \emptyset$ և $a \in A$: a տարրը կոչվում է X-ի **վերին (ստորին) եզր**, եթե $x \leqslant a$ (համապատասխանաբար՝ $a \leqslant x$) ցանկացած $x \in X$ տարրի համար: a տարրը կոչվում է X-ի **վերին (ստորին) ճշգրիտ եզր** և նշանակվում է $a = \sup X$ կամ $a = \sup(X)$ ($a = \inf X$ կամ $a = \inf(X)$), եթե

ա) a-ն վերին (ստորին) եզր է X-ի համար;

բ) X-ի ցանկացած c վերին (ստորին) եզրի համար՝ $a \leqslant c$ (համապատասխանաբար՝ $c \leqslant a$):

Վերին (ստորին) եզր ունեցող X բազմությունը կոչվում է նաև **վերևից (ներքևից) սահմանափակ բազմություն**:

Հակահամաչափությունից բխում է, որ վերին և ստորին ճշգրիտ եզրերը որոշվում են միարժեքորեն, եթե դրանք գոյություն ունեն: Եթե $X = \{a_1, \ldots, a_n\}$, ապա նշանակվում է նաև

$$\sup X = \sup\{a_1, \ldots, a_n\},$$

$$\inf X = \inf\{a_1, \ldots, a_n\}:$$

Օրինակ, եթե $a \leqslant b$, ապա $\sup\{a, b\} = b$, իսկ $\inf\{a, b\} = a$: (Վերին և ստորին (ճշգրիտ) եզրերը կարելի է սահմանել նաև կամայական $A(\leqslant)$ զույգի դեպքում, որտեղ A բազմության վրա որոշված «$\leqslant$» հարաբերությունը կամայական է:)

$A(\leqslant)$ մասնակի կարգավորված բազմությունը կոչվում է **կավարածև կարգավորված**, եթե $\sup\{a, b\}$-ն և $\inf\{a, b\}$-ն գոյություն ունեն A-ում՝ ցանկացած $a, b \in A$ տարրերի համար: Օրինակ, միևնույն Q բազմության բոլոր ենթաբազմությունների 2^Q համախմբությունը կլինի կավարածև կարգավորված բազմություն՝ տեսա-բազմային ներդրման նկատմամբ, այսինքն՝

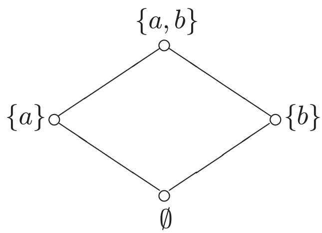
$$X_1 \leqslant X_2 \leftrightarrow X_1 \subseteq X_2,$$

որտեղ $X_1, X_2 \in 2^Q$: Այս $2^Q(\leqslant)$ մասնակի կարգավորված բազմությունը նշանակվում է նաև $2^Q(\subseteq)$-ով: Այստեղ,

$$\sup\{X_1, X_2\} = X_1 \cup X_2, \quad \inf\{X_1, X_2\} = X_1 \cap X_2, \quad X_1, X_2 \in 2^Q \, :$$

Այս բանաձևերը ճիշտ են նաև ցանկացած թվով ենթաբազմությունների դեպքում: Տրված Q բազմության բոլոր վերջավոր ենթաբազմությունների բազմությունը նշանակվում է $2^{fin(Q)}$-ով և այս բազմությունը ևս կլինի կավարաձև կարգավորված բազմություն՝ նույն «$\subseteq$» մասնակի կարգի նկատմամբ:

Կասենք, որ $A(\leqslant)$ մասնակի կարգավորված բազմության $y \in A$ տարրը **ծածկում է** $x \in A$ տարրին կամ x-ը ծածկվում է y-ով, եթե $x < y$ և գոյություն չունի այնպիսի $z \in A$ տարր, որ $x < z < y$: Մասնակի կարգավորված բազմությունները պատկերվում են հարթության մեջ՝ **գրաֆների** տեսքով, հետևյալ կերպ. A բազմության տարրերը պատկերվում են որպես հարթության կետեր և կոչվում են **գրաֆի գագաթներ**, իսկ **գրաֆի կողերը** որոշվում են հետևյալ կերպ. եթե y-ը ծածկում է x-ին, ապա y տարրը պատկերվում է x տարրից վերև և x, y տարրերին համապատասխանող կետերը միացվում են ուղղի հատվածով: Օրինակ, երկու տարրանի $Q = \{a, b\}$ բազմության բոլոր ենթաբազմությունների բազմության $2^Q(\subseteq)$ մասնակի կարգավորված բազմությունը պատկերվում է հետևյալ կերպ.



:

Դիտարկենք $A(\leqslant)$ մասնակի կարգավորված բազմությունը և դիցուք $a, b \in A$, $a \leqslant b$: a և b ծայրակետերով **հատված** ասելով հասկացվում է

$$[a, b] = \{x \in A \mid \ a \leqslant x \leqslant b\} \subseteq A$$

ենթաբազմությունը: Եթե $a < b$, ապա սահմանվում են նաև հետևյալ

$$(a, b) = \{x \in A \mid \ a < x < b\} \, ,$$

$$[a,b) = \{x \in A \mid \ a \leqslant x < b\},$$

$$(a,b] = \{x \in A \mid \ a < x \leqslant b\}$$

միջակայքերը: Ակնհայտ է, որ $a,b \in [a,b]$: $[a,b]$ հատվածը կոչվում է **պարզ**, եթե $a < b$ և $[a,b] = \{a,b\}$: $[a,b]$ հատվածը կլինի պարզ այն և միայն այն դեպքում, երբ b-ն ծածկում է a-ին:

$A(\leqslant)$ մասնակի կարգավորված բազմության a և b տարրերը կոչվում են **համեմատելի**, եթե $a \leqslant b$ կամ $b \leqslant a$: Հակառակ դեպքում a և b տարրերը կոչվում են **ոչ համեմատելի**: Մասնակի կարգավորված բազմությունը կոչվում է **գծային** (կամ գծայնորեն) **կարգավորված** կամ **շղթա**, եթե նրա կամայական երկու տարրեր համեմատելի են: Օրինակ, $\mathbb{R}$-ը իրական թվերի սովորական «$\leqslant$» կարգի նկատմամբ այդպիսին է:

$A(\leqslant)$ մասնակի կարգավորված բազմության $u \in A$ տարրը կոչվում է նրա **մեծագույն տարր**, եթե $x \leqslant u$ ցանկացած $x \in A$ տարրի համար: Եթե $v \leqslant x$ ցանկացած $x \in A$ տարրի համար, ապա $v \in A$ տարրը կոչվում է $A(\leqslant)$ մասնակի կարգավորված բազմության **փոքրագույն տարր**:

Ակնհայտ է, որ մեծագույն (փոքրագույն) տարրը, եթե այն գոյություն ունի, ապա որոշվում է միարժեքորեն: Սովորաբար մեծագույն տարրը կոչվում է **մեկ** և նշանակվում է 1-ով, իսկ փոքրագույն տարրը կոչվում է **զրո** և նշանակվում է 0-ով: Փոքրագույն և մեծագույն տարրերով օժտված մասնակի կարգավորված բազմությունը կոչվում է **սահմանափակ**:

$a \in A$ տարրը կոչվում է **մաքսիմալ տարր**, եթե գոյություն չունի այնպիսի $x \in A$ տարր, որ $a < x$:

$b \in A$ տարրը կոչվում է **մինիմալ տարր**, եթե գոյություն չունի այնպիսի $x \in A$ տարր, որ $x < a$:

Ակնհայտ է, որ մեծագույն (փոքրագույն) տարրը, եթե այն գոյություն ունի, ապա կլինի նաև միակ մաքսիմալ (մինիմալ) տարրը:

Եթե մասնակի կարգավորված բազմությունն օժտված է 0 փոքրագույն տարրով, ապա 0-ին ծածկող ցանկացած տարր կոչվում է **ատոմ**: Իսկ եթե մասնակի կարգավորված բազմությունն օժտված է 1 մեծագույն տարրով, ապա ցանկացած տարր, որը ծածկվում է 1-ով կոչվում է **երկակի ատոմ** կամ **կոատոմ**:

$A(\leqslant)$ մասնակի կարգավորված բազմությունը կոչվում է վերջավոր, եթե A բազմությունը վերջավոր է: Նույնիսկ, վերջավոր մասնակի կարգավորված բազմությունը կարող է չունենալ մեծագույն կամ փոքրագույն տարրեր: Սակայն տեղի ունի հետևյալ պնդումը:

Թեորեմ 0.10: *Վերջավոր մասնակի կարգավորված բազմությունն ունի գոնե մեկ հատ մաքսիմալ և գոնե մեկ հատ մինիմալ տարր:*

Ապացուցում: Նախ ապացուցենք մաքսիմալ տարրի գոյությունը: Դիցուք $A(\leqslant)$ զույգը վերջավոր մասնակի կարգավորված բազմություն է, իսկ $a \in A$: Եթե a տարրը մաքսիմալ է, ապա պնդումն ապացուցված է: Հակառակ դեպքում, գոյություն կունենա այնպիսի $a_1 \in A$ տարր, որ $a < a_1$: Եթե a_1-ը մաքսիմալ է, ապա պնդումը կլինի ապացուցված: Հակառակ դեպքում, գոյություն կունենա այնպիսի $a_2 \in A$ տարր, որ $a_1 < a_2$: Եվ այսպես շարունակ: Արդյունքում կստանանք $a < a_1 < a_2 < \cdots$ շղթան: Քանի որ A բազմությունը վերջավոր է, ապա ստացված շղթան ևս կլինի վերջավոր, որի վերջին տարրը ակնհայտորեն կլինի դիտարկվող մասնակի կարգավորված բազմության համար մաքսիմալ տարր: Մինիմալ տարրի գոյությունն ապացուցվում է համանման դատողություններով: □

Հետևություն 0.10: *Եթե վերջավոր մասնակի կարգավորված բազմությունն օժտված է միակ մաքսիմալ (մինիմալ) տարրով, ապա այդ տարրը կլինի նաև նրա մեծագույն (փոքրագույն) տարրը:*

Ապացուցում: Դիցուք a-ն $A(\leqslant)$ վերջավոր մասնակի կարգավորված բազմության միակ մաքսիմալ տարրն է: Դիտարկենք կամայական $x \in A$ տարրից սկսվող $x < x_1 < x_2 < \cdots$ (աճող) շղթան: Քանի որ A բազմությունը վերջավոր է, ապա այս շղթան ևս կլինի վերջավոր և նրա վերջին x_n տարրը կլինի $A(\leqslant)$ մասնակի կարգավորված բազմության մաքսիմալ տարրը: Համաձայն մաքսիմալ տարրի միակության պայմանի՝ $x_n = a$: Հետևաբար,

$$x < x_1 < x_2 < \cdots < x_{n-1} < x_n = a$$

և $x \leqslant a$: Այսպիսով, a տարրը կլինի դիտարկվող մասնակի կարգավորված բազմության մեծագույն տարրը:

Համանման դատողություններով ապացուցվում է, որ միակ մինիմալ տարրով օժտված վերջավոր մասնակի կարգավորված բազմությունն օժտված է նաև փոքրագույն տարրով: □

Լեմմ 0.7: *Եթե $A(\leqslant)$ զույգը կավարաձև կարգավորված բազմություն է, ապա $\sup X$-ը և $\inf X$-ը գոյություն ունեն ցանկացած ոչ դատարկ $X \subseteq A$ վերջավոր ենթաբազմության համար: Մասնավորապես, վերջավոր կավարաձև կարգավորված բազմությունը սահմանափակ է: Եթե $A(\leqslant)$ զույգը մասնակի կարգավորված բազմություն է և $\sup\{a,b\}$-ն ($\inf\{a,b\}$-ն) գոյություն ունի ցանկացած $a, b \in A$ տարրերի համար, ապա $\sup(X)$-ը ($inf(X)$-ը) գոյություն կունենա ցանկացած ոչ դատարկ $X \subseteq A$ վերջավոր ենթաբազմության համար:*

Ապացույց: Լեմմն ապացուցվում է վերհանգման եղանակով՝ ըստ $|X| = n$ բնական թվի: Եթե $n = 1$ կամ $n = 2$, ապա պնդումը ճիշտ է: Ենթադրենք պնդումը ճիշտ է n-ից փոքր կարգ ունեցող $X \subseteq Q$ ենթաբազմությունների համար: Դիցուք $|X| = n$ և $X = \{x_1, x_2, \ldots, x_n\}$: Տեղի ունեն

$$\sup X = \sup\{\sup\{x_1, \ldots, x_{n-1}\}, x_n\}$$

և

$$\inf X = \inf\{\inf\{x_1, \ldots, x_{n-1}\}, x_n\}$$

հավասարությունները: Օրինակ, եթե $\sup\{x_1, \ldots, x_{n-1}\} = a$ և $\sup\{a, x_n\} = b$, ապա $x_i \leqslant a \leqslant b$, որտեղ $i = 1, \ldots, n-1$ և $x_n \leqslant b$: Հետևաբար, $x_i \leqslant b$, որտեղ $i = 1, \ldots, n$, այսինքն՝ b-ն $X \subseteq Q$ ենթաբազմության վերին եզր է: Դիցուք $x_i \leqslant c$, որտեղ $i = 1, \ldots, n$: Հետևաբար, $a \leqslant c$ և $x_n \leqslant c$, այսինքն՝ c-ն կլինի $\{a, x_n\} \subseteq Q$ ենթաբազմության վերին եզրը, ուստի՝ $b \leqslant c$: Այսպիսով, b-ն $X \subseteq Q$ ենթաբազմության վերին ճշգրիտ եզրն է:

Եթե $A(\leqslant)$ զույգը վերջավոր կավարաձև կարգավորված բազմություն է, ապա $\sup A$-ն կլինի նրա մեծագույն տարրը, իսկ $\inf A$-ն՝ փոքրագույն տարրը: □

Ապացուցենք հետևյալ հայտանիշը:

Թեորեմ 0.11: *Որպեսզի $A(\leqslant)$ վերջավոր մասնակի կարգավորված բազմությունը լինի կավարաձև կարգավորված բազմություն անհրաժեշտ է և բավարար, որ այն լինի օժտված մեծագույն տարրով և գոյություն ունենա $\inf\{a,b\}$-ն ցանկացած $a, b \in A$ տարրերի համար:*

Ապացույց: *Անհրաժեշտությունը* բխում է նախորդ լեմմից: Ապացուցենք *բավարարությունը:* Դիցուք $A(\leqslant)$ վերջավոր մասնակի կարգավորված բազմությունն օժտված է մեծագույն տարրով և դիցուք

$\inf\{a,b\}$-ն գոյություն ունի ցանկացած $a,b \in A$ տարրերի համար: Պահանջվում է ապացուցել $\sup\{a,b\}$-ի գոյությունը ցանկացած $a,b \in A$ տարրերի համար: Դիտարկենք

$$A_a^b = \{x \in A \,|\, x \geqslant a, x \geqslant b\}$$

բազմությունը, որը դատարկ չէ, որովհետև այն պարունակում է A-ի մեծագույն տարրը: A_a^b-ն ևս կլինի վերջավոր մասնակի կարգավորված բազմություն` նույն «$\leqslant$» կարգի նկատմամբ: Թեորեմ 0.10-ի համաձայն, $A_a^b(\leqslant)$ մասնակի կարգավորված բազմությունն օժտված է մինիմալ տարրով: Ապացուցենք, որ այն օժտված է միակ մինիմալ տարրով: Դիցուք $\alpha, \beta \in A_a^b$ տարրերը մինիմալ տարրեր են: Ըստ թեորեմի պայմանի, գոյություն ունի այնպիսի $\gamma \in A$ տարր, որ $\gamma = \inf\{\alpha,\beta\}$: Այնուհետև, $\alpha \geqslant a$, $\alpha \geqslant b$, $\beta \geqslant a$, $\beta \geqslant b$, այսինքն` $a$ և $b$ տարրերը հանդիսանում են $\{\alpha,\beta\}$ ենթաբազմության ստորին եզրեր: Հետևաբար, $a \leqslant \gamma$ և $b \leqslant \gamma$, այսինքն` $\gamma \in A_a^b$: Սակայն, ըստ $\inf\{\alpha,\beta\}$-ի սահմանման, $\gamma \leqslant \alpha$, $\gamma \leqslant \beta$ և, համաձայն α-ի և β-ի մինիմալության պայմանի, $\gamma = \alpha$ և $\gamma = \beta$: Ուստի` $\alpha = \beta = \gamma$, իսկ ըստ հետևություն 0.10-ի, $A_a^b(\leqslant)$ մասնակի կարգավորված բազմության միակ $\gamma \in A_a^b$ մինիմալ տարրը կլինի դրա փոքրագույն տարրը, այսինքն` $\gamma \leqslant x$ ցանկացած $x \in A_a^b$ տարրի համար: Այժմ ապացուցենք $\gamma = \sup\{a,b\}$ հավասարությունը:

Իրոք, γ-ն $\{a,b\}$-ի վերին եզր է, որովհետև $\gamma \in A_a^b$: Իսկ եթե $c \geqslant a$ և $c \geqslant b$, ապա $c \in A_a^b$ և $\gamma \leqslant c$, որովհետև γ-ն A_a^b բազմության փոքրագույն տարրն է:

Երկրորդ ապացուցում: Գոյություն ունի $\inf\left(A_a^b\right)$-ն` համաձայն նախորդ լեմմի: Դիցուք $\gamma = \inf\left(A_a^b\right)$: Քանի որ $a,b \in A$ տարրերը A_a^b բազմության ստորին եզրեր են, իսկ γ-ն A_a^b-ի ստորին ճշգրիտ եզրն է, ապա $a \leqslant \gamma$ և $b \leqslant \gamma$: Հետևաբար, γ-ն $\{a,b\}$ ենթաբազմության վերին եզր է: Իսկ եթե c-ն $\{a,b\}$-ի կամայական վերին եզր է, ապա $c \in A_a^b$ և $\gamma \leqslant c$: Այսպիսով, $\gamma = \sup\{a,b\}$: □

Թեորեմ 0.12*: Որպեսզի $A(\leqslant)$ վերջավոր մասնակի կարգավորված բազմությունը լինի կավարածև կարգավորված բազմություն անհրաժեշտ է և բավարար, որ այն լինի օժտված փոքրագույն տարրով և գոյություն ունենա $\sup\{a,b\}$-ն ցանկացած $a,b \in A$ տարրերի համար:* □

Ցոռնի աքսիոմը (M. Zorn): *Եթե $A(\leqslant)$ մասնակի կարգավորված բազմության մեջ յուրաքանչյուր գծային կարգավորված* *ենթաբազմություն օժտված է վերին եզրով, ապա* $A(\leqslant)$ *մասնակի կարգավորված բազմությունն օժտված է մաքսիմալ տարրով, իսկ յուրաքանչյուր* $x \in A$ *տարրի համար գոյություն ունի այնպիսի* $m \in A$ *մաքսիմալ տարր, որ* $x \leqslant m$*:*

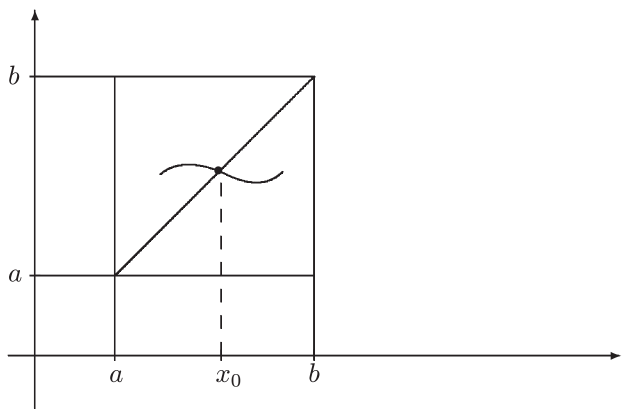
0.5. Անշարժ կետի վերաբերյալ Քնաստեր-Տարսկիի և Բիրկհոֆ-Տարսկիի թեորեմները: Բանախի և Կանտոր-Շրյոդեր-Բեռնշտայնի թեորեմները

Վերհիշենք հետևյալ սահմանումը:

Դիցուք Q-ն կամայական ոչ դատարկ բազմություն է: $x_0 \in Q$ տարրը կոչվում է $f : Q \to Q$ **արտապատկերման անշարժ կետ**, եթե $f(x_0) = x_0$: Անշարժ կետի գոյության վերաբերյալ առաջին թեորեմներից մեկը հանդիպում է մաթեմատիկական անալիզի դասընթացում:

Թեորեմ 0.13 (Բրաուեր): *Յուրաքանչյուր* $f : [a, b] \to [a, b]$ *անընդհատ ֆունկցիա ունի անշարժ կետ* $(a \leqslant b)$*:*

Ապացուցում: Իրոք, եթե $f(a) \neq a$ և $f(b) \neq b$, ապա $g(x) = f(x) - x$ անընդհատ ֆունկցիան $[a, b] \subseteq \mathbb{R}$ հատվածի ծայրակետերում կունենա տարբեր նշանի արժեքներ՝ $g(a) > 0$ և $g(b) < 0$: Հետևաբար, միջանկյալ արժեքի վերաբերյալ Բոլցանո-Կոշիի թեորեմի համաձայն, գոյություն կունենա այնպիսի $x_0 \in (a, b)$, որ $g(x_0) = 0$, այսինքն՝ $f(x_0) = x_0$: □



Սակայն թեորեմ 0.15-ից բխում է նաև, որ ապացուցված թեորեմը մնում է ուժի մեջ, եթե $f : [a, b] \to [a, b]$ անընդհատ ֆունկցիան փոխարինենք աճող ֆունկցիայով՝

$$x \leqslant y \longrightarrow f(x) \leqslant f(y),$$

որտեղ $x, y \in [a, b]$:

$Q(\leqslant)$ մասնակի կարգավորված բազմությունը կոչվում է **լրիվ կավարածև կարգավորված բազմություն**, եթե $\sup(X)$-ը և $\inf(X)$-ը գոյություն ունեն ցանկացած ոչ դատարկ $X \subseteq Q$ ենթաբազմության համար:

Թեորեմ 0.14: *$Q(\leqslant)$ մասնակի կարգավորված բազմությունը կլինի լրիվ կավարածև կարգավորված բազմություն, եթե տեղի ունի հետևյալ պայմաններից որևէ մեկը.*
1) դրանում գոյություն ունի մեծագույն տարր և $\inf(X)$-ը գոյություն ունի ցանկացած ոչ դատարկ $X \subseteq Q$ ենթաբազմության համար;
2) դրանում գոյություն ունի փոքրագույն տարր և $\sup(X)$-ը գոյություն ունի ցանկացած ոչ դատարկ $X \subseteq Q$ ենթաբազմության համար:

Ապացուցում: 1) Նշանակենք X^0-ով X-ի բոլոր վերին եզրերի բազմությունը՝

$$X^0 = \{a \in Q \,|\, x \leqslant a, \ \forall x \in X\}$$

և նկատենք, որ $X^0 \neq \emptyset$, որովհետև Q-ի մեծագույն տարրը պարունակվում է X^0-ում: Հետևաբար, գոյություն ունի $b = \inf(X^0) \in Q$: Ապացուցենք, որ $b = \sup(X)$: Իրոք, քանի որ յուրաքանչյուր $x \in X$ տարր X^0 բազմության ստորին եզր է, ապա $x \leqslant b$ (այսինքն՝ $b \in X^0$): Մյուս կողմից, եթե $c \in Q$ տարրը X-ի կամայական վերին եզր է, այսինքն՝ $x \leqslant c$ ցանկացած $x \in X$ տարրի համար, ապա $c \in X^0$ և, հետևաբար, $b \leqslant c$: Այսպիսով, $b = \sup(X)$: □

Դիցուք, տրված են $Q(\leqslant)$ և $Q'(\leqslant)$ մասնակի կարգավորված բազմությունները: $\varphi : Q \to Q'$ արտապատկերումը կոչվում է **մոնոտոն** կամ **իզոտոն**, եթե

$$x \leqslant y \longrightarrow \varphi(x) \leqslant \varphi(y),$$

որտեղ $x, y \in Q$:

Դժվար չէ ստուգել, որ երկու մոնոտոն արտապատկերումների արտադրյալը նորից մոնոտոն արտապատկերում է (եթե այն գոյություն ունի):

Անշարժ կետի գոյության վերաբերյալ հետևյալ դասական արդյունքը կոչվում է Քնաստեր-Տարսկիի թեորեմ (B. Knaster, A. Tarski), որտեղ $Fix(\varphi)$-ով նշանակված է φ-ի բոլոր անշարժ կետերի բազմությունը:

Թեորեմ 0.15 (Քնաստեր, Տարսկի): *Ցանկացած $Q(\leqslant)$ լրիվ կավարածև կարգավորված բազմության յուրաքանչյուր $\varphi : Q \to Q$ մոնոտոն արտապատկերում ունի անշարժ կետ:*
1) Դեռ ավելին,

$$\alpha = \sup\{x \in Q \,|\, x \leqslant \varphi(x)\} \in Q$$

տարրը φ-ի անշարժ կետ է և այն հանդիսանում է φ-ի բոլոր անշարժ կետերից մեծագույնը, այսինքն՝ $a \leqslant \alpha$, որտեղ a-ն φ-ի ցանկացած անշարժ կետ է:
2) Այնուհետև,

$$\beta = \inf\{x \in Q \,|\, \varphi(x) \leqslant x\} \in Q$$

տարրը նույնպես φ-ի անշարժ կետ է և այն հանդիսանում է φ-ի բոլոր անշարժ կետերից փոքրագույնը, այսինքն՝ $\beta \leqslant a$, որտեղ a-ն φ-ի ցանկացած անշարժ կետ է:
3) $Fix(\varphi)$ մասնակի կարգավորված բազմությունը լրիվ կավարածև կարգավորված բազմություն է:

Ապացուցում: 1) Դիցուք

$$X = \{x \in Q \,|\, x \leqslant \varphi(x)\};$$

Ակնհայտ է, որ $X \neq \emptyset$, որովհետև $0 \in X$, որտեղ $0 = \inf(Q)$ տարրը Q-ի փոքրագույն տարրն է: Հետևաբար, գոյություն ունի $\alpha = \sup(X) \in Q$: Ցանկացած $x \in X$ տարրի համար՝ $x \leqslant \alpha$ և $x \leqslant \varphi(x) \leqslant \varphi(\alpha)$, այսինքն՝ $\varphi(\alpha)$-ն X-ի վերին եզր է և, հետևաբար, $\alpha \leqslant \varphi(\alpha)$: Ուստի, $\varphi(\alpha) \leqslant \varphi(\varphi(\alpha))$ և $\varphi(\alpha) \in X$, որտեղից $\varphi(\alpha) \leqslant \alpha = \sup(X)$: Այսպիսով, $\varphi(\alpha) = \alpha$: Իսկ, եթե $\varphi(a) = a$, որտեղ $a \in Q$, ապա $a \in X$ և $a \leqslant \alpha$:
2) Երկրորդ պնդումն ապացուցվում է երկակի դատողություններով:
Ապացուցենք 3)-ը: Դիցուք $Y \subseteq Fix(\varphi)$, $Y \neq \emptyset$ և $\sup(Y) = a$: Դիտարկենք $[a, 1] = \{x \in Q | \, a \leqslant x \leqslant 1\} \subseteq Q$ ենթաբազմությունը, որտեղ $1 = \sup(Q)$ և նշանակենք $A = [a, 1]$: Ակնհայտ է, որ $A(\leqslant)$ մասնակի կարգավորված բազմությունը լրիվ կավարածև կարգավորված բազմություն է: Եթե $y \in Y$, ապա $y \leqslant a$ և $y = \varphi(y) \leqslant \varphi(a)$,

այսինքն՝ $\varphi(a)$-ն վերին եզր է Y-ի համար, ուստի՝ $a \leqslant \varphi(a)$: Դիցուք $t \in A$: Հետևաբար, $a \leqslant t$ և $a \leqslant \varphi(a) \leqslant \varphi(t)$, այսինքն՝ $a \leqslant \varphi(t)$ և $\varphi(t) \in A$: Այսպիսով, φ-ն A բազմությունն արտապատկերում է A-ի մեջ ու $A(\leqslant)$ լրիվ կավարաձև կարգավորված բազմության համար կարելի է կիրառել 2) պնդումը, այսինքն՝

$$b = \inf\{x \in A \,|\, \varphi(x) \leqslant x\} \in A$$

տարրը φ-ի անշարժ կետ է և փոքր է կամ հավասար A-ին պատկանող φ-ի բոլոր անշարժ կետերից: Մնում է նկատել, որ b-ն կլինի Y-ի վերին ճշգրիտ եզրը $Fix(\varphi)$-ում և օգտվել նախորդ թեորեմից:

Իրոք, b-ն Y-ի վերին եզր է, որովհետև $y \leqslant a \leqslant b$ և $y \leqslant b$ ցանկացած $y \in Y$ տարրի համար: Այնուհետև, եթե $b' \in Fix(\varphi)$ տարրը Y-ի վերին եզր է, ապա ցանկացած $y \in Y$ տարրի համար՝

$$y \leqslant b' \in Fix(\varphi) \longrightarrow a \leqslant b' \longrightarrow b' \in A \longrightarrow b \leqslant b':$$ □

Քնաստեր-Տարսկիի ապացուցված թեորեմից կարելի է բխեցնել հետևյալ երկու հայտնի արդյունքները:

Թեորեմ 0.16 (Բանախ): *Ցանկացած $f : X \to Y$ և $g : Y \to X$ արտապատկերումների համար գոյություն ունեն այնպիսի $X_1, X_2 \subseteq X$ և $Y_1, Y_2 \subseteq Y$ ենթաբազմություններ, որ*

$$f(X_1) = Y_1, \quad g(Y_2) = X_2,$$

որտեղ

$$X = X_1 \cup X_2,\ X_1 \cap X_2 = \emptyset,$$
$$Y = Y_1 \cup Y_2,\ Y_1 \cap Y_2 = \emptyset:$$

Ապացուցում: Նախ նկատենք, որ X բազմության բոլոր ենթաբազմությունների 2^X բազմությունը լրիվ կավարաձև կարգավորված բազմություն է (տեսա-բազմային «$\subseteq$» ներդրման նկատմամբ): Սահմանենք $\varphi : 2^X \to 2^X$ արտապատկերումը հետևյալ կերպ՝

$$\varphi(S) = X \setminus g(Y \setminus f(S)), \qquad S \subseteq X:$$

Ակնհայտ է, որ φ-ն մոնոտոն արտապատկերում է, այսինքն՝

$$S_1 \subseteq S_2 \longrightarrow \varphi(S_1) \subseteq \varphi(S_2):$$

Հետևաբար, ըստ նախորդ թեորեմի, φ-ն կունենա անշարժ կետ, այսինքն՝ գոյություն կունենա այնպիսի $S_0 \subseteq X$, որ $\varphi(S_0) = S_0$, կամ՝

$$X \setminus g(Y \setminus f(S_0)) = S_0 :$$

Նշանակելով՝ $S_0 = X_1$, $f(S_0) = Y_1$, $Y \setminus Y_1 = Y_2$, $g(Y_2) = X_2$, այստեղից կունենանք՝ $X \setminus X_2 = X_1$: □

Թեորեմ 0.17 (Կանտոր, Շրյոդեր, Բեռնշտայն): *Եթե գոյություն ունեն $f : X \to Y$ և $g : Y \to X$ ներդրող (ինյեկտիվ) արտապատկերումներ, ապա գոյություն կունենա նաև որևէ $\varphi : X \to Y$ փոխմիարժեք (բիեկտիվ) արտապատկերում:*

Ապացույց: Ըստ նախորդ թեորեմի, գոյություն ունեն այնպիսի $X_1, X_2 \subseteq X$ և $Y_1, Y_2 \subseteq Y$ ենթաբազմություններ, որ $f(X_1) = Y_1$, $g(Y_2) = X_2$, որտեղ

$$X = X_1 \cup X_2, \quad X_1 \cap X_2 = \emptyset,$$
$$Y = Y_1 \cup Y_2, \quad Y_1 \cap Y_2 = \emptyset :$$

Հետևաբար, որոնելի $\varphi : X \to Y$ փոխմիարժեք (բիեկտիվ) արտապատկերումը կարելի է սահմանել հետևյալ կերպ՝

$$\varphi(x) = \begin{cases} f(x), & \text{եթե } x \in X_1, \\ y, & \text{եթե } x \in X_2 \text{ և } g(y) = x,\ y \in Y_2 : \end{cases}$$ □

$A(\leqslant)$ մասնակի կարգավորված բազմությունը կոչվում է վերին (ներքին) լրիվ պայմանական կավարաձև կարգավորված բազմություն, եթե նրա վերին (ստորին) եզր ունեցող ցանկացած ոչ դատարկ ենթաբազմություն ունի նաև վերին (ստորին) ճշգրիտ եզր: Տեղի ունի հետևյալ արդյունքը, որը կոչվում է Բիրկհոֆ-Տարսկիի թեորեմ (G. Birkhoff) և հանդիսանում է Քնաստեր-Տարսկիի թեորեմի ընդհանրացումը:

Թեորեմ 0.18 (Բիրկհոֆ, Տարսկի): *Ցանկացած $A(\leqslant)$ վերին կամ ներքին լրիվ պայմանական կավարաձև կարգավորված բազմության յուրաքանչյուր $f : [a, b] \to [a, b]$ մոնոտոն արտապատկերում ունի անշարժ կետ, որտեղ $a \leqslant b$, $a, b \in A$:*

Ավելի ճշգրիտ՝

1) եթե $A(\leqslant)$ մասնակի կարգավորված բազմությունը վերին լրիվ պայմանական կավարաձև կարգավորված բազմություն է, ապա

$$\alpha = \sup\{x \in [a, b] \,|\, x \leqslant f(x)\} \in [a, b]$$

տարրը f-ի անշարժ կետ է և այն հանդիսանում է f-ի $[a,b]$-ին պատկանող բոլոր անշարժ կետերից մեծագույնը, այսինքն $d \leqslant \alpha$, որտեղ d-ն $[a,b]$-ին պատկանող f-ի ցանկացած անշարժ կետ է;
2) եթե $A(\leqslant)$ մասնակի կարգավորված բազմությունը ներքին լրիվ պայմանական կավարաձև կարգավորված բազմություն է, ապա

$$\beta = \inf\{x \in [a,b] \,|\, f(x) \leqslant x\} \in [a,b]$$

տարրը f-ի անշարժ կետ է և այն հանդիսանում է f-ի $[a,b]$-ին պատկանող բոլոր անշարժ կետերից փոքրագույնը, այսինքն $\beta \leqslant d$, որտեղ d-ն $[a,b]$-ին պատկանող f-ի ցանկացած անշարժ կետ է:

Ապացուցում: 1) Եթե A-ն վերին լրիվ պայմանական կավարաձև կարգավորված բազմություն է, ապա դիտարկում ենք

$$M = \{x \in [a,b] \,|\, x \leqslant f(x)\}$$

ոչ դատարկ $(a \in M)$ և b վերին եզր ունեցող բազմությունը: Հետևաբար, գոյություն ունի $x_0 = \sup(M) \in A$ վերին ճշգրիտ եզրը: Ակնհայտ է, որ $x_0 \in [a,b]$, որովհետև $a \leqslant x \leqslant x_0$ և $x \leqslant b$ ցանկացած $x \in M$ տարրի համար: Հետևաբար, $f(x_0) \in [a,b]$: Մնում է նկատել, որ ցանկացած $x \in M$ տարրի համար՝ $x \leqslant x_0$, $x \leqslant f(x) \leqslant f(x_0)$, հետևաբար, $x_0 \leqslant f(x_0)$ և $f(x_0) \leqslant f(f(x_0))$, այսինքն՝ $f(x_0) \in M$ և $f(x_0) \leqslant x_0$: Այսպիսով, $x_0 = f(x_0)$: Իսկ, եթե $f(d) = d$, որտեղ $d \in [a,b]$, ապա $d \leqslant f(d)$ և $d \in M$: Հետևաբար՝ $d \leqslant \alpha$:

2) Ներքին լրիվ պայմանական կավարաձև կարգավորված բազմության դեպքում դիտարկվում է $M = \{x \in [a,b] \,|\, f(x) \leqslant x\}$ բազմությունը: □

Կասենք, որ $Q(\leqslant)$ մասնակի կարգավորված բազմությունն օժտված է **անշարժ կետի հատկությամբ**, եթե յուրաքանչյուր $\varphi : Q \to Q$ մոնոտոն արտապատկերում ունի անշարժ կետ: Մինչ այժմ չեն բնութագրված բոլոր այն մասնակի կարգավորված բազմությունները, որոնք օժտված են անշարժ կետի հատկությամբ:

***Հետևություն 0.11**: Յուրաքանչյուր լրիվ կավարաձև կարգավորված բազմություն օժտված է անշարժ կետի հատկությամբ:* □

0.6. Հարաբերությունների արտադրյալ և հակադարձ հարաբերություն

$\alpha \subseteq A \times B$ հարաբերության հակադարձ հարաբերություն է կոչվում այն $\alpha^{-1} \subseteq B \times A$ հարաբերությունը, որը սահմանվում է հետևյալ կերպ՝

$$(x, y) \in \alpha^{-1} \longleftrightarrow (y, x) \in \alpha\,,$$

որտեղ $x \in B$, $y \in A$: Հետևաբար, յուրաքանչյուր $\alpha \subseteq A \times B$ հարաբերության համար $\left(\alpha^{-1}\right)^{-1} = \alpha$ և եթե $\alpha \subseteq \beta$, ապա $\alpha^{-1} \subseteq \beta^{-1}$: Եթե α-ի փոխարեն օգտագործվում է «$\leqslant$» նշանը, ապա α^{-1}-ի փոխարեն գրվում է «$\geqslant$» նշանը: Այսպիսով՝

$$x \geqslant y \longleftrightarrow y \leqslant x\,:$$

Ակնհայտ են նաև հետևյալ պնդումները.

1) $\alpha \subseteq A \times A$ հարաբերությունը բավարարում է ռեֆլեքսիվության պայմանին այն և միայն այն դեպքում, եթե $\alpha^{-1} \subseteq A \times A$ հարաբերությունն է բավարարում այդ պայմանին;

2) $\alpha \subseteq A \times A$ հարաբերությունը բավարարում է համաչափության պայմանին այն և միայն այն դեպքում, եթե $\alpha^{-1} \subseteq A \times A$ հարաբերությունն է բավարարում այդ պայմանին;

3) $\alpha \subseteq A \times A$ հարաբերությունը բավարարում է հակահամաչափության պայմանին այն և միայն այն դեպքում, եթե $\alpha^{-1} \subseteq A \times A$ հարաբերությունն է բավարարում այդ պայմանին;

4) $\alpha \subseteq A \times A$ հարաբերությունը բավարարում է փոխանցականության պայմանին այն և միայն այն դեպքում, եթե $\alpha^{-1} \subseteq A \times A$ հարաբերությունն է բավարարում այդ պայմանին;

5) Ցանկացած $\alpha \subseteq A \times A$ հարաբերության համար $\alpha \cap \alpha^{-1}$ հարաբերությունը բավարարում է համաչափության պայմանին;

6) Եթե $\alpha \subseteq A \times A$ հարաբերությունը քվազիկարգ է, ապա $\alpha \cap \alpha^{-1}$ հարաբերությունը կլինի համարժեքության հարաբերություն:

Երկու $\alpha \subseteq A \times B$ և $\beta \subseteq B \times C$ հարաբերությունների **արտադրյալ** (համադրություն, սուպերպոզիցիա) ասելով հասկացվում է այն $\alpha \cdot \beta \subseteq A \times C$ հարաբերությունը, որը որոշվում (սահմանվում) է հետևյալ կերպ՝

$$(x, z) \in \alpha \cdot \beta \longleftrightarrow \exists y \in B, \;\; (x, y) \in \alpha, \;\; (y, z) \in \beta \,,$$

որտեղ $x \in A$, $z \in C$: Տեղի ունեն հետևյալ հավասարությունները (նույնությունները).

$$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma \,,$$

$$(\alpha \cdot \beta)^{-1} = \beta^{-1} \cdot \alpha^{-1} \,,$$

$$(\alpha \cup \beta)^{-1} = \alpha^{-1} \cup \beta^{-1} \,,$$

$$(\alpha \cap \beta)^{-1} = \alpha^{-1} \cap \beta^{-1} \,,$$

$$\alpha(\beta \cup \gamma) = \alpha\beta \cup \alpha\gamma \,,$$

$$(\beta \cup \gamma)\alpha = \beta\alpha \cup \gamma\alpha \,,$$

եթե հավասարության ձախ և աջ մասերը որոշված են: Այս նույնությունները հեշտությամբ բխեցվում են սահմանումներից: Սակայն,

$$\alpha(\beta \cap \gamma) \neq \alpha\beta \cap \alpha\gamma \,,$$

$$(\beta \cap \gamma)\alpha \neq \beta\alpha \cap \gamma\alpha \; :$$

Օրինակ, եթե $\alpha = \{(2,1),(2,2)\} \subseteq \mathbb{N} \times \mathbb{N}$, $\beta = \{(1,2)\} \subseteq \mathbb{N} \times \mathbb{N}$,$\gamma = \{(2,2)\} \subseteq \mathbb{N} \times \mathbb{N}$, ապա $\beta \cap \gamma = \emptyset$, $\alpha(\beta \cap \gamma) = \emptyset$, $\alpha\beta = \{(2,2)\}$, $\alpha\gamma = \{(2,2)\}$, $\alpha\beta \cap \alpha\gamma = \{(2,2)\}$ և, հետևաբար, այս դեպքում,

$$\alpha(\beta \cap \gamma) \neq \alpha\beta \cap \alpha\gamma \; :$$

Եթե $\alpha \subseteq A \times A$, ապա $\alpha \cdot \alpha$ արտադրյալը նշանակվում է α^2-ով, իսկ $\alpha^n = \alpha^{n-1} \cdot \alpha$:

Լեմմ 0.8: *1) Որպեսզի $\alpha \subseteq A \times A$ հարաբերությունը լինի համարժեքության հարաբերություն անհրաժեշտ է և բավարար, որ*

$$\varepsilon_A \subseteq \alpha, \quad \alpha^{-1} = \alpha \quad \textit{և} \quad \alpha^2 = \alpha \,,$$

որտեղ $\varepsilon_A = \{(x, x) \mid x \in A\}$ հարաբերությունը կոչվում է A **բազմության նույնական հարաբերություն***:*

2) Որպեսզի $\alpha \subseteq A \times A$ հարաբերությունը լինի մասնակի կարգ անհրաժեշտ է և բավարար, որ

$$\varepsilon_A \subseteq \alpha, \quad \alpha^{-1} \cap \alpha = \varepsilon_A \quad \text{և} \quad \alpha^2 = \alpha \ :$$

3) Եթե $\alpha \subseteq A \times A$ հարաբերությունը մասնակի կարգ է, ապա $\alpha^{-1} \subseteq A \times A$ հակադարձ հարաբերությունը ևս կլինի մասնակի կարգ: □

Թեորեմ 0.19: *Որպեսզի երկու $\alpha \subseteq A \times A$ և $\beta \subseteq A \times A$ համարժեքության հարաբերությունների $\alpha \cdot \beta \subseteq A \times A$ արտադրյալը լինի համարժեքության հարաբերություն անհրաժեշտ է և բավարար, որ $\alpha \cdot \beta = \beta \cdot \alpha$:*

Ապացուցում: Անհրաժեշտություն: Եթե $\alpha \cdot \beta \subseteq A \times A$ արտադրյալը համարժեքության հարաբերություն է, ապա նախորդ լեմմի համաձայն՝

$$\alpha \cdot \beta = (\alpha \cdot \beta)^{-1} = \beta^{-1} \cdot \alpha^{-1} = \beta \cdot \alpha \ :$$

Բավարարություն: Եթե $\alpha \cdot \beta = \beta \cdot \alpha$, ապա $\alpha \cdot \beta \subseteq A \times A$ արտադրյալը համարժեքության հարաբերություն է, որովհետև

$$\varepsilon_A \subseteq \alpha \cdot \beta,$$

$$(\alpha \cdot \beta)^{-1} = \beta^{-1} \cdot \alpha^{-1} = \beta \cdot \alpha = \alpha \cdot \beta,$$

$$(\alpha \cdot \beta)^2 = (\alpha \cdot \beta) \cdot (\alpha \cdot \beta) = \alpha \cdot (\beta \cdot (\alpha \cdot \beta)) = \alpha \cdot ((\beta \cdot \alpha) \cdot \beta) = \alpha \cdot ((\alpha \cdot \beta) \cdot \beta) =$$

$$= \alpha \cdot (\alpha \cdot (\beta \cdot \beta)) = (\alpha \cdot \alpha) \cdot (\beta \cdot \beta) = \alpha^2 \cdot \beta^2 = \alpha \cdot \beta$$

և մնում է օգտվել նախորդ լեմմից: □

Թեորեմ 0.20: *Եթե $A(\leqslant)$ մասնակի կարգավորված բազմությունը (լրիվ) կավարածև կարգավորված բազմություն է, ապա $A(\geqslant)$ մասնակի կարգավորված բազմությունը ևս կլինի այդպիսին:* □

0.7. Մասնակի կարգավորված բազմությունների իզոմորֆիզմը

Դիցուք $A(\leqslant)$ և $A'(\leqslant)$ զույգերը մասնակի կարգավորված բազմություններ են: $\varphi : A \to A'$ արտապատկերումը կոչվում է **նույնաձնություն** կամ **իզոմորֆիզմ**՝ $A(\leqslant)$ մասնակի կարգավորված բազմությունից $A'(\leqslant)$ մասնակի կարգավորված բազմության մեջ, եթե տեղի ունեն հետևյալ երկու պահանջները.

ա) φ-ն փոխմիարժեք (բիեկտիվ) արտապատկերում է,

բ) $x \leqslant y \longleftrightarrow \varphi(x) \leqslant \varphi(y)$, որտեղ $x, y \in A$:

$A(\leqslant)$ և $A'(\leqslant)$ մասնակի կարգավորված բազմությունները կոչվում են **իզոմորֆ** կամ **նույնաձև** և գրվում է $A \simeq A'$ կամ $A \cong A'$, եթե գոյություն ունի որևէ $\varphi : A \to A'$ նույնաձևություն (իզոմորֆիզմ): Սահմանված «$\simeq$» (կամ «$\cong$») հարաբերությունը կոչվում է մասնակի կարգավորված բազմությունների **նույնաձևության** կամ **իզոմորֆության հարաբերություն**: Նույնաձևության (իզոմորֆիզմի) սահմանման մեջ φ-ի ինյեկտիվությունը բխում է մնացած պայմաններից: Իրոք, եթե $\varphi x = \varphi y$, ապա ռեֆլեքսիվության համաձայն՝ $\varphi x \leqslant \varphi y$ և $\varphi y \leqslant \varphi x$, հետևաբար, $x \leqslant y$ և $y \leqslant x$, այսինքն՝ $x = y$:

Լեմմ 0.9: *Մասնակի կարգավորված բազմությունների նույնաձևության «$\simeq$» հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $A \simeq A$,

բ) $A \simeq A' \longrightarrow A' \simeq A$,

գ) $A \simeq A'$, $A' \simeq A'' \longrightarrow A \simeq A''$:

Ապացուցում: ա) հատկությունը հաստատվում է $\varphi = \varepsilon_A$ արտապատկերման միջոցով, որտեղ ε_A-ն A բազմության նույնական արտապատկերումն է, այսինքն՝ $\varepsilon_A(x) = x$ ցանկացած $x \in A$ տարրի համար: Ապացուցենք բ)-ն: Դիցուք $\varphi : A \to A'$ փոխմիարժեք (բիեկտիվ) արտապատկերումն այնպիսին է, որ

$$x \leqslant y \longleftrightarrow \varphi(x) \leqslant \varphi(y) \ :$$

Պահանջվում է ապացուցել, որ $u \leqslant v \longleftrightarrow \varphi^{-1}(u) \leqslant \varphi^{-1}(v)$, որտեղ $u, v \in A'$: Կունենանք՝

$$\varphi^{-1}(u) \leqslant \varphi^{-1}(v) \longleftrightarrow \varphi\left(\varphi^{-1}(u)\right) \leqslant \varphi\left(\varphi^{-1}(v)\right) \longleftrightarrow$$

$$\left(\varphi^{-1} \cdot \varphi\right) u \leqslant \left(\varphi^{-1} \cdot \varphi\right) v \longleftrightarrow \varepsilon_B(u) \leqslant \varepsilon_B(v) \longleftrightarrow u \leqslant v \ :$$

Այսպիսով,

$$u \leqslant v \longleftrightarrow \varphi^{-1}(u) \leqslant \varphi^{-1}(v)\,,$$

որտեղ $\varphi^{-1} : B \to A$ արտապատկերումը՝ լինելով $\varphi : A \to B$ փոխմիարժեք արտապատկերման հակադարձ արտապատկերումը, նս փոխմիարժեք արտապատկերում է:

Ապացուցենք փոխանցականության գ) պայմանը: Եթե $A \simeq A'$ և $A' \simeq A''$, ապա գոյություն ունեն այնպիսի $\varphi_1 : A \to A'$ և $\varphi_2 : A' \to A''$ փոխմիարժեք արտապատկերումներ, որ

$$x \leqslant y \longleftrightarrow \varphi_1(x) \leqslant \varphi_1(y)\,,$$

$$u \leqslant v \longleftrightarrow \varphi_2(u) \leqslant \varphi_2(v)\,,$$

որտեղ $x, y \in A$, իսկ $u, v \in A'$: Հետևաբար, $\varphi_1 \cdot \varphi_2 : A \to A''$ փոխմիարժեք արտապատկերման համար կունենանք՝

$$(\varphi_1 \cdot \varphi_2)\, x \leqslant (\varphi_1 \cdot \varphi_2)\, y \longleftrightarrow \varphi_2\,(\varphi_1(x)) \leqslant$$

$$\leqslant \varphi_2\,(\varphi_1(y)) \longleftrightarrow \varphi_1(x) \leqslant \varphi_1(y) \longleftrightarrow x \leqslant y\ : \qquad \square$$

Օրինակ, Եթե X և Y բազմությունները հավասարազոր են, այսինքն՝ $X \sim Y$, ապա $2^X \simeq 2^Y$, որտեղ 2^X-ը դիտվում է որպես մասնակի կարգավորված բազմություն՝ «$\subseteq$» տեսա-բազմային ներդրման նկատմամբ: Իրոք, եթե գոյություն ունի որևէ $f : X \to Y$ փոխմիարժեք (բիեկտիվ) արտապատկերում, ապա սահմանելով

$$\varphi(U) = f(U), \qquad \emptyset \neq U \subseteq X\,, \qquad \varphi(\emptyset) = \emptyset\,,$$

կստանանք այնպիսի $\varphi : 2^X \to 2^Y$ փոխմիարժեք արտապատկերում, որի դեպքում՝

$$U_1 \subseteq U_2 \longleftrightarrow \varphi(U_1) \subseteq \varphi(U_2)\,, \qquad U_1, U_2 \in 2^X\ :$$

Ակնհայտ է նաև, որ $2^{fin(X)} \simeq 2^{fin(Y)}$, եթե $X \sim Y$ (հիշեցնենք, որ 2^X -ը X բազմության բոլոր ենթաբազմությունների բազմությունն է, իսկ $2^{fin(X)}$-ը X-ի բոլոր վերջավոր ենթաբազմությունների բազմությունն է): Ճիշտ է նաև հակառակը. եթե $2^X \simeq 2^Y$, ապա $X \sim Y$:

Եթե $A(\leqslant)$ զույգը մասնակի կարգավորված բազմություն է և $A' \subseteq A$, $A' \neq \emptyset$, ապա $A'(\leqslant)$ զույգը ևս կլինի մասնակի կարգավորված բազմություն, այսինքն՝ A'-ը մասնակի կարգավորված բազմություն է՝ նույն «$\leqslant$» մասնակի կարգի նկատմամբ: Կասենք, որ $A(\leqslant)$ մասնակի կարգավորված բազմությունը **ներդրվում է** $C(\leqslant)$ մասնակի կարգավորված բազմության մեջ, եթե գոյություն ունի այնպիսի $B \subseteq C$, $B \neq \emptyset$, ենթաբազմություն, որ $A \simeq B$, այսինքն՝ եթե գոյություն ունի այնպիսի $\varphi : A \to C$ ինյեկտիվ (ներդրող) արտապատկերում, որ

$x \leqslant y \longleftrightarrow \varphi x \leqslant \varphi y$: Այդպիսի $\varphi : A \to C$ արտապատկերումը կոչվում է **ներդրում**: Եթե այդ դեպքում նաև $\varphi(\inf X) = \inf \varphi(X)$ (կամ $\varphi(\sup X) = \sup \varphi(X)$) ցանկացած $\emptyset \neq X \subseteq A$ ենթաբազմության համար, երբ $\inf X$-ը (կամ $\sup X$-ը) գոյություն ունի, ապա կասենք, որ A-ն ներդրվում է C-ի մեջ այնպես, որ պահպանվում են A-ի ենթաբազմությունների ստորին (կամ վերին) ճշգրիտ եզրերը:

Թեորեմ 0.21 (Քելի): *Յուրաքանչյուր $A(\leqslant)$ մասնակի կարգավորված բազմություն ներդրվում է A բազմության բոլոր ենթաբազմությունների $2^A(\subseteq)$ մասնակի կարգավորված բազմության մեջ:*

Ապացուցում: $a \in A$ տարրի համապատասխան սահմանենք $J_a = \{x \in A \mid x \leqslant a\} \subseteq A$ ենթաբազմությունը և նկատենք, որ $J_a \neq \emptyset$ ցանկացած $a \in A$ տարրի դեպքում, որովհետև $a \leqslant a$, համաձայն մասնակի կարգի ռեֆլեքսիվության պայմանի: Նշանակենք՝ $B = \{J_a \mid a \in A\} \subseteq 2^A$ և ապացուցենք, որ $A \simeq B$: Սահմանենք $\varphi : A \to B$ արտապատկերումը հետևյալ կերպ՝

$$\varphi(a) = J_a, \qquad a \in A \ :$$

Ակնհայտ է, որ φ-ն սյուրեկտիվ է, ապացուցենք φ-ի ինյեկտիվությունը.

$$\varphi(a) = \varphi(b) \longrightarrow J_a = J_b \longrightarrow a \leqslant b, \ b \leqslant a \longrightarrow a = b \ :$$

Այսպիսով, φ-ն փոխմիարժեք (բիեկտիվ) է և մնում է ստուգել φ-ի իզոմորֆության պայմանը.

$$a \leqslant b \longleftrightarrow J_a \subseteq J_b \longleftrightarrow \varphi(a) \subseteq \varphi(b) \ : \qquad \square$$

Կառուցված $\varphi : A \to 2^A$ ներդրումը կոչվում է **Քելիի ներդրում** (A. Cayley):

Թեորեմ 0.22: *Յուրաքանչյուր $A(\leqslant)$ մասնակի կարգավորված բազմություն (մասնավորապես, յուրաքանչյուր կավարածն կարգավորված բազմություն) ներդրվում է $2^A(\subseteq)$ մասնակի կարգավորված բազմության մեջ այնպես, որ պահպանվում են A-ի ենթաբազմությունների ստորին ճշգրիտ եզրերը:*

Ապացուցում: Բավական է նախորդ թեորեմի ապացույցին ավելացնել հետևյալը: Եթե $\emptyset \neq X \subseteq A$, $X = \{x_i \mid i \in I\}$ և $\inf X$-ը գոյություն ունի, ապա նախորդ թեորեմում կառուցված $\varphi : A \to 2^A$ Քելիի ներդրման համար կունենանք՝

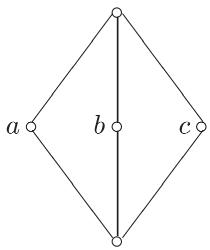
$$z \in \varphi\,(\inf\{x_i \,|\, i \in I\}) \longleftrightarrow z \in J_{\inf\{x_i \,|\, i \in I\}} \longleftrightarrow$$

$$z \leqslant \inf\{x_i \,|\, i \in I\} \longleftrightarrow z \leqslant x_i\,,\ \forall i \in I \longleftrightarrow z \in J_{x_i},\ \forall i \in I \longleftrightarrow$$

$$z \in \bigcap_{i \in I} J_{x_i} \longleftrightarrow z \in \bigcap_{i \in I} \varphi(x_i) \longleftrightarrow z \in \inf \varphi(X)\,,$$

որտեղ $\varphi(X) = \{\varphi(x_i) \mid\ i \in I\}$, իսկ $\varphi(x_i) = J_{x_i}$, $x_i \in X$: $\square$

Սակայն գոյություն ունի կավարաձև կարգավորված բազմություն, որը չի ներդրվում $2^A(\subseteq)$ տեսքի որևէ կավարաձև կարգավորված բազմության մեջ այնպես, որ պահպանվեն նրա ենթաբազմությունների ինչպես ստորին, այնպես էլ վերին ճշգրիտ եզրերը: Օրինակ, այդպիսին է հետևյալ հինգ տարրանի կավարաձև կարգավորված բազմությունը՝



,

որը երեք տարրանի $X = \{1, 2, 3\}$ բազմության բոլոր տրոհումների (կամ համարժեքությունների) մասնակի կարգավորված բազմությունն է՝ տեսա-բազմային ներդրման նկատմամբ: Պատճառն այն է, որ այստեղ՝

$$\inf\{a, \sup\{b, c\}\} \neq \sup\{\inf\{a, b\}, \inf\{a, c\}\}\ :$$

0.8. Տոպոլոգիա, տոպոլոգիական տարածություն

Դիցուք A-ն կամայական ոչ դատարկ բազմություն է, իսկ 2^A-ը կամ $pow(A)$-ն A-ի բոլոր ենթաբազմությունների բազմությունն է: $\tau \subseteq pow(A)$ ենթաբազմությունը կոչվում է A-ի (վրա որոշված) **տոպոլոգիա**, եթե այն բավարարում է հետևյալ երեք պայմաններին (որոնք կոչվում են տոպոլոգիայի աքսիոմներ).

ա) $A \in \tau$ և $\emptyset \in \tau$;

բ) τ-ի մեջ մտնող կամայական քանակի ենթաբազմությունների միավորումը նույնպես պատկանում է τ-ին;

գ) τ-ի մեջ մտնող վերջավոր թվով ենթաբազմությունների հատումը ևս պատկանում է τ-ին:

Այս դեպքում, $(A;\tau)$ զույգը կոչվում է **տոպոլոգիական տարածություն**, իսկ τ-ի տարրերը այդ տոպոլոգիական տարածության **բաց բազմություններ**: Հաճախ $(A;\tau)$ զույգը համառոտ նշանակվում է A-ով: Եթե $X \subseteq A$ ենթաբազմությունը բաց է A-ում, ապա $Y = A \setminus X$ լրացումը կոչվում է **փակ** A-ում, այսինքն՝ $Y \subseteq A$ ենթաբազմությունը կոչվում է փակ A-ում, եթե $A \setminus Y$ լրացումը բաց է A-ում: Հետևաբար, փակ բազմությունների համար տեղի ունեն հետևյալ երեք հատկությունները.

ա′) A և $\emptyset$ բազմությունները փակ են A-ում;

բ′) Կամայական քանակի փակ բազմությունների հատումը նորից փակ բազմություն է;

գ′) Վերջավոր թվով փակ բազմությունների միավորումը նորից փակ բազմություն է:

Իրոք, ա′) հատկությունը բխում է փակ բազմության սահմանումից, իսկ բ′) և գ′) հատկությունները բխում են բ) և գ) պայմաններից և

$$\bigcap_{i\in I}(A \setminus X_i) = A \setminus \bigcup_{i\in I} X_i,$$

$$\bigcup_{i\in J}(A \setminus X_i) = A \setminus \bigcap_{i\in J} X_i$$

նույնություններից (օրենքներից):

Օրինակներ: 1. Դիցուք A-ն կամայական բազմություն է, իսկ τ-ն կազմված է A-ի բոլոր ենթաբազմություններից: Այդ դեպքում, τ-ն կլինի տոպոլոգիա, որը կոչվում է A-ի **դիսկրետ տոպոլոգիա**, իսկ (A,τ) զույգը՝ **դիսկրետ տոպոլոգիական տարածություն**:
2. Եթե $\tau = \{A, \emptyset\}$, ապա τ-ն կլինի տոպոլոգիա, որը կոչվում է A-ի armb հակադիսկրետ տոպոլոգիա, իսկ (A,τ) զույգը՝ **հակադիսկրետ տոպոլոգիական տարածություն**:

3. Դիցուք $A = \{a, b\}$, իսկ $\tau = \{\emptyset, A, \{a\}\}$: Այդ դեպքում, τ-ն կլինի տոպոլոգիա, իսկ (A, τ) զույգը՝ տոպոլոգիական տարածություն:

Դիցուք A-ն տոպոլոգիական տարածություն է, իսկ $x \in A$: $U \subseteq A$ ենթաբազմությունը կոչվում է x-ի շրջակայք, եթե գոյություն ունի այնպիսի X բաց բազմություն, որ $x \in X \subseteq U$: $U \subseteq A$ ենթաբազմությունը կոչվում է $V \subseteq A$ ենթաբազմության շրջակայք, եթե գոյություն ունի այնպիսի X բաց բազմություն, որ $V \subseteq X \subseteq U$: $X \subseteq A$ ենթաբազմությունը կլինի բաց A-ում այն և միայն այն դեպքում, երբ X-ը իր յուրաքանչյուր տարրի շրջակայքն է: $x \in A$ տարրի որոշ քանակի շրջակայքերի β_x բազմությունը կոչվում է x-ի շրջակայքերի **հենք** (բազա), եթե x-ի յուրաքանչյուր շրջակայք պարունակում է β_x-ին պատկանող x-ի որևէ շրջակայք: Բաց բազմությունների β համախումբը կոչվում է տրված տոպոլոգիայի (կամ տոպոլոգիական տարածության) հենք, եթե յուրաքանչյուր ոչ դատարկ բաց բազմություն հանդիսանում է β-ին պատկանող որոշ քանակի բաց բազմությունների միավորում:

$x_0 \in A$ տարրը կոչվում է

$$x_1, x_2, \ldots, x_n, \ldots$$

հաջորդականության $(x_n \in A)$ սահման և գրվում է $x_0 = \lim\limits_{n\to\infty} x_n$ կամ $x_n \to x_0$, եթե x_0-ի յուրաքանչյուր U_0 շրջակայք պարունակում է հաջորդականության բոլոր անդամները՝ սկսած որևէ տեղից, այսինքն՝ գոյություն ունի այնպիսի n_0 համար, որ $x_n \in U_0$, եթե $n \geqslant n_0$: Այստեղ n_0 թիվը կախված է U_0 շրջակայքի ընտրությունից:

Ի տարբերություն սովորական թվային հաջորդականության սահմանի գաղափարի, երբ (գոյության դեպքում) հաջորդականության սահմանը որոշվում է միարժեքորեն, ընդհանուր դեպքում, այսինքն՝ կամայական տոպոլոգիական տարածություններում, սահմանը (գոյության դեպքում) միարժեքորեն չի որոշվում: Օրինակ, հակադիսկրետ տոպոլոգիական տարածության յուրաքանչյուր տարր հանդիսանում է իր (տարրերից կազմված) յուրաքանչյուր հաջորդականության սահման:

A տոպոլոգիական տարածությունը կոչվում է **Հաուսդորֆյան** կամ T_2-տարածություն, եթե դրա կամայական միմյանցից տարբեր $x_1, x_2 \in A$ տարրերի համար գոյություն ունեն այնպիսի $U_1 \ni x_1$ և $U_2 \ni x_2$ շրջակայքեր, որ $U_1 \cap U_2 = \emptyset$, այսինքն՝ $x_1 \neq x_2$ տարրերը օժտված են միմյանց հետ չհատվող շրջակայքերով: Ակնհայտ է, որ

Հաուսդորֆյան տարածության (տարրերից կազմված) յուրաքանչյուր հաջորդականության սահմանը որոշվում է միարժեքորեն (եթե այն գոյություն ունի):

Եթե $\lim\limits_{n\to\infty} x_n = x_0$ և $x_0 \neq x_n$, $n \in \mathbb{N}$, ապա դիտարկվող տոպոլոգիական տարածության տոպոլոգիան դիսկրետ չէ, որովհետև դիսկրետ տոպոլոգիական տարածության $\{x_0\}$ բաց բազմությունը (շրջակայքը) չի պարունակում x_n հաջորդականության որևէ տարր:

Շատ հաճախ կիրառվում է տոպոլոգիայի տրման հետևյալ եղանակը:

Թեորեմ 0.23: *Դիցուք $A \neq \emptyset$ բազմության յուրաքանչյուր $x \in A$ տարրին համապատասխանության մեջ է դրված A-ի ենթաբազմությունների այնպիսի $\mathcal{O}_x$ բազմություն, որն օժտված է հետևյալ 3 հատկություններով.*

ա) x-ը պատկանում է $\mathcal{O}_x$-ին պատկանող յուրաքանչյուր ենթաբազմությանը;

բ) Եթե $U, V \in \mathcal{O}_x$, ապա գոյություն ունի այնպիսի $W \in \mathcal{O}_x$, որ $W \subseteq U \cap V$;

գ) Եթե $U \in \mathcal{O}_x$ և $y \in U$, ապա գոյություն ունի $V \in \mathcal{O}_y$ այնպիսին, որ $V \subseteq U$:

Այդ դեպքում, եթե τ-ով նշանակենք այն բազմությունը, որը կազմված է A-ի դատարկ ենթաբազմությունից և բոլոր այն $X \subseteq A$ ենթաբազմություններից, որոնց յուրաքանչյուր $x \in X$ տարրի համար գոյություն ունի այնպիսի $U_x \in \mathcal{O}_x$, որ $U_x \subseteq X$, ապա τ-ն կլինի տոպոլոգիա, որի համար $\mathcal{O}_x$-ը կլինի x-ի շրջակայքերի հենք՝ կազմված բաց բազմություններից, իսկ $\beta = \bigcup\limits_{x\in A} \mathcal{O}_x$-ը՝ τ տոպոլոգիայի հենք:

Ապացուցում: Ակնհայտ է, որ $A \in \tau$: Դիցուք $X_1, X_2 \in \tau$ և $x \in X_1 \cap X_2$, այսինքն՝ $x \in X_1$ և $x \in X_2$: Հետևաբար, գոյություն կունենան այնպիսի $U_x^1 \in \mathcal{O}_x$ և $U_x^2 \in \mathcal{O}_x$, որ $U_x^1 \subseteq X_1$, իսկ $U_x^2 \subseteq X_2$: բ) պայմանի համաձայն գոյություն կունենա այնպիսի $W \in \mathcal{O}_x$, որ $W \subseteq U_x^1 \cap U_x^2 \subseteq X_1 \cap X_2$: Ուստի՝ $X_1 \cap X_2 \in \tau$:

Դիցուք $X = \bigcup\limits_{i\in I} X_i$, որտեղ $X_i \in \tau$ և $x \in X$, այսինքն՝ $x \in X_{i_0}$, որևէ $i_0 \in I$ նշիչի համար: Հետևաբար գոյություն կունենա այնպիսի

$U_x \in \mathcal{O}_x$, որ $U_x \subseteq X_{i_0} \subseteq X$: Ուստի՝ $X \in \tau$: Այսպիսով τ-ն բավարարում է տոպոլոգիայի սահմանման երեք պայմաններին: գ) պայմանից բխում է, որ $\mathcal{O}_x \subseteq \tau$ բոլոր $x \in A$ տարրերի համար: Դիցուք W-ն x-ի կամայական շրջակայք է՝ τ տոպոլոգիայում, այսինքն՝ գոյություն ունի այնպիսի $X \in \tau$, որ $x \in X \subseteq W$: Համաձայն τ-ի սահմանման, գոյություն կունենա այնպիսի $U_x \in \mathcal{O}_x$, որ $U_x \subseteq X$ և $x \in U_x \subseteq W$: Հետևաբար, կառուցված τ տոպոլոգիայում $\mathcal{O}_x$ բազմությունը կլինի x-ի շրջակայքերի հենք: Ակնհայտ է նաև, որ $\beta = \bigcup\limits_{x\in A} \mathcal{O}_x$ բազմությունը սահմանված τ տոպոլոգիայի համար հենք է, որովհետև յուրաքանչյուր $X \in \tau$ բաց բազմության ցանկացած $x \in X$ տարրի համար գոյություն ունի այնպիսի $U_x \in \mathcal{O}_x$ բաց բազմություն, որ $x \in U_x \subseteq X$: Հետևաբար՝

$$X = \bigcup_{x\in X} U_x \; : \qquad \square$$

Տոպոլոգիական տարածությունը կոչվում է T_1-տարածություն, եթե նրա կամայական միմյանցից տարբեր երկու տարրերից գոնե մեկն օժտված է մյուս տարրը չպարունակող որևէ շրջակայքով: Հետևաբար, յուրաքանչյուր T_2-տարածություն հանդիսանում է T_1-տարածություն:

A տոպոլոգիական տարածությունը կոչվում է T_3-տարածություն, եթե նրա ցանկացած $Y \subseteq A$ փակ բազմություն և դրանից դուրս գտնվող ցանկացած $x \in A$ տարր օժտված են չհատվող շրջակայքերով: Ընդհանուր դեպքում, T_3-տարածությունը չի հանդիսանում T_1-տարածություն: T_1-տարածությունը կոչվում է **ռեգուլյար**, եթե այն նաև T_3-տարածություն է:

Թեորեմ 0.24 (ռեգուլյարության հայտանիշը)*: Որպեսզի T_1-տարածությունը լինի ռեգուլյար անհրաժեշտ է և բավարար, որ նրա յուրաքանչյուր x տարրի համար գոյություն ունենա փակ բազմություններից կազմված x-ի շրջակայքերի հենք:* $\square$

Տոպոլոգիական տարածությունը կոչվում է T_4-տարածություն, եթե դրա ցանկացած երկու չհատվող փակ բազմություններ օժտված են (ունեն) չհատվող բաց շրջակայքերով: Ընդհանուր դեպքում, T_4-տարածությունը չի հանդիսանում T_1-տարածություն:

T_1-տարածությունը կոչվում է **նորմալ տարածություն**, եթե այն նաև T_4-տարածություն է: Յուրաքանչյուր նորմալ տարածություն ռեգուլյար է, իսկ յուրաքանչյուր ռեգուլյար տարածություն Հաուսդորֆյան է:

Թեորեմ 0.25 (Ա. Ն. Տիխոնով)*: Վերջավոր կամ հաշվելի հենքով օժտված յուրաքանչյուր ռեգուլյար տարածություն նորմալ տարածություն է:* □

Դիցուք A-ն կամայական ոչ դատարկ բազմություն է, իսկ $\mathbb{R}$-ը՝ բոլոր իրական թվերի բազմությունն է: $\rho : A \times A \to \mathbb{R}$ արտապատկերումը կոչվում է **մետրիկա**՝ որոշված A բազմության վրա, եթե այն բավարարում է հետևյալ պայմաններին (մետրիկայի աքսիոմներին).

M_1) $\rho(x,y) \geqslant 0$ բոլոր $x, y \in A$ տարրերի համար և $\rho(x,y) = 0 \longleftrightarrow x = y$;

M_2) $\rho(x,y) = \rho(y,x)$ բոլոր $x, y \in A$ տարրերի համար;

M_3) $\rho(x,y) \leqslant \rho(x,z) + \rho(z,y)$ բոլոր $x, y, z \in A$ տարրերի համար:

$(A;\rho)$ զույգը կոչվում է **մետրիկական տարածություն**, եթե ρ-ն մետրիկա է՝ որոշված A-ի վրա: Այդ դեպքում, A բազմության տարրերը կոչվում են կետեր, իսկ $\rho(x,y)$ ոչ բացասական թիվը՝ x, y կետերի հեռավորություն:

Օրինակ, եթե $A = \mathbb{R}$, $\rho(x,y) = |x - y|$, ապա $(A;\rho)$ զույգը մետրիկական տարածություն է:

Դիցուք $(A;\rho)$-ն մետրիկական տարածություն է; τ_ρ-ով նշանակենք բոլոր այն $U \subseteq A$ ենթաբազմությունների բազմությունը, որոնց համար տեղի ունի հետևյալ պայմանը. ցանկացած $a \in U$ տարրի համար գոյություն ունի այնպիսի $\varepsilon > 0$ իրական թիվ, որ $\{x \in A \mid \rho(x,a) < \varepsilon\} \subseteq U$: Հեշտությամբ ստուգվում է, որ τ_ρ-ն տոպոլոգիա է՝ որոշված A բազմության վրա, որը կոչվում է ρ մետրիկայով որոշված (ծնված) տոպոլոգիա:

$(A;\tau)$ տոպոլոգիական տարածությունը կոչվում է **մետրիկացվող** (կամ մետրիզացված), եթե գոյություն ունի A բազմության վրա որոշված այնպիսի ρ մետրիկա, որ $\tau = \tau_\rho$:

Թեորեմ 0.26 (Ուրըսոն)*: Որպեսզի վերջավոր կամ հաշվելի հենքով օժտված տոպոլոգիական տարածությունը լինի մետրիկացվող անհրաժեշտ է և բավարար, որ այն լինի նորմալ*[2]*:* □

[2]Թեորեմներ 0.24, 0.25, 0.26-ի ապացուցումները կարելի է գտնել տոպոլոգիայի վերաբերյալ ցանկացած ձեռնարկում (տես, օրինակ, Дж. Келли, *Общая топология*, М., 1968):

Ենթաբազմությունների $S = \{A_i \subseteq A|\ i \in I\}$ դասը կոչվում է $(A;\tau)$ տոպոլոգիական տարածության **ծածկույթ**, եթե $\bigcup\limits_{i\in I} A_i = A$: Եթե S ծածկույթի յուրաքանչյուր A_i տարր բաց (փակ) բազմություն է, ապա S-ը կոչվում է **բաց (փակ)** ծածկույթ:

$T \subseteq S$ ենթահամակարգը կոչվում է S ծածկույթի **ենթածածկույթ**, եթե T-ն նույնպես $(A;\tau)$ տոպոլոգիական տարածության ծածկույթ է:

Տոպոլոգիական տարածությունը կոչվում է **կոմպակտ տարածություն**, եթե նրա կամայական բաց ծածկույթից կարելի է առանձնացնել վերջավոր ենթածածկույթ:

Դիցուք $(A;\tau)$-ն կամայական տոպոլոգիական տարածություն է, իսկ $B \subseteq A$ ենթատարածությունը դատարկ չէ: Հեշտությամբ ստուգվում է, որ

$$\tau_B = \{B \cap U \mid U \in \tau\}$$

բազմությունը հանդիսանում է B-ի տոպոլոգիա: $(B;\tau_B)$ տոպոլոգիական տարածությունը կոչվում է $(A;\tau)$-ի ենթատարածություն: Այս ձևով, տոպոլոգիական տարածության յուրաքանչյուր ոչ դատարկ ենթաբազմություն կարելի է դիտել որպես տոպոլոգիական տարածություն:

Հատկություն 0.12: *Կոմպակտ տոպոլոգիական տարածության յուրաքանչյուր փակ ենթաբազմություն ևս կոմպակտ տոպոլոգիական տարածություն է:* □

Դիցուք $(A;\tau)$-ն կամայական տոպոլոգիական տարածություն է: τ-ով ծնված σ-հանրահաշիվը կոչվում է $(A;\tau)$ տոպոլոգիական տարածության **բորելյան հանրահաշիվ**, իսկ դրա տարրերը կոչվում են տոպոլոգիական տարածության **բորելյան բազմություններ**:

Դիցուք A-ն և B-ն կամայական երկու տոպոլոգիական տարածություններ են: $f : A \to B$ արտապատկերումը կոչվում է **անընդհատ** $x_0 \in A$ **կետում**, եթե $y_0 = f(x_0)$ պատկերի ցանկացած V շրջակայքի համար գոյություն ունի x_0 կետի այնպիսի U շրջակայք, որ $f(U) \subseteq V$, որտեղ $f(U) = \{f(x)|\ x \in U\}$: $f : A \to B$ արտապատկերումը կոչվում է **անընդհատ**, եթե այն անընդհատ է ցանկացած $x \in A$ կետում: Որպեսզի $f : A \to B$ արտապատկերումը լինի անընդհատ անհրաժեշտ է և բավարար, որ $f^{-1}(V) \subseteq A$ ենթաբազմությունը լինի A-ի բաց բազմություն՝ ցանկացած $V \subseteq B$ բաց բազմության համար, որտեղ $f^{-1}(V) = \{x \in A \mid f(x) \in V\}$:

0.9. Ոչ հստակ (fuzzy) ենթաբազմություններ

Սկսենք իրական թվերի $[0,1]$ հատվածի հետևյալ հանրահաշվական հատկություններից, որոնց մեծ մասը (բացառությամբ վերջին 10) և 11) հատկությունների) համընկնում է $\{0,1\}$ բազմության համապատասխան հատկությունների հետ: Կամայական $x, y \in [0,1]$ տարրերի համար սահմանելով՝

$$x \wedge y = \min\{x, y\}\,,$$

$$x \vee y = \max\{x, y\}\,,$$

$$\overline{x} = 1 - x\,,$$

կստանանք՝

1) $x \wedge y = y \wedge x$, $x \vee y = y \vee x$, (տեղափոխական օրենքներ)

2) $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \vee y) \vee z = x \vee (y \vee z)$, (զուգորդական օրենքներ)

3) $x \wedge x = x$, $x \vee x = x$, (ինքնահամընկնման օրենքներ)

4) $x \wedge (x \vee y) = x$, $x \vee (x \wedge y) = x$, (կլանման օրենքներ)

5) $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$, (բաշխական օրենքներ)

6) $x \vee 0 = x$, $x \wedge 1 = x$, (միավորի գոյության օրենքներ)

7) $\overline{(\overline{x})} = x$, (ինքնամփոփության օրենք)

8) $\overline{x \wedge y} = \overline{x} \vee \overline{y}$, $\overline{x \vee y} = \overline{x} \wedge \overline{y}$, (Դե Մորգանի օրենքներ)

9) $x \wedge \overline{x} \leqslant y \vee \overline{y} \longleftrightarrow (x \wedge \overline{x}) \vee (y \vee \overline{y}) = y \vee \overline{y}$, (Քլինիի անհավասարություն)

10) $\overline{\dfrac{1}{2}} = \dfrac{1}{2}$, (անշարժ կետի գոյության օրենք)

11) $(x \vee \overline{x}) \vee \dfrac{1}{2} = x \vee \overline{x}$: (Քլինիի նույնություն)

1)–8) պայմաններին բավարարող բազմությունները կոչվում են **Դե Մորգանի հանրահաշիվներ**: 1)–9) պայմաններին բավարարող բազմությունները կոչվում են **Քլինիի** (S.C. Kleene) **հանրահաշիվներ**, իսկ 1)–11) պայմաններին բավարարող բազմությունները կոչվում են **համաձայնեցված անշարժ կետով Քլինիի հանրահաշիվներ**: Վերջին 10-րդ և 11-րդ օրենքները, այդ դեպքում, ընթերցվում են հետևյալ կերպ. գոյություն ունի այնպիսի a տարր, որ

$$\overline{a} = a\,, \qquad \text{(անշարժ կետի գոյության օրենք)}$$

$$(x \vee \overline{x}) \vee a = x \vee \overline{x} \text{ : (Քլինիի նույնություն)}$$

Այսպիսով, իրական թվերի $[0,1]$ հատվածը կազմում է համաձայնեցված անշարժ կետով Քլինիի հանրահաշիվ (սահմանված գործողությունների նկատմամբ):

A բազմության կամայական $\Theta \subseteq A$ ենթաբազմությանը համապատասխան սովորաբար սահմանվում է $f_A^{\Theta} : A \to \{0,1\}$ ֆունկցիան՝

$$f_A^{\Theta}(x) = \begin{cases} 1, & \text{եթե } x \in \Theta, \\ 0, & \text{եթե } x \in A \setminus \Theta, \end{cases}$$

որը կոչվում է $\Theta \subseteq A$ ենթաբազմության **բնութագրիչ** կամ **պատկանելիության** ֆունկցիա: f_A^{Θ} բնութագրիչ ֆունկցիայով միարժեքորեն վերականգնվում է $\Theta \subseteq A$ ենթաբազմությունը: Հետևաբար, տալ $\Theta \subseteq A$ ենթաբազմությունը նշանակում է տալ համապատասխան f_A^{Θ} բնութագրիչ ֆունկցիան կամ որ նույնն է՝ $\{(x, f_A^{\Theta}(x)) \mid x \in A\}$ բազմությունը, որը կոչվում է f_A^{θ} ֆունկցիայի գրաֆիկ: Ուստի, A բազմության ենթաբազմություն ասելով կարելի է հասկանալ նաև $f : A \to \{0,1\}$ տեսքի ցանկացած ֆունկցիա:

Սակայն երբեմն բազմության կառուցվածքը (կազմը) հստակորեն չի որոշվում: Օրինակ, ո՞րն է լսարանում գտնվող այն ուսանողների բազմությունը, ովքեր հասկանում են դասախոսությունը, կամ ո՞րն է Հայաստանի գեղեցիկ ծաղիկների բազմությունը[3]: Այսպիսի դեպքերում միայն կարելի է խոսել նկարագրվող ենթաբազմությանը տրված բազմության տարրի պատկանելիության աստիճանի (չափի) մասին: Այսպիսի «ենթաբազմությունները» կոչվում են ոչ հստակ ենթաբազմություններ, ի տարբերություն սովորական ենթաբազմությունների, որոնց կարելի է նաև անվանել հստակ ենթաբազմություններ, երբ հստակորեն որոշվում է դրա կառուցվածքը (կազմը), այսինքն՝ հստակորեն կարելի է ասել (պնդել) պատկանում է թե ոչ դիտարկվող ենթաբազմությանը տրված A բազմության կամայական x տարրը:

Դասական մաթեմատիկան կառուցված է և զարգանում է հստակ բազմությունների տեսության հիման վրա: Սակայն կոմպյուտերային գիտության զարգացման հետ մեկտեղ, ակտիվորեն զարգանում է նաև ոչ հստակ (fuzzy) բազմությունների տեսությունը, իսկ վերջինիս հիման վրա նաև բազմաթիվ ուղղություններ: Տես, օրինակ, John Yen and

[3]Այդպիսին է նաև բոլոր բազմությունների բազմությունը (Ռասսել, Կանտոր):

Reza Langari *Fuzzy Logic: intelligence, control and information*, 1999 by Prentice-Hall, Inc., Upper Saddle River, New Jersey.

Անցնենք ճշգրիտ սահմանումների:

Դիցուք A-ն կամայական ոչ դատարկ բազմություն է: Յուրաքանչյուր $f_A : A \to [0,1]$ արտապատկերում (ֆունկցիա) կոչվում է A բազմության **ոչ հստակ ենթաբազմություն**: Երբեմն f_A ֆունկցիայի փոխարեն դրա $\{(x, f_A(x)) \mid x \in A\}$ գրաֆիկն է կոչվում A բազմության ոչ հստակ ենթաբազմություն: Ոչ հստակ ենթաբազմության գաղափարը ուսումնասիրվում է սկսած 1965 թ.:

(Իրական թվերի $[0,1]$ հատվածի փոխարեն վերցնելով ավելի ընդհանուր կառուցվածք ունեցող բազմություն (օրինակ, բաշխական կավար, Դե Մորգանի հանրահաշիվ (տես 20.3-ը), կամ մասնակի կարգավորված բազմություն), հանգում ենք ոչ հստակ ենթաբազմության ավելի ընդհանուր գաղափարի:)

Եթե $f_A(x) \in \{0,1\}$, ապա f_A-ն կհամընկնի A-ի որևէ սովորական ենթաբազմության բնութագրիչ ֆունկցիայի հետ: Հետևաբար, A բազմության սովորական ենթաբազմության գաղափարը կարելի է դիտել որպես ոչ հստակ ենթաբազմության հասկացության մասնավոր դեպք:

Դիցուք f_A-ն և g_A-ն A բազմության երկու ոչ հստակ ենթաբազմություններ են: Կասենք, որ f_A-ն ընկած է g_A-ում (կամ g_A-ն պարունակում է f_A-ն) և կգրենք՝ $f_A \leqslant g_A$ կամ $g_A \geqslant f_A$, եթե յուրաքանչյուր $x \in A$ տարրի համար, $f_A(x) \leqslant g_A(x)$ (որպես իրական թվեր): Ակնհայտ է, որ սահմանված «$\leqslant$» հարաբերությունը կլինի մասնակի կարգ:

f_A-ն կոչվում է g_A-ի **լրացում** և գրվում է $f_A = \overline{g}_A$, եթե յուրաքանչյուր $x \in A$ տարրի համար՝

$$f_A(x) = 1 - g_A(x) = \overline{g_A(x)}\,;$$

Ակնհայտ է, որ

$$\overline{(\overline{g}_A)} = g_A\ :$$

A բազմության f_A և g_A ոչ հստակ ենթաբազմությունների **հատում** է կոչվում A բազմության այն h_A ոչ հստակ ենթաբազմությունը, որը սահմանվում է

$$h_A(x) = \min\{f_A(x), g_A(x)\} = f_A(x) \wedge g_A(x)\,, \quad x \in A,$$

բանաձևով: Այն նշանակվում է $h_A = f_A \cap g_A$ ձևով և հանդիսանում է A բազմության այն «ամենամեծ» ոչ հստակ ենթաբազմությունը, որը միաժամանակ ընկած է f_A-ում և g_A-ում:

f_A և g_A ոչ հստակ ենթաբազմությունների **միավորում** է կոչվում այն h_A ոչ հստակ ենթաբազմությունը, որը սահմանվում է

$$h_A(x) = \max\{f_A(x), g_A(x)\} = f_A(x) \vee g_A(x)\,, \quad x \in A,$$

բանաձևով: Այն նշանակվում է $h_A = f_A \cup g_A$ ձևով և հանդիսանում է A բազմության այն «ամենափոքր» ոչ հստակ ենթաբազմությունը, որը միաժամանակ պարունակում է f_A-ն և g_A-ն:

Այսպիսով, միևնույն A բազմության բոլոր ոչ հստակ ենթաբազմությունների դասը կլինի կավարաձև կարգավորված բազմություն (սահմանված «$\leqslant$» մասնակի կարգի նկատմամբ), որտեղ $\sup\{f_A, g_A\} = f_A \cup g_A$, իսկ $\inf\{f_A, g_A\} = f_A \cap g_A$:

Երկու f_A և g_A ոչ հստակ ենթաբազմությունների **տարբերությունը** և **սիմետրիկ տարբերությունը** սահմանվում են հետևյալ կերպ`

$$f_A \setminus g_A = f_A \cap \overline{g}_A,$$

$$f_A \ominus g_A = (f_A \setminus g_A) \cup (g_A \setminus f_A)\,;$$

Սովորական ենթաբազմությունների նկատմամբ սահմանված գործողությունների հիմնական հատկությունները հեշտությամբ ստուգվում են նաև ոչ հստակ ենթաբազմությունների նկատմամբ սահմանված գործողությունների դեպքում, որոնք իրականում ժառանգվում են $[0,1]$ հատվածի վերոհիշյալ հանրահաշվական հատկություններից.

$$\left.\begin{aligned} &f_A \cap g_A = g_A \cap f_A, \\ &f_A \cup g_A = g_A \cup f_A, \end{aligned}\right\} (\text{ տեղափոխական օրենքներ})$$

$$\left.\begin{aligned} &(f_A \cap g_A) \cap \mu_A = f_A \cap (g_A \cap \mu_A)\,, \\ &(f_A \cup g_A) \cup \mu_A = f_A \cup (g_A \cup \mu_A)\,, \end{aligned}\right\} (\text{ զուգորդական օրենքներ})$$

$$\left.\begin{aligned} &f_A \cap f_A = f_A, \\ &f_A \cup f_A = f_A, \end{aligned}\right\} (\text{ ինքնահամընկնման օրենքներ})$$

$$\left.\begin{aligned} &f_A \cap (f_A \cup g_A) = f_A, \\ &f_A \cup (f_A \cap g_A) = f_A, \end{aligned}\right\} (\text{ կլանման օրենքներ})$$

$$\left.\begin{array}{l} f_A \cap (g_A \cup \mu_A) = (f_A \cap g_A) \cup (f_A \cap \mu_A)\,, \\ f_A \cup (g_A \cap \mu_A) = (f_A \cup g_A) \cap (f_A \cup \mu_A)\,, \end{array}\right\} (\text{ բաշխական օրենքներ})$$

$$\left.\begin{array}{r} \overline{f_A \cap g_A} = \overline{f}_A \cup \overline{g}_A, \\ \overline{f_A \cup g_A} = \overline{f}_A \cap \overline{g}_A \ : \end{array}\right\} (\text{ Դե Մորգանի օրենքներ})$$

Դիտարկելով A բազմության հետևյալ երկու ոչ հստակ ենթաբազմությունները՝ 0_A և 1_A, որտեղ $0_A(x) = 0$ և $1_A(x) = 1$ բոլոր $x \in A$ տարրերի համար, կունենանք՝

$$\bar{0}_A = 1_A, \quad \bar{1}_A = 0_A\,,$$

$$f_A \cup 0_A = f_A, \qquad f_A \cap 1_A = f_A\,, \quad (\text{միավորի գոյության օրենքներ})$$

և

$$f_A \cup 1_A = 1_A, \qquad f_A \cap 0_A = 0_A,$$

մինչդեռ՝

$$f_A \cap \overline{f}_A \neq 0_A, \qquad f_A \cup \overline{f}_A \neq 1_A,$$

եթե $f_A \neq 0_A,\ 1_A$:

Թեորեմ 0.27: *A բազմության բոլոր ոչ հստակ ենթաբազմությունները կազմում են համաձայնեցված անշարժ կետով Քլինիի հանրահաշիվ, որի անշարժ կետը $f(a) = \dfrac{1}{2}$, $a \in A$, պայմանով որոշվող $f:\ A \to [0,1]$ ոչ հստակ ենթաբազմությունն է:*

Ապացույց: Բխում է այն փաստից, որ $[0,1]$ հատվածը բավարարում է համաձայնեցված անշարժ կետով Քլինիի հանրահաշվի սահմանման պայմաններին: $\square$

Այսպիսով, ոչ հստակ ենթաբազմությունների հանրահաշվական հենքը իրական թվերի $[0,1]$ հատվածն է՝ իր գործողություններով:

Ոչ հստակ ենթաբազմությունների կառուցվածքից ելնելով սահմանվում են նաև հետևյալ երկու նոր գործողությունները:

h_A ոչ հստակ ենթաբազմությունը կոչվում է f_A և g_A ոչ հստակ ենթաբազմությունների **արտադրյալ** (**գումար**) և գրվում է $h_A = f_A \cdot g_A$ (համապատասխանաբար՝ $h_A = f_A + g_A$), եթե

$$h_A(x) = f_A(x) \cdot g_A(x) \in [0,1]$$

(համապատասխանաբար՝

$$h_A(x) = f_A(x) + g_A(x) - f_A(x) \cdot g_A(x) \in [0,1]) :$$

Այստեղ ի նկատի ենք ունենում այն հանգամանքը, որ

$$a, b \in [0,1] \longrightarrow a + b - a \cdot b \in [0,1];$$

Իրոք, ներկայացնելով a-ն $a = 1 - \varepsilon$ տեսքով, որտեղ $0 \leqslant \varepsilon \leqslant 1$, կունենանք՝

$$a + b - ab = 1 - \varepsilon + b - (1 - \varepsilon)b = 1 - \varepsilon + \varepsilon b = 1 - \varepsilon(1 - b) \in [0,1] :$$

Հեշտությամբ ստուգվում են նաև հետևյալ հիմնական հատկությունները (նույնությունները)՝

$f_A \cdot 1_A = f_A$, $f_A + 0_A = f_A$, (միավորի գոյության օրենքներ)

$$\left.\begin{aligned} &f_A \cdot g_A = g_A \cdot f_A, \\ &f_A + g_A = g_A + f_A, \end{aligned}\right\} \text{(տեղափոխական օրենքներ)}$$

$$\left.\begin{aligned} &(f_A \cdot g_A) \cdot \mu_A = f_A \cdot (g_A \cdot \mu_A), \\ &(f_A + g_A) + \mu_A = f_A + (g_A + \mu_A), \end{aligned}\right\} \text{(զուգորդական օրենքներ)}$$

$$\left.\begin{aligned} &\overline{f_A \cdot g_A} = \overline{f}_A + \overline{g}_A, \\ &\overline{f_A + g_A} = \overline{f}_A \cdot \overline{g}_A, \end{aligned}\right\} \text{(Դե Մորգանի օրենքներ)}$$

$$\left.\begin{aligned} &f_A \cdot (g_A \cup \mu_A) = (f_A \cdot g_A) \cup (f_A \cdot \mu_A), \\ &f_A \cdot (g_A \cap \mu_A) = (f_A \cdot g_A) \cap (f_A \cdot \mu_A), \\ &f_A + (g_A \cup \mu_A) = (f_A + g_A) \cup (f_A + \mu_A), \\ &f_A + (g_A \cap \mu_A) = (f_A + g_A) \cap (f_A + \mu_A) : \end{aligned}\right\} \text{(բաշխական օրենքներ)}$$

Սակայն գոյություն ունեն A բազմության այնպիսի f_A, g_A և μ_A ոչ հստակ ենթաբազմություններ, որ

$$f_A \cdot (g_A + \mu_A) \neq (f_A \cdot g_A) + (f_A \cdot \mu_A),$$

որովհետև՝

$$a \cdot (b + c - bc) \neq ab + ac - (ab)(ac),$$

եթե $a^2 \neq a$:

Եթե $[0,1]^A$-ով նշանակենք A-ի բոլոր ոչ հստակ ենթաբազմությունների բազմությունը, ապա յուրաքանչյուր

$f : B \to [0,1]^A$ արտապատկերում (ֆունկցիա) կոչվում է B-ի **երկրորդ կարգի ոչ հստակ ենթաբազմություն**: Ընտրելով «լավ» A բազմություններ, ստանում ենք համապատասխան երկրորդ կարգի ոչ հստակ ենթաբազմությունների «լավ» կիրառություններ:

Վարժություններ և խնդիրներ

1. Ստուգել հետևյալ հավասարությունները՝

$$\left.\begin{array}{l} A \cap (A \cup B) = A, \\ A \cup (A \cap B) = A, \end{array}\right\} \quad \text{(կլանման օրենքներ)}$$

$$\left.\begin{array}{l} A \cap (B \cup C) = (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C), \end{array}\right\} \quad \text{(բաշխական օրենքներ)}$$

$$\left.\begin{array}{l} A \cap (B \setminus C) = (A \cap B) \setminus C, \\ A \setminus (B \cup C) = (A \setminus B) \setminus C, \\ A \ominus (B \ominus C) = (A \ominus B) \ominus C, \end{array}\right\} \quad \text{(զուգորդական օրենքներ)}$$

$$\left.\begin{array}{l} A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C), \\ A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C), \\ (A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C), \\ A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C), \\ A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C), \\ (A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C), \\ A \cap (B \ominus C) = (A \cap B) \ominus (A \cap C), \end{array}\right\} \quad \text{(բաշխական օրենքներ)}$$

$$\left.\begin{array}{l} A \times (B \cup C) = (A \times B) \cup (A \times C), \\ (B \cup C) \times A = (B \times A) \cup (C \times A), \\ A \times (B \cap C) = (A \times B) \cap (A \times C), \\ (B \cap C) \times A = (B \times A) \cap (C \times A), \\ A \times (B \setminus C) = (A \times B) \setminus (A \times C), \\ (B \setminus C) \times A = (B \times A) \setminus (C \times A) \end{array}\right\} \quad \text{(բաշխական օրենքներ)}$$

բոլոր A, B, C բազմությունների համար:

2. Ապացուցել, որ կամայական $\alpha : A \to B$ արտապատկերման համար տեղի ունեն հետևյալ հատկությունները՝

$$\alpha\left(A_1 \cup A_2\right) = \alpha\left(A_1\right) \cup \alpha\left(A_2\right), \quad \alpha\left(\bigcup_{i\in I} A_i\right) = \bigcup_{i\in I} \alpha\left(A_i\right),$$

$$\alpha\left(A_1 \cap A_2\right) \subseteq \alpha\left(A_1\right) \cap \alpha\left(A_2\right), \quad \alpha\left(\bigcap_{i\in I} A_i\right) \subseteq \bigcap_{i\in I} \alpha\left(A_i\right),$$

$$\alpha\left(A_1\right) \setminus \alpha\left(A_2\right) \subseteq \alpha\left(A_1 \setminus A_2\right),$$

որտեղ $A_1, A_2, A_i \subseteq A$, $i \in I$:

3. Կամայական $\alpha : A \to B$ արտապատկերման և $C \subseteq B$ ենթաբազմության համար սահմանենք $\alpha^{-1}(C) \subseteq A$ ենթաբազմությունը հետևյալ կերպ՝

$$\alpha^{-1}(C) = \{x \in A \mid \alpha(x) \in C\}:$$

Ապացուցեք հետևյալ հավասարությունները՝

$$\alpha^{-1}\left(B_1 \cup B_2\right) = \alpha^{-1}\left(B_1\right) \cup \alpha^{-1}\left(B_2\right),$$

$$\alpha^{-1}\left(\bigcup_{i\in I} B_i\right) = \bigcup_{i\in I} \alpha^{-1}\left(B_i\right),$$

$$\alpha^{-1}\left(B_1 \cap B_2\right) = \alpha^{-1}\left(B_1\right) \cap \alpha^{-1}\left(B_2\right),$$

$$\alpha^{-1}\left(\bigcap_{i\in I} B_i\right) = \bigcap_{i\in I} \alpha^{-1}\left(B_i\right),$$

$$\alpha^{-1}\left(B_1 \setminus B_2\right) = \alpha^{-1}\left(B_1\right) \setminus \alpha^{-1}\left(B_2\right),$$

որտեղ $B_1, B_2, B_i \subseteq B$, $i \in I$:

4. Դիցուք $\mathbb{R}_+^0$-ը բոլոր ոչ բացասական իրական թվերի բազմությունն է և $f(x) = x^2$, որտեղ $x \in \mathbb{R}$:

   ա) Ապացուցել, որ $f : \mathbb{R}_+^0 \to \mathbb{R}$ արտապատկերումը հակադարձելի է աջից, բայց հակադարձելի չէ ձախից: Կառուցել (նշել) f-ի երկու աջ հակադարձներ:

բ) Ապացուցել, որ $f : \mathbb{R} \to \mathbb{R}^0_+$ արտապատկերումը հակադարձելի չէ աջից, բայց հակադարձելի է ձախից: Կառուցել (նշել) f-ի երկու ձախ հակադարձներ:

գ) Ապացուցել, որ $f : \mathbb{R}^0_+ \to \mathbb{R}^0_+$ արտապատկերումը հակադարձելի է:

դ) Ապացուցել, որ $f : \mathbb{N} \to \mathbb{N}$ արտապատկերումը հակադարձելի է աջից, բայց հակադարձելի չէ ձախից: Կառուցել (նշել) f-ի երկու աջ հակադարձներ:

5. Օգտվելով վերհանգման եղանակից, գումարման աքսիոմը բխեցնել հետևյալ հատկությունից՝

$$A \cap B = \emptyset \to |A \cup B| = |A| + |B|,$$

որտեղ A-ն և B-ն վերջավոր բազմություններ են:

6. Ապացուցել երեք վերջավոր բազմությունների միավորման կարգի հաշվման հետևյալ բանաձևը՝

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| :$$

7. Վերհանգման եղանակով ապացուցել $A_1, \ldots, A_n$ վերջավոր բազմությունների միավորման կարգի հաշվման հետևյալ բանաձևը՝

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leqslant i < j \leqslant n} |A_i \cap A_j| + \sum_{1 \leqslant i < j < k \leqslant n} |A_i \cap A_j \cap A_k| - \cdots$$

$$\cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n| :$$

8. Վերհանգման եղանակով ստուգել կարգավորված n-յակների հավասարության պայմանը՝

$$(x_1, \ldots, x_n) = (x'_1, \ldots, x'_n) \longleftrightarrow x_1 = x'_1, \ldots, x_n = x'_n :$$

9. Վերհանգման եղանակով ապացուցել, որ $A_1, \ldots, A_n$ վերջավոր բազմությունների $A_1 \times \cdots \times A_n$ դեկարտյան արտադրյալի կարգը որոշվում է հետևյալ բանաձևով՝

$$|A_1 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|,$$

որտեղ $n \geqslant 2$:

10. $A = \{1, 2, 3\}$ բազմության վրա կառուցեք համարժեքության հարաբերությունների այնպիսի $\alpha \subseteq A \times A$ և $\beta \subseteq A \times A$ օրինակներ, որ $\alpha \cdot \beta \neq \beta \cdot \alpha$:

11. Ապացուցել հետևյալ հայտանիշը. որպեսզի $\alpha \subseteq A \times B$ հարաբերությունը լինի բիեկտիվ արտապատկերում, անհրաժեշտ է և բավարար, որ
$$\alpha \cdot \alpha^{-1} = \varepsilon_A,$$
$$\alpha^{-1} \cdot \alpha = \varepsilon_B,$$
որտեղ α^{-1}-ը α-ի հակադարձ հարաբերությունն է:

12. Կառուցել T_3-տարածության այնպիսի օրինակ, որը T_1-տարածություն չէ:

13. Կառուցել T_4-տարածության այնպիսի օրինակ, որը T_1-տարածություն չէ:

14. Ապացուցել, որ դիսկրետ տոպոլոգիական տարածությունը մետրիկացվող է:

15. Եթե $(A; \rho)$-ն մետրիկական տարածություն է, ապա $(A; \tau_\rho)$ տոպոլոգիական տարածությունը Հաուսդորֆյան է:

16. Օգտվելով սահմանումից ապացուցել, որ աջից հակադարձելի երկու արտապատկերումների արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է աջից և
$$\beta' \cdot \alpha' = (\alpha \cdot \beta)',$$
այսինքն՝ $\beta' \cdot \alpha'$-ը կլինի $\alpha \cdot \beta$ արտադրյալի աջ հակադարձներից մեկը:

17. Վերհանգման եղանակով ապացուցել, որ վերջավոր թվով աջից հակադարձելի արտապատկերումների արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է աջից և
$$\alpha_n' \cdot \alpha_{n-1}' \cdots \alpha_1' = (\alpha_1 \cdot \alpha_2 \cdots \alpha_n)',$$
այսինքն՝ $\alpha_n' \cdot \alpha_{n-1}' \cdots \alpha_1'$-ը կլինի $\alpha_1 \cdot \alpha_2 \cdots \alpha_n$ արտադրյալի աջ հակադարձներից մեկը:

18. Օգտվելով սահմանումից ապացուցել, որ ձախից հակադարձելի երկու արտապատկերումների արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է ձախից և

$$\beta'' \cdot \alpha'' = (\alpha \cdot \beta)'' \,,$$

այսինքն՝ $\beta'' \cdot \alpha''$-ը կլինի $\alpha \cdot \beta$ արտադրյալի ձախ հակադարձներից մեկը:

19. Վերհանգման եղանակով ապացուցել, որ վերջավոր թվով ձախից հակադարձելի արտապատկերումների արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է ձախից և

$$\alpha''_n \cdot \alpha''_{n-1} \cdots \alpha''_1 = (\alpha_1 \cdot \alpha_2 \cdots \alpha_n)'' \,,$$

այսինքն՝ $\alpha''_n \cdot \alpha''_{n-1} \cdots \alpha''_1$-ը կլինի $\alpha_1 \cdot \alpha_2 \cdots \alpha_n$ արտադրյալի ձախ հակադարձներից մեկը:

20. Օգտվելով սահմանումից ապացուցել, որ եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը հակադարձելի է աջից, ապա α-ն հակադարձելի է աջից:

21. Օգտվելով սահմանումից ապացուցել, որ եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը հակադարձելի է ձախից, ապա β-ն հակադարձելի է ձախից:

22. Օգտվելով սահմանումից ապացուցել, որ եթե $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումների $\alpha \cdot \beta : A \to C$ արտադրյալը հակադարձելի է , ապա α-ն հակադարձելի է աջից, իսկ β-ն՝ ձախից:

23. Դիցուք $\alpha : A \to B$ և $\beta : B \to C$ արտապատկերումները հակադարձելի են աջից; $\bar{\alpha}$-ով նշանակենք α-ի բոլոր աջ հակադարձների բազմությունը՝

$$\bar{\alpha} = \{\alpha' : B \to A \,|\, \alpha \cdot \alpha' = \varepsilon_A\} \,:$$

Դիցուք

$$\bar{\beta} \cdot \bar{\alpha} = \left\{\beta' \cdot \alpha' : \beta' \in \bar{\beta},\, \alpha' \in \bar{\alpha}\right\} \,:$$

Ակնհայտ է, որ $\bar{\beta} \cdot \bar{\alpha} \subseteq \overline{\alpha \cdot \beta}$:

Բնութագրել բոլոր այն α, β աջից հակադարձելի արտապատկերումների զույգերը, որոնց համար՝

$$\overline{\alpha \cdot \beta} = \bar{\beta} \cdot \bar{\alpha}$$

(օրինակ, եթե α-ն և β-ն փոխմիարժեք (բիեկտիվ) են, ապա α, β զույգը հենց այդպիսին է):

24. Նախորդ խնդիրը վերաձևակերպել և լուծել ձախից հակադարձելի արտապատկերումների համար:

25. Ապացուցել արտապատկերման ինյեկտիվության հետևյալ հայտանիշը. որպեսզի $\alpha : A \to B$ արտապատկերումը լինի ինյեկտիվ, անհրաժեշտ է և բավարար, որ α-ն բավարարի հետևյալ պայմանին՝

$$\beta \cdot \alpha = \gamma \cdot \alpha \to \beta = \gamma,$$

որտեղ $\beta, \gamma : C \to A$:

26. Ապացուցել արտապատկերման սյուրեկտիվության հետևյալ հայտանիշը. որպեսզի $\alpha : A \to B$ արտապատկերումը լինի սյուրեկտիվ, անհրաժեշտ է և բավարար, որ

$$\alpha \cdot \beta = \alpha \cdot \gamma \to \beta = \gamma,$$

որտեղ $\beta, \gamma : B \to C$:

27. Ապացուցել, որ յուրաքանչյուր անվերջ բազմություն հավասարազոր է իրենից տարբեր իր որևէ ենթաբազմությանը:

28. Կարգավորված n-յակը կոչվում է առանց կրկնությունների (կամ կրկնություններ չունեցող), եթե $n = 1$ կամ նրա բաղադրիչները (կոորդինատները) զույգ առ զույգ տարբեր են: Հակառակ դեպքում կարգավորված n-յակը կոչվում է կրկնություններ ունեցող (կամ կրկնություններով):

Վերհանգման եղանակով ապացուցել, որ m-տարրանի բազմության վրա որոշված և կրկնություններ չունեցող բոլոր կարգավորված n-յակների թիվը հավասար է՝

$$m(m-1)\cdots(m-n+1),$$

որտեղ $1 \leqslant n \leqslant m$:

29. Եթե $|A| = n \geqslant 1$ և $|B| = m \geqslant n$, ապա $\alpha : A \to B$ տեսքի բոլոր ինյեկտիվ արտապատկերումների թիվը կլինի հավասար՝

$$m(m-1)\cdots(m-n+1):$$

30. n-տարրանի բազմության բոլոր k-տարրանի ենթաբազմությունների թիվը նշանակվում է $\begin{pmatrix} n \\ k \end{pmatrix}$-ով: Ապացուցել հետևյալ բանաձևը՝

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!}, \quad \text{որտեղ } 0 \leqslant k \leqslant n \quad \text{և} \quad 0! = 1:$$

31. Ապացուցել, որ եթե $|A| = n$ և $|B| = m \leqslant n$, ապա $\alpha : A \to B$ տեսքի բոլոր սյուրեկտիվ արտապատկերումների թիվը կլինի հավասար՝

$$\sum_{i=0}^{m-1} (-1)^i \begin{pmatrix} m \\ i \end{pmatrix} (m-i)^n :$$

32. Ապացուցել, որ n-տարրանի բազմության անշարժ կետ չունեցող բոլոր տեղադրությունների թիվը հավասար է՝

$$n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right):$$

33. Ապացուցել հետևյալ հավասարությունը՝

$$\begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} n \\ n-k \end{pmatrix}: \quad (\textit{սիմետրիկության օրենք})$$

34. Ապացուցել հետևյալ հավասարությունը՝

$$\begin{pmatrix} n+1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix}, \quad (\textit{Պասկալի օրենք})$$

որտեղ $1 \leqslant k \leqslant n$:

35. Վերհանգման եղանակով ապացուցել Նյուտոնի երկանդամի բանաձևը՝

$$(x+y)^n =$$
$$= \binom{n}{0} x^n + \binom{n}{1} x^{n-1}y + \cdots + \binom{n}{n-1} xy^{n-1} + \binom{n}{n} y^n;$$

Համառոտ՝

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k}y^k,$$

որտեղ $x, y \in \mathbb{R}$, $n \in \mathbb{N}$:

36. Ապացուցել, որ

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n$$

և

$$\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \binom{n}{3} + \cdots + (-1)^n \binom{n}{n} = 0,$$

այսինքն՝

$$1 + n + \frac{n(n-1)}{1 \cdot 2} + \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3} + \cdots + 1 = 2^n$$

և

$$1 - n + \frac{n(n-1)}{1 \cdot 2} - \frac{n(n-1)(n-2)}{1 \cdot 2 \cdot 3} + \cdots + (-1)^n = 0:$$

(Ցուցում. Նյուտոնի երկանդամի մեջ տեղադրել $x = 1$, $y = 1$ և $x = 1$, $y = -1$):

Մաս Ա

Թվերի տեսություն

Գ լ ու խ 1

ԱՄԲՈՂՋ ԹՎԵՐԻ ՄՆԱՑՈՐԴՈՎ ԲԱԺԱՆՄԱՆ ԷՎԿԼԻԴԵՍԻ (ԷՎԿԼԻԴԻ) ԿԱՆՈՆԸ (ԱԼԳՈՐԻԹՄԸ): ԲԱՂԴԱՏՈՒՄՆԵՐ, ՄՆԱՑՔՆԵՐԻ ԴԱՍԵՐ, ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐ ՄՆԱՑՔՆԵՐԻ ԴԱՍԵՐԻ ՀԵՏ: ԶՈՒԳՈՐԴԱԿԱՆ ԳՈՐԾՈՂՈՒԹՅՈՒՆՆԵՐ

1.1. Բաժանում և մնացորդով բաժանում

Եթե $|a|$-ն a իրական թվի բացարձակ արժեքն է (մոդուլը), այսինքն՝

$$|a| = \begin{cases} a, & \text{եթե } a \geqslant 0, \\ -a, & \text{եթե } a < 0, \end{cases} = \begin{cases} a, & \text{եթե } a > 0, \\ 0, & \text{եթե } a = 0, \\ -a, & \text{եթե } a < 0, \end{cases}$$

ապա $|a| \geqslant 0$ և $|a| = 0$ այն և միայն այն դեպքում, երբ $a = 0$: Կունենանք նաև $|a \cdot b| = |a| \cdot |b|$ ցանկացած $a, b \in \mathbb{R}$ իրական թվերի համար: Ներմուծելով a իրական թվի նշանի գաղափարը և նշանակելով նրան $sign(a)$-ով՝

$$sign(a) = \begin{cases} 1, & \text{եթե } a > 0, \\ 0, & \text{եթե } a = 0, \\ -1, & \text{եթե } a < 0, \end{cases}$$

կունենանք՝

$$|a| = a \cdot sign(a),$$

$$a = |a| \cdot sign(a)$$

և

$$sign(a \cdot b) = sign(a) \cdot sign(b)$$

ցանկացած $a, b \in \mathbb{R}$ իրական թվերի համար:

Կասենք, որ a ամբողջ թիվը **բաժանվում է** b ամբողջ թվի վրա և կգրենք a/b կամ $b\backslash a$, եթե գոյություն ունի այնպիսի c ամբողջ թիվ, որ $a = b \cdot c$ (այս դեպքում ասում են նաև, որ a-ն առանց մնացորդի է բաժանվում b-ի վրա): a-ն կոչվում է բաժանելի կամ b-ի պատիկ (երբեմն նաև բազմապատիկ), b-ն՝ a-ի բաժանարար, իսկ c-ն քանորդ (եթե $b \neq 0$): Հակառակ դեպքում գրվում է՝ $a \not/ b$ կամ $b \not\backslash a$ և կարդացվում է՝ a-ն չի բաժանվում b-ի վրա: Եթե $a = bc$ և $b \neq 0$, ապա c-ն որոշվում է միարժեքորեն:

a ամբողջ թիվը կոչվում է **հակադարձելի**, եթե այն 1-ի բաժանարար է, այսինքն՝ գոյություն ունի այնպիսի x ամբողջ թիվ, որ $a \cdot x = 1$: Ակնհայտ է, որ ± 1-ը հակադարձելի է: Ամբողջ թիվը կոչվում է զույգ, եթե այն բաժանվում է 2-ի վրա, և կենտ՝ հակառակ դեպքում:

Հետևյալ հատկությունները բխում են ամբողջ թվերի բաժանման սահմանումից:

1° Զրոն բաժանվում է ցանկացած ամբողջ թվի (մասնավորապես և զրոյի) վրա:

2° Եթե $a \neq 0$ և $b = 0$, ապա a-ն չի բաժանվում b-ի վրա, այսինքն՝ ոչ զրոյական ամբողջ թիվը չի բաժանվում զրոյի վրա:

3° Եթե a-ն բաժանվում է b-ի վրա, ապա a-ն կբաժանվի նաև $-b$-ի և հետևաբար նաև $|b|$-ի վրա:

4° Յուրաքանչյուր a ամբողջ թիվ բաժանվում է իր և 1-ի վրա:

5° Եթե a-ն բաժանվում է b-ի վրա և b-ն բաժանվում է c-ի վրա, ապա a-ն կբաժանվի c-ի վրա:

6° Եթե a-ն և b-ն բաժանվում են c-ի վրա, ապա $ax \pm by$-ը նույնպես կբաժանվի c-ի վրա, որտեղ $x, y \in \mathbb{Z}$:

7° Եթե a-ն բաժանվում է b-ի վրա և $|a| < |b|$, ապա $a = 0$:

Ապացուցում: Եթե $a = b \cdot c$, որտեղ $c \in \mathbb{Z}$ և $0 \leqslant |a| < |b|$, ապա՝

$$|b \cdot c| = |a| < |b|,$$

$$|b| \cdot |c| < |b| :$$

Վերջին անհավասարությունը կրճատելով $|b| > 0$ ամբողջ դրական թվով, կստանանք $|c| < 1$: Հետևաբար $|c| = 0$ և $c = 0$: Ուստի $a = b \cdot c = b \cdot 0 = 0$:

8° Եթե $a \neq 0$ և a-ն բաժանվում է b-ի վրա, ապա $|a| \geqslant |b|$:

Ապացուցում: Բխում է հատկություն 7°-ից:

9° Եթե b ամբողջ թիվը հակադարձելի է, ապա $b = \pm 1$:

Ապացուցում: Համաձայն հատկություն 8°-ի՝ $|1| \geqslant |b|$, որտեղ $b \neq 0$: Հետևաբար՝ $|b| = 1$ և $b = \pm 1$:

10° Եթե a-ն բաժանվում է b-ի վրա և b-ն բաժանվում է a-ի վրա, ապա $a = b$ կամ $a = -b$, այսինքն՝ $|a| = |b|$:

Ապացուցում: Գոյություն ունեն այնպիսի $t, s \in \mathbb{Z}$ ամբողջ թվեր, որ $a = bt$ և $b = as$: Հետևաբար՝ $a = ast$, $a - ast = 0$, $a(1 - st) = 0$, որտեղից կամ $a = 0 = 0 \cdot s = b$ կամ $st = 1$, այսինքն՝ $s = \pm 1$ (հատկություն 9°) և $b = \pm a$:

11° Սահմանելով $a, b \in \mathbb{N}$ բնական թվերի համար՝

$$a \preceq b \longleftrightarrow {}^{b}/_{a},$$

ստանում ենք մի «$\preceq$» հարաբերություն, որը մասնակի կարգ է և կոչվում է **բաժանման հարաբերություն**:

12° Սահմանելով $a, b \in \mathbb{Z}$ ամբողջ թվերի համար՝

$$a \preceq b \longleftrightarrow {}^{b}/_{a},$$

ստանում ենք մի հարաբերություն, որը բավարարում է ռեֆլեքսիվության և փոխանցականության պայմաններին, բայց չի բավարարում համաչափության և հակահամաչափության պայմաններին:

Ապացուցենք ամբողջ թվերի մնացորդով բաժանման հետևյալ օրենքը (կանոնը, ալգորիթմը, ընթացանին), որը առաջին անգամ ձևակերպվել է («երկրաչափորեն») և ապացուցվել հույն հայտնի մաթեմատիկոս Էվկլիդեսի (Էվկլիդի) կողմից, մեր թվարկությունից առաջ 3-րդ դարում՝ իր «Սկզբունքներ» հանրահայտ աշխատության մեջ (գիրք VII, թեորեմներ 1, 2):

Թեորեմ 1.1 (Էվկլիդես)*: Ցանկացած a և $b \neq 0$ ամբողջ թվերի համար գոյություն ունեն միարժեքորեն որոշվող այնպիսի q և r ամբողջ թվեր, որ*

$$a = bq + r \quad \text{և} \quad 0 \leqslant r < |b|;$$

Ապացուցում: Նախ ապացուցենք գոյության մասը՝ օգտվելով փոքրագույն տարրի սկզբունքից: Դիտարկենք $a - bx$ տեսքի բոլոր ամբողջ թվերի բազմությունը, որտեղ x-ը փոփոխվում է $\mathbb{Z}$ բազմության մեջ՝

$$M = \{a - bx \mid x \in \mathbb{Z}\};$$

Ակնհայտ է, որ M բազմության մեջ գոյություն կունենան ոչ բացասական ամբողջ թվեր, որովհետև $a - bx \geqslant 0$ անհավասարումն ունի $\mathbb{Z}$ բազմությանը պատկանող լուծումներ (օրինակ, եթե $a \geqslant 0$, ապա $x = 0$, իսկ եթե $a < 0$, ապա $x = ab$): Նշանակելով M բազմությանը պատկանող փոքրագույն ոչ բացասական ամբողջ թիվը r-ով, կունենանք՝

$$r = a - bx_0 \geqslant 0,$$

որտեղ $x_0 = q \in \mathbb{Z}$: Հետևաբար՝ $a = bq + r$: Ապացուցենք $r < |b|$ անհավասարությունը: Ենթադրելով $r \geqslant |b|$ անհավասարությունը, կունենանք՝

$$r - |b| = r_1 \geqslant 0, \ \ r_1 < r,$$

և

$$r_1 = r - |b| = a - bx_0 - b \cdot sign(b) = a - b(x_0 + sign(b)) \in M;$$

Այսպիսով $0 \leqslant r_1 < r$ և $r_1 \in M$, որը հակասում է r-ի ընտրությանը: Ստացված հակասությունը ապացուցում է $r < |b|$ անհավասարությունը: Գոյությունն ապացուցված է:

Գոյության մասը ստացվում է նաև հետևյալ կերպ: Գոյություն ունի այնպիսի q' ամբողջ թիվ, որ

$$q' \leqslant \frac{a}{|b|} < q' + 1;$$

Հետևաբար՝

$$q'|b| \leqslant a < q'|b| + |b|,$$

$$0 \leqslant a - q'|b| < |b|;$$

նշանակելով՝ $r = a - q'|b|$, կստանանք՝

$$a = q'|b| + r = q'b \cdot sign(b) + r = bq + r,$$

որտեղ $q = q' \cdot sign(b)$, $0 \leqslant r < |b|$;

Ապացուցենք q և r ամբողջ թվերի միակությունը, այսինքն, եթե

$$a = bq_1 + r_1, \quad \text{որտեղ} \quad 0 \leqslant r_1 < |b|,$$

$$a = bq_2 + r_2, \quad \text{որտեղ} \quad 0 \leqslant r_2 < |b|,$$

ապա $q_1 = q_2$ և $r_1 = r_2$: Իրոք՝

$$bq_1 + r_1 = bq_2 + r_2,$$

$$b(q_1 - q_2) = r_2 - r_1,$$

որտեղ $|r_2 - r_1| < |b|$: Քանի որ $|r_2 - r_1| < |b|$ և $(r_2 - r_1)$-ը բաժանվում է b-ի վրա, ապա ըստ հատկության 7°-ի $r_2 - r_1 = 0$, հետևաբար $r_2 = r_1$: Որից հետո ստանում ենք՝

$$b(q_1 - q_2) = 0,$$

որտեղ, ըստ պայմանի, $b \neq 0$: Հետևաբար՝ $q_1 - q_2 = 0$ և $q_1 = q_2$: □

a ամբողջ թվի

$$a = bq + r, \quad 0 \leqslant r < |b|$$

ներկայացման մեջ a-ն կոչվում է բաժանելի, b-ն՝ բաժանարար, q-ն՝ (ոչ լրիվ) քանորդ, իսկ r-ը մնացորդ և նշանակվում է նաև $a\, mod(b)$-ով կամ $a(mod\, b)$-ով: Օրինակ, $8(mod\, 3) = 2$, $9(mod\, 4) = 1$, ...

$b = 2$ դեպքում թեորեմ 1.1-ն ակնհայտ է, որովհետև յուրաքանչյուր ամբողջ թիվ կամ զույգ է կամ կենտ:

Հետևություն 1.1: *Եթե ամբողջ թվերի $K \subseteq \mathbb{Z}$ ոչ դատարկ բազմությունը պարունակում է իր ցանկացած երկու տարրերի գումարը և տարբերությունը, ապա կամ $K = \{0\}$ կամ K-ն կազմված է իր փոքրագույն դրական b տարրի (թվի) բազմապատիկներից, այսինքն՝*

$$K = \{bq \mid q \in \mathbb{Z}\} :$$

Ապացուցում: Եթե $K \neq \{0\}$, ապա գոյություն ունի $a \in K$, $a \neq 0$: Հետևաբար, $a - a = 0 \in K$, $0 - a = -a \in K$ և K-ն կպարունակի $|a| > 0$ դրական թիվը: Նշանակենք b-ով K-ի կազմում գոյություն ունեցող փոքրագույն ամբողջ և դրական թիվը: Այնուհետև, վերհանգման եղանակով ստանում ենք $nb \in K$, որտեղ $n \in \mathbb{N}$: Հետևաբար, $mb \in K$, որտեղ $m \in \mathbb{Z}$: Ուստի՝ $\{bq | \, q \in \mathbb{Z}\} \subseteq K$: Մնում է ապացուցել հակառակը: Դիցուք $c \in K$ և $c = bq + r$, որտեղ $0 \leqslant r < b$: Ենթադրելով $r \neq 0$, ստանում ենք $0 < r < b$ և $r = c - bq \in K$, որը հակասում է b-ի ընտրությունը: □

Հետևություն 1.2: *Ցանկացած a և $b \neq 0$ ամբողջ թվերի համար գոյություն ունեն միարժեքորեն որոշվող այնպիսի q և r ամբողջ թվեր, որ*

$$a = bq + r,$$

որտեղ $|r| < |b|$ և r, b թվերն ունեն նույն նշանը (եթե $r \neq 0$):

Ապացուցում: Թեորեմ 1.1-ի համաձայն՝

$$a = bq + r, \quad 0 \leqslant r < |b| :$$

Եթե $b > 0$, ապա հետևությունը կլինի ապացուցված: Դիցուք $b < 0$ և $r \neq 0$: Այդ դեպքում $|b| = -b$ և $r < -b$, $r_1 = r + b < 0$: Միաժամանակ,

$$b < b + r,$$

$$-b > -(b + r),$$

$$|b| > |b + r| = |r_1|$$

և

$$a = bq + r = bq - b + b + r = b(q - 1) + (b + r) = b(q - 1) + r_1 :$$

Միակության մասի ապացուցումը կրկնում է թեորեմ 1.1-ի միակության մասի ապացուցումը: □

Հետևություն 1.3: *Ցանկացած a և $b \neq 0$ ամբողջ թվերի համար գոյություն ունեն միարժեքորեն որոշվող այնպիսի q և r ամբողջ թվեր, որ*

$$a = bq + r, \quad -\frac{|b|}{2} < r \leqslant \frac{|b|}{2};$$

Ապացուցում: Նախորդ հետևության համաձայն՝

$$a = bq + r,$$

որտեղ $|r| < |b|$ և r, b ամբողջ թվերն ունեն նույն նշանը (եթե $r \neq 0$): Եթե այստեղ $-\frac{|b|}{2} < r \leqslant \frac{|b|}{2}$, ապա գոյության մասը կլինի ապացուցված: Հակառակ դեպքում՝ $|r - b| \leqslant \frac{|b|}{2}$ և $|r - b| = \frac{|b|}{2}$, եթե $r - b > 0$: Հետևաբար, $-\frac{|b|}{2} < r - b \leqslant \frac{|b|}{2}$ և

$$a = bq + r = bq + b - b + r = b(q + 1) + (r - b) :$$

Միակության մասի ապացուցումը կրկնում է թեորեմ 1.1-ի միակության մասի ապացուցումը: □

***Հետևություն 1.4**: Դիցուք a-ն և b-ն ամբողջ և դրական թվեր են, $b > 1$: Գոյություն ունեն միարժեքորեն որոշվող այնպիսի $c_0, c_1, \ldots, c_k$ ամբողջ թվեր, որ*

$$a = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0,$$

որտեղ $0 \leqslant c_i < b$, $i = 0, 1, \ldots, k$ և $c_k \neq 0$:

Ապացուցում: Մնացորդով բաժանման ալգորիթմից (թեորեմ 1.1) բխում է, որ $a = bq_1 + c_0$, որտեղ $0 \leqslant c_0 < b$ և $q_1 = \dfrac{a - c_0}{b} < a$: Եթե $q_1 \geqslant b$, ապա նորից բաժանման ալգորիթմի համաձայն՝ $q_1 = bq_2 + c_1$, որտեղ $0 \leqslant c_1 < b$ և $q_2 < q_1$: Եթե $q_2 \geqslant b$, ապա շարունակելով նշված եղանակով, ստանում ենք ամբողջ և դրական թվերի նվազող հաջորդականություն՝

$$q_1 > q_2 > \cdots,$$

որն անվերջ լինել չի կարող: Այսինքն՝ գոյություն կունենա այնպիսի k համար, որի դեպքում՝ $q_k < b$, իսկ $q_{k-1} \geqslant b$: Այսպիսով, հանգում ենք հետևյալ համակարգին՝

$$\begin{aligned}
&a = bq_1 + c_0,\\
&q_1 = bq_2 + c_1,\\
&\cdots\ \cdots\ \cdots\ \cdots,\\
&q_{k-2} = bq_{k-1} + c_{k-2},\\
&q_{k-1} = bq_k + c_{k-1},\\
&q_k = b \cdot 0 + c_k :
\end{aligned}$$

Հետևաբար, $q_k \neq 0$, որովհետև հակառակ դեպքում կունենայինք հակասություն՝

$$c_{k-1} = q_{k-1} \geqslant b :$$

Այժմ գրված համակարգից արտաքսելով $q_k, q_{k-1}, \ldots, q_1$ բնական թվերը, կստանանք՝

$$a = c_k b^k + \cdots + c_1 b + c_0,$$

որտեղ $0 \leqslant c_i < b$, $i = 0, 1, \ldots, k$ և $c_k \neq 0$:

Մնում է ապացուցել վերլուծության c_i գործակիցների միակությունը: Դիցուք ունենք նաև հետևյալ վերլուծությունը՝

$$a = d_k b^k + \cdots + d_1 b + d_0,$$

որտեղ $0 \leqslant d_i < b$, $i = 0, 1, \ldots, k$ և $d_k \neq 0$: Քանի որ առաջին և երկրորդ վերլուծություններից կունենանք՝

$$a = bx + c_0, \qquad \text{որտեղ } 0 \leqslant c_0 < b,$$

$$a = by + d_0, \qquad \text{որտեղ } 0 \leqslant d_0 < b,$$

ապա $c_0 = d_0$ (թեորեմ 1.1): Այնուհետև՝

$$\frac{a - c_0}{b} = bu + c_1, \qquad \text{որտեղ } 0 \leqslant c_1 < b,$$

$$\frac{a - c_0}{b} = bv + d_1, \qquad \text{որտեղ } 0 \leqslant d_1 < b,$$

ուստի $c_1 = d_1$ (թեորեմ 1.1), և այսպես շարունակ: Ի վերջո ստանում ենք $c_i = d_i$ հավասարությունը՝ բոլոր $i = 0, 1, \ldots, k$ արժեքների համար: □

Ապացուցված ներկայացումը կոչվում է a բնական թվի ներկայացում b-**ական համակարգում** և համառոտ գրվում է՝

$$a = (c_k c_{k-1} \cdots c_1 c_0)_b\,,$$

որտեղ $c_0, c_1, \ldots, c_k$ թվերը կոչվում են այդ ներկայացման գործակիցներ, իսկ k-ն՝ **ներկայացման երկարություն**:

Օրինակ, 2-ական համակարգում 43-ը ներկայացվում է հետևյալ կերպ՝

$$43 = (101011)_2,$$

որովհետև

$$43 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1,$$

իսկ 3-ական համակարգում՝

$$43 = (1121)_3,$$

որովհետև

$$43 = 1 \cdot 3^3 + 1 \cdot 3^2 + 2 \cdot 3 + 1 :$$

Եթե $x \in \mathbb{Z}$, $x \neq 0$, ապա սահմանելով $\delta(x)$-ը որպես $|x|$-ի 2-ական համակարգում ունեցած ներկայացման երկարություն և, ելնելով հետևություն 1.3-ից, կարող ենք պնդել, որ *ցանկացած* a *և* $b \neq 0$ *ամբողջ թվերի համար գոյություն ունեն այնպիսի* q *և* r *ամբողջ թվեր, որ*

$$a = bq + r,$$

որտեղ կամ $r = 0$*, կամ* $\delta(r) < \delta(b)$*:* Իրոք,

$$|r| \leqslant \frac{|b|}{2} \longleftrightarrow \delta(r) < \delta(b) :$$

Ըստ որում, նշված հատկությամբ q և r ամբողջ թվերն արդեն միարժեքորեն չեն որոշվում: *Օրինակ*, $a = 30$, $b = 4$ դեպքում՝

$$30 = 4 \cdot 8 - 2, \quad q = 8, \quad r = -2,$$

$$30 = 4 \cdot 7 + 2, \quad q = 7, \quad r = 2$$

և $|r| \leqslant \frac{|b|}{2}$: Դժվար չէ նկատել, որ $2^{\delta(x)} \leqslant |x| < 2^{\delta(x)+1}$: Սահմանված $\delta(x)$ ֆունկցիայի առանձնահատկության մասին տես գլուխ 19-ի վերջում զետեղված 12-րդ խնդիրը:

1.2. Բաղդատումներ: Մնացքային տոպոլոգիա

Անցնենք բաղդատման գաղափարին: Դիցուք n-ը (ոչ զրոյական) բնական թիվ է, որը հետևյալ սահմանման մեջ կոչվում է նաև բաղդատման **մոդուլ**, **հենաթիվ** կամ **հենք**: a և b թվերը կոչվում են *բաղդատելի ըստ մոդուլ* n-ի և գրվում է

$$a \equiv b (mod\, n),$$

եթե նրանց $a - b$ տարբերությունը բաժանվում է n-ի վրա: Հակառակ դեպքում a և b ամբողջ թվերը կոչվում են **ոչ բաղդատելի** ըստ մոդուլ n-ի և գրվում է՝ $a \not\equiv b (mod\, n)$:

Այս «$\equiv$» հարաբերությունը կոչվում է **բաղդատման հարաբերություն**:

Օրինակ, եթե $a = b (mod\, n)$, ապա $a \equiv b (mod\, n)$:

Հատկություն 1.1: *Որպեսզի a և b ամբողջ թվերը լինեն բաղդատելի ըստ մոդուլ n-ի անհրաժեշտ է և բավարար, որ*

$$a = nq + r, \quad b = nq_1 + r, \quad 0 \leqslant r < n;$$

Այսինքն՝ $a \equiv b(mod\, n) \longleftrightarrow a(mod\, n) = b(mod\, n)$:

Ապացույց: Եթե

$$a \equiv b(mod\, n),$$

ապա $a - b = nt$, $t \in \mathbb{Z}$; Դիցուք՝

$$a = nq + r, \quad 0 \leqslant r < n;$$

Այդ դեպքում՝

$$b = a - nt = nq + r - nt = n(q - t) + r = nq_1 + r,$$

որտեղ $q_1 = q - t \in \mathbb{Z}$:

Եվ հակառակը, եթե

$$a = nq + r, \quad b = nq_1 + r,$$

ապա $a - b = nq - nq_1 = n(q - q_1)$ և $a \equiv b(mod\, n)$:

Հատկություն 1.1-ն ապացուցված է: □

Բաղդատման հետևյալ հատկությունները նման են հավասարության համապատասխան հատկություններին:

Հատկություն 1.2: *$a \equiv a(mod\, n)$ (ռեֆլեքսիվություն); Եթե $a \equiv b(mod\, n)$, ապա $b \equiv a(mod\, n)$ (սիմետրիկություն կամ համաչափություն); Եթե $a \equiv b(mod\, n)$ և $b \equiv c(mod\, n)$, ապա $a \equiv c(mod\, n)$ (փոխանցականություն): Այլ կերպ ասած, բաղդատման հարաբերությունը համարժեքության հարաբերություն է՝ որոշված $\mathbb{Z}$ բազմության վրա:*

Ապացույց: $a - a = 0$ և հետևաբար բաժանվում է յուրաքանչյուր $n \geqslant 1$ բնական թվի վրա:

Եթե $a - b$ ամբողջ թիվը բաժանվում է n-ի վրա, ապա $b - a = -(a - b)$ ամբողջ թիվը ևս կբաժանվի n-ի վրա: Եթե $a - b$ և $b - c$ ամբողջ թվերը բաժանվում են n-ի վրա, ապա $a - c = (a - b) + (b - c)$ ամբողջ թիվը ևս կբաժանվի n-ի վրա: □

Հատկություն 1.3: *Եթե* $a_1 \equiv b_1(mod\, n)$ *և* $a_2 \equiv b_2(mod\, n)$, *ապա* $a_1 \pm a_2 \equiv b_1 \pm b_2(mod\, n)$ *և* $a_1a_2 \equiv b_1b_2(mod\, n)$*: Ընդհանուր դեպքում, եթե* $a_1 \equiv b_1(mod\, n)$, $\ldots$, $a_n \equiv b_n(mod\, n)$, *ապա* $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n(mod\, n)$ *և* $a_1 \cdots a_n \equiv b_1 \cdots b_n(mod\, n)$, *այսինքն՝ միևնույն մոդուլով բաղդատումները կարելի է անդամ առ անդամ գումարել և անդամ առ անդամ բազմապատկել:*

Ապացուցում: Եթե $a_1 - b_1$ և $a_2 - b_2$ ամբողջ թվերը բաժանվում են n-ի վրա, ապա

$$(a_1 \pm a_2) - (b_1 \pm b_2) = (a_1 - b_1) \pm (a_2 - b_2)$$

և

$$a_1a_2 - b_1b_2 = a_1a_2 - a_1b_2 + a_1b_2 - b_1b_2 = a_1(a_2 - b_2) + b_2(a_1 - b_1)$$

ամբողջ թվերը ևս կբաժանվեն n-ի վրա:

Ընդհանուր դեպքի ապացուցումը կատարվում է վերհանգման եղանակով: □

Հետևություն 1.5: *Բաղդատման երկու կողմերին կարելի է ավելացնել միևնույն ամբողջ թիվը՝ առանց փոխելու բաղդատման մոդուլը: Բաղդատման երկու կողմերը կարելի է բազմապատկել միևնույն ամբողջ թվով՝ առանց փոխելու բաղդատման մոդուլը: Բաղդատման երկու կողմերը կարելի է բարձրացնել միևնույն բնական ցուցիչով աստիճան՝ առանց փոխելու բաղդատման մոդուլը: Բաղդատման որևէ կողմում եղած գումարելին կարելի է տեղափոխել բաղդատման մյուս կողմ՝ փոխելով գումարելու նշանը և չփոխելով բաղդատման մոդուլը:*

□

Հետևություն 1.6: *Եթե* $a \equiv b(mod\, m)$, *ապա ամբողջ գործակիցներով ցանկացած*

$$f(x) = c_0 + c_1x + \cdots + c_nx^n$$

բազմանդամի համար՝

$$f(a) \equiv f(b)(mod\, m):$$

Ապացուցում: Եթե $a \equiv b(mod\, m)$, ապա $a^k \equiv b^k(mod\, m)$, $c_ka^k \equiv c_kb^k(mod\, m)$ և հետևաբար՝

$$c_0 + c_1a + \cdots + c_na^n \equiv c_0 + c_1b + \cdots + c_nb^n(mod\, m): \qquad \square$$

Օգտվելով այս հետևությունից կարելի է հանգել թվերի բաժանելիության վերաբերյալ դպրոցական դասընթացից հայտնի մի շարք հայտանիշների: Օրինակ, եթե 10-ական համակարգում a բնական թիվն ունի հետևյալ ներկայացումը՝

$$a = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 \cdot 10 + a_0,$$

և u-ով նշանակենք a-ի բոլոր թվանշանների գումարը՝

$$u = \sum_{i=0}^{k} a_i,$$

իսկ v-ով՝

$$v = \sum_{i=0}^{k} (-1)^i a_i,$$

ապա՝

0) a-ն կբաժանվի 10-ի (վրա) այն և միայն այն դեպքում, երբ a_0-ն բաժանվում է 10-ի, այսինքն, երբ $a_0 = 0$: a-ն կբաժանվի 5-ի (վրա) այն և միայն այն դեպքում, երբ a_0-ն բաժանվում է 5-ի, այսինքն, երբ $a_0 = 0$ կամ $a_0 = 5$:

1) a-ն կբաժանվի 3-ի (վրա) այն և միայն այն դեպքում, երբ u-ն բաժանվում է 3-ի:

2) a-ն կբաժանվի 9-ի (վրա) այն և միայն այն դեպքում, երբ u-ն բաժանվում է 9-ի:

3) a-ն կբաժանվի 11-ի (վրա) այն և միայն այն դեպքում, երբ v-ն բաժանվում է 11-ի:

4) a-ն կբաժանվի 2^s-ի (վրա) այն և միայն այն դեպքում, երբ a բնական թվի վերջին s թվանշաններից կազմված $a_{s-1}a_{s-2}\ldots a_1 a_0$ բնական թիվը բաժանվում է 2^s-ի վրա:

Իրոք, եթե

$$f(x) = a_0 + a_1 x + \cdots + a_{k-1} x^{k-1} + a_k x^k,$$

ապա $f(10) = a$, $f(1) = u$, $f(-1) = v$: Քանի որ $10 \equiv 1 (mod\, 9)$, ապա (հետևություն 1.6)՝ $f(10) \equiv f(1) (mod\, 9)$, այսինքն՝ $a \equiv u (mod\, 9)$ և $a -$

$u = 9l$, $l \in \mathbb{N}$: Հետևաբար, a-ն կբաժանվի 9-ի (վրա) այն և միայն այն դեպքում, երբ u-ն բաժանվում է 9-ի:

$a - u = 9l$ հավասարությունից նաև բխում է, որ a-ն կբաժանվի 3-ի (վրա) այն և միայն այն դեպքում, երբ u-ն բաժանվում է 3-ի:

Քանի որ $10 \equiv (-1)(mod\, 11)$, ապա (հետևություն 1.6)՝ $f(10) \equiv f(-1)(mod\, 11)$, այսինքն՝ $a \equiv v(mod\, 11)$, $a - v = 11t$, $t \in \mathbb{N}$: Հետևաբար, a-ն կբաժանվի 11-ի (վրա) այն միայն այն դեպքում, երբ v-ն բաժանվում է 11-ի:

Վերջին պնդման ապացուցման համար բավական է նկատել հետևյալ հավասարությունը՝ $a - a_{s-1}a_{s-2}\ldots a_1a_0 = 10^s \cdot w = 2^s \cdot m, \quad w, m \in \mathbb{N}$:

Սևեռենք $n \geqslant 1$ բնական թիվը և կամայական $a \in \mathbb{Z}$ ամբողջ թվի համար սահմանենք ամբողջ թվերի $[a]$ դասը հետևյալ կերպ՝

$$[a] = \{x \in \mathbb{Z} \mid x \equiv a(mod\, n)\},$$

որը կոչվում է a թվի մնացքների դաս ըստ n հենքի (հենաթվի, մոդուլի) կամ համառոտ՝ a-ի դաս (ըստ n հենքի կամ n-ի): $[a]$ դասը a-ի համարժեքության դասն է ըստ բաղդատման «$\equiv$» համարժեքության:

$[a]$ դասի յուրաքանչյուր տարր կոչվում է այդ դասի ներկայացուցիչ կամ մնացք:

Լեմմ 1.1: *Միևնույն n հենքով մնացքների դասերի համար տեղի ունի հավասարության հետևյալ հայտանիշը՝*

$$[a] = [b] \longleftrightarrow a \equiv b(mod\, n) :$$

Ապացուցում: Բխում է լեմմ 0.2-ից: □

Ակնհայտ է, որ յուրաքանչյուր n մոդուլի համար՝

$$\begin{aligned} &[0] = \{nq \mid q \in \mathbb{Z}\}, \\ &[1] = \{nq + 1 \mid q \in \mathbb{Z}\}, \\ &\ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots \\ &[n-1] = \{nq + (n-1) \mid q \in \mathbb{Z}\}; \end{aligned}$$

Հաճախ $[0], [1], \ldots, [m]$ դասերը համառոտ նշանակվում են՝ $\mathbf{0}, \mathbf{1}, \ldots, \mathbf{m}$:

Լեմմ 1.2: *Ըստ n հենքի $[0], [1], \ldots, [n-1]$ մնացքների դասերը զույգ առ զույգ չեն հատվում և ըստ n հենքի ցանկացած $[a]$ մնացքների դաս համընկնում է նշված դասերից որևէ մեկի հետ:*

Ապացուցում: Պնդման առաջին մասը բխում է թեորեմ 1.1-ի միակության մասից, իսկ երկրորդ մասը՝ թեորեմ 1.1-ի գոյության մասից: Իրոք, եթե $0 \leqslant i, j \leqslant n-1$, $i \neq j$ և $x \in [i] \cap [j]$, ապա $x = nq + i$ և $x = nq' + j$, որը հակասում է թեորեմ 1.1-ի միակության պայմանին: Իսկ, եթե $a = nq + r$, $0 \leqslant r \leqslant n-1$, ապա $a - r = nq$, այսինքն՝ $a \equiv r(mod\, n)$ և հետևաբար $[a] = [r]$ (համաձայն Լեմմ 1.1-ի): □

$[0], [1], \ldots, [n-1]$ դասերից մեկական վերցրած ամբողջ թվերի համակարգը կոչվում է մնացքների լրիվ համակարգ՝ ըստ n հենքի (մոդուլի):

Ընդհանրապես, եթե $a \in \mathbb{Z}$, $n \in \mathbb{N}$, ապա սահմանելով $(n) = \{nt \mid t \in \mathbb{Z}\}$ և $a + (n) = \{a + nt \mid t \in \mathbb{Z}\}$ բազմությունները, կունենանք՝ $[a] = a + (n)$, որտեղ $[a]$-ը a թվի մնացքների դասն է ըստ n հենքի: Նկատենք, որ

$$\mathcal{O}_x = \{x + (n) \mid n \in \mathbb{N}\}$$

բազմությունները ($x \in \mathbb{Z}$) բավարարում են թեորեմ 0.23-ի երեք պայմաններին.

ա) x-ը պատկանում է $\mathcal{O}_x$-ին պատկանող յուրաքանչյուր բազմությանը;

բ) Եթե $U, V \in \mathcal{O}_x$, ապա գոյություն ունի այնպիսի $W \in \mathcal{O}_x$, որ $W \subseteq U \cap V$: Իրոք, եթե $U = x + (n)$ և $V = x + (m)$, ապա $W = x + (mn)$;

գ) Եթե $U \in \mathcal{O}_x$ և $y \in U$, ապա գոյություն ունի $V \in \mathcal{O}_y$ այնպիսին, որ $V \subseteq U$: Իրոք, եթե $U = x + (n)$ և $y = x + nt$, ապա $V = y + (n) \subseteq U$:

Հետևաբար, համաձայն թեորեմ 0.23-ի, գոյություն ունի $\mathbb{Z}$-ի վրա որոշված այնպիսի τ տոպոլոգիա, որ $\mathcal{O}_x \subseteq \tau$ բոլոր $x \in \mathbb{Z}$ ամբողջ թվերի համար: Ընդ որում, $\mathcal{O}_x$-ը կլինի x-ի շրջակայքերի հենք, որը հաշվելի է, իսկ $\beta = \bigcup\limits_{x \in \mathbb{Z}} \mathcal{O}_x$-ը՝ τ տոպոլոգիայի հենք, որը նույնպես հաշվելի է: Այս τ տոպոլոգիան կոչվում է $\mathbb{Z}$-ի **մնացքային** կամ **պոլիադիկ** տոպոլոգիա: $(\mathbb{Z}; \tau)$ տոպոլոգիական տարածությունը մետրիզացվող է:

Իրոք, բավական է ապացուցել, որ այդ տոպոլոգիական տարածությունը նորմալ է և օգտվել թեորեմ 0.26-ից: Իսկ դիտարկվող տոպոլոգիական տարածության նորմալ լինելը ապացուցելու համար, համաձայն թեորեմ 0.25-ի, բավական է ապացուցել, որ այն ռեգուլյար է: Նախ ակնհայտ է, որ

$(\mathbb{Z};\tau)$ տոպոլոգիական տարածությունը T_1-տարածություն է (այն նույնիսկ T_2-տարածություն է): Այնուհետև, քանի որ

$$\mathbb{Z} = \bigcup_{a=0}^{n-1}\{a+(n)\}$$

և բաց բազմությունների միավորումը բաց է, ապա յուրաքանչյուր $x+(n)$ բազմություն կլինի հավասար $n-1$ հատ բաց բազմությունների միավորման լրացմանը ($\mathbb{Z}$-ում) և, հետևաբար, յուրաքանչյուր $x+(n)$ բաց բազմություն նաև փակ է: Ուստի $\mathcal{O}_x$-ը, բոլոր $x\in\mathbb{Z}$ ամբողջ թվերի համար, կազմված է փակ բազմություններից: Մնում է օգտվել թեորեմ 0.24-ից:

Վերնագրի վերջում ապացուցենք նաև հետևյալ արդյունքը, որը հաճախ կիրառվում է այսպես կոչված դիսկրետ լոգարիթմների ուսումնասիրության ժամանակ:

Թեորեմ 1.2*: Դիցուք $r,t\in\mathbb{N}$ և $r^2\geqslant t$: Յուրաքանչյուր $a\in\mathbb{Z}$ ամբողջ թվի համար գոյություն ունեն այնպիսի $x,y\in\mathbb{Z}$ ամբողջ թվեր, որ*

$$a\equiv xr+y(mod\, t),\quad 0\leqslant x<r,\ \ 0\leqslant y<r:$$

Ապացուցում: Թեորեմ 1.1-ի համաձայն՝

$$a=tq+l,\quad 0\leqslant l<t,$$

$$l=xr+y,\quad 0\leqslant y<r:$$

Երկրորդ հավասարությունից բխում է, որ $x\geqslant 0$: Իրոք, եթե $l<r$, ապա $x=0$ և $y=l$, իսկ $l\geqslant r$ դեպքում կունենանք $l>y$ և

$$x=\frac{l-y}{r}>0:$$

Հետևաբար, $a\equiv l(mod\, t)$, այսինքն՝ $a\equiv xr+y(mod\, t)$, որտեղ $0\leqslant y<r$, $0\leqslant \dfrac{y}{r}<1$, $0\leqslant \dfrac{l}{r}=x+\dfrac{y}{r}$ և

$$0\leqslant x\leqslant\frac{l}{r}<\frac{t}{r}\leqslant\frac{r^2}{r}=r: \qquad \square$$

1.3. Գործողություններ մնացքների դասերի հետ

Այժմ սահմանենք միևնույն n հենքով (հենաթվով, մոդուլով) **դասերի գումարման** և **բազմապատկման** (արտադրյալ) հետևյալ գործողությունները՝

$$[a] + [b] = [a + b],$$

$$[a] \cdot [b] = [a \cdot b] \ :$$

Հատկություն 1.3-ից և լեմմ 1.1-ից բխում է, որ սահմանված գործողությունների արժեքները կախված չեն մնացքների դասերում ներկայացուցիչների ընտրությունից, այսինքն, եթե $[a] = [a']$ և $[b] = [b']$, ապա $[a+b] = [a'+b']$ և $[a \cdot b] = [a' \cdot b']$: Իրոք, եթե $[a] = [a']$ և $[b] = [b']$, ապա ըստ լեմմ 1.1-ի՝ $a \equiv a'(mod\, n)$ և $b \equiv b'(mod\, n)$, իսկ ըստ հատկության 1.3-ի՝ $a + b \equiv a' + b'(mod\, n)$ և $a \cdot b \equiv a' \cdot b'(mod\, n)$, հետևաբար ըստ լեմմ 1.1-ի՝ $[a + b] = [a' + b']$ և $[a \cdot b] = [a' \cdot b']$:

Օրինակ, եթե $n = 2$, ապա $[1] + [1] = [0]$, իսկ, եթե $n = 3$, ապա $[1] + [1] = [2]$, $[2] \cdot [2] = [1]$, $\ldots$

Մնացքների դասերի նկատմամբ սահմանված գումարման և բազմապատկման գործողությունները ունեն հետևյալ հատկությունները.

1. Մնացքների դասերի գումարման և բազմապատկման գործողությունները զուգորդական են՝

$$([a] + [b]) + [c] = [a] + ([b] + [c])\,,$$

$$([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])\,;$$

Իրոք՝

$$([a] + [b]) + [c] = [a + b] + [c] = [(a + b) + c] = [a + (b + c)] =$$

$$= [a] + [b + c] = [a] + ([b] + [c]) \ :$$

Նույն եղանակով ստուգվում է մնացքների դասերի բազմապատկման զուգորդականությունը:

2. Մնացքների դասերի գումարման և բազմապատկման գործողությունները տեղափոխական են՝

$$[a] + [b] = [b] + [a],$$

$$[a] \cdot [b] = [b] \cdot [a] \ :$$

3. Մնացքների դասերի գումարը և բազմապատկումը (արտադրյալը) օժտված են միավորով՝

$$[a] + [0] = [0] + [a] = [a],$$

$$[a] \cdot [1] = [1] \cdot [a] = [a] :$$

4. Մնացքների յուրաքանչյուր $[a]$ դաս գումարման նկատմամբ ունի հակադիր՝

$$[a] + [-a] = [-a] + [a] = [0] :$$

Ըստ որում, գումարման զուգորդականությունից բխում է, որ $[a]$ դասի հակադիրը որոշվում է միարժեքորեն և այն նշանակվում է $-[a]$-ով: Այսպիսով՝ $-[a] = [-a]$:

5. Մնացքների դասերի գումարը և բազմապատկումը (արտադրյալը) կապված են ձախ և աջ բաշխական օրենքներով՝

$$[a]\left([b] + [c]\right) = [a][b] + [a][c],$$

$$\left([a] + [b]\right)[c] = [a][c] + [b][c] :$$

Օրինակ: Կազմենք մնացքների դասերի գումարման և բազմապատկման աղյուսակները ըստ $n = 4$ հենքի՝

+	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

·	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Ըստ n հենքի մնացքների դասերի բազմությունը սովորաբար նշանակվում է $\mathbb{Z}_n$-ով կամ $\mathbb{Z}/(n)$-ով՝

$$\mathbb{Z}_n = \{[0], \ldots, [n-1]\} = \mathbb{Z}/(n)$$

$[1]$ դասը կոչվում է **միավոր դաս**, $[0]$ դասը կոչվում է **զրոյական դաս**, հակառակ դեպքում մնացքների դասը կոչվում է **ոչ զրոյական**՝ $[a] \neq [0]$: Որպեսզի $[a] \in \mathbb{Z}_n$ դասը լինի ոչ զրոյական, անհրաժեշտ է և բավարար, որ a-ն չբաժանվի n-ի վրա:

$[a] \in \mathbb{Z}_n$ մնացքների դասը կոչվում է **հակադարձելի** (ըստ n հենքի, հենաթվի, մոդուլի), եթե գոյություն ունի այնպիսի $[a'] \in \mathbb{Z}_n$ մնացքների դաս, որ

$$[a] \cdot [a'] = [a'] \cdot [a] = [1];$$

Այստեղ $[a']$ մնացքների դասը որոշվում է միարժեքորեն, այն կոչվում է $[a]$ դասի **հակադարձ** (դաս) և նշանակվում է՝ $[a'] = [a]^{-1}$: Իրոք, եթե

$$[a] \cdot [a'] = [1]$$

և

$$[a''] \cdot [a] = [1],$$

ապա

$$[a''] = [a''] \cdot [1] = [a''] \left([a] \cdot [a']\right) = \left([a''] \cdot [a]\right) \cdot [a'] = [1] \cdot [a'] = [a'] :$$

Որպես հակադարձելի մնացքների դասերի ակնհայտ օրինակներ նշենք $[1]$ և $[n-1]$ դասերը; Իրոք՝

$$[1] \cdot [1] = [1],$$

$$[n-1] \cdot [n-1] = [(n-1)(n-1)] =$$
$$= \left[n^2 - 2n + 1\right] = \left[n^2 - 2n\right] + [1] = [0] + [1] = [1],$$

այսինքն՝

$$[1]^{-1} = [1]$$

և

$$[n-1]^{-1} = [n-1];$$

Մասնավորապես, կարելի է ասել, որ, օրինակ, $n = 3$ դեպքում $\mathbb{Z}_n$-ի յուրաքանչյուր ոչ զրոյական տարր հակադարձելի է, որովհետև այդ դեպքում $\mathbb{Z}_n$-ը ունի ընդամենը երկու ոչ զրոյական տարրեր՝ $[1]$ և $[2] = [n-1]$ մնացքների դասերը, որոնք ինչպես նկատեցինք հակադարձելի են:

Եթե $n > 1$, ապա $[0] \in \mathbb{Z}_n$ զրոյական դասը հակադարձելի չէ, որովհետև $n > 1$ դեպքում $[0] \neq [1]$ և ենթադրելով զրոյական դասի հակադարձելի լինելը, հանգում ենք հակասության՝

$$[0] \cdot [b] = [1],$$

$$[0 \cdot b] = [1],$$

$$[0] = [1];$$

Իսկ եթե $n = 1$, ապա $[0] = [1]$ և հետևաբար զրոյական դասը կլինի հակադարձելի:

Հատկություն 1.4: *ա) Եթե* $[a], [b] \in Z_n$ *մնացքների դասերը հակադարձելի են, ապա դրանց* $[a] \cdot [b] \in \mathbb{Z}_n$ *արտադրյալը նս կլինի հակադարձելի և արտադրյալի հակադարձը հավասար է արտադրիչների հակադարձների արտադրյալին:*

բ) Եթե $[a] \in \mathbb{Z}_n$ *մնացքների դասը հակադարձելի է , ապա* $[a]^{-1} \in \mathbb{Z}_n$ *մնացքների դասը նս կլինի հակադարձելի, ընդ որում՝*

$$\left([a]^{-1}\right)^{-1} = [a]:$$

Ապացուցում: ա) Եթե $[a] \cdot [a'] = [1]$ և $[b] \cdot [b'] = [1]$, ապա մնացքների դասերի բազմապատկման զուգորդականության համաձայն՝

$$([a] \cdot [b])([b'] \cdot [a']) = [a] \cdot ([b] \cdot ([b'] \cdot [a'])) =$$

$$= [a] \cdot (([b] \cdot [b']) \cdot [a']) = [a] \cdot ([1] \cdot [a']) = [a] \cdot [a'] = [1];$$

բ) պնդումը բխում է հակադարձի սահմանումից: □

$\mathbb{Z}_n$-ի բոլոր հակադարձելի դասերի (տարրերի) բազմությունը սովորաբար նշանակվում է $\mathbb{Z}_n^*$-ով:

1.4. Զուգորդական գործողություն և ընդհանրացված զուգորդականություն

Կասենք, որ $Q \neq \emptyset$ բազմության մեջ սահմանված (կամ տրված, որոշված) է գործողություն, եթե Q-ից վերցված կամայական x, y տարրերի (x, y) կարգավորված զույգին համապատասխանության մեջ է դրված միարժեքորեն որոշվող $z \in Q$ տարր, այսինքն՝ տրված է որևէ արտապատկերում՝ $Q \times Q$ դեկարտյան արտադրյալից Q բազմության մեջ: Սովորաբար գործողության համար օգտագործվում են արտադրյալային $\circ$, $*$, $\cdot$, $\times$, $\otimes$, $\boxtimes$, $\ldots$ կամ գումարային $+$, $\#$, $\oplus$, $\boxplus$, $\ldots$ նշանակումներ (գրելաձևեր): Առաջին դեպքում z-ը կոչվում է x և y տարրերի արտադրյալ (բազմապատկում) և համապատասխանաբար գրվում է՝ $z = x \circ y$, $z = x * y$, $z = x \cdot y$, ... Այս դեպքում x, y-ը կոչվում են արտադրիչներ: Երկրորդ դեպքում z-ը կոչվում է x և y տարրերի գումար և համապատասխանաբար գրվում է՝ $z = x + y$, $z = x\#y$, $z = x \oplus y$, ... Այս դեպքում x, y-ը կոչվում են գումարելիներ:

Եթե Q բազմության մեջ սահմանված է $\circ$ գործողություն, ապա օգտվելով փակագծերից կարելի է կազմել Q բազմության նաև վերջավոր թվով տարրերի արտադրյալներ: Օրինակ, $x \circ (y \circ z)$, $x \circ (y \circ (z \circ u))$, $x \circ ((y \circ z) \circ u)$, ...

Կասենք, որ Q բազմության մեջ սահմանված $\circ$ գործողությունը օժտված է միավորով, եթե գոյություն ունի այնպիսի $e \in Q$ տարր, որ $x \circ e = e \circ x = x$ ցանկացած $x \in Q$ տարրի համար: Ակնհայտ է, որ գոյության դեպքում e տարրը որոշվում է միարժեքորեն և այն կոչվում է $\circ$ գործողության միավոր: Իրոք, եթե $e_1, e_2 \in Q$ տարրերը բավարարում են $x \circ e_1 = e_1 \circ x = x$ և $x \circ e_2 = e_2 \circ x = x$ պայմաններին՝ ցանկացած $x \in Q$ տարրի դեպքում, ապա առաջին հավասարության մեջ տեղադրելով $x = e_2$, կստանանք՝ $e_1 \circ e_2 = e_2$, իսկ երկրորդում տեղադրելով $x = e_1$, ստանում ենք՝ $e_1 \circ e_2 = e_1$: Հետևաբար՝ $e_1 = e_1 \circ e_2 = e_2$:

Q բազմության մեջ սահմանված (կամ տրված) գործողությունը համառոտ կոչվում է նաև այդ բազմության գործողություն:

Q բազմության $\circ$ գործողությունը կոչվում է զուգորդական, եթե այն բավարարում է զուգորդական (զուգորդականության) օրենքին (նույնությանը)՝

$$(x \circ y) \circ z = x \circ (y \circ z)$$

ցանկացած $x, y, z \in Q$ տարրերի համար: Հակառակ դեպքում Q բազմության $\circ$ գործողությունը կոչվում է ոչ զուգորդական:

Օրինակ, ամբողջ (ռացիոնալ, իրական) թվերի գումարը և արտադրյալը զուգորդական են, մնացքների դասերի գումարը և արտադրյալը զուգորդական են: Առաջին դեպքում $Q = \mathbb{Z}$ (համապատասխանաբար $\mathbb{Q}$, $\mathbb{R}$), իսկ երկրորդ օրինակում՝ $Q = \mathbb{Z}_n$: Ամբողջ (ռացիոնալ, իրական) թվերի հանումը արդեն զուգորդական չէ: Երկու իրական թվերի միջին թվաբանականը ևս զուգորդական չէ, այսինքն՝ $\mathbb{R}$-ի մեջ սահմանված $\circ$ գործողությունը, որտեղ $x \circ y = \dfrac{x+y}{2}$, զուգորդական չէ: Սակայն հանումը և միջին թվաբանականը բավարարում են հետևյալ նույնությանը՝

$$(x \circ y) \circ (u \circ v) = (x \circ u) \circ (y \circ v) :$$

Բոլոր ոչ զրոյական ռացիոնալ (իրական) թվերի բազմության մեջ սահմանված բաժանման գործողությունը ևս զուգորդական չէ: Հետաքրքրական է, որ այն նույնպես բավարարում է

$$(x \circ y) \circ (u \circ v) = (x \circ u) \circ (y \circ v)$$

նույնությանը:

Զուգորդական օրենքի շնորհիվ $(x \circ y) \circ z = x \circ (y \circ z)$ տարրը կարելի է գրել առանց փակագծերի՝ $x \circ y \circ z$: Նույն պատճառով, եթե Q բազմության $\circ$ գործողությունը զուգորդական է, ապա Q բազմության կամայական x_1, x_2, x_3, x_4 տարրերի հաջորդականությունից փակագծերի տարբեր դասավորությամբ կազմված բոլոր 5 արտադրյալները կլինեն միմյանց հավասար՝

$$((x_1 \circ x_2) \circ x_3) \circ x_4 = (x_1 \circ (x_2 \circ x_3)) \circ x_4 = x_1 \circ ((x_2 \circ x_3) \circ x_4) =$$

$$= x_1 \circ (x_2 \circ (x_3 \circ x_4)) = (x_1 \circ x_2) \circ (x_3 \circ x_4):$$

Կարելի է ապացուցել, որ $x_1, x_2, \ldots, x_n$ հաջորդականությունից փակագծերի տարբեր դասավորությամբ ստացվող բոլոր հնարավոր արտադրյալների թիվը հավասար է՝ $\frac{1}{n}\left(\begin{array}{c} 2n-2 \\ n-1 \end{array}\right)$, որտեղ $\left(\begin{array}{c} m \\ k \end{array}\right) = \frac{m(m-1)(m-2)\ldots(m-k+1)}{k!}$, իսկ $k! = 1 \cdot 2 \cdot\ \ldots\ \cdot k$, $1 \leqslant k \leqslant m$:

$\left(\begin{array}{c} m \\ k \end{array}\right)$ թիվը նշանակվում է նաև C_m^k-ով և կոչվում է զուգորդություն m տարրերից k-ական կամ Նյուտոնի երկանդամային գործակից:

$a_n = \frac{1}{n}\left(\begin{array}{c} 2n-2 \\ n-1 \end{array}\right)$ թիվը կոչվում է Քաթալանի n-րդ թիվ (E. C. Catalan (1814-1894)) և հաճախ է հանդիպում հետազոտություններում[4]: Մասնավորապես՝

$$a_3 = \frac{1}{3} \cdot \left(\begin{array}{c} 4 \\ 2 \end{array}\right) = \frac{1}{3} \cdot \frac{4 \cdot 3}{1 \cdot 2} = 2,$$

[4] Հայտնի է նաև Քաթալանի հետևյալ խնդիրը (1844 թ.). ապացուցել, որ 0,1 և 8, 9 զույգերը ամբողջ հաջորդական թվերի միակ զույգերն են, որոնք հանդիսանում են ամբողջ թվերի մեկից մեծ աստիճաններ (P. Ribenboim, Catalan's conjecture, Amer. Math. Monthly, 103(1996), p.p. 529–538): Այս խնդիրը լուծվել է վերջերս (P. Mihailescu, 2002):

$$a_4 = \frac{1}{4} \cdot \left(\begin{array}{c} 6 \\ 3 \end{array} \right) = \frac{1}{4} \cdot \frac{6 \cdot 5 \cdot 4}{1 \cdot 2 \cdot 3} = 5,$$

$$a_5 = \frac{1}{5} \cdot \left(\begin{array}{c} 8 \\ 4 \end{array} \right) = \frac{1}{5} \cdot \frac{8 \cdot 7 \cdot 6 \cdot 5}{1 \cdot 2 \cdot 3 \cdot 4} = 14 :$$

Հետևյալ արդյունքը կոչվում է զուգորդական գործողության ընդհանրացված զուգորդական օրենք (նույնություն):

Թեորեմ 1.3: *Եթե $Q \neq \emptyset$ բազմության $\circ$ գործողությունը զուգորդական է, ապա Q բազմության կամայական $x_1, \ldots, x_n$ տարրերի հաջորդականությունից փակագծերի տարբեր դասավորությամբ ստացվող բոլոր արտադրյալները միմյանց հավասար են և այդ պատճառով էլ այդ արտադրյալներից յուրաքանչյուրը կարելի է գրել առանց փակագծերի՝ $x_1 \circ x_2 \circ \cdots \circ x_n$, որտեղ $n \geqslant 3$:*

Ապացուցում: Նախ $n \geqslant 2$ դեպքում ներմուծենք $y_1, y_2, \ldots, y_n \in Q$ հաջորդականության, այսպես կոչված, կանոնական արտադրյալը, հետևյալ կերպ՝

$$(\cdots((y_1 \circ y_2) \circ y_3) \circ \cdots \circ y_{n-1}) \circ y_n;$$

Այժմ վերհանգման եղանակով ապացուցենք, որ $n \geqslant 3$ դեպքում տրված $x_1, \ldots, x_n$ հաջորդականությունից փակագծերի տարբեր դասավորությամբ ստացվող յուրաքանչյուր արտադրյալ հավասար է դրանց կանոնական արտադրյալին:

Իրոք, $n = 3$ դեպքում կունենանք ընդամենը երկու արտադրյալներ, մեկը կանոնականն է՝ $(x_1 \circ x_2) \circ x_3$, իսկ մյուսը՝ $x_1 \circ (x_2 \circ x_3)$, որոնք հավասար են՝ շնորհիվ $\circ$ գործողության զուգորդականության պայմանի: Ենթադրելով ձևակերպված պնդումը ճիշտ n-ից քիչ թվով արտադրիչների դեպքում, դիտարկենք $x_1, \ldots, x_n$ հաջորդականությունից փակագծերի կամայական դասավորությամբ կազմված արտադրյալ՝

$$(x_1 \circ \ldots \circ x_k) \circ (x_{k+1} \circ \ldots \circ x_n) :$$

Նշված առաջին՝ $x_1 \circ \ldots \circ x_k$ և երկրորդ՝ $x_{k+1} \circ \ldots \circ x_n$ արտադրյալները գրված են առանց փակագծերի, որովհետև դրանցից յուրաքանչյուրում արտադրիչների թիվը փոքր է n-ից և ըստ կատարված ենթադրության, դրանցից յուրաքանչյուրը, առնվազն երկու արտադրիչ պարունակելու դեպքում, կլինի հավասար համապատասխան կանոնական արտադրյալին, և հետևաբար կախված չէ փակագծերի դասավորությունից:

Քննարկենք հետևյալ երկու ենթադեպքերը՝

ա) $k = n-1$, այսինքն՝ երկրորդ արտադրյալը մեկ տարրանի է: Կատարված վերհանգման ենթադրության համաձայն $n-1$ թվով արտադրիչների $x_1 \circ \cdots \circ x_{n-1}$ արտադրյալը հավասար է կանոնականին, իսկ կանոնական արտադրյալը, աջից բազմապատկելով x_n-ով նորից ստանում ենք կանոնական արտադրյալ:

բ) $1 \leqslant k < n-1$ և հետևաբար երկրորդ՝ $x_{k+1} \circ \ldots \circ x_n$ արտադրյալը կպարունակի առնվազն երկու արտադրիչներ:

Ըստ կատարված վերհանգման ենթադրության, նախ $x_{k+1} \circ \ldots \circ x_n$ արտադրյալը կլինի հավասար համապատասխան կանոնականին և այնուհետև օգտվելով $\circ$ գործողության զուգորդականությունից կունենանք՝

$$(x_1 \circ \ldots \circ x_k) \circ (x_{k+1} \circ \ldots \circ x_n) = (x_1 \circ \ldots \circ x_k) \circ ((x_{k+1} \circ \ldots \circ x_{n-1}) \circ x_n) =$$

$$((x_1 \circ \ldots \circ x_k) \circ (x_{k+1} \circ \ldots \circ x_{n-1})) \circ x_n;$$

Մնում է $n-1$ արտադրիչների

$$(x_1 \circ \ldots \circ x_k) \circ (x_{k+1} \circ \ldots \circ x_{n-1})$$

արտադրյալը գրել համապատասխան կանոնական տեսքով: □

Մասնավորապես՝

$$[a_1] + \cdots + [a_n] = [a_1 + \cdots + a_n],$$

$$[a_1] \cdot [a_2] \cdots [a_n] = [a_1 a_2 \cdots a_n]$$

ցանկացած $[a_1], \ldots, [a_n]$ մնացքների դասերի համար՝ ըստ մոդուլ m-ի:

Եթե (ոչ դատարկ) Q բազմության $\circ$ գործողությունը զուգորդական է, ապա դրան համապատասխան կարելի է սահմանել Q բազմության ցանկացած տարրի ցանկացած բնական ցուցիչով աստիճանը հետևյալ կերպ՝

$$a^n = \underbrace{a \circ \cdots \circ a}_{n},$$

որտեղ $a \in Q$, $n \geqslant 1$ (կարդացվում է a-ի n աստիճան կամ n-րդ աստիճան): Եթե Q բազմության $\circ$ գործողությունը օժտված է e միավորով, ապա ընդունվում է նաև $a^\circ = e$ ցանկացած $a \in Q$ տարրի համար: Հետևյալ երկու հավասարություններն (նույնություններն) ակնհայտ են՝

$$a^n \circ a^m = a^{n+m},$$

$$(a^n)^m = a^{n \cdot m}$$

ցանկացած $a \in Q$ տարրի և ցանկացած $n, m \in \mathbb{N}$ բնական թվերի համար:

Գումարային գրելաձևի ժամանակ e միավորը նշանակվում է 0-ով, a^n-ի փոխարեն գրվում է na և կարդացվում է a-ի n-պատիկ, իսկ նշված համապատասխան հավասարություններն այդ դեպքում կլինեն՝

$$0a = 0,$$

$$na + ma = (n+m)a,$$

$$m(na) = (m \cdot n)a;$$

Օրինակ, $n[a] = [0]$, որտեղ $[a]$-ն ցանկացած մնացքների դաս է՝ ըստ մոդուլ n-ի: Ընդ որում, n-ը նշված հատկությամբ օժտված ամենափոքր ամբողջ դրական թիվն է: Իրոք՝

$$n[a] = \underbrace{[a] + \cdots + [a]}_{n} = [\underbrace{a + \cdots + a}_{n}] = [na] = [0];$$

Եթե $s \in \mathbb{N}$, $0 < s < n$, ապա

$$s[1] = \underbrace{[1] + \cdots + [1]}_{s} = [\underbrace{1 + \cdots + 1}_{s}] = [s] \neq [0];$$

Նմանատիպ հարցի քննարկումը մնացքների դասերի արտադրյալի տեսանկյունից ($[a]^s = [1]$) բերում է Լ. Էյլերի և Պ. Ֆերմայի թեորեմներին (գլուխ 9), իսկ ընդհանուր դեպքում՝ խմբերի տեսության Ժ. Լագրանժի թեորեմին (գլուխ 18): Սակայն համարվում է, որ պատմականորեն խմբի գաղափարը ծագել է բարձր աստիճանի հանրահաշվական հավասարումները արմատանշաններով լուծելու խնդրից (Ա. Ռուֆֆինի, Ն. Աբել, Է. Գալուա, Ա. Լ. Կոշի, Լ. Սիլով, . . .): Մինչդեռ բաղդատումները դիտարկվել են հին Չինաստանում (դեռևս մեր թվարկության I դարում), որոնք նույնպես հանգեցնում են վերջավոր խմբի գաղափարին:

Վարժություններ և խնդիրներ

1. Ապացուցել, որ ցանկացած $4t+3$ տեսքի ամբողջ թիվ հնարավոր չէ ներկայացնել երկու ամբողջ թվերի քառակուսիների գումարով:

   Եթե n_1 և n_2 բնական թվերից յուրաքանչյուրը ներկայացվում է երկու ամբողջ թվերի քառակուսիների գումարով, ապա դրանց $n_1 \cdot n_2$ արտադրյալը ևս օժտված է այդ հատկությամբ (Diophantus): Նույն պնդումը տեղի ունի նաև չորս ամբողջ թվերի քառակուսիների գումարի համար (Euler, 1743):

   (Ցուցում. եթե $n_1 = x_1^2 + y_1^2$, $n_2 = x_2^2 + y_2^2$, ապա $n_1 \cdot n_2 = (x_1x_2 + y_1y_2)^2 + (x_1y_2 - y_1x_2)^2$):

2. Դիցուք ցանկացած $a > b > 0$ ամբողջ թվերի համար՝

$$r_0 = a, \ \ r_1 = b, \ \ r_{k+1} = r_{k-1} (mod\, r_k),$$

   այսինքն՝

$$r_{k-1} = q_k r_k + r_{k+1},$$

   որտեղ $r_k \neq 0$, $k = 1, 2, \ldots, n$, և $r_0 > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$: Ապացուցել, որ $q_k \geqslant 1$, որտեղ $k = 1, \ldots, n-1$, իսկ $q_n \geqslant 2$:

3. Լուծել հետևյալ համակարգերը՝

$$\begin{cases} 1 \equiv x (mod\, 2), \\ 1 \equiv x (mod\, 3), \end{cases}$$

   ամբողջ թվերով ($x \in \mathbb{Z}$): Նույն համակարգերը լուծել նաև բնական թվերով ($x \in \mathbb{N}$):

4. Լուծել հետևյալ համակարգը՝

$$\begin{cases} 1 \equiv x (mod\, 2), \\ 1 \equiv x (mod\, 3), \\ 1 \equiv x (mod\, 5), \end{cases}$$

   ամբողջ թվերով ($x \in \mathbb{Z}$): Նույն համակարգերը լուծել նաև բնական թվերով ($x \in \mathbb{N}$):

5. Ապացուցել, որ
$$1+2+3+\cdots+(n-1)\equiv 0(mod\, n)$$
այն և միայն այն դեպքում, երբ n-ը կենտ է:

6. Ապացուցել, որ
$$1^2+2^2+3^2+\cdots+(n-1)^2\equiv 0(mod\, n)$$
այն և միայն այն դեպքում, երբ
$$n\equiv \pm 1(mod\, 6)$$
(Fibonacci): (Ցուցում. Ապացուցվելիք բաղդատման ձախ մասը հավասար է՝ $\dfrac{(n-1)n(2n-1)}{6}$):

7. Ապացուցել, որ
$$1^3+2^3+3^3+\cdots+(n-1)^3\equiv 0(mod\, n)$$
այն և միայն այն դեպքում, երբ
$$n\not\equiv 2(mod\, 4)$$
(Aryabhata, Bachet): (Ցուցում. Ապացուցվելիք բաղդատման ձախ մասը հավասար է՝ $\left(\dfrac{(n-1)n}{2}\right)^2$):

8. Որոշել $\mathbb{Z}_4$ բազմությանը պատկանող բոլոր հակադարձելի մնացքների դասերը:

9. Ապացուցել, որ $\mathbb{Z}_5$ բազմությանը պատկանող յուրաքանչյուր ոչ զրոյական մնացքների դաս հակադարձելի է:

10. Գտնել 3^{97} թվի վերջին թվանշանը: (Ցուցում. $3^{97}=\left(3^4\right)^{24}\cdot 3\equiv 1^{24}\cdot 3(mod\, 10)$):

11. Ապացուցել, որ $5^{2n}+3\cdot 2^{5n-2}$ թիվը բաժանվում է 7-ի վրա $(n\in\mathbb{N})$:

12. Ապացուցել, որ $3^{n+2}+4^{2n+1}$ թիվը բաժանվում է 13-ի վրա $(n\in\mathbb{N})$:

13. Ապացուցել, որ $5^{2n}+7$ թիվը բաժանվում է 8-ի վրա $(n\in\mathbb{N})$:

14. Ապացուցել, որ $3^{3n+1}+2^{n+1}$ թիվը բաժանվում է 5-ի վրա $(n\in\mathbb{N})$:

15. Ներկայացնել $(201201)_3$ թիվը 10-ական համակարգում:

16. Որոշել $1!+2!+\cdot+100!$ թիվը 15-ի վրա բաժանելուց ստացվող մնացորդը: (Ցուցում. $5!\equiv 0(mod\, 15)$):

17. Դիցուք τ-ն $\mathbb{Z}$-ի մնացքային տոպոլոգիան է, $a\in\mathbb{Z}$, իսկ

$$x_n = a+n!, \quad n\geqslant 1:$$

Ապացուցել, որ $(\mathbb{Z};\tau)$ տոպոլոգիական տարածության մեջ՝

$$\lim_{n\to\infty} x_n = a,$$

մասնավորապես՝

$$\lim_{n\to\infty} n! = 0:$$

Այստեղից բխեցնել, որ τ տոպոլոգիան դիսկրետ չէ:

18. Ապացուցել, որ $(\mathbb{Z};\tau)$ տոպոլոգիական տարածությունը Հաուսդորֆյան է:

19. Ապացուցել, որ (բաց) բազմությունների

$$\alpha=\{i+(n!)\mid n\in\mathbb{N},\, 0\leqslant i\leqslant n!-1\}$$

համախումբը կազմում է $(\mathbb{Z};\tau)$ տոպոլոգիական տարածության հենք: Եթե այդ հենքի երկու բաց բազմություններ հատվում են, ապա դրանցից մեկը պարունակում է մյուսին:

20. Ապացուցել, որ $(\mathbb{Z};\tau)$ տոպոլոգիական տարածության մեջ $\sum\limits_{n=1}^{\infty} n\cdot n!$ և $\sum\limits_{n=1}^{\infty}(n^2+1)n!$ շարքերը զուգամետ են և ունեն հետևյալ գումարները՝

$$\sum_{n=1}^{\infty} n\cdot n! = -1,$$

$$\sum_{n=1}^{\infty}(n^2+1)n! = 0 :$$

Ընդ որում, $x \in \mathbb{Z}$ թիվը կոչվում է $\sum\limits_{n=1}^{\infty} a_n$ շարքի գումար ($a_n \in \mathbb{Z}$) $(\mathbb{Z};\tau)$ տոպոլոգիական տարածության մեջ և գրվում է $x = \sum\limits_{n=1}^{\infty} a_n$, եթե $(\mathbb{Z};\tau)$ տոպոլոգիական տարածության մեջ՝

$$x = \lim_{x\to\infty} x_n,$$

որտեղ $x_n = a_1 + \cdots + a_n$ (շարքը կոչվում է զուգամետ, եթե այն ունի գումար):

Գ լ ու խ 2

ԵՐԿՈՒ ԱՄԲՈՂՋ ԹՎԵՐԻ ԱՄԵՆԱՄԵԾ ԸՆԴՀԱՆՈՒՐ ԲԱԺԱՆԱՐԱՐԸ: ԷՎԿԼԻԴԵՍԻ ԱԼԳՈՐԻԹՄԸ: ՖԻԲՈՆԱՉԻԻ ՀԱՋՈՐԴԱԿԱՆՈՒԹՅՈՒՆԸ

Եթե c ամբողջ թիվը միաժամանակ բաժանարար է a և b ամբողջ թվերի համար, ապա c-ն կոչվում է a և b ամբողջ թվերի **ընդհանուր բաժանարար**: Ընդհանուր բաժանարարներից ամենամեծը, եթե այն գոյություն ունի, կոչվում է a և b ամբողջ թվերի **ամենամեծ ընդհանուր բաժանարար** և նշանակվում է ԱԸԲ (a, b)-ով կամ համառոտ՝ (a, b)-ով: Ակնհայտ է, որ եթե (a, b)-ն գոյություն ունի, ապա այն կլինի բնական թիվ, որովհետև 1-ը լինելով ընդհանուր բաժանարար ցանկացած ամբողջ a-ի և b-ի համար, կունենանք՝ $(a, b) \geqslant 1$: Այսպիսով, d բնական թիվը կոչվում է a և b ամբողջ թվերի ամենամեծ ընդհանուր բաժանարար, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա) d-ն ընդհանուր բաժանարար է a-ի և b-ի համար,

բ) եթե c-ն a-ի և b-ի ցանկացած ընդհանուր բաժանարար է, ապա $c \leqslant d$;

Սահմանումից բխում է ամենամեծ ընդհանուր բաժանարարի միակությունը, եթե այն գոյություն ունի: Մյուս ակնհայտ հատկությունը՝ ամենամեծ ընդհանուր բաժանարարի տեղափոխական հատկությունն է՝ $(a, b) = (b, a)$: Ավելի ճիշտ, եթե գոյություն ունի a և b ամբողջ թվերի (a, b) ամենամեծ ընդհանուր բաժանարարը, ապա գոյություն կունենա նաև b և a ամբողջ թվերի (b, a) ամենամեծ ընդհանուր բաժանարարը և դրանք կլինեն հավասար:

Հատկություն 2.1: *a և b ամբողջ թվերի (a, b) ամենամեծ ընդհանուր բաժանարարը գոյություն կունենա այն և միայն այն դեպքում, երբ a-ն և b-ն միաժամանակ զրո չեն, այսինքն երբ $a^2 + b^2 \neq 0$:*

Ապացույց: Եթե $a = 0$ և $b = 0$, ապա դրանց ընդհանուր բաժանարարների բազմությունը կհամընկնի բոլոր ամբողջ թվերի $\mathbb{Z}$ բազմության հետ, որը չունի ամենամեծ տարր:

Դիցուք $a^2 + b^2 \neq 0$, այսինքն կամ $a \neq 0$ կամ $b \neq 0$: Ենթադրելով $a \neq 0$, կարող ենք ասել, որ a և b ամբողջ թվերի յուրաքանչյուր c ընդհանուր բաժանարար բավարարում է $|c| \leqslant |a|$ անհավասարությանը (հատկություն 8°, գլուխ 1): Այսպիսով, եթե $a \neq 0$, ապա $-|a| \leqslant c \leqslant |a|$, այսինքն a և b ամբողջ թվերի (բոլոր) ընդհանուր բաժանարարի բազմությունը կլինի ամբողջ թվերի վերջավոր բազմություն և հետևաբար այն կպարունակի ամենամեծ տարր: Նույն արդյունքին ենք հանգում նաև $b \neq 0$ դեպքում: □

Օրինակ, եթե $a^2+b^2 \neq 0$ և a-ն բաժանվում է b-ի վրա, ապա $(a,b) = |b|$, որտեղ $a, b \in \mathbb{Z}$: Մասնավորապես, եթե $a \neq 0$, ապա $(a,a) = |a|$:

Անցնենք ամենամեծ ընդհանուր բաժանարարի հիմնական հատկություններից մեկի ապացուցմանը:

Թեորեմ 2.1: *$a^2+b^2 \neq 0$ պայմանին բավարարող ցանկացած a և b ամբողջ թվերի համար գոյություն ունեն այնպիսի u և v ամբողջ թվեր, որ*

$$(a,b) = au + bv\,,$$

որտեղ u, v ամբողջ թվերը կոչվում են a, b զույգի Բեզուի գործակիցներ: Ավելի ճիշտ՝

$$(a,b) = \min\{ax+by \mid\ x,y \in \mathbb{Z},\ ax+by > 0\}\ :$$

Ապացուցում: Դիտարկենք ամբողջ թվերի հետևյալ բազմությունը՝

$$M = \{ax+by \mid\ x,y \in \mathbb{Z}\}\ :$$

Այս բազմության մեջ կան նաև դրական ամբողջ թվեր (օրինակ՝ $ax+by$-ը, երբ $x=a$, $y=b$):

Նշանակելով M-ին պատկանող ամբողջ և դրական թվերի փոքրագույն տարրը d-ով, կունենանք $d>0$ և

$$d = au + bv,$$

որտեղ $u, v \in \mathbb{Z}$: Ապացուցենք $d = (a,b)$ հավասարությունը, այսինքն, որ տեղի ունեն հետևյալ երկու պայմանները՝

ա) d-ն a-ի և b-ի համար ընդհանուր բաժանարար է;

բ) եթե c-ն a-ի և b-ի ցանկացած ընդհանուր բաժանարար է, ապա $c \leqslant d$:

Համաձայն մնացորդով բաժանման կանոնի՝

$$a = dq + r, \quad 0 \leqslant r < d;$$

Եթե այստեղ ենթադրենք $r \neq 0$, ապա կունենանք $0 < r < d$ և

$$r = a - dq = a - (au + bv)q = a(1 - uq) + b(-vq) \in M:$$

Այսպիսով՝ $r \in M$ և $0 < r < d$, որը հակասում է d-ի ընտրությանը: Ստացված հակասությունը նշանակում է, որ $r \neq 0$ ենթադրությունը սխալ է: Ուստի $r = 0$ և $a = dq$, այսինքն a-ն բաժանվում է d-ի վրա: Նման եղանակով ստանում ենք նաև, որ b-ն ևս բաժանվում է d-ի վրա:

Դիցուք c-ն a-ի և b-ի համար ընդհանուր բաժանարար է: Եթե $c < 0$, ապա $c < d$: Հետևաբար, կարող ենք ենթադրել, որ $c > 0$: Քանի որ $a = c \cdot a_1$ և $b = c \cdot b_1$, ապա ելնելով $d = au + bv$ հավասարությունից կստանանք, որ d-ն բաժանվում է c-ի վրա: Ուստի, $d \geqslant c$ (համաձայն գլուխ 1-ի հատկություն 8°-ի): □

Հետևություն 2.1: *Եթե $a^2 + b^2 \neq 0$, ապա a և b ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարը բաժանվում է a-ի և b-ի բոլոր ընդհանուր բաժանարարների վրա:*

Ապացուցում: Բխում է թեորեմ 2.1-ում ապացուցած $(a, b) = au + bv$ ներկայացումից: □

Հետևություն 2.2: *Որպեսզի $ax + by = c$ հավասարումն ($a^2 + b^2 \neq 0$, $a, b, c \in \mathbb{Z}$) ունենա ամբողջ թվերով լուծում անհրաժեշտ է և բավարար, որ c-ն բաժանվի (a, b)-ի վրա:*

Ապացուցում: Եթե $d = (a, b)$ և $ax + by = c$ հավասարումն ունի ամբողջ թվերով լուծում $(x, y \in \mathbb{Z})$, ապա c-ն կբաժանվի d-ի վրա, որովհետև d-ի վրա բաժանվում են a-ն ու b-ն: Եվ հակառակը, եթե c-ն բաժանվում է d-ի վրա, այսինքն $c = d \cdot k$, որտեղ $k \in \mathbb{Z}$, ապա համաձայն թեորեմ 2.1-ի, $c = d \cdot k = (au + bv)k = auk + bvk = ax + by$, որտեղ $x, y \in \mathbb{Z}$, որովհետև $x = uk$, $y = vk$: □

Դիտողություն: Հետևյալ հավասարությունից՝

$$au + bv = \left(u - k\frac{b}{d}\right)a + \left(v + k\frac{a}{d}\right)b, \quad k \in \mathbb{Z}, \ d = (a, b),$$

բխում է, որ տրված a, b զույգի Բեզուի գործակիցները չեն որոշվում միարժեքորեն: Հետևաբար, եթե c-ն բաժանվում է d-ի վրա, ապա $c = ax + by$ հավասարումը կունենա անվերջ թվով (x, y) լուծումներ, որտեղ $x, y \in \mathbb{Z}$: Մասնավորապես, եթե $(a, b) = 1$, ապա ցանկացած $c \in \mathbb{Z}$ թվի համար

$$ax + by = c$$

հավասարումը կունենա անվերջ թվով (x, y) լուծումներ, որտեղ $x, y \in \mathbb{Z}$:

Հատկություն 2.2*: a և b ամբողջ թվերի ընդհանուր բաժանարարների բազմությունը համընկնում է*

ա) a և $-b$ ամբողջ թվերի ընդհանուր բաժանարարների բազմության հետ: Հետևաբար, $(a, -b)$-ն գոյություն կունենա այն և միայն այն դեպքում, երբ գոյություն ունի (a, b)-ն, ընդ որում `

$$(a, b) = (a, -b);$$

բ) a և $|b|$ ամբողջ թվերի ընդհանուր բաժանարարների բազմության հետ: Հետևաբար, $(-a, b)$-ն գոյություն կունենա այն և միայն այն դեպքում, երբ գոյություն ունի (a, b)-ն, ընդ որում՝

$$(a, b) = (-a, b);$$

գ) $-a$ և b ամբողջ թվերի ընդհանուր բաժանարարների բազմության հետ: Հետևաբար, $(-a, b)$-ն գոյություն կունենա այն և միայն այն դեպքում, երբ գոյություն ունի (a, b)-ն, ընդ որում՝

$$(a, b) = (-a, b);$$

դ) $|a|$ և $-b$ ամբողջ թվերի ընդհանուր բաժանարարների բազմության հետ: Հետևաբար, $(-a, -b)$-ն գոյություն կունենա այն և միայն այն դեպքում, երբ գոյություն ունի (a, b)-ն, ընդ որում՝

$$(a, b) = (-a, -b);$$

ե) $-a$ և $-b$ ամբողջ թվերի ընդհանուր բաժանարարների բազմության հետ: Հետևաբար, $(-a, -b)$-ն գոյություն կունենա այն և միայն այն դեպքում, երբ գոյություն ունի (a, b)-ն, ընդ որում՝

$$(a, b) = (-a, -b);$$

գ) $|a|$ և $|b|$ ամբողջ թվերի ընդհանուր բաժանարարների բազմության հետ: Հետևաբար, $(|a|, |b|)$-ն գոյություն կունենա այն և միայն այն դեպքում, երբ գոյություն ունի (a, b)-ն, ընդ որում՝

$$(a, b) = (|a|, |b|) :$$

Ապացուցում: Ապացուցենք, օրինակ, հատկության գ) մասը: գ) հատկության երկրորդ մասը բխում է դրա առաջին մասից: Իսկ առաջին մասի պնդումը բխում է հավասարությունների հետևյալ երկու համակարգերից՝

$$\begin{cases} |a| = a \cdot sign(a), \\ |b| = b \cdot sign(b), \end{cases} \quad \begin{cases} a = |a| \cdot sign(a), \\ b = |b| \cdot sign(b) : \end{cases}$$

Առաջին համակարգից հետևում է, որ a և b ամբողջ թվերի յուրաքանչյուր c ընդհանուր բաժանարար կլինի ընդհանուր բաժանարար նաև $|a|$ և $|b|$ ամբողջ թվերի համար, իսկ երկրորդ համակարգից կունենանք հակառակը՝ $|a|$ և $|b|$ ամբողջ թվերի յուրաքանչյուր c ընդհանուր բաժանարար կլինի ընդհանուր բաժանարար նաև a և b ամբողջ թվերի համար: $\square$

Վերջին հատկության համաձայն երկու ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու խնդիրը հանգում է երկու ոչ բացասական ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու խնդրին: Մյուս կողմից ակնհայտ է, որ

$$(|a|, 0) = |a| = (0, |a|) ,$$

որտեղ $a \neq 0$; Հետևաբար, մնում է նկարագրել երկու բնական (ամբողջ և դրական) թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու եղանակը:

Երկու բնական թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու եղանակը (ալգորիթմը) տրվել է Էվկլիդեսի կողմից և հայտնի Էվկլիդեսի ալգորիթմ անունով: Այն հենվում է հետևյալ պարզ դիտողության վրա.

Հատկություն 2.3: *Եթե a, r ամբողջ և b բնական թվերի համար $a \equiv r(mod\ b)$, այսինքն $a = bq + r$, որտեղ $q \in \mathbb{Z}$, ապա a և b թվերի ընդհանուր բաժանարարների բազմությունը համընկնում է b և r թվերի* *ընդհանուր բաժանարարների բազմության հետ; Մասնավորապես, (b,r)-ը գոյություն կունենա այն և միայն այն դեպքում, երբ գոյություն ունի (a,b)-ն և*

$$(a,b)=(b,r):$$

Ապացուցում: Եթե $a=bq+r$ և c-ն a և b ամբողջ թվերի համար ընդհանուր բաժանարար է, ապա $a=c\cdot a_1$, $b=c\cdot b_1$ և

$$r=a-bq=c\cdot a_1-cb_1q=c(a_1-b_1q),$$

որտեղ $a_1,b_1,a_1-b_1q\in\mathbb{Z}$: Հետևաբար, c-ն կլինի ընդհանուր բաժանարար նաև b և r ամբողջ թվերի համար: Ճիշտ է նաև հակառակը՝ b և r ամբողջ թվերի յուրաքանչյուր c ընդհանուր բաժանարար կլինի ընդհանուր բաժանարար նաև $a=bq+r$ պայմանին բավարարող a և b ամբողջ թվերի համար: □

Այժմ կարելի է շարադրել (նկարագրել) երկու բնական թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու Էվկլիդեսի հետևյալ ալգորիթմը, որն արդիական է նաև այժմ:

Օգտվենք մնացորդով բաժանման կանոնից (թեորեմ 1.1)՝

$$a=bq_1+r_2,\quad 0\leqslant r_2<b; \qquad \text{(I քայլ)}$$

Նշանակելով $r_0=a$, $r_1=b$, առաջին քայլը կգրվի հետևյալ կերպ՝ $r_0=r_1q_1+r_2$: Եթե այստեղ $r_2=0$, ապա կունենանք $(a,b)=b$: Իսկ եթե $r_2\neq 0$, ապա նորից ենք օգտվում մնացորդով բաժանման կանոնից՝

$$b=r_1=r_2q_2+r_3,\quad 0\leqslant r_3<r_2; \qquad \text{(II քայլ)}$$

Եթե այստեղ $r_3=0$, ապա համաձայն հատկության 2.3-ի կունենանք՝ $(a,b)=(b,r_2)=r_2$; Իսկ եթե $r_3\neq 0$, ապա նորից ենք գրում՝

$$r_2=r_3q_3+r_4,\quad 0\leqslant r_4<r_3; \qquad \text{(III քայլ)}$$

և այսպես շարունակ: Քանի որ $b>r_2>r_3>\cdots\geqslant 0$, ապա վերջավոր թվով քայլերից հետո (ամենաշատը b թվով քայլերից հետո) կունենանք՝

$$r_{n-1}=r_nq_n+r_{n+1},\quad 0=r_{n+1}<r_n; \qquad \text{(n-րդ քայլ)}$$

Այսպիսով, հատկություն 2.3-ի համաձայն՝

$$(a,b)=(b,r_2)=(r_2,r_3)=\cdots=(r_{n-2},r_{n-1})=(r_{n-1},r_n)=(r_n,0)=r_n;$$

Հանգում ենք հետևյալ արդյունքին.

Հատկություն 2.4 (Էվկլիդեսի ալգորիթմը): *a և b բնական թվերի ամենամեծ ընդհանուր բաժանարարը հավասար է նկարագրված եղանակի (Էվկլիդեսի ալգորիթմի) նախավերջին քայլում ստացվող ոչ զրոյական r_n մնացորդին: Այդ դեպքում n-ը Էվկլիդեսի ալգորիթմում պահանջվող քայլերի թիվն է և այն կոչվում է Էվկլիդեսի ալգորիթմի բարդություն:* □

Էվկլիդեսի ալգորիթմից օգտվելով նորից հանգում ենք հետևություն 2.1-ին. *a և b բնական թվերի ընդհանուր բաժանարարների բազմությունը համընկնում է դրանց ամենամեծ ընդհանուր բաժանարարի բոլոր բաժանարարների բազմության հետ:*

Որպես օրինակ Էվկլիդեսի ալգորիթմով (կանոնով) հաշվենք 11 և 30 թվերի ամենամեծ ընդհանուր բաժանարարը՝

$$30 = 11 \cdot 2 + 8,$$

$$11 = 8 \cdot 1 + 3,$$

$$8 = 3 \cdot 2 + 2,$$

$$3 = 2 \cdot 1 + 1,$$

$$2 = 1 \cdot 2 + 0;$$

Ուստի՝

$$(11, 30) = (30, 11) = 1 :$$

Թեորեմ 2.1-ին կարելի է հանգել նաև ելնելով Էվկլիդեսի ալգորիթմից, այսինքն՝ Էվկլիդեսի ալգորիթմով կարելի է որոշել (հաշվել) նաև a, b զույգի Բեզուի գործակիցները: Նախ նկատենք, որ $a \neq 0$ դեպքում՝

$$(a, 0) = |a| = au + 0 \cdot v,$$

որտեղ $u = sign(a)$, $v \in \mathbb{Z}$: Իսկ եթե $a \neq 0$ և $b \neq 0$, ապա հաշվի առնելով

$$(a, b) = (|a|, |b|)$$

հավասարությունը, գրենք Էվկիդեսի ալգորիթմը $|a|$ և $|b|$ բնական թվերի համար՝

$$\begin{aligned}
&|a| = |b|\cdot q_1 + r_2,\\
&|b| = r_2 q_2 + r_3,\\
&r_2 = r_3 q_3 + r_4,\\
&\cdots\ \cdots\ \cdots\ \cdots\ \cdots,\\
&r_{n-3} = r_{n-2} q_{n-2} + r_{n-1},\\
&r_{n-2} = r_{n-1} q_{n-1} + r_n,\\
&r_{n-1} = r_n q_n;
\end{aligned}$$

Որտեղից՝

$$\begin{gathered}
(|a|,|b|) = r_n = r_{n-2} + r_{n-1}\left(-q_{n-1}\right) =\\
= r_{n-3}x + r_{n-2}y = \cdots = |a|u + |b|v, \qquad u,v\in\mathbb{Z}:
\end{gathered}$$

Հաջորդ արդյունքի ձևակերպման համար ներմուծենք բնական թվերի հետևյալ

$$f_0, f_1, \ldots, f_m, \ldots$$

հաջորդականությունը, որտեղ

$$f_0 = 0, \quad f_1 = 1,$$

իսկ $m \geqslant 2$ դեպքում՝

$$f_m = f_{m-1} + f_{m-2}:$$

Մասնավորապես, $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $\ldots$

Այս հաջորդականությունը կոչվում է Ֆիբոնաչիի հաջորդականություն, իսկ նրա անդամները Ֆիբոնաչիի թվեր, ի պատիվ XII-XIII դարերի իտալացի մաթեմատիկոս Լեոնարդո Ֆիբոնաչիի, որն առաջինն է օգտվել այս թվերից: Առաջին հայացքից Ֆիբոնաչիի հաջորդականությունը չի թվում շատ բնական, սակայն բացի մաթեմատիկայից և կոմպյուտերային գիտությունից, այն հաճախ հանդիպում է նաև արվեստում, ճարտարապետության և կենսաբանության մեջ, և այլուր:

Թեորեմ 2.2: *Ցանկացած $n \geqslant 1$ բնական թվի համար գոյություն ունեն այնպիսի $a > b > 0$ բնական թվեր, որոնց ամենամեծ ընդհանուր բաժանարարը Էվկլիդեսի ալգորիթմով որոշելու համար պահանջվում է ճիշտ n հատ քայլեր, այսինքն $(a,b) = r_n$: Եվ հակառակը, եթե $a > b > 0$ բնական թվերի ամենամեծ ընդհանուր բաժանարարը Էվկլիդեսի ալգորիթմով որոշելու համար պահանջվում է ճիշտ n թվով քայլեր, ապա $a \geqslant f_{n+2}$ և $b \geqslant f_{n+1}$, որտեղ f_{n+1}, f_{n+2}-ը Ֆիբոնաչիի թվերն են:*

Ապացուցում: Թեորեմի առաջին մասի ապացուցման համար որպես a, b կարելի է վերցնել հենց Ֆիբոնաչիի հետևյալ թվերը՝ $a = f_{n+2}$ և $b = f_{n+1}$: Իրոք՝

$$\begin{aligned} &f_{n+2} = f_{n+1} + f_n, \text{ որտեղ } f_n < f_{n+1}, \\ &f_{n+1} = f_n + f_{n-1}, \text{ որտեղ } f_{n-1} < f_n, \\ &\cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots\ \cdots \\ &f_4 = f_3 + f_2, \text{ որտեղ } f_2 < f_3, \\ &f_3 = f_2 + f_1 = f_2 + f_2 = f_2 \cdot 2, \end{aligned}$$

այսինքն՝ Էվկլիդեսի ալգորիթմի համաձայն (այստեղ $q_1 = \cdots = q_n = 1$)՝

$$(f_{n+2}, f_{n+1}) = f_2 = 1$$

և այս արդյունքին հասնելու համար Էվկլիդեսի ալգորիթմով իրոք պահանջվեց ճիշտ n հատ քայլեր: Անցնենք երկրորդ մասի ապացուցմանը: Քանի որ $r_n = (a, b)$, ապա $r_n \geqslant 1$ և $r_n < r_{n-1}$, այսինքն $r_{n-1} \geqslant 2$ և հետևաբար՝ $r_n \geqslant f_2$ և $r_{n-1} \geqslant f_3$: Մյուս կողմից,

$$r_{i-1} = r_i q_i + r_{i+1} \geqslant r_i + r_{i+1},$$

քանի որ այստեղ $q_i \geqslant 1$, որովհետև $a > b > 0$ (տես նաև լեմմ 8.3-ը): Վերհանգման եղանակով այժմ ապացուցենք

$$r_{n-i} \geqslant f_{2+i}$$

անհավասարությունը, բոլոր $i = 0, 1, \ldots, n$ արժեքների դեպքում:

Իրոք, $i = 0, 1$ դեպքում գրված անհավասարությունը ճիշտ է: Այնուհետև, ենթադրելով այն ճիշտ $(i+1)$-ից փոքր թվերի համար ապացուցենք $(i+1)$-ի համար.

$$r_{n-(i+1)} = r_{(n-i)-1} \geqslant r_{n-i} + r_{n-i+1} = r_{n-i} + r_{n-(i-1)} \geqslant$$

$$\geqslant f_{2+i} + f_{2+(i-1)} = f_{2+i} + f_{1+i} = f_{3+i} = f_{2+(i+1)};$$

Այսպիսով, $i = n$ և $i = n-1$ դեպքերում կունենանք՝

$$a = r_0 \geqslant f_{n+2},$$

$$b = r_1 \geqslant f_{n+1}: \qquad \square$$

Վերիանգման եղանակով դժվար չէ նաև ապացուցել Ֆիբոնաչիի հաջորդականության n-րդ f_n անդամի որոշման հետևյալ բանաձևը, որը կոչվում է Բինեթի կամ Լամեի բանաձև՝

$$f_n = \frac{\left(1+\sqrt{5}\right)^n - \left(1-\sqrt{5}\right)^n}{2^n\sqrt{5}}$$

(Նիկոլաս (1728), Բինեթ (1843), Լամե (1844)):

Իրոք, $n = 0$ դեպքում գրված բանաձևը ակնհայտորեն ճիշտ է: Դիցուք՝

$$f_k = \frac{\left(1+\sqrt{5}\right)^k - \left(1-\sqrt{5}\right)^k}{2^k\sqrt{5}}$$

և ապացուցենք

$$f_{k+1} = \frac{\left(1+\sqrt{5}\right)^{k+1} - \left(1-\sqrt{5}\right)^{k+1}}{2^{k+1}\sqrt{5}}$$

բանաձևը:

$$f_{k+1} = f_{k-1} + f_k = \frac{\left(1+\sqrt{5}\right)^{k-1} - \left(1-\sqrt{5}\right)^{k-1}}{2^{k-1}\sqrt{5}} + \frac{\left(1+\sqrt{5}\right)^k - \left(1-\sqrt{5}\right)^k}{2^k\sqrt{5}} =$$

$$= \frac{4\left[\left(1+\sqrt{5}\right)^{k-1} - \left(1-\sqrt{5}\right)^{k-1}\right] + 2\left[\left(1+\sqrt{5}\right)^k - \left(1-\sqrt{5}\right)^k\right]}{2^{k+1}\sqrt{5}} =$$

$$= \frac{\left[-\left(1+\sqrt{5}\right)\left(1-\sqrt{5}\right)\right]\left[\left(1+\sqrt{5}\right)^{k-1} - \left(1-\sqrt{5}\right)^{k-1}\right] + \left[\left(1+\sqrt{5}\right) + \left(1-\sqrt{5}\right)\right]\cdot}{2^{k+1}\sqrt{5}}$$

$$\frac{\cdot\left[\left(1+\sqrt{5}\right)^k - \left(1-\sqrt{5}\right)^k\right]}{} = \frac{\left(1+\sqrt{5}\right)^{k+1} - \left(1-\sqrt{5}\right)^{k+1}}{2^{k+1}\sqrt{5}};$$

Բանաձևն ապացուցված է:

Նշանակելով՝

$$\tau = \frac{1+\sqrt{5}}{2}, \qquad \sigma = \frac{1-\sqrt{5}}{2},$$

կունենանք՝

$$f_n = \frac{\tau^n - \sigma^n}{\tau - \sigma},$$

$$1+\tau = 1+\frac{1+\sqrt{5}}{2} = \frac{3+\sqrt{5}}{2} = \tau^2,$$

$$1+\sigma = 1+\frac{1-\sqrt{5}}{2} = \frac{3-\sqrt{5}}{2} = \sigma^2;$$

Վերհանգման եղանակով ապացուցվում է նաև

$$f_n > \tau^{n-2}$$

անհավասարությունը, որտեղ $n > 2$: Իրոք, $n = 3$ դեպքում այն ճիշտ է, որովհետև $f_3 = 2 > \dfrac{1+\sqrt{5}}{2} = \tau$: Ենթադրելով $f_{n-2} > \tau^{n-4}$, $f_{n-1} > \tau^{n-3}$ անհավասարությունները, կունենանք՝

$$f_n = f_{n-1} + f_{n+2} > \tau^{n-4} + \tau^{n-3} = \tau^{n-4}(1+\tau) = \tau^{n-4}\cdot\tau^2 = \tau^{n-2};$$

Եթե $a > b > 0$ բնական թվերի ամենամեծ ընդհանուր բաժանարարը էվկլիդեսի ալգորիթմով որոշելու համար պահանջվում է ճիշտ n թվով քայլեր, ապա թեորեմ 2.2-ի համաձայն՝ $b \geqslant f_{n+1}$: Այժմ օգտվելով $f_{n+1} > \tau^{n-1}$ անհավասարությունից կստանանք՝

$$b \geqslant f_{n+1} > \tau^{n-1},$$

$$b > \tau^{n-1},$$

$$\lg b > (n-1)\lg\tau,$$

$$n-1 < \frac{\lg b}{\lg\tau};$$

Սակայն $\lg\tau > \dfrac{1}{5}$, այսինքն $\dfrac{1+\sqrt{5}}{2} > \sqrt[5]{10}$ կամ [5] $\left(\dfrac{1+\sqrt{5}}{2}\right)^5 > 10,$ հետևաբար՝

$$n-1 < 5\lg b,$$

$$n < 5\lg b + 1:$$

Այսպիսով, հանգում ենք հետևյալ արդյունքին *(Գ. Լամե, 1844 թ.).*

---

[5]Իրոք՝ $\sqrt{5} > 2.2$, $\frac{1+\sqrt{5}}{2} > 1.6$, $(1.6)^2 = 2.56 > 2.5$, $(1.6)^4 > (2.5)^2 = 6.25$, $(1.6)^5 > 6.25\cdot 1.6 = 10$ և հետևաբար $\left(\frac{1+\sqrt{5}}{2}\right)^5 > (1.6)^5 > 10$:

$a > b > 0$ *բնական թվերի ամենամեծ ընդհանուր բաժանարարը էվկլիդեսի ալգորիթմով որոշելու համար պահանջվող քայլերի* n *թիվը բավարարում է հետևյալ անհավասարությանը*

$$n < 5\lg b + 1 :$$

Իրականում այստեղ տեղի ունի ավելի խիստ գնահատական՝ $n < 5\lg b$, որը հետագայում բարելավվել է Ջ. Դիքսոնի (J. Dixon) կողմից (1970 թ.):

Հատկություն 2.5: *Յանկացած* a, b, c *ամբողջ թվերի համար, որտեղ* $c > 0$ *և* $a^2 + b^2 \neq 0$, *տեղի ունի հետևյալ հավասարությունը՝*

$$c \cdot (a, b) = (ca, cb);$$

Ապացուցում: Նշանակենք $d = (a, b)$ և ապացուցենք $c \cdot d = (ca, cb)$ հավասարությունը: Քանի որ d-ն ընդհանուր բաժանարար է a-ի և b-ի համար, ապա $c \cdot d$-ն կլինի ընդհանուր բաժանարար ca-ի և cb-ի համար: Օգտվելով թեորեմ 2.1-ում ապացուցված

$$d = au + bv$$

ներկայացումից, կարող ենք գրել՝

$$cd = (ca)u + (cb)v$$

և ասել, որ cd-ն բաժանվում է ca և cb ամբողջ թվերի յուրաքանչյուր k ընդհանուր բաժանարարի վրա: Հետևաբար $k \leqslant c \cdot d$; $\square$

Հետևություն 2.3: *Եթե* a, b, c *ամբողջ թվերի համար* $a^2 + b^2 \neq 0$, $c > 0$ *և* c*-ն ընդհանուր բաժանարար է* a*-ի և* b*-ի համար, ապա*

$$\left(\frac{a}{c}\,,\ \frac{b}{c}\right) = \frac{(a, b)}{c} :$$

Մասնավորապես, եթե $\left(\frac{a}{c}\,,\ \frac{b}{c}\right) = 1$, *ապա* $(a, b) = c$*:*

Ապացուցում: Ըստ նախորդ հատկության՝

$$c \cdot \left(\frac{a}{c}\,,\ \frac{b}{c}\right) = \left(c \cdot \frac{a}{c}\,,\ c \cdot \frac{b}{c}\right) = (a, b),$$

այսինքն՝
$$\left(\frac{a}{c}\,,\ \frac{b}{c}\right) = \frac{(a,b)}{c}\ : \qquad \square$$

Հատկություն 2.6 (ամենամեծ ընդհանուր բաժանարարի զուգորդականությունը): *Ցանկացած a, b, c ամբողջ թվերի համար, որտեղ $a^2 + b^2 \neq 0$ և $b^2 + c^2 \neq 0$, տեղի ունի հետևյալ հավասարությունը՝*

$$(a,(b,c)) = ((a,b),c);$$

Ապացույց: Նախ նկատենք, որ $a^2 + b^2 \neq 0$ և $b^2 + c^2 \neq 0$ պայմանների դեպքում հավասարության ձախ և աջ մասերը գոյություն ունեն: Ապացուցենք դրանց հավասարությունը:

Նշանակելով $d' = (b,c)$ և $d = (a,d')$ ստանանք $d = ((a,b),c)$ հավասարությունը: Քանի, որ d-ն a-ի և d'-ի ընդհանուր բաժանարարն է, ապա d-ն միաժամանակ կլինի a-ի b-ի և c-ի ընդհանուր բաժանարարը: Հետևաբար, d-ն կլինի նաև (a,b)-ի և c-ի ընդհանուր բաժանարարը (որովհետև (a,b) ամենամեծ ընդհանուր բաժանարարը բաժանվում է a-ի և b-ի բոլոր ընդհանուր բաժանարարների վրա): Ենթադրենք թե d''-ը (a,b)-ի և c-ի կամայական ընդհանուր բաժանարար է: Այդ դեպքում այն միաժամանակ կլինի a-ի, b-ի և c-ի ընդհանուր բաժանարարը: Հետևաբար, d''-ը կլինի նաև a-ի և (b,c)-ի ընդհանուր բաժանարարը: Ուստի $d'' \leqslant d$: $\square$

Վարժություններ և խնդիրներ

1. Դիցուք $(a,b) = au+bv$, որտեղ $a,b,u,v \in \mathbb{Z}$ և $a^2+b^2 \neq 0$: Ապացուցել $(u,v) = 1$ հավասարությունը:

2. Դիցուք ցանկացած $a > b > 0$ ամբողջ թվերի համար՝

$$r_0 = a, \ \ r_1 = b,$$

$$r_{k+1} = r_{k-1}(mod\, r_k), \ \ r_k \neq 0,$$

և

$$r_{k-1} = q_k r_k + r_{k+1}, \ \ k = 1, \ldots, n,$$

$$d = (a, b) = r_n > r_{n+1} = 0 :$$

Այնուհետև, դիցուք՝

$$x_0 = 1, \quad x_1 = 0, \quad y_0 = 0, \quad y_1 = 1$$

$$x_{k+1} = q_k x_k + x_{k-1},$$

$$y_{k+1} = q_k y_k + y_{k-1},$$

որտեղ $k = 1, 2, \ldots, n$:

Ապացուցել (N. Saunderson, 1740), որ

$$r_k = (-1)^k x_k a + (-1)^{k+1} y_k b,$$

որտեղ $k = 0, 1, \ldots, n+1$: Մասնավորապես,

$$r_n = (-1)^n x_n a + (-1)^{n+1} y_n b :$$

3. Դիցուք $a = 120$ և $b = 35$: Ելնելով նախորդ վարժության արդյունքներից, հաշվել $x = (-1)^n x_n$ և $y = (-1)^{n+1} y_n$ մեծությունները և ստանալ

$$(a, b) = r_n = xa + yb$$

ներկայացումը:

4. Դիցուք $a, b \in \mathbb{N}$ և $a \geqslant b > 0$: Գոյություն ունեն միարժեքորեն որոշվող այնպիսի $q_1, r_1 \in \mathbb{Z}$ ամբողջ թվեր, որ (հետևություն 1.3)՝

$$a = bq_1 + r_1, \quad -\frac{b}{2} < r_1 \leqslant \frac{b}{2};$$

Եթե $r_1 \neq 0$, ապա գոյություն կունենան այնպիսի $q_2, r_2 \in \mathbb{Z}$ ամբողջ թվեր, որ

$$b = r_1 q_2 + r_2, \quad -\frac{|r_1|}{2} < r_2 \leqslant \frac{|r_1|}{2};$$

Եթե $r_2 \neq 0$, ապա գոյություն կունենան այնպիսի $q_3, r_3 \in \mathbb{Z}$ ամբողջ թվեր, որ

$$r_1 = r_2 q_3 + r_3, \quad -\frac{|r_2|}{2} < r_3 \leqslant \frac{|r_2|}{2};$$

Եվ այսպես շարունակ . . .

Ապացուցել, որ գոյություն ունի այնպիսի n բնական թիվ, որ $r_n = 0$: Այդ դեպքում, եթե $n > 1$, ապա

$$(a, b) = |r_{n-1}| :$$

5. Ապացուցել հետևյալ հավասարությունը՝

$$(2n, 2n + 2) = 2;$$

6. Ապացուցել, որ 4-ը հնարավոր չէ ներկայացնել $12x + 18y$ տեսքով, որտեղ $x, y \in \mathbb{Z}$: (Ցուցում. տես հետևություն 2.2-ը):

7. Ապացուցել, որ 7-ը հնարավոր չէ ներկայացնել $18209x + 19043y$ տեսքով, որտեղ $x, y \in \mathbb{Z}$:

8. Լուծել հետևյալ համակարգը՝

$$\begin{cases} x + y = 120, \\ (x, y) = 30 \end{cases}$$

բնական թվերով $(x, y \in \mathbb{N})$:

(Ցուցում. $(x, y) = 30$ պայմանը համարժեք է հետևյալ համակարգին՝

$$\begin{cases} x = 30u, \\ y = 30v, \\ (u, v) = 1; \end{cases}) :$$

9. Ապացուցել, որ

$$\begin{cases} (x, y) = 3, \\ x + y = 65 \end{cases}$$

համակարգը չունի ամբողջ թվերով լուծումներ:

10. Ապացուցել, որ կամայական ոչ զրոյական a, b, c, d ամբողջ թվերի համար տեղի ունեն հետևյալ հավասարությունները՝

$$(((a, b), c), d) = ((a, (b, c)), d) = (a, ((b, c), d)) =$$
$$= (a, (b, (c, d))) = ((a, b), (c, d)) :$$

11. Բնական թվերի $L_1, L_2, \ldots$ հաջորդականությունը կոչվում է Լուկասի հաջորդականություն (E. Lucas), եթե

$$L_1 = 1, \quad L_2 = 3,$$

$$L_n = L_{n-1} + L_{n-2}, \quad n \geqslant 3:$$

Ապացուցել, որ այս հաջորդականության կապը Ֆիբոնաչիի հաջորդականության հետ տրվում է հետևյալ կերպ՝

$$L_{n+2} = f_n + f_{n+2}, \quad n \geqslant 1,$$

որտեղ $f_1, f_2, \ldots$ հաջորդականությունը Ֆիբոնաչիի հաջորդականությունն է:

12. Ապացուցել, որ յուրաքանչյուր n բնական թիվ կարելի է (միարժեքորեն) ներկայացնել Ֆիբոնաչիի թվերի գումարի տեսքով՝

$$n = f_{n_1} + f_{n_2} + \cdots + f_{n_k},$$

որտեղ $n_1 \geqslant n_2 + 2$, $n_2 \geqslant n_3 + 2$, …, $n_{k-1} \geqslant n_k + 2$, $n_k \geqslant 2$:

13. Ապացուցել հետևյալ հավասարությունը՝

$$\sum_{i=1}^{n} f_i = f_{n+2} - 1:$$

14. Ապացուցել հետևյալ հավասարությունը՝

$$f_{n-1}f_{n+1} - f_n^2 = (-1)^n, \quad n \geqslant 1$$

(G. D. Cassini (1680), R. Simson (1753)):

15. Ապացուցել հետևյալ բանաձևերը՝

$$f_{n+1}^2 + f_n^2 = f_{2n+1}, \quad n \geqslant 1,$$

$$f_{n+1}^2 - f_{n-1}^2 = f_{2n}, \quad n \geqslant 2$$

(E. Lucas):

Գ լ ու խ 3

ՓՈԽԱԴԱՐՁԱԲԱՐ ՊԱՐԶ ԱՄԲՈՂՋ ԹՎԵՐ: ՉԻՆԱԿԱՆ ԹԵՈՐԵՄԸ ԲԱՂԴԱՏՈՒՄՆԵՐԻ (ՄՆԱՑՈՐԴՆԵՐԻ) ՎԵՐԱԲԵՐՅԱԼ

3.1. Փոխադարձաբար պարզ ամբողջ թվերի հատկությունները

Երկու a և b ամբողջ թվեր կոչվում են **փոխադարձաբար** (փոխադարձ) **պարզ**, եթե դրանց ամենամեծ ընդհանուր բաժանարարը հավասար է մեկի՝ $(a,b)=1$: Այս փաստը երբեմն նշվում է նաև $a\perp b$ ձևով:

Հատկություն 2.3-ից բխում է, որ եթե m բնական թիվը և a ամբողջ թիվը փոխադարձաբար պարզ են, ապա a-ի հետ ըստ (մոդուլ) m-ի բաղդատելի յուրաքանչյուր c ամբողջ թիվ ևս կլինի փոխադարձաբար պարզ m-ի հետ, այսինքն՝

$$(a,m)=1, \quad c\equiv a(mod\, m)\to (c,m)=1:$$

Ապացուցենք փոխադարձաբար պարզության հետևյալ հայտանիշը:

Թեորեմ 3.1: *a և b ամբողջ թվերը կլինեն փոխադարձաբար պարզ այն և միայն այն դեպքում, երբ գոյություն ունեն այնպիսի x և y ամբողջ թվեր, որ*

$$ax+by=1:$$

Ապացուցում: *Անհրաժեշտությունը* բխում է թեորեմ 2.1-ից, երբ $d=1$: Ապացուցենք *բավարարությունը* :

Նախ, եթե $ax+by=1$ որևէ x, y ամբողջ թվերի համար, ապա a-ն և b-ն միաժամանակ զրո լինել չեն կարող և հետևաբար գոյություն կունենա դրանց $(a,b)=d$ ամենամեծ ընդհանուր բաժանարարը: Ուստի, ax-ը և by-ը կբաժանվեն d-ի վրա, հետևաբար $ax+by=1$-ը ևս կբաժանվի d-ի վրա: Այսպիսով, d-ն կլինի հակադարձելի և, հետևաբար, $d=1$ (գլուխ 1, հատկություն 9°): □

Հետևություն 3.1: *Եթե $d=(a,b)$, ապա $\left(\dfrac{a}{d}, \dfrac{b}{d}\right)=1$: Ճիշտ է նաև հակառակ պնդումը (տես հետևություն 2.3-ը):*

Ապացուցում: Գոյություն ունեն այնպիսի x, y ամբողջ թվեր, որ $ax+by=d$ (թեորեմ 2.1): Հետևաբար, $\frac{a}{d}x+\frac{b}{d}y=1$: Մնում է կիրառել թեորեմ 3.1 հայտանիշը: □

Առանց ապացուցման նշենք հետևյալ հետաքրքրական փաստը (Դիրիխլե). Եթե u, v-ն (պատահական վերցրած) երկու բնական թվեր են, ապա հավանականությունը այն բանի, որ դրանք կլինեն փոխադարձաբար պարզ, հավասար է $\frac{6}{\pi^2}\approx 0.6079$: Ավելի ճիշտ, եթե

$$H_n=\{(u,v)\mid\ 1\leqslant u\leqslant n,\ 1\leqslant v\leqslant n,\ (u,v)=1\}\,,$$

ապա

$$\lim_{n\to\infty}\frac{|H_n|}{n^2}=\frac{6}{\pi^2},$$

որտեղ $|H_n|$-ը H_n բազմության կարգն է:

Հատկություն 3.1: *Եթե a ամբողջ թիվը փոխադարձաբար պարզ է b_1, b_2 ամբողջ թվերից յուրաքանչյուրի հետ, ապա a-ն կլինի փոխադարձաբար պարզ նաև դրանց $b_1\cdot b_2$ արտադրյալի հետ: Հետևաբար, a ամբողջ թիվը կլինի փոխադարձաբար պարզ b_1, b_2 ամբողջ թվերի $b_1\cdot b_2$ արտադրյալի հետ այն և միայն այն դեպքում, երբ a-ն փոխադարձաբար պարզ է b_1, b_2 արտադրիչներից յուրաքանչյուրի հետ:*

Ապացուցում: Ըստ պայմանի՝ $(a,b_1)=1$ և $(a,b_2)=1$: Հետևաբար, ըստ փոխադարձաբար պարզության հայտանիշի (թեորեմ 3.1), գոյություն կունենան այնպիսի x_1, y_1 և x_2, y_2 ամբողջ թվեր, որ

$$ax_1+b_1y_1=1$$

և

$$ax_2+b_2y_2=1;$$

Բազմապատկելով գրված հավասարությունները կստանանք՝

$$(ax_1+b_1y_1)(ax_2+b_2y_2)=1\cdot 1,$$

$$ax_1ax_2+ax_1b_2y_2+b_1y_1ax_2+b_1y_1b_2y_2=1,$$

$$a(x_1ax_2+x_1b_2y_2+b_1y_1x_2)+b_1b_2y_1y_2=1,$$

որտեղ $x_1ax_2+x_1b_2y_2+b_1y_1x_2$ և y_1y_2 թվերը ամբողջ են: Մնում է օգտվել փոխադարձաբար պարզության հայտանիշից: Պնդման երկրորդ մասն ակնհայտ է: □

Հատկություն 3.2: *Եթե a ամբողջ թիվը փոխադարձաբար պարզ է $b_1, b_2, \ldots, b_n$ ամբողջ թվերից յուրաքանչյուրի հետ, ապա a-ն կլինի փոխադարձաբար պարզ նաև դրանց $b_1 \cdot b_2 \cdot \ldots \cdot b_n$ արտադրյալի հետ, որտեղ $n \geqslant 2$:*

Ապացուցում (վերհանգման եղանակ): Եթե $n = 2$, ապա պնդումը ճիշտ է՝ համաձայն նախորդ հատկության: Ենթադրելով պնդումը ճիշտ $n-1$ արտադրիչների դեպքում, ապացուցենք այն n արտադրիչների համար: Ըստ պայմանի a-ն փոխադարձաբար պարզ է b_1-ի հետ, իսկ ըստ վերհանգման ենթադրության a-ն կլինի փոխադարձաբար պարզ նաև $b_2 \cdot \ldots \cdot b_n$ արտադրյալի հետ: Հետևաբար, ըստ նախորդ հատկության a-ն կլինի փոխադարձաբար պարզ նաև $b_1 \cdot b_2 \cdot \ldots \cdot b_n = b_1 \cdot (b_2 \cdot \ldots \cdot b_n)$ արտադրյալի հետ: □

Հատկություն 3.3: *Եթե $a_1, \ldots, a_n$ ամբողջ թվերից յուրաքանչյուրը փոխադարձաբար պարզ է $b_1, \ldots, b_m$ ամբողջ թվերից ցանկացածի հետ, ապա $a_1 \cdot \ldots \cdot a_n$ և $b_1 \cdot \ldots \cdot b_m$ արտադրյալները ևս կլինեն փոխադարձաբար պարզ:*

Ապացուցում: Նախ n անգամ օգտվելով նախորդ հատկությունից ստանում ենք, որ $a_1, \ldots, a_n$ ամբողջ թվերից յուրաքանչյուրը փոխադարձաբար պարզ է $b_1 \cdot \ldots \cdot b_m$ արտադրյալի հետ, որից հետո նորից կիրառելով նախորդ հատկությունը ստանում ենք, որ $b_1 \cdot \ldots \cdot b_m$ արտադրյալը փոխադարձաբար պարզ է $a_1 \cdot \ldots \cdot a_n$ արտադրյալի հետ:

Հետևություն 3.2: *Եթե a և b ամբողջ թվերը փոխադարձաբար պարզ են, ապա a^n և b^m թվերը ևս կլինեն փոխադարձաբար պարզ՝ ցանկացած n, m բնական թվերի դեպքում:*

Ապացուցում: Ստացվում է նախորդ հատկությունից, եթե վերցնենք՝ $a_1 = \cdots = a_n = a$ և $b_1 = \cdots = b_m = b$: □

Հետևություն 3.3: *Եթե ռացիոնալ թիվը ամբողջ չէ, ապա նրա ցանկացած բնական ցուցիչով աստիճանը ևս չի լինի ամբողջ թիվ: Հետևաբար, եթե $\sqrt[m]{c} \notin \mathbb{Z}$, ապա $\sqrt[m]{c} \notin \mathbb{Q}$, որտեղ $c \in \mathbb{Z}$:*

Ապացուցում: Դիցուք $\dfrac{a}{b}$-ն ռացիոնալ թիվ է, որտեղ a, b-ն ամբողջ են, $b > 0$ և m-ը բնական թիվ է: Դիցուք $\dfrac{a}{b}$-ն ամբողջ չէ (հետևաբար $b \neq 1$) և a, b ամբողջ թվերը փոխադարձաբար պարզ են (հակառակ դեպքում նրանց կկրճատեինք իրենց ամենամեծ ընդհանուր բաժանարարով): $\left(\frac{a}{b}\right)^m = \frac{a^m}{b^m}$ կոտորակի համարիչը և հայտարարը ևս կլինեն փոխադարձաբար պարզ (համաձայն հետևության 3.2-ի) և հետևաբար a^m-ը չի կարող բաժանվել b^m-ի վրա (հակառակ դեպքում կունենայինք՝ $(a^m, b^m) = b^m > 1$): □

Հետևություն 3.4: Ամբողջ գործակիցներով հետևյալ տեսքի

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

բազմանդամի յուրաքանչյուր ռացիոնալ արմատ ամբողջ է: Հետևաբար, այդպիսի բազմանդամի յուրաքանչյուր իրական արմատ կամ ամբողջ թիվ է կամ՝ իռացիոնալ:

Ապացույց: Դիցուք $\alpha \in \mathbb{Q}$ ռացիոնալ թիվը տրված $f(x)$ բազմանդամի համար արմատ է, այսինքն՝ $f(\alpha) = 0$: Պահանջվում է ապացուցել, որ $\alpha \in \mathbb{Z}$:

Դիցուք $\alpha = \frac{a}{b}$, որտեղ $a, b \in \mathbb{Z}$, $b > 0$ և $(a, b) = 1$: Հետևություն 3.2-ից բխում է՝ $(a^n, b) = 1$, իսկ $f(\alpha) = 0$ պայմանից հետևում է՝

$$\left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + a_{n-2}\left(\frac{a}{b}\right)^{n-2} + \cdots + a_1\frac{a}{b} + a_0 = 0 :$$

Հավասարության երկու կողմերը բազմապատկելով b^n-ով, կունենանք՝

$$a^n + a_{n-1}ba^{n-1} + a_{n-2}b^2a^{n-2} + \cdots + a_1 b^{n-1}a + a_0 b^n = 0,$$

$$a^n = b(-a_{n-1}a^{n-1} - a_{n-2}ba^{n-2} - \cdots - a_1 b^{n-2}a - a_0 b^{n-1}),$$

այսինքն՝ a^n-ը բաժանվում է b-ի (վրա) և քանի որ $(a^n, b) = 1$, ապա $b = 1$ և $\alpha = \frac{a}{b} = a \in \mathbb{Z}$: □

Սակայն հետևություն 3.4-ի հակադարձը ճիշտ չէ, այսինքն գոյություն ունեն այնպիսի իռացիոնալ թվեր, որոնք չեն հանդիսանում ամբողջ գործակիցներով բազմանդամների արմատներ (օրինակ, π և e թվերը): Այդպիսի թվերը կոչվում են **տրանսցենդենտ թվեր**, իսկ այն թվերը, որոնք հանդիսանում են ամբողջ գործակիցներով բազմանդամների արմատներ, կոչվում են **հանրահաշվական թվեր**:

Հատկություն 3.4 (էվկլիդես): *Եթե երկու a և b ամբողջ թվերի $a \cdot b$ արտադրյալը բաժանվում է c ամբողջ թվի վրա և a-ն փոխադարձաբար պարզ է c-ի հետ, ապա b-ն բաժանվում է c-ի վրա:*

Ապացույց: Ըստ պայմանի, $(a, c) = 1$, ուստի, թեորեմ 3.1-ի համաձայն, կունենանք այնպիսի x, y ամբողջ թվեր, որ

$$ax + cy = 1;$$

Հավասարության երկու կողմերը բազմապատկելով b-ով կստանանք՝

$$(ab)x + c(by) = b,$$

որտեղ ձախ մասի երկու գումարելիները բաժանվում են c-ի վրա: Հետևաբար, հավասարության աջ մասն էլ կբաժանվի c-ի վրա: □

Հատկություն 3.5 (Էվկլիդես): *Եթե a ամբողջ թիվը բաժանվում է b և c փոխադարձաբար պարզ ամբողջ թվերից յուրաքանչյուրի վրա, ապա a-ն կբաժանվի նաև դրանց $b \cdot c$ արտադրյալի վրա:*

Ապացույց: Ըստ պայմանի՝

$$a = b \cdot b_1,$$

$$a = c \cdot c_1,$$

որտեղ b_1, c_1-ը ամբողջ թվեր են: Ուստի,

$$b \cdot b_1 = c \cdot c_1,$$

որտեղ $(b, c) = 1$; Հետևաբար, ըստ նախորդ հատկության, b_1-ը կբաժանվի c-ի վրա, այսինքն $b_1 = c \cdot c_2$, որտեղ c_2-ը ամբողջ է: Այսպիսով՝

$$a = b \cdot b_1 = b(c \cdot c_2) = (bc)c_2 :$$

Հատկությունն ապացուցված է: □

$a_1, \ldots, a_n$ ամբողջ թվերը (հաջորդականության թվերը) կոչվում են զույգ առ զույգ փոխադարձաբար պարզ, եթե դրանցից յուրաքանչյուրը փոխադարձաբար պարզ է մնացած ամբողջ թվերից յուրաքանչյուրի հետ՝ $(a_i, a_j) = 1$, որտեղ $i \neq j$ և $i, j = 1, \ldots, n$:

Հատկություն 3.6: *Եթե a ամբողջ թիվը բաժանվում է զույգ առ զույգ փոխադարձաբար պարզ $a_1, \ldots, a_n$ ամբողջ թվերից յուրաքանչյուրի վրա, ապա a-ն կբաժանվի նաև դրանց $a_1 \cdot \ldots \cdot a_n$ արտադրյալի վրա:*

Ապացուցում (վերհանգման եղանակ): Եթե $n = 2$, ապա պնդումը ճիշտ է` ըստ նախորդ հատկության: Ենթադրենք թե այն ճիշտ է $n-1$ հատ արտադրիչների դեպքում: Դիցուք a ամբողջ թիվը բաժանվում է զույգ առ զույգ փոխադարձաբար պարզ $a_1, \ldots, a_n$ ամբողջ թվերից յուրաքանչյուրի վրա: Այդ դեպքում, ըստ վերհանգման ենթադրության, a-ն կբաժանվի նաև $a_1 \cdot \ldots \cdot a_{n-1}$ արտադրյալի վրա: Քանի որ համաձայն հատկություն 3.2–ի, a_n-ը փոխադարձաբար պարզ է $a_1 \cdot \ldots \cdot a_{n-1}$ արտադրյալի հետ, ապա մնում է օգտվել նախորդ հատկությունից: □

$(x_1, x_2, \ldots, x_n)$ հաջորդականությունը կոչվում է **ամբողջ-արժեք**, եթե $x_1, x_2, \ldots, x_n \in \mathbb{Z}$:

Մեկ կամ մի քանի անհայտներից (փոփոխականներից) կախված հավասարման (հավասարումների համակարգի) ամբողջ-արժեք լուծումը կոչվում է **Դիոֆանտյան լուծում**: Հավասարման (հավասարումների համակարգի) բոլոր Դիոֆանտյան լուծումները գտնելու խնդիրը կոչվում է **Դիոֆանտյան խնդիր**, իսկ եթե լուծվող հավասարման (հավասարումների համակարգի) մեջ մասնակցող բոլոր հաստատունները ամբողջ թվեր են, ապա այդ դեպքում այն կոչվում է **Դիոֆանտյան հավասարում** (համակարգ): Լուծել Դիոֆանտյան հավասարումը (համակարգը) նշանակում է որոշել դրա լուծելիության պայմանները և գտնել դրա բոլոր Դիոֆանտյան լուծումները: $(x_1, x_2, \ldots, x_n)$ Դիոֆանտյան լուծումը կոչվում է դրական, եթե $x_i > 0$, $i = 1, 2, \ldots, n$ և` ոչ բացասական, եթե $x_i \geqslant 0$, $i = 1, 2, \ldots, n$:

$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ հավասարումը, որտեղ $a_i \in \mathbb{Z}$, $a_i \neq 0$, $i = 1, 2 \ldots, n$, կոչվում է **գծային Դիոֆանտյան հավասարում**: Հակառակ դեպքում, Դիոֆանտյան հավասարումը կոչվում է **ոչ գծային**: Օրինակ, $x^n + y^n = z^n$, $n > 1$, հավասարումը ոչ գծային Դիոֆանտյան հավասարում է, որը կոչվում է Ֆերմայի հավասարում: $n = 2$ դեպքում այս հավասարման դիոֆանտյան լուծումների գոյությունն ակնհայտ է ($x = 3$, $y = 4$, $z = 5$):

Մինչև 1994 թ. թվերի տեսության ամենահայտնի չլուծված խնդիրը վերաբերում էր հենց այս Դիոֆանտյան հավասարման Դիոֆանտյան լուծման գոյությանը $n \geqslant 3$ դեպքում, որը ձևակերպվել էր 1637 թ. ֆրանսիացի հայտնի մաթեմատիկոս (և իրավաբան) Պ. Ֆերմայի (Pierre de Fermat, 1601-1665) կողմից` հետևյալ կերպ.

Ֆերմայի մեծ (կամ վերջին) թեորեմը: *Ապացուցել, որ*

$$x^n + y^n = z^n$$

հավասարումը $n \geqslant 3$ *դեպքում չունի* (x, y, z) *Դիոֆանտյան լուծումներ* *(*$xyz \neq 0$*):*

Պ. Ֆերմային հաջողվել է լուծել այս խնդիրը միայն $n = 4$ դեպքում և սա մինչ այժմ հայտնի միակ դեպքն է, երբ Ֆերմայի մեծ թեորեմը լուծվում է տարրական եղանակով: Նույնիսկ $n = 3$ դեպքում, խնդիրը տարրական եղանակով չի լուծվում (Էյլեր (1768), Գաուս): $n = 5$ դեպքի լուծումը (Դիրիխլե (1825), Լեժանդր) արդեն կարելի է համարել բավական բարդ:

Այս թեորեմի վերջնական ապացուցումը ստացվել է 1994 թ. Պրինստոնի համալսարանի պրոֆեսոր Էնդրյու Ուայլսի կողմից (Andrew Wiles) և համարվում է XX դարում մաթեմատիկական գիտության ամենամեծ հաջողություններից մեկը: Մինչ այդ, 1983 թ. նույն համալսարանի պրոֆեսոր Գ. Ֆալթինգսը (Gerd Faltings) ապացուցել էր Լ. Մորդելլի վարկածը (Louis Mordell), որ Ֆերմայի հավասարման բոլոր Դիոֆանտյան լուծումների բազմությունը վերջավոր է, եթե $n \geqslant 3$:

Ներկայումս դրված է հետևյալ ավելի ընդհանուր խնդիրը (Andrew Beal, 1994), որը դեռևս չի լուծված.

Ապացուցել, որ

$$x^m + y^n = z^r$$

հավասարումը չունի (x, y, z) դրական Դիոֆանտյան լուծում, որտեղ $((x, y), z) = 1$, իսկ $m, n, r \geqslant 3$:

Ակնհայտ է, որ մեկ անհայտով $a_1 x_1 = b$ գծային Դիոֆանտյան հավասարումը ($a_1, b \in \mathbb{Z}$, $a_1 \neq 0$) կունենա Դիոֆանտյան լուծում այն և միայն այն դեպքում, երբ b-ն բաժանվում է a_1-ի վրա: Եվ այդ դեպքում այն կունենա միակ լուծում՝ $x_1 = \dfrac{b}{a_1} \in \mathbb{Z}$: Անցնելով երկու անհայտով գծային Դիոֆանտյան հավասարման դեպքին, նախ նկատենք, որ համաձայն հետևություն 2.2-ի, $ax + by = c$ հավասարումն ունի Դիոֆանտյան լուծում այն և միայն այն դեպքում, երբ c-ն բաժանվում է $(a, b) = d$-ի վրա ($a, b, c \in \mathbb{Z}$, $a^2 + b^2 \neq 0$): Ըստ որում, այս դեպքում նշված հավասարումը կունենա անվերջ թվով լուծումներ, որովհետև եթե (x_0, y_0) զույգը նշված հավասարման որևէ (մասնավոր) Դիոֆանտյան լուծում է, ապա $\left(x_0 - \dfrac{b}{d}k,\ y_0 + \dfrac{a}{d}k\right)$ զույգը $(k \in \mathbb{Z})$ ևս կլինի այդ հավասարման Դիոֆանտյան լուծում: Տեղի ունի նաև հակառակ պնդումը:

Հատկություն 3.7: (Brahmagupta, Aryabhata)*: Եթե* $a, b, c \in \mathbb{Z}$*,* $a, b \neq 0$ *և* $ax + by = c$ *հավասարումն ունի որևէ* (x_0, y_0) *Դիոֆանտյան լուծում, ապա դրա ցանկացած* (x, y) *Դիոֆանտյան լուծում որոշվում է հետևյալ կերպ՝*

$$x = x_0 - \frac{b}{d}k \quad y = y_0 + \frac{a}{d}k,$$

որտեղ $k \in \mathbb{Z}$*,* $d = (a, b)$*: Մասնավորապես, եթե* $(a, b) = 1$*, ապա*

$$x = x_0 - bk, \quad y = y_0 + ak, \qquad k \in \mathbb{Z}:$$

Ապացուցում: $c = ax_0 + by_0 = ax + by$, $a(x_0 - x) = b(y - y_0)$, $\frac{a}{d}(x_0 - x) = \frac{b}{d}(y - y_0)$, որտեղ $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$: Հատկություն 3.4-ի համաձայն, գոյություն կունենա այնպիսի $k \in \mathbb{Z}$ ամբողջ թիվ, որ $x_0 - x = k\frac{b}{d}$, $x = x_0 - \frac{b}{d}k$; Այնուհետև՝ $\frac{a}{d}k\frac{b}{d} = \frac{b}{d}(y - y_0)$, $y - y_0 = \frac{a}{d}k$, $y = y_0 + \frac{a}{d}k$: □

3.2. Բաղդատումներով հավասարումներ և համակարգեր

Հատկություն 3.8: *Եթե* $ca_1 \equiv ca_2 (mod\, m)$ *և* $(c, m) = 1$*, ապա* $a_1 \equiv a_2 (mod\, m)$*:*

Ապացուցում: Եթե $ca_1 - ca_2 = c(a_1 - a_2)$ արտադրյալը բաժանվում է m-ի վրա և $(c, m) = 1$, ապա հատկություն 3.4-ի համաձայն՝ $a_1 - a_2$ տարբերությունը կբաժանվի m-ի վրա, այսինքն՝ $a_1 \equiv a_2 (mod\, m)$: □

x_0 ամբողջ թիվը կոչվում է $ax \equiv b(mod\, m)$ բաղդատման լուծում, եթե $ax_0 \equiv b(mod\, m)$: Նշված բաղդատումը կոչվում է լուծելի, եթե այն ունի որևէ լուծում: Համանման իմաստով սահմանվում է նաև մի քանի փոփոխականից կախված բաղդատման ինչպես նաև բաղդատումների համակարգի լուծումը և լուծելիությունը:

Եթե $ax \equiv 1(mod\, m)$ բաղդատումը ունի լուծում, ապա a-ն կոչվում է հակադարձելի ըստ մոդուլ m-ի, իսկ x-ը՝ a-ի հակադարձ ըստ մոդուլ m-ի:

Թեորեմ 3.2: *Որպեսզի* $ax \equiv 1(mod\, m)$ *բաղդատումը լինի լուծելի անհրաժեշտ է և բավարար, որ* a *և* m *թվերը լինեն փոխադարձաբար պարզ՝* $(a, m) = 1$*, որտեղ* $a \in \mathbb{Z}$*:*

Ապացուցում: Եթե $ax_0 \equiv b(mod\, m)$, ապա $ax_0 - 1 = mt$, որտեղ $t \in \mathbb{Z}$; Հետևաբար, $ax_0 + m(-t) = 1$ և $(a, m) = 1$ համաձայն թեորեմ 3.1-ի:

Բավարարություն: Եթե $(a, m) = 1$, ապա ըստ թեորեմ 3.1-ի գոյություն կունենան այնպիսի u, v ամբողջ թվեր, որ $au + mv = 1$: Հետևաբար՝ $au-1 = m(-v)$, այսինքն $au \equiv 1(mod\, m)$ և u-ն հանդիսանում է $ax \equiv 1(mod\, m)$ բաղդատման լուծում: □

Հետևություն 3.5: *Որպեսզի $[a] \in \mathbb{Z}_m$ մնացքների դասը լինի հակադարձելի անհրաժեշտ է և բավարար, որ a և m թվերը լինեն փոխադարձաբար պարզ: Հետևաբար, a-ն կլինի հակադարձելի ըստ մոդուլ m-ի այն և միայն այն դեպքում, երբ $[a] \in \mathbb{Z}_m$ մնացքների դասը լինի հակադարձելի:*

Ապացուցում:

$$[a] \cdot [a'] = [1] \Longleftrightarrow [a \cdot a'] = [1] \Longleftrightarrow a \cdot a' \equiv 1(mod\, m) \Longleftrightarrow (a, m) = 1 : \quad \square$$

$[x_0] \in \mathbb{Z}_m$ մնացքների դասը կոչվում է $ax \equiv b(mod\, m)$ բաղդատման լուծում, եթե $[x_0]$ դասին պատկանող յուրաքանչյուր ամբողջ թիվ լուծում է բաղդատման համար:

Ակնհայտ է, որ եթե $ax_0 \equiv b(mod\, m)$ և $x_1 \equiv x_0(mod\, m)$, ապա $ax_1 \equiv ax_0(mod\, m)$ այսինքն $ax_1 \equiv b(mod\, m)$ (հատկություն 1.2): Այսպիսով, եթե x_0-ն $ax \equiv b(mod\, m)$ բաղդատման համար լուծում է, ապա x_0-ի հետ ըստ մոդուլ m-ի բաղդատելի ցանկացած x_1 ամբողջ թիվ ևս կլինի լուծում նույն բաղդատման համար: Այլ կերպ, եթե x_0-ն լուծում է $ax_0 \equiv b(mod\, m)$ բաղդատման համար, ապա $[x_0] \in \mathbb{Z}_m$ մնացքների դասը ևս կլինի լուծում նույն բաղդատման համար:

Թեորեմ 3.3 (C. Bachet, 1612): *Եթե $(a, m) = 1$, $a \in \mathbb{Z}$, ապա ցանկացած b ամբողջ թվի համար $ax \equiv b(mod\, m)$ բաղդատումը լուծելի է: Ընդ որում, լուծում հանդիսացող մնացքների դասը (ըստ մոդուլ m-ի) որոշվում է միարժեքորեն (միակն է):*

Ապացուցում: եթե $(a, m) = 1$, ապա համաձայն թեորեմ 3.2-ի $ax \equiv 1(mod\, m)$ բաղդատումը կունենա լուծում: Դիցուք՝ $x = a'$, այսինքն $aa' \equiv 1(mod\, m)$: Այդ դեպքում՝ $aa'b \equiv b(mod\, m)$, այսինքն՝ $a' \cdot b$ արտադրյալը կլինի $ax \equiv b(mod\, m)$ բաղդատման լուծում:

Եվ հակառակը, եթե x_0-ն այդ բաղդատման կամայական լուծում է, ապա $ax_0 \equiv b(mod\, m)$ և $aa'x_0 \equiv a'b(mod\, m)$: Մյուս կողմից՝ $aa' \equiv$

$1(mod\, m)$ և $aa'x_0 \equiv x_0(mod\, m)$: Այսպիսով՝ $x_0 \equiv a'b(mod\, m)$, այսինքն $ax \equiv b(mod\, m)$ բաղդատման կամայական x_0 լուծում բաղդատելի է դրա $a'b$ լուծման հետ և հետևաբար՝ $[x_0] = [a'b] \in \mathbb{Z}_m$: □

Թեորեմ 3.4: *Եթե $(a, m) = d$, ապա $ax \equiv b(mod\, m)$ բաղդատումը կլինի լուծելի այն և միայն այն դեպքում, երբ b-ն բաժանվում է d-ի վրա: Այդ պայմանի դեպքում նշված բաղդատումը կունենա լուծում հանդիսացող ճիշտ d հատ մնացքների դասեր ըստ մոդուլ m-ի (որոնց միավորումը կազմում է մի մնացքների դաս ըստ մոդուլ $\frac{m}{d}$-ի):*

Ապացուցում: Եթե $(a, m) = d$ և $ax \equiv b(mod\, m)$ բաղդատումն ունի x_0 լուծումը, ապա $ax_0 - b = mt$, որտեղ $t \in \mathbb{Z}$: Հետևաբար, $b = ax_0 - mt$ տարբերությունը կբաժանվի d-ի վրա: Եվ հակառակը, եթե $b = ds$ և $d = au + mv$ (համաձայն թեորեմ 2.1-ի), ապա $ds = aus + mvs$, այսինքն՝

$$b = aus + mvs,$$

$$aus - b = m(-vs) :$$

Հետևաբար, $ax \equiv b(mod\, m)$ բաղդատումն ունի $x_0 = us$ լուծումը: Այժմ պարզենք բաղդատման լուծումների քանակը, եթե այն լուծելի է:

Դիցուք $a = da_1$, $b = db_1$ և $m = dm_1$; Ըստ հետևություն 3.1-ի՝ $(a_1, m_1) = 1$, մյուս կողմից,

$$ax_0 \equiv b(mod\, m) \Longleftrightarrow a_1x_0 \equiv b_1(mod\, m_1) :$$

Համաձայն թեորեմ 3.3-ի, $a_1x \equiv b_1(mod\, m_1)$ բաղդատման լուծում հանդիսացող միակ մնացքների դասը ըստ մոդուլ m_1-ի կլինի $[a_1'b_1] \in \mathbb{Z}_{m_1}$ դասը, որտեղ $a_1a_1' \equiv 1(mod\, m_1)$: Ըստ (մոդուլ m_1-ի) մնացքների դասի սահմանման՝

$$[a_1'b_1] = \{x \in \mathbb{Z} \mid \ x \equiv a_1'b_1(mod\, m_1)\},$$

այսինքն $x - a_1'b_1$ տարբերությունը բաժանվում է m_1-ի վրա՝

$$x - a_1'b_1 = m_1q, \quad q \in \mathbb{Z} :$$

Այժմ, համաձայն թեորեմ 1.1-ի, հնարավոր են հետևյալ դեպքերը՝

$$\begin{aligned}
&q = dt, \ \ t \in \mathbb{Z},\\
&q = dt + 1, \ \ t \in \mathbb{Z},\\
&\quad \vdots\\
&q = dt + (d-1), \ \ t \in \mathbb{Z};
\end{aligned}$$

Հետևաբար $x - a_1'b_1 = m_1q$, $q \in \mathbb{Z}$ պայմանին բավարարող x ամբողջ թվերի համար հնարավոր են հետևյալ դեպքերը՝

$$\begin{array}{l} x - a_1'b_1 = m_1q = m_1dt = mt, \\ x - a_1'b_1 = m_1q = m_1(dt+1) = m_1dt + m_1 = mt + m_1, \\ \dots \ \dots \ \dots \ \dots \ \dots \ \dots \ \dots \ \dots \ \dots \ \dots \\ x - a_1'b_1 = m_1q = m_1(dt+(d-1)) = m_1dt + m_1(d-1) = mt + (d-1)m_1 \end{array}$$

կամ՝

$$\begin{array}{l} x - a_1'b_1 = mt, \\ x - (a_1'b_1 + m_1) = mt, \\ \dots \ \dots \ \dots \ \dots \ \dots \\ x - (a_1'b_1 + (d-1)m_1) = mt; \end{array}$$

Ուստի, $x - a_1'b_1 = m_1q$, $q \in \mathbb{Z}$ պայմանին բավարարող x ամբողջ թվերի համար հնարավոր են հետևյալ բաղդատումները ըստ մոդուլ m-ի՝

$$\begin{array}{l} x \equiv a_1'b_1 (mod\, m), \\ x \equiv (a_1'b_1 + m_1)(mod\, m), \\ \dots \ \dots \ \dots \ \dots \ \dots \\ x \equiv (a_1'b_1 + (d-1)m_1)(mod\, m); \end{array}$$

Ըստ որում, նշված բաղդատումներից որևէ երկուսը միաժամանակ տեղի ունենալ չեն կարող, որովհետև $i \neq j$ դեպքում

$$(a_1'b_1 + im_1) - (a_1'b_1 + jm_1) = (i-j)m_1 \neq 0$$

տարբերությունը չի բաժանվում m-ի վրա ($|i-j| < d$ և հետևաբար $|(i-j)m_1| < d \cdot m_1 = m$):

Այսպիսով, դիտարկվող $ax \equiv b(mod\, m)$ լուծելի բաղդատման համար ստացվում են այդ բաղդատման լուծում հանդիսացող և միմյանցից տարբեր ճիշտ $d = (a, m)$ հատ մնացքների դասեր ըստ մոդուլ m-ի՝

$$[a_1'b_1],\ [a_1'b_1 + m_1],\ [a_1'b_1 + 2m_1],\ \dots,\ [a_1'b_1 + (d-1)m_1]:$$

Թեորեմն ապացուցված է: $\square$

Այժմ անցնենք բաղդատումների այսպես կոչված Չինական համակարգի լուծման խնդրին:

Թեորեմ 3.5 (Չինական թեորեմ): *Եթե $m_1, m_2, \ldots, m_n$ բնական թվերը $(n \geqslant 2)$ զույգ առ զույգ փոխադարձաբար պարզ են, ապա ցանկացած $a_1, a_2, \ldots, a_n$ ամբողջ թվերի համար բաղդատումների հետևյալ համակարգը (որը կոչվում է բաղդատումների Չինական համակարգ)՝*

$$\begin{cases} x \equiv a_1 (mod\, m_1), \\ x \equiv a_2 (mod\, m_2), \\ \cdots \;\; \cdots \;\; \cdots \;\; \cdots \\ x \equiv a_n (mod\, m_n) \end{cases}$$

ունի լուծում: Ընդ որում, եթե x_0-ն նշված համակարգի որևէ լուծում է և $x_1 \equiv x_0 (mod\, m_1 m_2 \ldots m_n)$, ապա x_1-ը ևս կլինի նշված համակարգի լուծում; Եվ հակառակը, եթե x, x'-ը նշված համակարգի երկու լուծումներ են, ապա $x \equiv x' (mod\, m_1 m_2 \ldots m_n)$, այսինքն լուծումը որոշվում է միարժեքորեն ըստ $m = m_1 \cdot m_2 \cdot \ldots \cdot m_n$ մոդուլի (հենքի): Այլ կերպ, լուծում հանդիսացող մնացքների դասը որոշվում է միարժեքորեն:

Ապացուցում: Նախ հաստատենք լուծման գոյությունը: Նշանակելով՝

$$k_i = m_1 \cdot \ldots \cdot m_{i-1} \cdot m_{i+1} \cdot \ldots \cdot m_n, \quad i = 1, \ldots n,$$

կստանանք $(k_i, m_i) = 1$ (հատկություն 3.2): Հետևաբար, թեորեմ 3.2-ի համաձայն, $k_i x_i \equiv 1 (mod\, m_i)$ բաղդատումը կունենա լուծում: Որտեղից՝ $k_i x_i a_i \equiv a_i (mod\, m_i)$, այսինքն՝ $k_i z_i \equiv a_i (mod\, m_i)$, որտեղ $z_i = x_i a_i$, $i = 1, \ldots, n$: Ակնհայտ է նաև, որ

$$k_j z_j \equiv 0 (mod\, m_i), \quad i \neq j,$$

որովհետև k_j-ն բաժանվում է m_i-ի վրա, եթե $i \neq j$:

Հետևաբար, յուրաքանչյուր $i = 1, \ldots, n$ արժեքի համար կունենանք՝

$$k_1 z_1 + k_2 z_2 + \cdots + k_n z_n \equiv a_i (mod\, m_i),$$

այսինքն $x = k_1 z_1 + k_2 z_2 + \cdots + k_n z_n$ ամբողջ թիվը կլինի տրված համակարգի համար լուծում, որովհետև՝

$$k_1 z_1 + \cdots + k_{i-1} z_{i-1} + k_i z_i + k_{i+1} z_{i+1} + \cdots + k_n z_n \equiv 0 + \cdots$$
$$+ 0 + a_i + 0 + \cdots + 0 (mod\, m_i):$$

Լուծման միակությանը վերաբերող մասն ակնհայտ է: Իրոք, եթե x_0-ն նշված համակարգի համար լուծում է և $x_1 \equiv x_0 (mod m_1 m_2 \cdots m_n)$, ապա $x_1 \equiv x_0 (mod\, m_i)$, $i = 1, \ldots, n$, և բաղդատումների փոխանցական հատկության համաձայն (հատկություն 1.2) կունենանք $x_1 \equiv a_i (mod\, m_i)$, $i = 1, \ldots, n$:

Իսկ եթե x, x'-ը նշված համակարգի երկու լուծումներ են, ապա $x - x' \equiv 0 (mod\, m_i)$, $i = 1, \ldots, n$, և քանի որ $m_1, m_2, \cdots, m_n$ բնական թվերը $(n \geqslant 2)$ զույգ առ զույգ փոխադարձաբար պարզ են, ապա հատկություն 3.6-ի համաձայն, $x - x' \equiv 0 (mod\, m_1 m_2 \cdots m_n)$, այսինքն $x \equiv x' (mod\, m_1 m_2 \cdots m_n)$: □

Չինական թեորեմի ապացուցումը հանդիսանում է նաև բաղդատումների Չինական համակարգի լուծման ալգորիթմ: Որպես օրինակ լուծենք հետևյալ խնդիրը. գտնել այն ամբողջ թիվը, որը բաժանելով 3-ի ստացվում է 2 մնացորդ, բաժանելով 4-ի ստացվում է 3 մնացորդ և բաժանելով 5-ի ստացվում է 1 մնացորդ: Այսպիսով, պահանջվում է լուծել բաղդատումների հետևյալ Չինական համակարգը՝

$$\begin{cases} x \equiv 2 (mod\, 3), \\ x \equiv 3 (mod\, 4), \\ x \equiv 1 (mod\, 5), \end{cases}$$

որտեղ 3, 4 և 5 թվերը զույգ առ զույգ փոխադարձաբար պարզ են: Այստեղ $a_1 = 2$, $a_2 = 3$, $a_3 = 1$, $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 4 \cdot 5 = 60$, $k_1 = 4 \cdot 5 = 20$, $k_2 = 3 \cdot 5 = 15$, $k_3 = 3 \cdot 4 = 12$: Հաջորդ քայլում պահանջվում է լուծել $k_i x_i \equiv 1 (mod\, m_i)$ բաղդատումը $(i = 1, 2, 3)$: $i = 1$ դեպքում կունենանք՝

$$\begin{aligned} &20 x_1 \equiv 1 (mod\, 3), \\ &2 x_1 \equiv 1 (mod\, 3), \\ &x_1 \equiv 2 (mod\, 3); \end{aligned}$$

Նույն կերպ ստանում ենք՝ $x_2 \equiv 3 (mod\, 4)$, $x_3 \equiv 3 (mod\, 5)$: Հետևաբար՝

$$x = k_1 x_1 a_1 + k_2 x_2 a_2 + k_3 x_3 a_3 = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 1 =$$
$$= 80 + 135 + 36 = 251 \equiv 11 (mod\, 60) :$$

Գործածական է նաև բաղդատումների Չինական համակարգի լուծման հետևյալ ալգորիթմը.

$$\begin{aligned} x_1 &= a_1(mod\, m_1), \\ x_2 &= N_2(C_2(a_2 - x_1) mod\, m_2) + x_1, \\ x_3 &= N_3(C_3(a_3 - x_2) mod\, m_3) + x_2, \\ &\dots\ \dots\ \dots\ \dots\ \dots \\ x = x_n &= N_n(C_n(a_n - x_{n-1}) mod\, m_n) + x_{n-1}, \end{aligned}$$

որտեղ $N_i = m_1 \cdot m_2 \cdot \ldots \cdot m_{i-1}$, իսկ C_i ամբողջ թվերը բավարարում են $C_i N_i \equiv 1(mod\, m_i)$ պայմանին և ստացվում են Էվկլիդեսի ալգորիթմով՝ որպես N_i և m_i փոխադարձաբար պարզ թվերի Բեզուի գործակիցներ:

Նշենք նաև բաղդատումների Չինական թեորեմի հետևյալ ընդհանրացումը:

Թեորեմ 3.6 *(Yi Xing, 700): Որպեսզի բաղդատումների հետևյալ համակարգը* $(n \geqslant 2)$

$$\begin{cases} x \equiv a_1(mod\, m_1), \\ x \equiv a_2(mod\, m_2), \\ \dots\ \dots\ \dots\ \dots \\ x \equiv a_n(mod\, m_n) \end{cases}$$

ունենա լուծում անհրաժեշտ > և բավարար, որ $a_i - a_j$ տարբերությունը բաժանվի (m_i, m_j) ամենամեծ ընդհանուր բաժանարարի վրա՝ բոլոր i, j զույգերի դեպքում, որտեղ $1 \leqslant i < j \leqslant n$: Լուծման գոյության դեպքում այն որոշվում է միարժեքորեն ըստ $m = (m_1, m_2, \ldots, m_n)$ մոդուլի: □

Չինական թեորեմի առաջին ձևակերպումը հայտնաբերվել է ոտանավորների տեսքով՝ գրված մեր թվարկության I դարում՝ Չին հայտնի մաթեմատիկոս Սուն Ցզուի կողմից: Հետաքրքրական է, որ այս թեորեմը ձևակերպվում է նաև խմբերի և օղակների լեզվով, ինչը վկայում է ժամանակակից հանրահաշվի շատ վաղ ակունքների մասին:

Վարժություններ և խնդիրներ

1. Ապացուցել, որ երկու հաջորդական ամբողջ թվերի զույգը փոխադարձաբար պարզ է: (Ցուցում. $(m + 1) - m = 1$):

2. Ապացուցել, որ երկու հաջորդական կենտ թվերի զույգը փոխադարձաբար պարզ է:

3. Ապացուցել, որ $22m + 7$ և $33m + 10$ ամբողջ թվերի զույգը ($m \in \mathbb{Z}$) փոխադարձաբար պարզ է: Նույն պնդումն ապացուցել $2m + 1$ և $9m + 4$ ամբողջ թվերի համար:

4. Ապացուցել, որ $\left(n, 2^{2^n} + 1\right) = 1$, որտեղ $n = 1, 2, \ldots$:

5. Ապացուցել, որ $a \neq b$ ամբողջ թվերի համար գոյություն ունեն անվերջ թվով այնպիսի n բնական թվեր, որ $(a + n, b + n) = 1$:

6. Ապացուցել, որ ցանկացած $n > 6$ բնական թիվ կարելի է ներկայացնել երկու մեկից մեծ և փոխադարձաբար պարզ բնական թվերի գումարի տեսքով:

7. Ապացուցել, որ ցանկացած $n > 17$ բնական թիվ կարելի է ներկայացնել երեք մեկից մեծ և զույգ առ զույգ փոխադարձաբար պարզ բնական թվերի գումարի տեսքով:

8. Դիցուք m-ը բնական թիվ է: Ապացուցել, որ յուրաքանչյուր զույգ բնական թիվ կարելի է ներկայացնել երկու այնպիսի բնական թվերի տարբերության տեսքով, որոնցից յուրաքանչյուրը փոխադարձաբար պարզ է տրված m-ի հետ:

9. Դիցուք $a, b \neq 0$, $a, b \in \mathbb{Z}$, $d = (a, b)$ և դիցուք $u_0, v_0 \in \mathbb{Z}$ զույգը a, b զույգի Բեզուի գործակիցներն են, այսինքն՝ $d = au_0 + bv_0$: Ապացուցել, որ a, b զույգի ցանկացած u, v Բեզուի գործակիցներ որոշվում են հետևյալ կերպ՝
$$u = u_0 - k\frac{b}{d}\ , \quad v = v_0 + k\frac{a}{d}\ , \qquad k \in \mathbb{Z}:$$

10. Եթե $a, b, c \in \mathbb{Z}$, ապա
$$ca \equiv cb (mod\, n) \longleftrightarrow a \equiv b \left(mod\, \frac{n}{(n, c)}\right):$$

11. Օգտվելով հատկություն 3.7-ից, լուծել հետևյալ գծային Դիոֆանտյան հավասարումները՝
$$2x + 3y = 5,$$
$$12x + 9y = 21,$$
$$6x + 10y = 18:$$

12. Օգտվելով հատկություն 3.7-ից, լուծել հետևյալ գծային Դիոֆանտյան հավասարումը՝

$$9x_1 + 12x_2 + 5x_3 = 11;$$

(Ցուցում. քանի որ $(9, 12) = 3$, ապա $9x_1 + 12x_2 = 3y$ հավասարումը կունենա Դիոֆանտյան լուծում՝ ցանկացած $y \in \mathbb{Z}$ ամբողջ թվի դեպքում: Այդ պատճառով նախ լուծենք $3y + 5x_3 = 11$ Դիոֆանտյան հավասարումը, օգտվելով հատկություն 3.7-ից՝

$$y = y_0 - 5k, \quad x_3 = x_0 + 3k,$$

որտեղ $k \in \mathbb{Z}$, իսկ (x_0, y_0)-ն նշված հավասարման որևէ (մասնակի) Դիոֆանտյան լուծում է (հետևություն 2.2): Վերցնելով $(x_0, y_0) = (2, 1)$, կստանանք՝

$$y = 1 - 5k, \quad x_3 = 2 + 3k, \quad k \in \mathbb{Z} :$$

Այժմ լուծենք $9x_1 + 12x_2 = 3y$ կամ $3x_1 + 4x_2 = y$ Դիոֆանտյան հավասարումը, որտեղ $y = 1 - 5k$, $k \in \mathbb{Z}$: Նկատելով $3x_1 + 4x_2 = 1 - 5k$, $k \in \mathbb{Z}$ հավասարման $(x_1^\circ, x_2^\circ) = (3 - 3k, -2 + k)$ (մասնակի) Դիոֆանտյան լուծումը, կունենանք՝

$$x_1 = 3 - 3k - 4k', \quad x_2 = -2 + k + 3k', \quad k' \in \mathbb{Z} :$$

Այսպիսով, սկզբնական հավասարման Դիոֆանտյան լուծումներն են՝

$$x_1 = 3 - 3k - 4k', \; x_2 = -2 + k + 3k', \; x_3 = 2 + 3k, \quad k, k' \in \mathbb{Z} \;) :$$

13. Օգտվելով հատկություն 3.7-ից, լուծել հետևյալ գծային Դիոֆանտյան հավասարումները՝

$$8x_1 - 4x_2 + 10x_3 = 6,$$

$$3x_1 + 5x_2 + 2x_3 + 8x_4 = 15 :$$

14. Ապացուցել, որ հետևյալ ոչ գծային Դիոֆանտյան հավասարումը չունի Դիոֆանտյան լուծում՝

$$9x^2 + 2 = y^2 :$$

(Ցուցում. ենթադրելով հակառակը, կունենանք՝ $9x^2 + 2 \equiv y^2 (mod\, 3)$, $2 \equiv y^2 (mod\, 3)$, որը հնարավոր չէ):

15. Լուծել

$$\begin{aligned}&5x \equiv 12(mod\,16),\\&16x \equiv 27(mod\,29),\\&22x \equiv 5(mod\,12)\end{aligned}$$

հավասարումները:

16. Լուծել

$$\begin{aligned}&2x + y \equiv 4(mod\,7),\\&4x + 2y \equiv 6(mod\,8)\end{aligned}$$

հավասարումները: (Ցուցում. առաջին հավասարումը գրել $2x \equiv 4 - y(mod\,7)$ տեսքով և $y = 0, 1, \ldots, 6$ արժեքների դեպքում լուծել համապատասխան հավասարումը):

17. Լուծել բաղդատումների հետևյալ Չինական համակարգերը՝

$$\begin{cases} x \equiv 3(mod\,4), \\ x \equiv 1(mod\,3), \end{cases}$$

$$\begin{cases} x \equiv 2(mod\,5), \\ x \equiv 1(mod\,6), \\ x \equiv 3(mod\,7) : \end{cases}$$

18. Լուծել բաղդատումների հետևյալ համակարգը՝

$$\begin{cases} 2x \equiv 1(mod\,3), \\ 3x \equiv 2(mod\,5), \\ 5x \equiv 4(mod\,7), \end{cases}$$

նախ հավասարումներից յուրաքանչյուրը բերելով $x \equiv a(mod\,b)$ տեսքի (օգտվելով թեորեմ 3.2-ից):

Գ լ ու խ 4

ԵՐԿՈՒ ԱՄԲՈՂՋ ԹՎԵՐԻ ԱՄԵՆԱՓՈՔՐ ԸՆԴՀԱՆՈՒՐ ԲԱԶՄԱՊԱՏԻԿԸ

q ամբողջ թիվը կոչվում է a և b ամբողջ թվերի **ընդհանուր բազմապատիկ** (պատիկ), եթե q-ն միաժամանակ a-ի և b-ի պատիկն է, այսինքն միաժամանակ բաժանվում է a-ի և b-ի վրա: Ակնհայտ է, որ եթե a և b ամբողջ թվերից գոնե մեկը հավասար է զրոյի, ապա դրանց միակ ընդհանուր բազմապատիկը կլինի զրոն, որովհետև միակ ամբողջ թիվը, որ բաժանվում է զրոյի վրա զրոն է՝ $0 = 0 \cdot c$: Հակառակ դեպքում, այսինքն երբ $a \neq 0$ և $b \neq 0$, դրանց ընդհանուր բազմապատիկների բազմության մեջ գոյություն կունենա բնական (ամբողջ և դրական) թիվ; Այդպիսին է, օրինակ,

$$|a \cdot b| = a \cdot b \cdot sign(a \cdot b) > 0$$

բնական թիվը: Սակայն բնական թվերի յուրաքանչյուր բազմություն ունի միարժեքորեն որոշվող ամենափոքր (կամ փոքրագույն) տարր: Այսպիսով հանգում ենք հետևյալ գաղափարին (հասկացությանը):

Երկու ոչ զրոյական a, b ամբողջ թվերի բոլոր ընդհանուր բազմապատիկների բազմության մեջ գոյություն ունեցող ամենափոքր բնական թիվը կոչվում է a, b ամբողջ թվերի **ամենափոքր ընդհանուր բազմապատիկ** և նշանակվում է ԸԱԲ $[a, b]$-ով կամ համառոտ՝ $[a, b]$-ով:

Ակնհայտ է, որ ցանկացած ոչ զրոյական a և b ամբողջ թվերի համար $[a, b] = [b, a]$ և $[a, a] = |a|$:

Հաջորդ հատկությունը ևս ակնհայտ է:

Հատկություն 4.1: *Ոչ զրոյական a և b ամբողջ թվերի ընդհանուր բազմապատիկների բազմությունը համընկնում է*

ա) a և $-b$ ամբողջ թվերի ընդհանուր բազմապատիկների բազմության հետ;

բ) a և $|b|$ ամբողջ թվերի ընդհանուր բազմապատիկների բազմության հետ;

գ) $-a$ և b ամբողջ թվերի ընդհանուր բազմապատիկների բազմության հետ;

դ) $|a|$ *և* b *ամբողջ թվերի ընդհանուր բազմապատիկների բազմության հետ;*

ե) $-a$ *և* $-b$ *ամբողջ թվերի ընդհանուր բազմապատիկների բազմության հետ;*

զ) $|a|$ *և* $|b|$ *բնական թվերի ընդհանուր բազմապատիկների բազմության հետ:*

Հետևաբար՝

$$[a,b] = [a,-b] = [a,|b|] = [-a,b] = [|a|,b] = [-a,-b] = [|a|,|b|] : \quad \square$$

Անցնենք ոչ զրոյական a և b ամբողջ թվերի բոլոր ընդհանուր բազմապատիկների (բազմության) նկարագրությանը, որտեղից և կստացվի դրանց ամենափոքր ընդհանուր բազմապատիկի որոշման եղանակը:

Թեորեմ 4.1*: Որպեսզի* q *ամբողջ թիվը լինի ոչ զրոյական* a *և* b *ամբողջ թվերի ընդհանուր բազմապատիկը անհրաժեշտ է և բավարար, որ գոյություն ունենա այնպիսի* t *ամբողջ թիվ, որ*

$$q = \frac{ab}{d} \cdot t,$$

որտեղ $d = (a,b)$*:*

Ապացուցում: Նախ նկատենք, որ յուրաքանչյուր t ամբողջ թվի դեպքում $\frac{ab}{d} \cdot t$ տեսքի թիվը ամբողջ է և այն միշտ բաժանվում է a-ի և b-ի վրա: Իրոք, քանի որ d-ն a-ի և b-ի (ամենամեծ) ընդհանուր բաժանարարն է , ապա գոյություն ունեն այնպիսի a_1 և b_1 ամբողջ թվեր, որ

$$a = da_1, \quad b = db_1;$$

Հետևաբար՝

$$\frac{ab}{d} \cdot t = a(b_1 t) = b(a_1 t),$$

որտեղ $b_1 t$-ն և $a_1 t$-ն ևս ամբողջ են: Այսպիսով, *բավարարությունն* ապացուցված է: Ապացուցենք *անհրաժեշտությունը*:

Դիցուք q-ն ոչ զրոյական a և b ամբողջ թվերի համար ընդհանուր բազմապատիկ է և դիցուք $d = (a, b)$; Այդ դեպքում $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ (հատկություն 3.1) և գոյություն կունենան այնպիսի k_1, k_2, a_1 և b_1 ամբողջ թվեր, որ $q = ak_1 = bk_2$, $a = da_1$ և $b = db_1$; Հետևաբար

$$ak_1 = bk_2,$$

$$\frac{a}{d}k_1 = \frac{b}{d}k_2$$

և քանի որ $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, ապա, համաձայն հատկություն 3.4-ի, k_1-ը կբաժանվի $\frac{b}{d} = b_1$-ի վրա, այսինքն $k_1 = \frac{b}{d} \cdot t$ որևէ t ամբողջ թվի համար:

Այսպիսով՝

$$q = a \cdot k_1 = a\frac{b}{d} \cdot t, \quad t \in \mathbb{Z} : \qquad \square$$

Որպես անմիջական հետևություն ստանում ենք հետևյալ արդյունքը:

Հետևություն 4.1: *Ոչ զրոյական a և b ամբողջ թվերի բոլոր ընդհանուր բազմապատիկների M բազմությունը որոշվում է հետևյալ կերպ՝*

$$M = \left\{\frac{ab}{d} \cdot t \mid t \in \mathbb{Z}\right\},$$

որտեղ $d = (a, b)$: $\square$

Հետևություն 4.2: *Երկու ոչ զրոյական a և b ամբողջ թվերի ամենափոքր ընդհանուր բազմապատիկը որոշվում է հետևյալ բանաձևով՝*

$$[a, b] = \frac{a \cdot b}{(a, b)} sign(a \cdot b) = \frac{|ab|}{(a, b)}$$

(հետևաբար $[a, b]$-ն կարելի է որոշել (հաշվել) օգտվելով էվկլիդեսի ալգորիթմից): Մասնավորապես, եթե a-ն և b-ն բնական թվեր են, ապա

$$[a, b] = \frac{a \cdot b}{(a, b)} :$$

Ապացույց: Քանի որ ոչ զրոյական a և b ամբողջ թվերի յուրաքանչյուր q ընդհանուր բազմապատիկ ունի

$$q = \frac{ab}{d} \cdot t, \quad d = (a, b)$$

տեսքը, որտեղ t-ն ամբողջ թիվ է, ապա բնական թիվ հանդիսացող յուրաքանչյուր ընդհանուր բազմապատիկ կլինի հետևյալ տեսքի`

$$|q| = \left| \frac{ab}{d} \cdot t \right| = \frac{|ab|}{d} \cdot |t| \geqslant \frac{|ab|}{d} :$$

Հետևաբար, ըստ ամենափոքր ընդհանուր բազմապատիկի սահմանման,

$$[a, b] = \frac{|ab|}{d} = \frac{ab}{d} sign(a \cdot b) :$$

□

Հետևություն 4.3: *Ոչ զրոյական a և b ամբողջ թվերի յուրաքանչյուր q ընդհանուր բազմապատիկ բաժանվում է դրանց $[a, b]$ ամենափոքր ընդհանուր բազմապատիկի վրա:*

Ապացույց: Համաձայն թեորեմ 4.1-ի գոյություն ունի այնպիսի t ամբողջ թիվ, որ

$$q = \frac{ab}{d} \cdot t = \frac{ab \cdot sign(a \cdot b)}{d} \cdot \frac{t}{sign(a \cdot b)} = [a, b] \cdot \frac{t}{sign(a \cdot b)},$$

որտեղ $\dfrac{t}{sign(a \cdot b)} = \pm t$ թիվը ևս ամբողջ է: □

Այս հատկությունը հեշտությամբ ապացուցվում է նաև անմիջական ստուգման եղանակով: Իրոք, համաձայն մնացորդով բաժանման կանոնի, նախ գրում ենք $q = [a, b] \cdot l + r$, $0 \leqslant r < [a, b]$, և ապացուցում, որ այստեղ $r = 0$, որովհետև հակառակ դեպքում r-ը կլինի $[a, b]$-ից փոքր դրական ընդհանուր բազմապատիկ a-ի և b-ի համար, որը հակասում է $[a, b]$-ի սահմանմանը:

Հետևություն 4.4: *Ոչ զրոյական a և b ամբողջ թվերը կլինեն փոխադարձաբար պարզ այն և միայն այն դեպքում, երբ*

$$[a, b] = |a \cdot b| = ab \cdot sign(a \cdot b) :$$

Մասնավորապես, a և b բնական թվերը կլինեն փոխադարձաբար պարզ այն և միայն այն դեպքում, երբ

$$[a, b] = a \cdot b :$$

Ապացուցում: Քանի որ այս դեպքում $d = (a, b) = 1$, ապա համաձայն հետևություն 4.2-ի՝

$$[a, b] = \frac{|ab|}{d} = |a \cdot b| : \qquad \square$$

Հետևություն 4.5: *Ոչ զրոյական a և b ամբողջ թվերի համար $\frac{[a,b]}{a}$ և $\frac{[a,b]}{b}$ ամբողջ թվերը կլինեն փոխադարձաբար պարզ: Եվ հակառակը, եթե x-ը դրական ընդհանուր բազմապատիկ է ոչ զրոյական a և b ամբողջ թվերի համար և $\left(\frac{x}{a}, \frac{x}{b}\right) = 1$, ապա $x = [a, b]$:*

Ապացուցում: Ելնելով

$$[a, b] = \frac{a \cdot b}{d} \cdot sign(a \cdot b), \quad d = (a, b)$$

հավասարություններից, կունենանք՝

$$\frac{[a, b]}{a} = \frac{b}{d} \cdot sign(a \cdot b) = \pm\frac{b}{d},$$

$$\frac{[a, b]}{b} = \frac{a}{d} \cdot sign(a \cdot b) = \pm\frac{a}{d} :$$

Մյուս կողմից՝

$$\left(\pm\frac{a}{d}, \pm\frac{b}{d}\right) = \left(\frac{a}{d}, \frac{b}{d}\right) = 1 :$$

Եվ հակառակը, եթե $x = [a, b] \cdot t$, որտեղ $t > 0$, ապա ըստ պայմանի՝ $\left(\frac{[a,b] \cdot t}{a}, \frac{[a,b] \cdot t}{b}\right) = 1$, $t\left(\frac{ab\, sign(a,b)}{da}, \frac{ab\, sign(a,b)}{db}\right) = 1$, $t\left(\pm\frac{b}{d}, \pm\frac{a}{d}\right) = 1$, $t\left(\frac{b}{d}, \frac{a}{d}\right) = 1$, $t = 1$ և $x = [a, b]$: $\square$

Հետևություն 4.6: *Ոչ զրոյական a և b ամբողջ թվերի և k բնական թվի համար տեղի ունի հետևյալ հավասարությունը՝*

$$[ak, bk] = k \cdot [a, b] :$$

Ապացույց: Եթե $d = (ak, bk)$, ապա

$$[ak, bk] = \frac{|ak \cdot bk|}{d} = \frac{|ak \cdot bk|}{(ak, bk)} = \frac{k^2|a \cdot b|}{k \cdot (a, b)} = k\frac{|a \cdot b|}{(a, b)} = k \cdot [a, b] : \qquad \square$$

Հետևություն 4.7*: Եթե ոչ զրոյական a և b ամբողջ թվերը բաժանվում են միևնույն k բնական թվի վրա, ապա $[a, b]$-ն ևս կբաժանվի k-ի վրա, ընդ որում տեղի ունի հետևյալ հավասարությունը՝*

$$\frac{[a, b]}{k} = \left[\frac{a}{k}, \frac{b}{k}\right] :$$

Ապացույց: Ըստ նախորդ հետևության՝

$$k \cdot \left[\frac{a}{k}, \frac{b}{k}\right] = \left[k \cdot \frac{a}{k}, k \cdot \frac{b}{k}\right] = [a, b],$$

այսինքն $[a, b]$-ն ևս բաժանվում է k-ի վրա, ընդ որում՝

$$\frac{[a, b]}{k} = \left[\frac{a}{k}, \frac{b}{k}\right] : \qquad \square$$

Հատկություն 4.2 (ամենափոքր ընդհանուր բազմապատիկի զուգորդականությունը): *Կամայական ոչ զրոյական a, b և c ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$[a, [b, c]] = [[a, b], c] :$$

Ապացույց: Բավական է ապացուցել, որ a և $[b, c]$ ամբողջ թվերի ընդհանուր բազմապատիկների բազմությունը համընկնում է $[a, b]$ և c ամբողջ թվերի ընդհանուր բազմապատիկների բազմության հետ: Իրոք, եթե q ամբողջ թիվը բաժանվում է a-ի և $[b, c]$-ի վրա, ապա այն կբաժանվի նաև b-ի և c-ի վրա:

Հետևաբար, q-ն լինելով a-ի և b-ի ընդհանուր բազմապատիկը, կբաժանվի նաև դրանց $[a, b]$ ամենափոքր ընդհանուր բազմապատիկի վրա (հետևություն 4.3):

Նույնանման քայլերով ապացուցվում է նաև հակառակը, որ $[a, b]$ և c ամբողջ թվերի յուրաքանչյուր ընդհանուր բազմապատիկ ընդհանուր բազմապատիկ է նաև a և $[b, c]$ ամբողջ թվերի համար: $\square$

Վարժություններ և խնդիրներ

1. Ապացուցել, որ $[a,b]$-ն բաժանվում է (a,b)-ի վրա:

2. Ապացուցել, որ a և b բնական թվերի համար $(a,b) = [a,b]$ այն և միայն այն դեպքում, երբ $a = b$:

3. Որոշել $[221, 324]$-ը՝ օգտվելով հետևություն 4.2-ից և էվկլիդեսի ալգորիթմից:

4. Ցանկացած $n > 0$ բնական թվի համար ապացուցել հետևյալ հավասարությունը՝

$$[n, n+1] = n(n+1);$$

5. Լուծել հետևյալ համակարգը՝

$$\begin{cases} (x,y) = 12, \\ [x,y] = 360, \end{cases}$$

բնական թվերով $(x, y \in \mathbb{N})$:

6. Լուծել հետևյալ համակարգը՝

$$\begin{cases} xy = 20, \\ [x,y] = 10, \end{cases}$$

բնական թվերով $(x, y \in \mathbb{N})$:

7. Ապացուցել, որ կամայական ոչ զրոյական a, b, c, d ամբողջ թվերի համար տեղի ունեն հետևյալ հավասարությունները՝

$$[[[a,b],c],d] = [[a,[b,c]],d] = [a,[[b,c],d]] = [a,[b,[c,d]]] = [[a,b],[c,d]] :$$

Գ լ ու խ 5

ՄԻ ՔԱՆԻ ԱՄԲՈՂՋ ԹՎԵՐԻ ԱՄԵՆԱՄԵԾ ԸՆԴՀԱՆՈՒՐ ԲԱԺԱՆԱՐԱՐԸ ԵՎ ԱՄԵՆԱՓՈՔՐ ԸՆԴՀԱՆՈՒՐ ԲԱԶՄԱՊԱՏԻԿԸ

c ամբողջ թիվը կոչվում է վերջավոր թվով ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի $(n \geqslant 2)$ ընդհանուր բաժանարար, եթե c-ն բաժանարար է $a_1, \ldots, a_n$ ամբողջ թվերից յուրաքանչյուրի համար: Քանի որ ոչ զրոյական a ամբողջ թվի բոլոր բաժանարարների բազմությունը վերջավոր է, ապա ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի բոլոր ընդհանուր բաժանարարների բազմությունը ևս կլինի ամբողջ թվերի վերջավոր բազմություն, հետևաբար այդ բազմությունը կպարունակի միարժեքորեն որոշվող ամենամեծ տարր, որը և կոչվում է ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենամեծ ընդհանուր բաժանարար ու նշանակվում է ԱԸԲ$(a_1, \ldots, a_n)$-ով կամ համառոտ՝ $(a_1, \ldots, a_n)$-ով: Ակիայտ է, որ $(a_1, \ldots, a_n) \geqslant 1$:

Այսպիսով $d > 0$ բնական թիվը կոչվում է ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենամեծ ընդհանուր բաժանարար, եթե տեղի ունեն հետևյալ երկու պայմանները՝

ա$_1$) d-ն ընդհանուր բաժանարար է $a_1, \ldots, a_n$ ամբողջ թվերի համար;

ա$_2$) եթե d' ամբողջ թիվը $a_1, \ldots, a_n$ ամբողջ թվերի համար ընդհանուր բաժանարար է, ապա $d' \leqslant d$:

q ամբողջ թիվը կոչվում է վերջավոր թվով ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի $(n \geqslant 2)$ ընդհանուր բազմապատիկ, եթե q-ն բաժանվում է $a_1, \ldots, a_n$ ամբողջ թվերից յուրաքանչյուրի վրա: Ակնհայտ է, որ ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ընդհանուր բազմապատիկների բազմության մեջ գոյություն ունի բնական (ամբողջ և դրական) թիվ: Այդպիսին է, օրինակ,

$$|a_1 \cdot \ldots \cdot a_n| = a_1 \cdot \ldots \cdot a_n \cdot sign(a_1 \cdots a_n) > 0$$

բնական թիվը:

Ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի բոլոր ընդհանուր բազմապատիկների բազմության մեջ գոյություն ունեցող և միարժեքորեն որոշվող ամենափոքր բնական թիվը կոչվում է $a_1, \ldots, a_n$

ամբողջ թվերի ամենափոքր ընդհանուր բազմապատիկ և նշանակվում է ԸԱԲ $[a_1, \ldots, a_n]$-ով կամ համառոտ՝ $[a_1, \ldots, a_n]$-ով:

Այսպիսով $m > 0$ բնական թիվը կոչվում է ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենափոքր ընդհանուր բազմապատիկ, եթե տեղի ունեն հետևյալ երկու պայմանները

- բ$_1$) m-ը ընդհանուր բազմապատիկ է $a_1, \ldots, a_n$ ամբողջ թվերի համար;
- բ$_2$) $a_1, \ldots, a_n$ ամբողջ թվերի կամայական $m' > 0$ ընդհանուր բազմապատիկի համար, տեղի ունի $m \leqslant m'$ անհավասարությունը:

Վերջավոր թվով ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարի որոշման խնդիրը հանգեցվում է երկու ոչ զրոյական ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու խնդրին, որն արդեն քննարկվել է գլուխ 2-ում: Իրոք, եթե նշանակենք՝

$$\begin{aligned} &(a_1, a_2) = d_2, \\ &(d_2, a_3) = d_3, \\ &\ldots \quad \ldots \\ &(d_{n-1}, a_n) = d_n, \end{aligned}$$

ապա՝ $d_n = (a_1, \ldots, a_n)$: Այս հավասարությունը կապացուցենք վերհանգման եղանակով: Նախ $\mathcal{D}_{a_1,\ldots,a_n}$-ով նշանակենք $a_1, \ldots, a_n$ ամբողջ թվերի բոլոր ընդհանուր բաժանարարների բազմությունը ($n \geqslant 1$): Մասնավորապես, $\mathcal{D}_a$-ն a-ի բոլոր բաժանարարների բազմությունն է:

Հատկություն 5.1: *Ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$\mathcal{D}_{a_1,\ldots,a_n} = \mathcal{D}_{d_{n-1},a_n} = \mathcal{D}_{d_n}$$

և, հետևաբար, $(a_1, \ldots, a_n) = (d_{n-1}, a_n) = d_n$, որտեղ $n \geqslant 3$;

Ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարը բաժանվում է դրանց յուրաքանչյուր ընդհանուր բաժանարարի վրա:

Ապացուցում: Երկրորդ

$$\mathcal{D}_{d_{n-1},a_n} = \mathcal{D}_{d_n}$$

հավասարությունը տեղի ունի շնորհիվ հետևություն 2.1-ի: Առաջին

$$\mathcal{D}_{a_1,\ldots,a_n} = \mathcal{D}_{d_{n-1},a_n}$$

հավասարությունը ապացուցենք վերհանգման եղանակով: $n = 3$ դեպքում կունենանք

$$\mathcal{D}_{a_1,a_2,a_3} = \mathcal{D}_{d_2,a_3},$$

որը ճիշտ է: Իրոք, ակնհայտ է՝

$$\mathcal{D}_{d_2,a_3} \subseteq \mathcal{D}_{a_1,a_2,a_3},$$

իսկ հակառակ ներդրումը՝

$$\mathcal{D}_{a_1,a_2,a_3} \subseteq \mathcal{D}_{d_2,a_3},$$

նորից բխում է հետևություն 2.1-ից, որ a_1, a_2-ի յուրաքանչյուր ընդհանուր բաժանարար կլինի բաժանարար նաև $(a_1, a_2) = d_2$-ի համար:

Ենթադրելով ապացուցվելիք հավասարությունը ճիշտ $n-1$ հատ ամբողջ թվերի դեպքում, այսինքն՝

$$\mathcal{D}_{a_1,\ldots,a_{n-1}} = \mathcal{D}_{d_{n-2},a_{n-1}} = \mathcal{D}_{d_{n-1}},$$

կունենանք՝

$$\mathcal{D}_{d_{n-1},a_n} \subseteq \mathcal{D}_{a_1,\ldots,a_n}$$

և

$$\mathcal{D}_{a_1,\ldots,a_n} \subseteq \mathcal{D}_{d_{n-1},a_n};$$

Այսպիսով՝

$$\mathcal{D}_{a_1,\ldots,a_n} = \mathcal{D}_{d_{n-1},a_n}; \qquad \square$$

Համանման եղանակով նկարագրվում է նաև վերջավոր թվով ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենափոքր ընդհանուր բազմապատիկը: Իրոք, եթե նշանակենք՝

$$\begin{aligned}
&[a_1, a_2] = m_2,\\
&[m_2, a_3] = m_3,\\
&\cdots \quad \cdots\\
&[m_{n-1}, a_n] = m_n,
\end{aligned}$$

ապա՝

$$m_n = [a_1, \ldots, a_n];$$

Այս հավասարությունն էլ է ապացուցվում վերհանգման եղանակով: Նախ $\mathcal{M}_{a_1,\ldots,a_n}$-ով նշանակում ենք $a_1, \ldots, a_n$ ամբողջ թվերի բոլոր ընդհանուր բազմապատիկների բազմությունը $(n \geqslant 1)$: Մասնավորապես, $\mathcal{M}_a$-ն a-ի բոլոր բազմապատիկների բազմությունն է:

Հատկություն 5.2: *Ոչ զրոյական* $a_1, \ldots, a_n$ *ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$\mathcal{M}_{a_1,\ldots,a_n} = \mathcal{M}_{m_{n-1},a_n} = \mathcal{M}_{m_n} :$$

և, հետևաբար, $[a_1, \ldots, a_n] = [m_{n-1}, a_n] = m_n$*, որտեղ* $n \geqslant 3$*:*

Ոչ զրոյական $a_1, \ldots, a_n$ *ամբողջ թվերի յուրաքանչյուր ընդհանուր բազմապատիկ բաժանվում է դրանց ամենափոքր ընդհանուր բազմապատիկի վրա:*

Ապացույց: Կրկնվում են նախորդ հատկության ապացուցման քայլերը: Երկրորդ հավասարությունը տեղի ունի շնորհիվ հետևություն 4.3-ի, իսկ առաջին հավասարությունը ստուգվում է վերհանգման եղանակով: □

Հատկություն 5.3: *Զույգ առ զույգ փոխադարձաբար պարզ* $a_1, \ldots, a_n$ *ոչ զրոյական ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$[a_1, \ldots, a_2] = |a_1 \cdot a_2 \cdot \ldots \cdot a_n|,$$

որտեղ $n \geqslant 2$*:*

Ապացույց: Իրոք, համաձայն հետևություն 4.4-ի,

$$m_2 = [a_1, a_2] = |a_1 \cdot a_2| :$$

Այսպիսով ձևակերպված հատկությունը ճիշտ է $n = 2$ դեպքում: Ենթադրելով այն ճիշտ $n-1$ թվով անդամներ ունեցող $a_1, \ldots, a_{n-1}$ հաջորդականության համար կունենանք՝

$$m_n = [m_{n-1}, a_n] = |m_{n-1} \cdot a_n| = |a_1 \cdot a_2 \cdot \ldots \cdot a_{n-1} \cdot a_n|,$$

համաձայն վերհանգման ենթադրության, հետևություն 4.4-ի և հատկություն 3.2-ի, ըստ որի a_n-ը կլինի փոխադարձաբար պարզ նաև $a_1 \cdots a_{n-1}$ արտադրյալի հետ: □

Հատկություն 5.4: *Ոչ զրոյական* $a_1, \ldots, a_n$ *ամբողջ թվերի համար գոյություն ունեն այնպիսի* $x_1, \ldots, x_n$ *ամբողջ թվեր, որ*

$$(a_1, \ldots, a_n) = a_1x_1 + \cdots + a_nx_n, \quad n \geqslant 2 :$$

Ավելի ճիշտ՝

$$(a_1, \ldots, a_n) =$$
$$= \min\{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in \mathbb{Z},\ a_1x_1 + \cdots + a_nx_n > 0\} :$$

Ապացուցում: Պետք է կրկնել թեորեմ 2.1-ի ապացուցումը, վերցնելով ՝

$$\mathcal{M} = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_1, x_2, \ldots, x_n \in \mathbb{Z}\} :$$ □

Սահմանում: Ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերը (հաջորդականությունը, համակարգը) կոչվում են փոխադարձաբար պարզ, եթե

$$(a_1, \ldots, a_n) = 1 :$$

Հատկություն 5.5*: Ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերը կլինեն փոխադարձաբար պարզ այն և միայն այն դեպքում, երբ գոյություն ունեն այնպիսի $x_1, \ldots, x_n$ ամբողջ թվեր, որ $a_1x_1 + \cdots + a_nx_n = 1$:*

Ապացուցում: Թեորեմ 3.1-ի ապացուցման կրկնությունն է: □

Հատկություն 5.6*: Եթե d-ն ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարն է, ապա $\dfrac{a_1}{d}, \ldots, \dfrac{a_n}{d}$ ամբողջ թվերը կլինեն փոխադարձաբար պարզ:*

Ապացուցում: Հետևություն 3.1-ի ապացուցման կրկնությունն է և բխում է հատկություն 5.5-ից: □

Հատկություն 5.7*: Յանկացած ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի և յուրաքանչյուր $c > 0$ ամբողջ թվի համար տեղի ունի հետևյալ հավասարությունը՝*

$$c \cdot (a_1, \ldots, a_n) = (ca_1, \ldots, ca_n) :$$

Ապացուցում: Հատկություն 2.5-ի ապացուցման կրկնությունն է: □

Հատկություն 5.8*: Եթե ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերը բաժանվում են $c > 0$ ամբողջ թվի վրա, ապա $(a_1, \ldots, a_n)$-ը ևս կբաժանվի c-ի վրա, ընդ որում տեղի ունի հետևյալ հավասարությունը՝*

$$\frac{(a_1, \ldots, a_n)}{c} = \left(\frac{a_1}{c}, \ldots, \frac{a_n}{c}\right) :$$

Ապացուցում: Հետևություն 2.3-ի ապացուցման կրկնությունն է: □

Հատկություն 5.9: *Ցանկացած ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի և յուրաքանչյուր $c > 0$ ամբողջ թվի համար տեղի ունի հետևյալ հավասարությունը՝*

$$c \cdot [a_1, \ldots, a_n] = [ca_1, \ldots, ca_n] :$$

Ապացուցում: Հավասարությունը հեշտ է ապացուցել անմիջական ստուգման եղանակով: Դիցուք $m = [a_1, \ldots, a_n]$, այդ դեպքում cm-ը կլինի $ca_1, \ldots, ca_n$ ամբողջ թվերի ընդհանուր բազմապատիկը: Քանի որ $cm > 0$, ապա մնում է ապացուցել, որ գոյություն չունի cm-ից փոքր և $ca_1, \ldots, ca_n$ ամբողջ թվերի ընդհանուր բազմապատիկ հանդիսացող $q > 0$ ամբողջ թիվ: Իրոք, եթե $q > 0$ և q-ն $ca_1, \ldots, ca_n$ ամբողջ թվերի համար ընդհանուր բազմապատիկ է, ապա գոյություն կունենան այնպիսի $t_1, \ldots, t_n$ ամբողջ թվեր, որ

$$\begin{gathered} q = (ca_1)t_1, \\ \cdots \\ q = (ca_n)t_n; \end{gathered}$$

Հետևաբար՝

$$c\,(a_1t_1) = \cdots = c\,(a_nt_n)\,,$$

որտեղից կստանանք՝

$$a_1t_1 = \cdots = a_nt_n,$$

այսինքն, a_1t_1-ը կլինի $a_1, \ldots, a_n$ ամբողջ թվերի (դրական) ընդհանուր բազմապատիկը: Ուստի, այն կբաժանվի $[a_1, \ldots, a_n] = m$-ի վրա՝

$$a_1t_1 = m \cdot t, \quad t \in \mathbb{Z}, \;\; t \geqslant 1,$$

որտեղից՝

$$ca_1t_1 = cmt,$$

այսինքն՝

$$q = (cm) \cdot t \geqslant cm :$$ □

Հատկություն 5.10: *Եթե ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերը բաժանվում են $c > 0$ ամբողջ թվի վրա, ապա $[a_1, \ldots, a_n]$-ը ևս կբաժանվի c-ի վրա, ընդ որում տեղի ունի հետևյալ հավասարությունը՝*

$$\frac{[a_1, \ldots, a_n]}{c} = \left[\frac{a_1}{c}, \ldots, \frac{a_n}{c}\right] :$$

Ապացուցում: Հետևություն 4.7-ի ապացուցման կրկնությունն է: □

Վերջավոր թվով ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի ամենամեծ ընդհանուր բաժանարարի և ամենափոքր ընդհանուր բազմապատիկի միջև եղած կապը բացահայտվում է հետևյալ հատկությամբ.

Հատկություն 5.11: *Կամայական ոչ զրոյական $a_1, \ldots, a_n$ ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$[a_1, \ldots, a_n] = \frac{|a_1 \cdot \ldots \cdot a_n|}{(A_1, \ldots, A_n)}, \quad n \geqslant 2,$$

որտեղ՝

$$A_1 = \frac{a_1 \cdot \ldots \cdot a_n}{a_1},$$
$$A_2 = \frac{a_1 \cdot \ldots \cdot a_n}{a_2},$$
$$\ldots \quad \ldots \quad \ldots$$
$$A_n = \frac{a_1 \cdot \ldots \cdot a_n}{a_n} :$$

Մասնավորապես, $n = 2$ դեպքում ստանում ենք հետևութուն 4.2-ից հայտնի բանաձևը, իսկ $n = 3$ դեպքում կունենանք՝

$$[a_1, a_2, a_3] = \frac{|a_1 a_2 a_3|}{(a_2 a_3, a_1 a_3, a_1 a_2)} :$$

Ապացուցում: Դիցուք $d = (A_1, \ldots, A_n)$ և $\dfrac{|a_1 \cdots a_n|}{d} = x$: Քանի որ

$$x = a_1 \frac{A_1}{d} sign(a_1 A_1),$$
$$x = a_2 \frac{A_2}{d} sign(a_2 A_2),$$
$$\ldots \quad \ldots \quad \ldots$$
$$x = a_n \frac{A_n}{d} sign(a_n A_n),$$

ապա x-ը $a_1, \ldots, a_n$ ամբողջ թվերի համար ընդհանուր բազմապատիկ է: Հետևաբար (հատկություն 5.2), x-ը կբաժանվի նաև $[a_1, \ldots, a_n] = m$-ի վրա, այսինքն գոյություն ունի այնպիսի t ամբողջ թիվ, որ $x = m \cdot t$, որտեղ $t \geqslant 1$: Այսպիսով կունենանք՝

$$\frac{A_1}{d} = \frac{m}{a_1} t \, sign(a_1 A_1),$$

$$\frac{A_2}{d} = \frac{m}{a_2} t\, sign(a_2 A_2),$$
$$\dots \quad \dots \quad \dots$$
$$\frac{A_n}{d} = \frac{m}{a_n} t\, sign(a_n A_n);$$

Ուստի, t բնական թիվը հանդիսանում է ընդհանուր բաժանարար փոխադարձաբար պարզ (համաձայն հատկություն 5.6-ի) $\frac{A_1}{d}, \dots, \frac{A_n}{d}$ ամբողջ թվերի համար: Հետևաբար $t = 1$ և $x = m$, այսինքն՝

$$\frac{|a_1 \cdots a_n|}{d} = [a_1, \dots, a_n] :$$ □

Վարժություններ և խնդիրներ

1. Ապացուցել, որ
$$(a_1, a_2, a_3) = (a_1, (a_2, a_3))\,,$$
$$[a_1, a_2, a_3] = [a_1, [a_2, a_3]]\,;$$

2. Ապացուցել, որ
$$(a_1, a_2, a_3, a_4) = ((a_1, a_2), (a_3, a_4))\,,$$
$$[a_1, a_2, a_3, a_4] = [[a_1, a_2], [a_3, a_4]]\,;$$

3. Ապացուցել, որ
$$(a_1, a_2, a_3, a_4) = ((a_1, a_2), a_3, a_4)\,,$$
$$[a_1, a_2, a_3, a_4] = [[a_1, a_2], a_3, a_4]\,;$$

4. Ապացուցել, որ
$$(a_1, a_2, a_3, \dots, a_n) = ((a_1, a_2), a_3, \dots, a_n)\,,$$
$$[a_1, a_2, a_3, \dots, a_n] = [[a_1, a_2], a_3, \dots, a_n] :$$

5. $15, 42, 70$ բնական թվերի հաջորդականությունը փոխադարձաբար պարզ է, սակայն դրա ցանկացած զույգը փոխադարձաբար պարզ չէ: Կառուցել չորս (և հինգ) ոչ զրոյական բնական թվերի այդպիսի հաջորդականություն: Գոյություն կունենա արդյոք n ոչ զրոյական բնական թվերի այդպիսի հաջորդականություն՝ ցանկացած $n \geqslant 3$ բնական թվի դեպքում:

6. Որպեսզի $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ գծային Դիոֆանտյան հավասարումը ունենա Դիոֆանտյան լուծում անհրաժեշտ է և բավարար, որ b-ն բաժանվի $d = (a_1, a_2, \ldots, a_n)$-ի վրա: Վերհանգման եղանակով ապացուցել, որ այս դեպքում նշված հավասարումը կունենա անվերջ թվով լուծումներ:

7. Դիցուք $d = (a_1, a_2, \ldots, a_n, m)$, որտեղ $m \in \mathbb{N}$, $a_i \neq 0$, $i = 1, \ldots, n$: Որպեսզի

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b(mod\, m)$$

բաղդատումն ունենա լուծում անհրաժեշտ է և բավարար, որ b-ն բաժանվի d-ի վրա:

Գ լ ու խ 6

ՊԱՐԶ ԹՎԵՐ: ՎԻԼՍՈՆԻ ԹԵՈՐԵՄԸ: ԹՎԱԲԱՆՈՒԹՅԱՆ ՀԻՄՆԱԿԱՆ ԹԵՈՐԵՄԸ: ՄՅՈԲԻՈՒՍԻ ՖՈՒՆԿՑԻԱՆ: ՀԱՆՐԱՀԱՇՎԻ ՀԻՄՆԱԿԱՆ ԹԵՈՐԵՄԸ ՊԱՐԶ ՀԵՆՔՈՎ ԲԱՂԴԱՏՈՒՄՆԵՐԻ ՎԵՐԱԲԵՐՅԱԼ

6.1. Թվի պարզության Վիլսոնի հայտանիշը

Բնական թիվ հանդիսացող բաժանարարները կոչվում են նաև **բնական բաժանարարներ**:

Մեկից մեծ p բնական թիվը կոչվում է **պարզ թիվ**, եթե այն բացի 1-ից և p-ից ուրիշ բնական բաժանարարներ չունի, այսինքն p-ն ունի ընդամենը երկու տարբեր բնական բաժանարարներ՝ 1-ը և p-ն:

Ակնհայտ է, որ 2-ը միակ զույգ պարզ թիվն է:

Մեկից մեծ բնական թիվը կոչվում է **բաղադրյալ**, եթե այն պարզ թիվ չէ (1-ը չի համարվում պարզ կամ բաղադրյալ թիվ): Այսպիսով, $n > 1$ բնական թիվը կոչվում է բաղադրյալ, եթե գոյություն ունի դրա այնպիսի n_1 բնական բաժանարար, որ $1 < n_1 < n$:

Ակնհայտ է, որ բոլոր բաղադրյալ թվերի քանակն անվերջ է, որովհետև, եթե $a \in \mathbb{N}$, $a > 1$, ապա $a \cdot x$-ը կլինի բաղադրյալ թիվ՝ բոլոր $x \in \mathbb{N}$, $x > 1$ բնական թվերի համար: Առաջին անգամ Էվկլիդեսն է ապացուցել, որ բոլոր պարզ թվերի քանակն անվերջ է (թեորեմ 7.1):

Ակնհայտ է, որ երկու կենտ պարզ թվերի տարբերությունը զույգ թիվ է: Սակայն մինչ այժմ հայտնի չէ, կարելի է արդյոք յուրաքանչյուր զույգ թիվ ներկայացնել երկու պարզ թվերի տարբերության տեսքով:

Պարզ թիվ հանդիսացող բաժանարարները կոչվում են նաև **պարզ բաժանարարներ**:

Հատկություն 6.1*: Եթե p-ն որևէ n բնական թվի մեկից մեծ ամենափոքր բնական բաժանարարն է, ապա p-ն պարզ թիվ է: Հետևաբար, մեկից մեծ յուրաքանչյուր բնական թիվ (ուստի և ± 1-ից տարբեր յուրաքանչյուր ամբողջ թիվ) բաժանվում է որևէ պարզ թվի վրա: Մասնավորապես, յուրաքանչյուր n բաղադրյալ թիվ բաժանվում է $\sqrt{n}$-ը չգերազանցող որևէ պարզ թվի վրա:*

Ապացուցում: Ենթադրելով հակառակը ստանում ենք հակասություն: Իրոք, դիցուք p-ն պարզ թիվ չէ, այսինքն այն ունի $1 < a < p$

պայմանին բավարարող a բաժանարար, այդ դեպքում a-ն կլինի նաև n-ի բաժանարար, որը հակասում է p-ի ընտրությանը: Հատկության առաջին մասն ապացուցված է: Դիցուք n-ը բաղադրյալ թիվ է և $n = a \cdot b$, որտեղ $1 < a < n$, $1 < b < n$ և դիցուք $a \leqslant b$: Ուստի $a \leqslant \sqrt{n}$, որովհետև հակառակ դեպքում կունենայինք հակասություն՝ $n = ab > \sqrt{n} \cdot \sqrt{n} = n$: Դիցուք p-ն a-ի որևէ պարզ բաժանարար է: Հետևաբար՝ $p \leqslant a \leqslant \sqrt{n}$, $p \leqslant \sqrt{n}$: □

Հատկություն 6.2*: a ամբողջ թիվը և p պարզ թիվը կամ փոխադարձաբար պարզ են, կամ a-ն բաժանվում է p-ի վրա, այսինքն՝ կամ $(a, p) = 1$ կամ $(a, p) = p$: Մասնավորապես, միմյանցից տարբեր երկու պարզ թվեր փոխադարձաբար պարզ են:*

Ապացուցում: p պարզ թվի միակ բնական բաժանարարներն են 1-ը և p-ն: Հետևաբար, կամ $(a, p) = 1$, կամ $(a, p) = p$: □

***Հետևություն 6.1**: Եթե բաղդատման m մոդուլը պարզ թիվ է, ապա յուրաքանչյուր ոչ զրոյական $[a] \in \mathbb{Z}_m$ մնացքների դաս կլինի հակադարձելի:*

Ապացուցում: Տես հետևություն 3.5-ը: □

Հատկություն 6.3 (էվկլիդես): *Եթե երկու a և b ամբողջ թվերի $a \cdot b$ արտադրյալը բաժանվում է p պարզ թվի վրա, ապա արտադրիչներից գոնե մեկը կբաժանվի p-ի վրա: Մասնավորապես, եթե երկու պարզ թվերի արտադրյալը բաժանվում է p պարզ թվի վրա, ապա արտադրիչներից գոնե մեկը կհամընկնի p-ի հետ:*

Ապացուցում: Եթե a-ն չի բաժանվում p-ի վրա, ապա ըստ նախորդ հատկության՝ $(a, p) = 1$: Հետևաբար, ըստ հատկություն 3.4-ի, b-ն կբաժանվի p-ի վրա: Երկրորդ մասն ակնհայտ է: □

Հետևյալ ընդհանրացումը հեշտությամբ ապացուցվում է վերհանգման եղանակով:

Հատկություն 6.4*: Եթե վերջավոր թվով ամբողջ թվերի արտադրյալը բաժանվում է պարզ թվի վրա, ապա այդ պարզ թվի վրա կբաժանվի նաև արտադրիչներից գոնե մեկը: Մասնավորապես, եթե վերջավոր թվով պարզ թվերի արտադրյալը բաժանվում է p պարզ թվի վրա, ապա արտադրիչներից գոնե մեկը կհամընկնի p-ի հետ:* □

Թեորեմ 6.1 (Վիլսոն (1770 թ.), Լագրանժ (1771 թ.))*: Որպեսզի* $m > 1$ *բնական թիվը լինի պարզ անհրաժեշտ է և բավարար, որ* $(m-1)! \equiv -1 (mod\, m)$, *այսինքն* $(m-1)!+1$ *գումարը բաժանվի* m*-ի վրա:*

Ապացույց: Եթե $m > 1$ բնական թիվը պարզ է, ապա ըստ հետևություն 6.1-ի,

$$\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$$

բազմության բոլոր ոչ զրոյական տարրերը կլինեն հակադարձելի: Որոշենք $\mathbb{Z}_m$-ի բոլոր այն ոչ զրոյական $[a]$ տարրերը, որոնցից յուրաքանչյուրը համընկնում է իր հակադարձի հետ: Ակնհայտ է, որ $[1]^{-1} = [1]$ և $[m-1]^{-1} = [m-1]$: Մյուս կողմից, եթե $[a] = [a]^{-1}$, ապա ըստ հակադարձի սահմանման $[a] \cdot [a] = [1]$, այսինքն՝

$$\begin{aligned}
&\left[a^2\right] = [1]\,, \\
&\left[a^2\right] + [-1] = [0]\,, \\
&\left[a^2 + (-1)\right] = [0]\,, \\
&\left[a^2 - 1\right] = [0]\,, \\
&[(a-1)(a+1)] = [0]\,;
\end{aligned}$$

Այսպիսով, $(a-1)(a+1)$ արտադրյալը կբաժանվի m պարզ թվի վրա: Ուստի, հատկություն 6.3-ի համաձայն, արտադրիչներից գոնե մեկը կբաժանվի m-ի վրա: Հետևաբար, $a-1 = mt$ կամ $a+1 = ms$, այսինքն՝ $[a] = [1]$ կամ $[a] = [-1] = [m-1]$:

Այսպիսով $\mathbb{Z}_m$-ի մյուս բոլոր

$$[2], [3], \ldots, [m-2]$$

տարրերի հաջորդականությունը կարելի է պատկերացնել չհատվող զույգերով այնպես, որ յուրաքանչյուր զույգի մեջ ընկած լինեն միմյանց նկատմամբ հակադարձ տարրերը և, հետևաբար, դրանց բոլորի արտադրյալը կտա $[1]$ դասը՝

$$[2] \cdot [3] \cdot \ldots \cdot [m-2] = [1];$$

Որտեղից՝

$$[2] \cdot [3] \cdot \ldots \cdot [m-2] \cdot [m-1] = [m-1],$$

$$[2 \cdot 3 \cdot \ldots \cdot (m-1)] + [1] = [m-1] + [1],$$

$$[(m-1)! + 1] = [m] = [0]$$

և $(m-1)!+1$ գումարը կբաժանվի m-ի վրա:

Բավարարությունն ակնհայտ է. որովհետև, եթե m բնական թիվը պարզ չէ, ապա $m = m_1 \cdot m_2$, որտեղ $1 < m_1$, $m_2 < m$, և, հետևաբար, m_1-ը որպես արտադրիչ կմասնակցի $1 \cdot 2 \cdot \ldots \cdot (m-1)$ արտադրյալին, այսինքն՝

$$(m-1)! = m_1 t$$

և $(m-1)!+1$ գումարն արդեն չի բաժանվի m_1-ի վրա, առավել ևս՝ m-ի վրա: □

Հետևություն 6.2 (Լայբնից): *Որպեսզի $m > 1$ բնական թիվը լինի պարզ անհրաժեշտ է և բավարար, որ $(m-2)! \equiv 1 (mod\, m)$:* □

Դեռևս հայտնի չէ վերջավոր է թե անվերջ բոլոր այն պարզ թվերի քանակը, որոնց կարելի է ներկայացնել $n!+1$ տեսքով, սակայն ապացուցված թեորեմից բխում է, որ $n!+1$ տեսքի բաղադրյալ թվերի քանակն անվերջ է:

p պարզ թիվը կոչվում է Վիլսոնի պարզ թիվ, եթե $(p-1)! \equiv -1 \left(mod\, p^2\right)$:

Մինչ այժմ հայտնաբերվել են ընդամենը երեք հատ Վիլսոնի պարզ թվեր՝ 5, 13 և 563: Համակարգիչների օգնությամբ ապացուցվել է նաև, որ $5 \cdot 10^8$-ից փոքր ուրիշ Վիլսոնի պարզ թվեր գոյություն չունեն: Սակայն հայտնի չէ, վերջավոր է թե անվերջ բոլոր Վիլսոնի պարզ թվերի բազմությունը (քանակը):

6.2. Բնական թվի վերլուծությունը պարզ արտադրիչների: Մյոբիուսի ֆունկցիան

Հատկություն 6.5*: Եթե*

$$p_1 \cdots p_m = q_1 \cdots q_l,$$

որտեղ $p_1, \ldots, p_m$, $q_1, \ldots, q_l$ բնական թվերը պարզ են, ապա $m = l$ և գոյություն ունեն զույգ առ զույգ միմյանցից տարբեր այնպիսի $i_1, \ldots, i_m \in \{1, \ldots, m\}$ համարներ, որ $p_1 = q_{i_1}, \ldots, p_m = q_{i_m}$:

Ապացուցում: Եթե

$$p_1 \cdots p_m = q_1 \cdots q_l,$$

ապա, ըստ հատկություն 6.4-ի, q պարզ թվերից որևէ մեկը կհամընկնի p_1-ի հետ: Դիցուք $q_{i_1} = p_1$; Կրճատելով հավասարության երկու մասերը $q_{i_1} = p_1$-ով և նորից կիրառելով հատկություն 6.4-ը կարող ենք ասել, որ գոյություն ունի այնպիսի q_{i_2} պարզ թիվ, որը համընկնում է p_2-ի հետ և այսպես շարունակ:

Այժմ, եթե $m \neq l$, ապա կամ $m < l$, կամ $m > l$: Առաջին (երկրորդ) դեպքում նշված կրճատումների հետևանքով հավասարության ձախ (համապատասխանաբար աջ) մասում կսպառվեն բոլոր p (համապատասխանաբար q) պարզ թվերը, իսկ աջ (ձախ) մասում դեռևս կմնան մեկ կամ ավելի պարզ թվեր, որը հակասություն է, որովհետև պարզ թիվը (լինելով մեծ մեկից) հակադարձելի չէ: Ուստի՝ $m = l$: □

Հաջորդ արդյունքը կոչվում է թվաբանության հիմնական թեորեմ և առաջին անգամ ձևակերպվել է Էվկլիդեսի կողմից («Սկզբունքներ», գիրք IX, հատկություն 14):

Թեորեմ 6.2 (թվաբանության հիմնական թեորեմը): *Մեկից մեծ յուրաքանչյուր n բնական թիվ կամ պարզ է, կամ վերածվում է պարզ թվերի արտադրյալի: Ընդ որում, այդ վերլուծությունը արտադրիչների տեղափոխելիության ճշտությամբ որոշվում է միարժեքորեն, այսինքն՝ եթե*

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_m,$$

$$n = q_1 \cdot q_2 \cdot \ldots \cdot q_l,$$

որտեղ $p_1, \ldots, p_m$, $q_1, \ldots, q_l$ բնական թվերը պարզ են, ապա $m = l$ և գոյություն ունեն զույգ առ զույգ միմյանցից տարբեր այնպիսի $i_1, \ldots, i_m \in \{1, \ldots, m\}$ համարներ, որ $p_1 = q_{i_1}, \ldots, p_m = q_{i_m}$:

Ապացույցում: Նախ վերհանգման եղանակով ապացուցենք վերլուծության գոյությունը: $n = 2$ բնական թիվը պարզ թիվ է: Դիցուք $n > 2$ և ենթադրենք թե n թվից փոքր և մեկից մեծ յուրաքանչյուր բնական թիվ կամ պարզ է կամ վերածվում է պարզ թվերի արտադրյալի և նույն պնդումն ապացուցենք n-ի համար: Եթե n-ը պարզ թիվ է, ապա պնդումը կլինի ապացուցված: Դիցուք n-ը պարզ թիվ չէ (քանի որ $n > 1$, ապա այն կլինի բաղադրյալ), այսինքն գոյություն կունենան դրա այնպիսի n_1, n_2 բաժանարարներ, որ

$$n = n_1 \cdot n_2,$$

որտեղ $1 < n_1, n_2 < n$; Ըստ վերիանգման ենթադրության, n_1 և n_2 բնական թվերից յուրաքանչյուրը կամ պարզ է, կամ հանդիսանում է պարզ թվերի արտադրյալ՝

$$n_1 = p_1 \cdot \ldots \cdot p_k, \quad k \geqslant 1,$$

$$n_2 = q_1 \cdot \ldots \cdot q_s, \quad s \geqslant 1,$$

որտեղ $p_1, \ldots, p_k$ և $q_1, \ldots, q_s$ բնական թվերը պարզ են: Հետևաբար՝

$$n = n_1 \cdot n_2 = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_s$$

և գոյության մասն ապացուցված է:

Վերլուծության միակությունը բխում է նախորդ հատկությունից: $\square$

Ստանալ տրված մեծ բնական թվի վերլուծությունը պարզ արտադրիչների, ոչ դյուրին խնդիր է: Օրինակ, 125 և ավելի տասնորդական նիշերով բնական թվի վերլուծությունը ժամանակակից համակարգիչների օգնությամբ ստանալու համար, կպահանջվի տարիների անընդմեջ աշխատանք:

$n > 1$ բնական թվի

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k, \quad p_i\text{-ն պարզ է}, \quad i = 1, \ldots, k\ ,$$

վերլուծության մեջ հնարավոր է լինեն նաև հավասար պարզ թվեր: Միմյանց հավասար բոլոր պարզ թվերի արտադրյալը գրելով p^α տեսքով, կստանանք n բնական թվի այսպես կոչված **կանոնական վերլուծությունը**՝

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m},$$

որտեղ $p_1 < p_2 < \cdots < p_m$ պարզ թվերն արդեն զույգ առ զույգ միմյանցից տարբեր են, $\alpha_1 > 0, \alpha_2 > 0, \ldots, \alpha_m > 0$; Հետևաբար, յուրաքանչյուր $a \neq 0, \pm 1$ ամբողջ թվի համար կունենանք դրա հետևյալ կանոնական վերլուծությունը՝

$$a = sgn(a) \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m},$$

որտեղ $p_1 < p_2 < \cdots < p_m$, իսկ $\alpha_1 > 0, \alpha_2 > 0, \ldots, \alpha_m > 0$:

Բնական թվի կանոնական վերլուծության հետ սերտորեն կապված է այսպես կոչված $\mu : \mathbb{N} \to \mathbb{Z}$ **Մյոբիուսի ֆունկցիան**, որը սահմանվում է հետևյալ կերպ՝

$$\mu(n)=\begin{cases} 1, & \text{երբ } n=1,\\ (-1)^k, & \text{երբ } n=p_1\cdots p_k, \text{ որտեղ բոլոր } p_i \text{ թվերը պարզ են,}\\ & p_i\neq p_j, \text{ եթե } i\neq j,\\ 0, & \text{երբ } n\text{-ը բաժանվում է որևէ } p \text{ պարզ թվի քառակուսու}\\ & \text{վրա :}\end{cases}$$

Երկրորդ դեպքում՝ n բնական թիվը կոչվում է **էվկլիդեսյան**: Օրինակ, $\mu(2)=-1$, $\mu(3)=-1$, $\mu(4)=0$, $\mu(5)=-1$, $\mu(6)=1$, $\mu(7)=-1$, $\mu(8)=0, \ldots$

Մյոբիուսի ֆունկցիայի համար μ նշանակումը առաջարկվել է Ֆ. Մերթենսի կողմից (1874 թ.):

Թեորեմ 6.3 (էյլեր (1748 թ.), Ա. Մյոբիուս (1832 թ.)): *Մյոբիուսի ֆունկցիան արտադրյալային է, այսինքն՝ ցանկացած փոխադարձաբար պարզ m, n բնական թվերի համար՝*

$$\mu(n\cdot m)=\mu(n)\cdot\mu(m):$$

Ապացուցում: Եթե $n=1$ կամ $m=1$, ապա պնդումն ակնհայտորեն ճիշտ է: Եթե $n\neq 1$, $m\neq 1$ և $(m,n)=1$, ապա հնարավոր են հետևյալ երկու դեպքերը:

1. $\mu(n)\neq 0$, $\mu(m)\neq 0$, այսինքն $n=p_1\cdot\ldots\cdot p_k$, $m=q_1\cdot\ldots\cdot q_s$, որտեղ p_i (և q_j) պարզ թվերը զույգ առ զույգ տարբեր են և $p_i\neq q_j$, որովհետև $(n,m)=1$: Հետևաբար, $\mu(n)=(-1)^k$, $\mu(m)=(-1)^s$, $\mu(n\cdot m)=(-1)^{k+s}$, ուստի

$$\mu(n\cdot m)=\mu(n)\cdot\mu(m);$$

2. $\mu(n)=0$ կամ $\mu(m)=0$, հետևաբար՝ $\mu(n\cdot m)=0$ և

$$\mu(n\cdot m)=\mu(n)\cdot\mu(m): \qquad \square$$

Հատկություն 6.6: *Որպեսզի d բնական թիվը լինի*

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_m^{\alpha_m}$$

կանոնական վերլուծությամբ օժտված $n > 1$ *բնական թվի բնական բաժանարար, անհրաժեշտ է և բավարար, որ*

$$d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_m^{\beta_m},$$

որտեղ $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$, …, $0 \leqslant \beta_m \leqslant \alpha_m$*;*

Ապացույց: Մի կողմից ակնհայտ է, որ նշված տեսքի d թիվը n բնական թվի համար բաժանարար է: Իրոք, նշանակելով $\alpha_1 - \beta_1 = k_1$, $\alpha_2 - \beta_2 = k_2$, …, $\alpha_m - \beta_m = k_m$, կունենանք՝

$$n = d \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m},$$

որտեղ $k_1 \geqslant 0$, $k_2 \geqslant 0$, …, $k_m \geqslant 0$; Մյուս կողմից, եթե d-ն n բնական թվի բնական բաժանարարն է, ապա d-ն կունենա նշված տեսքը (հետևում է թեորեմ 6.2-ից): □

Թեորեմ 6.4*: Եթե* $d_1, d_2, \ldots, d_k$ *թվերը* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ *կանոնական վերլուծություն ունեցող բնական թվի բոլոր բնական բաժանարարներն են, ապա*

$$\frac{\mu(d_1)}{d_1} + \frac{\mu(d_2)}{d_2} + \cdots + \frac{\mu(d_k)}{d_k} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right);$$

Համառոտ՝

$$\sum_{n/d, d>0} \frac{\mu(d)}{d} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right):$$

Ապացույց: Նախ վերհանգման եղանակով դժվար չէ ապացուցել հետևյալ հավասարությունը՝

$$\left(1 - \frac{1}{x_1}\right)\left(1 - \frac{1}{x_2}\right) \cdots \left(1 - \frac{1}{x_n}\right) =$$

$$= 1 - \sum_{i=1}^{n} \frac{1}{x_i} + \sum_{i<j} \frac{1}{x_i x_j} - \sum_{i<j<l} \frac{1}{x_i x_j x_l} + \cdots + (-1)^n \frac{1}{x_1 x_2 \cdots x_n}:$$

Քանի որ $\mu(d) = 0$, եթե d-ն բաժանվում է որևէ p պարզ թվի քառակուսու վրա, ապա բանաձևն ապացուցելիս կարելի է սահմանափակվել միայն $p_1p_2\cdots p_m$ բնական թվի բնական բաժանարարներով՝

$$\sum_{n/d,d>0}\frac{\mu(d)}{d}=\sum_{p_1p_2\cdots p_m/d,d>0}\frac{\mu(d)}{d},$$

իսկ $p_1p_2\cdots p_m$ արտադրյալի բոլոր բնական բաժանարարներն են (հատկություն 6.6)՝ 1-ը, p_i պարզ թվերը ($i=1,2,\ldots,m$), p_ip_j տեսքի բոլոր արտադրյալները ($i<j$), $p_ip_jp_l$ տեսքի բոլոր արտադրյալները ($i<j<l$), և այսպես շարունակ: Հետևաբար՝

$$\sum_{p_1p_2\cdots p_m/d,d>0}\frac{\mu(d)}{d}=1-\sum_{i=1}^{m}\frac{1}{p_i}+\sum_{i<j}\frac{1}{p_ip_j}-\sum_{i<j<l}\frac{1}{p_ip_jp_l}+\cdots$$

$$+(-1)^n\frac{1}{p_1p_2\cdots p_m}=\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_m}\right): \qquad \square$$

Ի լրումն ապացուցված թեորեմի նշենք նաև, որ

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n}=0,$$

իսկ

$$\sum_{n=1}^{\infty}\frac{\mu(n)}{n^2}=\frac{6}{\pi^2}:$$

Ավարտելով ներկա պարագրաֆը, ստանանք նաև դպրոցական դասընթացից հայտնի ամենամեծ ընդհանուր բաժանարարի և ամենափոքր ընդհանուր բազմապատիկի որոշման եղանակները: Այդ նպատակով մեկից մեծ երկու a և b բնական թվերի կանոնական վերլուծությունների մեջ, անհրաժեշտության դեպքում, որպես արտադրիչներ ավելացնելով պարզ թվերի զրոյական աստիճաններ, կարող ենք գրել՝

$$a=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_m^{\alpha_m},$$
$$b=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdot\ldots\cdot p_m^{\beta_m},$$

որտեղ $\alpha_i\geqslant 0$, $\beta_i\geqslant 0$, $i=1,\ldots,m$, $p_1<p_2<\ldots<p_m$: Տեղի ունի հետևյալ հատկությունը:

Հատկություն 6.7: *Եթե մեկից մեծ a և b բնական թվերի համար՝ $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$ և $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_m^{\beta_m}$, ապա*

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\min\{\alpha_2, \beta_2\}} \cdot \ldots \cdot p_m^{\min\{\alpha_m, \beta_m\}} = \prod_{i=1}^{m} p_i^{\min\{\alpha_i, \beta_i\}},$$

$$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} \cdot p_2^{\max\{\alpha_2, \beta_2\}} \cdot \ldots \cdot p_m^{\max\{\alpha_m, \beta_m\}} = \prod_{i=1}^{m} p_i^{\max\{\alpha_i, \beta_i\}},$$

որտեղ՝ $\min\{\alpha, \beta\} = \alpha$ և $\max\{\alpha, \beta\} = \beta$, եթե $\alpha \leqslant \beta$;

Ապացուցում: Առաջին բանաձևը բխում է այն փաստից, որ $\prod_{i=1}^{m} p_i^{\min\{\alpha_i, \beta_i\}}$ բնական թիվը a և b բնական թվերի համար ընդհանուր բաժանարար է, և այն բաժանվում է a-ի և b-ի յուրաքանչյուր ընդհանուր բնական բաժանարարի վրա:

Երկրորդ բանաձևը բխում է այն հանգամանքից, որ $\prod_{i=1}^{m} p_i^{\max\{\alpha_i, \beta_i\}}$ բնական թիվը բաժանվում է a-ի և b-ի վրա, և a-ի և b-ի յուրաքանչյուր ընդհանուր բնական բազմապատիկ բաժանվում է $\prod_{i=1}^{m} p_i^{\max\{\alpha_i, \beta_i\}}$ բնական թվի վրա: □

Օրինակ, $36 = 2^2 \cdot 3^2 = 2^2 \cdot 3^2 \cdot 5^0 \cdot 11^0$,

$110 = 2 \cdot 5 \cdot 11 = 2^1 \cdot 3^0 \cdot 5^1 \cdot 11^1$.

և հետևաբար $(36, 110) = 2^1 \cdot 3^0 \cdot 5^0 \cdot 11^0 = 2$, $[36, 110] = 2^2 \cdot 3^2 \cdot 5^1 \cdot 11^1 = 1980$.

Հետևություն 6.3: *Մեկից մեծ a և b բնական թվերի համար գոյություն ունեն այնպիսի*

$$a = m_0 \cdot m_1,$$

$$b = n_0 \cdot n_1$$

վերլուծություններ, որ $(n_0, m_0) = 1$, իսկ $[a, b] = m_0 \cdot n_0$: □

Օրինակ, եթե $a = 2^3 \cdot 5 \cdot 7^4$, $b = 2^2 \cdot 3^4 \cdot 5^3$, ապա $m_0 = 2^3 \cdot 7^4$, $n_0 = 3^4 \cdot 5^3$, $m_1 = 5$, $n_1 = 2^2$:

Օգտվելով հատկություն 6.7-ում ստացված բանաձևերից ապացուցենք հետևյալ կարևոր հատկությունները՝ ամենամեծ ընդհանուր բաժանարարի և ամենափոքր ընդհանուր բազմապատիկի կապը բացահայտող բաշխական նույնությունները:

Թեորեմ 6.5: *Ցանկացած a, b, c բնական թվերի համար տեղի ունի բաշխականության հետևյալ հավասարությունը՝*

$$[(a,b),c] = ([a,c],[b,c]) :$$

Ապացուցում: Դիցուք a, b և c բնական թվերի համար՝

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}, \quad p_1 < p_2 < \ldots < p_m \ \alpha_i \geqslant 0, \ i = 1,\ldots,m;$$

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_m^{\beta_m}, \quad \beta_i \geqslant 0, \ i = 1,\ldots,m;$$

$$c = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \ldots \cdot p_m^{\gamma_m}, \quad \gamma_i \geqslant 0, \ i = 1,\ldots,m;$$

Այդ դեպքում՝

$$(a,b) = \prod_{i=1}^{m} p_i^{\min\{\alpha_i,\beta_i\}},$$

$$[(a,b),c] = \prod_{i=1}^{m} p_i^{\max\{\min\{\alpha_i,\beta_i\},\gamma_i\}},$$

$$[a,c] = \prod_{i=1}^{m} p_i^{\max\{\alpha_i,\gamma_i\}},$$

$$[b,c] = \prod_{i=1}^{m} p_i^{\max\{\beta_i,\gamma_i\}},$$

$$([a,c],[b,c]) = \prod_{i=1}^{m} p_i^{\min\{\max\{\alpha_i,\gamma_i\},\max\{\beta_i,\gamma_i\}\}};$$

Մնում է նկատել, որ

$$\max\{\min\{\alpha_i,\beta_i\},\gamma_i\} = \min\{\max\{\alpha_i,\gamma_i\},\max\{\beta_i,\gamma_i\}\} :$$

Վերջին հավասարությունը ստուգվում է բոլոր հնարավոր դեպքերի քննարկումով՝

$$\alpha_i \leqslant \beta_i \leqslant \gamma_i,$$

$$\alpha_i \leqslant \gamma_i \leqslant \beta_i,$$

$$\gamma_i \leqslant \alpha_i \leqslant \beta_i,$$

$$\gamma_i \leqslant \beta_i \leqslant \alpha_i,$$

$$\beta_i \leqslant \alpha_i \leqslant \gamma_i,$$

$$\beta_i \leqslant \gamma_i \leqslant \alpha_i;$$

Օրինակ, չորրորդ դեպքում կունենանք՝

$$\min\{\alpha_i, \beta_i\} = \beta_i,$$

$$\max\{\min\{\alpha_i, \beta_i\}, \gamma_i\} = \max\{\beta_i, \gamma_i\} = \beta_i,$$

$$\max\{\alpha_i, \gamma_i\} = \alpha_i,$$

$$\max\{\beta_i, \gamma_i\} = \beta_i,$$

$$\min\left\{\max\{\alpha_i, \gamma_i\}, \max\{\beta_i, \gamma_i\}\right\} = \min\{\alpha_i, \beta_i\} = \beta_i :$$ □

Թեորեմ 6.6*: Ցանկացած a, b, c բնական թվերի համար տեղի ունի բաշխականության հետևյալ հավասարությունը՝*

$$([a, b], c) = [(a, c), (b, c)] :$$

Ապացույց: Կրկնում ենք նախորդ թեորեմի ապացուցման քայլերը, վերջում հաշվի առնելով

$$\min\{\max\{\alpha_i, \beta_i\}, \gamma_i\} = \max\left\{\min\{\alpha_i, \gamma_i\}, \min\{\beta_i, \gamma_i\}\right\}$$

հավասարությունը: □

Հաշվի առնելով (a, b)-ի և $[a, b]$-ի վերաբերյալ ապացուցված արդյունքները (նույնությունները), կարելի է եզրակացնել, որ բնական թվերի $\mathbb{N}$ բազմությունը բաշխական կավար է՝ (a, b) և $[a, b]$ գործողությունների նկատմամբ (տես՝ 20.3-ը):

Եթե բնական թվերի $\mathbb{N}$ բազմության վրա դիտարկենք բաժանման հարաբերությունը՝

$$x \preccurlyeq y \longleftrightarrow y/x, \quad \text{որտեղ } x, y \in \mathbb{N},$$

ապա այն ակնհայտորեն կլինի մասնակի կարգ, այսինքն՝

1) $x \preccurlyeq x$ յուրաքանչյուր $x \in \mathbb{N}$ բնական թվի համար,

2) $x \preccurlyeq y$, $y \preccurlyeq x \to x = y$,

3) $x \preccurlyeq y$, $y \preccurlyeq z \to x \preccurlyeq z$;

Հետաքրքրական է, որ այս կարգի նկատմամբ բնական թվերի $\mathbb{N}$ բազմությունը դառնում է կավարաձև կարգավորված բազմություն, ուր երկու բնական թվերի վերին և ստորին ճշգրիտ եզրերը որոշվում են հետևյալ կերպ՝

$$\sup\{x,y\}=[x,y],$$
$$\inf\{x,y\}=(x,y):$$

Այլ կերպ ասած, առաջին հավասարությունը նշանակում է՝

ա) $x\preccurlyeq[x,y]$, $y\preccurlyeq[x,y]$,

բ) $x\preccurlyeq c$, $y\preccurlyeq c\to[x,y]\preccurlyeq c$,

իսկ երկրորդ հավասարությունը՝

ա') $(x,y)\preccurlyeq x$, $(x,y)\preccurlyeq y$,

բ') $c\preccurlyeq x$, $c\preccurlyeq y\to c\preccurlyeq(x,y)$:

6.3. Հանրահաշվական բաղդատումներ

Անցնենք պարզ հենքով (հենաթվով, մոդուլով) հանրահաշվական բաղդատումներին:

$$a_nx^n+\cdots+a_1x+a_0\equiv 0(mod\,m) \tag{6.1}$$

տեսքի բաղդատումը կոչվում է **հանրահաշվական բաղդատում**, որտեղ $a_0,a_1,\ldots,a_n$ գործակիցները ամբողջ թվեր են, իսկ m բնական թիվը բաղդատման հենքն է: Եթե $a_n\not\equiv 0(mod\,m)$, այսինքն a_n-ը չի բաժանվում m-ի վրա, ապա n-ը կոչվում է **հանրահաշվական բաղդատման աստիճան**, իսկ հանրահաշվական բաղդատումն այդ դեպքում կոչվում է n-րդ աստիճանի: Եթե m բնական թիվը պարզ է, ապա (6.1) հանրահաշվական բաղդատումը կոչվում է պարզ հենքով:

x_0 ամբողջ թիվը կոչվում է (6.1) հանրահաշվական բաղդատման **լուծում**, եթե

$$a_nx_0^n+\cdots+a_1x_0+a_0\equiv 0(mod\,m);$$

Հանրահաշվական բաղդատումը կոչվում է **լուծելի**, եթե այն ունի որևէ լուծում:

Ըստ m հենքի $[a]\in\mathbb{Z}_m$ մնացքների դասը կոչվում է (6.1) հանրահաշվական բաղդատման լուծում, եթե $[a]$ դասին պատկանող յուրաքանչյուր ամբողջ թիվ լուծում է նշված բաղդատման համար:

Ակնհայտ է, որ եթե x_0 ամբողջ թիվը լուծում է (6.1) հանրահաշվական բաղդատման համար, ապա $[x_0]\in\mathbb{Z}_m$ մնացքների դասը ևս կլինի լուծում նշված բաղդատման համար: Իրոք, եթե $x_1 \in [x_0]$, այսինքն $x_1 \equiv x_0 (mod\, m)$, ապա $x_1^k \equiv x_0^k (mod\, m)$ և $ax_1^k \equiv ax_0^k (mod\, m)$: Հետևաբար (հետևություն 1.6)՝

$$a_n x_1^n + \cdots + a_1 x_1 + a_0 \equiv a_n x_0^n + \cdots + a_1 x_0 + a_0 (mod\, m)$$

և

$$a_n x_1^n + \cdots + a_1 x_1 + a_0 \equiv 0 (mod\, m) :$$

Թեորեմ 6.7 (Լագրանժ): *Պարզ հենքով n-րդ աստիճանի հանրահաշվական բաղդատման լուծում հանդիսացող մնացքների դասերի թիվը չի գերազանցում n-ը:*

Ապացուցում (վերիանգման եղանակ): $n = 0, 1$ դեպքում պնդումը ճիշտ է: Իրոք, $n = 0$ դեպքում կունենանք $a_0 \equiv 0 (mod\, p)$ բաղդատումը, որը լուծում չունի, որովհետև աստիճանի սահմանման համաձայն $a_0 \not\equiv 0 (mod\, p)$; Իսկ $n = 1$ դեպքում կունենանք $a_1 x + a_0 \equiv 0 (mod\, p)$, կամ $a_1 x \equiv -a_0 (mod\, p)$ բաղդատումը, որտեղ $a_1 \not\equiv 0 (mod\, p)$, այսինքն $(a_1, p) = 1$ և հետևաբար համաձայն թեորեմ 3.3-ի այդ բաղդատումը լուծելի է և լուծում հանդիսացող մնացքների դասը միակն է: Կատարենք վերիանգման ենթադրություն և դիցուք պարզ հենքով

$$a_n x^n + \cdots + a_1 x + a_0 \equiv 0 (mod\, p) \tag{6.2}$$

հանրահաշվական բաղդատումը n-րդ աստիճանի է: Եթե (6.2) բաղդատումը չունի որևէ լուծում, ապա թեորեմի պնդումը նորից ճիշտ է: Դիցուք (6.2) հանրահաշվական բաղդատումն ունի որևէ x_0 լուծում՝

$$a_n x_0^n + \cdots + a_1 x_0 + a_0 \equiv 0 (mod\, p); \tag{6.3}$$

Հանենք (6.2) բաղդատումից (6.3) բաղդատումը (հատկություն 1.3)՝

$$a_n \left(x^n - x_0^n\right) + \cdots + a_1 (x - x_0) \equiv 0 (mod\, p)$$

և օգտվելով

$$x^k - x_0^k = (x - x_0) \left(x^{k-1} + x_0 x^{k-2} + \cdots + x_0^{k-2} x + x_0^{k-1}\right)$$

վերլուծությունից կունենանք՝

$$(x - x_0) \left(b_{n-1} x^{n-1} + \cdots + b_0\right) \equiv 0 (mod\, p),$$

որտեղ $b_{n-1}, \ldots, b_0$ գործակիցները ամբողջ թվեր են (մասնավորապես՝ $b_{n-1} = a_n$):

Հետևաբար (6.2) հանրահաշվական բաղդատման մեկ այլ x_1 լուծում, որտեղ $x_1 \not\equiv x_0 (mod\, p)$ կլինի արդեն լուծում

$$b_{n-1}x^{n-1} + \cdots + b_0 \equiv 0(mod\, p) \qquad (6.4)$$

բաղդատման համար: Իրոք,

$$(x_1 - x_0)\left(b_{n-1}x_1^{n-1} + \cdots + b_0\right) \equiv 0(mod\, p)$$

բաղդատումից բխում է, որ բաղդատման ձախ մասը բաժանվում է p պարզ թվի վրա: Հատկություն 6.3-ի համաձայն արտադրիչներից գոնե մեկը պիտի բաժանվի p-ի վրա: Սակայն $x_1 \not\equiv x_0(mod\, p)$ պայմանը նշանակում է, որ $x_1 - x_0$ արտադրիչը չի բաժանվում p-ի վրա, հետևաբար երկրորդ արտադրիչն է բաժանվում p-ի վրա՝

$$b_{n-1}x_1^{n-1} + \cdots + b_0 \equiv 0(mod\, p);$$

Քանի որ (6.4) հանրահաշվական բաղդատման աստիճանը հավասար է $(n-1)$-ի, ապա ըստ վերհանգման ենթադրության (6.4) հանրահաշվական բաղդատման լուծում հանդիսացող մնացքների դասերի թիվը չի գերազանցում $(n-1)$-ը: Այսպիսով սկզբնական (6.2) հանրահաշվական բաղդատման լուծում հանդիսացող մնացքների դասերի թիվը չի գերազանցում n-ը: □

Եթե բաղդատման հենքը պարզ թիվ չէ, ապա թեորեմ 6.5-ի պնդումը ճիշտ չէ: Օրինակ, երկրորդ աստիճանի $x^2 - 1 \equiv 0(mod\, 8)$ հանրահաշվական բաղդատման համար լուծում են հանդիսանում $[1]$, $[3]$, $[5]$ և $[7]$ մնացքների դասերը:

***Հետևություն 6.4**: Եթե պարզ հենքով*

$$a_n x_0^n + \cdots + a_1 x + a_0 \equiv 0(mod\, p)$$

հանրահաշվական բաղդատման լուծում հանդիսացող մնացքների դասերի թիվը մեծ է n-ից, ապա բաղդատման բոլոր գործակիցները կբաժանվեն p-ի վրա:

Ապացուցում: Եթե նշված հանրահաշվական բաղդատման գործակիցներից որևէ մեկը չբաժանվի p-ի վրա, ապա այն կունենա աստիճան և աստիճանը չի գերազանցի n-ը: Հետևաբար թեորեմ 6.5-ի համաձայն նրա համար լուծում հանդիսացող մնացքների դասերի թիվը ևս չի գերազանցում n-ը: Հակասություն! □

Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ

1. Ապացուցել, որ եթե p-ն պարզ թիվ է, իսկ $1 \leqslant k \leqslant p-1$, ապա $\binom{p}{k}$-ն բաժանվում է p-ի վրա:

2. Օգտվելով Նյուտոնի երկանդամից և նախորդ վարժությունից, ապացուցել հետևյալ բաղդատումը՝

$$(a+b)^p \equiv a^p + b^p (mod\, p),$$

որտեղ p-ն պարզ թիվ է, $a, b \in \mathbb{Z}$: Այլ կերպ ասած (լեմմ 1.1), $\mathbb{Z}_p$-ում տեղի ունի հետևյալ հավասարությունը՝

$$[(a+b)^p] = [a^p + b^p],$$

կամ՝

$$([a]+[b])^p = [a]^p + [b]^p :$$

3. Վերիանգման եղանակով ապացուցել հետևյալ բաղդատումը՝

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p (mod\, p),$$

որտեղ p-ն պարզ թիվ է, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$: Այլ կերպ ասած (լեմմ 1.1), $\mathbb{Z}_p$-ում տեղի ունի հետևյալ հավասարությունը՝

$$[(a_1 + a_2 + \cdots + a_n)^p] = [a_1^p + a_2^p + \cdots + a_n^p],$$

կամ՝

$$([a_1] + [a_2] + \cdots + [a_n])^p = [a_1]^p + [a_2]^p + \cdots + [a_n]^p :$$

4. Վերհանգման եղանակով ապացուցել հետևյալ բաղդատումը՝

$$(a+b)^{p^n} \equiv a^{p^n} + b^{p^n} (mod\, p),$$

որտեղ p-ն պարզ թիվ է, $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$: Հետևաբար,

$$a^{p^n} = ((a-b)+b)^{p^n} \equiv (a-b)^{p^n} + b^{p^n} (mod\, p)$$

և

$$(a-b)^{p^n} \equiv a^{p^n} - b^{p^n} (mod\, p) :$$

Այլ կերպ ասած (լեմմ 1.1), $\mathbb{Z}_p$-ում տեղի ունեն հետևյալ հավասարությունները՝

$$\left[(a+b)^{p^n}\right] = \left[a^{p^n} + b^{p^n}\right],$$

$$\left[(a-b)^{p^n}\right] = \left[a^{p^n} - b^{p^n}\right],$$

կամ՝

$$([a]+[b])^{p^n} = [a]^{p^n} + [b]^{p^n},$$

$$([a]-[b])^{p^n} = [a]^{p^n} - [b]^{p^n} :$$

5. Ապացուցել, որ 3, 5, 7 բնական թվերը երեք հաջորդական կենտ և պարզ թվերից կազմված միակ հաջորդականությունն է:

6. Եթե $p > 3$ և $p+2$ բնական թվերը պարզ են, ապա $2(p+1)$ արտադրյալը բաժանվում է 12-ի վրա:

7. Ապացուցել, որ եթե n^2+1 բնական թիվը $(n>1)$ պարզ է, ապա այն կարելի է ներկայացնել $4k+1$ տեսքով $(k \in \mathbb{N})$:

8. Ապացուցել, որ $9 \cdot 243^k + 2$ բնական թիվը բաղադրյալ է: (Ցուցում. $243 \equiv 1 (mod\, 11)$):

9. Ապացուցել, որ $8 \cdot 32^{2k} + 3$ բնական թիվը բաղադրյալ է: (Ցուցում. $32 \equiv -1 (mod\, 11)$):

10. Գտնել բոլոր այն $n > 0$ բնական թվերը, որոնց դեպքում n, $n+10$ և $n+14$ թվերը կլինեն պարզ:

    (Ցուցում. n-ը ներկայացնել $3q+r$, $0 \leqslant r \leqslant 2$ տեսքով):

11. Ապացուցել, որ $3m+2$ տեսքի $(m \geqslant 1)$ բնական թվի քառակուսին հնարավոր չէ ներկայացնել բնական թվի քառակուսու և պարզ թվի գումարի տեսքով:

12. Գտնել բոլոր այն p պարզ թվերը, որոնց համար $2p^2+1$ թիվը ևս պարզ է:

    (Ցուցում. եթե $p>3$, ապա $p=3q+1$ կամ $p=3q+2$):

13. Ապացուցել, որ եթե $p>3$ բնական թիվը պարզ է, ապա

$$2(p-3)! \equiv -1 (mod\, p) :$$

    (Ցուցում. $2(p-3)! \equiv (p-1)! (mod\, p)$):

14. Եթե $n>4$ բնական թիվը բաղադրյալ է, ապա

$$(n-1)! \equiv 0 (mod\, n) :$$

15. Ապացուցել, որ $p>2$ պարզ թվի համար

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv (-1)^{\frac{p+1}{2}} (mod\, p) :$$

    (Ցուցում.

$$\left(\left(\frac{p-1}{2}\right)!\right)^2 = 1\cdot 2\cdot 3 \cdots \frac{p-1}{2} \cdot \frac{p-1}{2} \cdots 3\cdot 2\cdot 1 =$$

$$= 1\cdot 2\cdot 3 \cdots \frac{p-1}{2} \cdot \left(\frac{-\frac{p-1}{2}}{-1} \cdots \frac{-3}{-1} \cdot \frac{-2}{-1} \cdot \frac{-1}{-1}\right) \equiv$$

$$\equiv 1\cdot 2\cdot 3 \cdots \frac{p-1}{2} \cdot \frac{\left(p-\frac{p-1}{2}\right)}{-1} \cdots \frac{p-3}{-1} \cdot \frac{p-2}{-1} \cdot \frac{p-1}{-1} (mod\, p) \equiv$$

$$\equiv (-1)^{\frac{p-1}{2}} 1\cdot 2\cdot 3 \cdots \frac{p-1}{2} \cdot \left(\frac{p-1}{2}+1\right) \cdots (p-3)(p-2)(p-1) (mod\, p) =$$

$$\equiv (-1)^{\frac{p-1}{2}} \cdot (p-1)! (mod\, p) \quad :$$

    Մնում է օգտվել Վիլսոնի թեորեմից):

16. Ապացուցել, որ եթե $2^n > (1+n)^k$, ապա $1, 2, 3, \dots, 2^n$ հաջորդականությունը պարունակում է առնվազն $k+1$ հատ պարզ թվեր:

(Ցուցում. դիցուք $p_1, p_2, \dots, p_l$-ը $1, 2, 3, \dots, 2^n$ հաջորդականության բոլոր պարզ թվերն են: Հետևաբար, յուրաքանչյուր $m \in \{1, 2, 3, \dots, 2^n\}$ բնական թիվ կունենա հետևյալ վերլուծությունը՝

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l} \leqslant 2^n,$$

որտեղ $2^{\alpha_i} \leqslant p_i^{\alpha_i} \leqslant 2^n$ և, հետևաբար, $\alpha_i \leqslant n$, $\alpha_i \in \{0, 1, \dots, n\}$: Այսպիսով, յուրաքանչյուր α_i կարող է ընդունել $n+1$ հատ արժեքներ, իսկ այդ դեպքում m-ը կընդունի $\underbrace{(n+1)(n+1)\cdots(n+1)}_{l} = (n+1)^l$ հատ արժեքներ: Ուստի՝ $(n+1)^l \geqslant 2^n > (n+1)^k$, որտեղից՝ $l > k$, այսինքն՝ $l \geqslant k+1$):

17. Դիցուք $\omega(n)$-ը $n \geqslant 2$ բնական թվի բոլոր պարզ բաժանարարների թիվն է, իսկ $d_1, d_2, \dots, d_k$-ն n-ի բոլոր բնական բաժանարարներն են: Ապացուցել հետևյալ հավասարությունը՝

$$|\mu(d_1)| + |\mu(d_2)| + \cdots + |\mu(d_k)| = 2^{\omega(n)},$$

որտեղ μ-ն Մյոբիուսի ֆունկցիան է:

Համառոտ՝

$$\sum_{n/d, d>0} |\mu(d)| = 2^{\omega(n)} :$$

18. Ապացուցել, որ

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0 :$$

19. Ապացուցել, որ

$$\sum_{k=1}^{\infty} \mu(k!) = 1 :$$

20. Դիցուք $k > 0$ ամբողջ թիվը զույգ է, իսկ n բնական թվի կանոնական վերլուծությունը ունի հետևյալ տեսքը՝

$$n = p_1 p_2 \cdots p_k :$$

Ապացուցել հետևյալ հավասարությունը՝

$$\sum_{n/d, 0<d<\sqrt{n}} \mu(d) = 0 :$$

21. Ապացուցել, որ $10^n + 3$ $(n = 1, 2, \ldots)$ բնական թվերի հաջորդականությունը պարունակում է անվերջ թվով բաղադրյալ թվեր: Սակայն մինչ այժմ հայտնի չէ, վերջավոր է թե անվերջ այս հաջորդականության բոլոր պարզ թվերի քանակը:

22. Ապացուցել, որ եթե ամբողջ գործակիցներով $f(x)$ բազմանդամի աստիճանը $\geqslant 1$, ապա

$$f(x) \equiv 0 (mod\, p)$$

համրահաշվական բաղդատումը կունենա լուծում՝ անվերջ թվով p պարզ թվերի դեպքում:

23. Օգտվելով թվաբանության հիմնական թեորեմից ապացուցել, որ

$$\prod_{p\text{-ն պարզ է}} \frac{1}{1 - \frac{1}{p}}$$

արտադրյալը տարամետ է:

24. Օգտվելով թվաբանության հիմնական թեորեմից ապացուցել, որ պարզ թվերի քանակն անվերջ է:

25. Ապացուցել, որ յուրաքանչյուր պարզ թիվ կարելի է ներկայացնել չորս բնական թվերի քառակուսիների գումարի տեսքով:

26. Ապացուցել, որ յուրաքանչյուր բնական թիվ կարելի է ներկայացնել չորս բնական թվերի քառակուսիների գումարի տեսքով (Lagrange, 1770):

27. Ապացուցել, որ $p \equiv 1 (mod\, 4)$ տեսքի յուրաքանչյուր p պարզ թիվ կարելի է ներկայացնել երկու բնական թվերի քառակուսիների գումարի տեսքով:

Գ լ ու խ 7

ՊԱՐԶ ԹՎԵՐԻ ԲԱՇԽՈՒՄԸ: ԷՎԿԼԻԴԵՍԻ, ԷՅԼԵՐԻ, ԲԵՐԹՐԱՆԻ, ՊՈՅԱՅԻ, ԴԻՐԻԽԼԵԻ, ԳՈԼԴԲԱԽԻ ԹԵՈՐԵՄՆԵՐԸ

Որ պարզ թվերի քանակն անվերջ է, հայտնի է եղել դեռևս անտիկ աշխարհում: Առաջին անգամ այդ փաստը ապացուցվել է էվկլիդեսի կողմից, մեր թվարկությունից առաջ 3-րդ դարում՝ իր «Սկզբունքներ» աշխատության մեջ (գիրք IX, հատկություն 20):

Թեորեմ 7.1 (էվկլիդես)*: Պարզ թվերի քանակն անվերջ է:*

Ապացուցում (էվկլիդես): Ենթադրենք հակառակը, որ պարզ թվերի քանակը վերջավոր է և կստանանք հակասություն: Դիցուք $p_1 < p_2 < \cdots < p_n$ բնական թվերը բոլոր պարզ թվերն են՝ դասավորված աճման կարգով: Այդ դեպքում, մեկից մեծ

$$q = p_1 p_2 \cdots p_n + 1$$

բնական թիվը, համաձայն հատկություն 6.1-ի, կբաժանվի որևէ p պարզ թվի վրա: Սակայն ակնհայտ է, որ այդ p պարզ բաժանարարը չի կարող լինել $p_1, p_2, \ldots, p_n$ պարզ թվերից որևէ մեկը, որովհետև հակառակ դեպքում կունենայինք $p = p_i$ և

$$\begin{aligned} &q = p_i t, \quad 1 \leqslant i \leqslant n, \\ &q = p_1 \cdots p_n + 1, \end{aligned}$$

որը հակասում է մնացորդով բաժանման կանոնին (թեորեմ 1.1), ավելի ճիշտ դրա միակության մասին: Կամ որը հանգեցնում է p_i պարզ թվի հակադարձելի լինելուն՝

$$p_i t = p_1 \cdots p_n + 1,$$

$$p_i (t - p_1 \cdots p_{i-1} p_{i+1} \cdots p_n) = 1,$$

որը նույնպես հնարավոր չէ:

Թեորեմն ապացուցված է[6]: □

[6]Տես նաև ավելի ընդհանուր թեորեմ 19.16-ը, որտեղից երևում է նաև պարզ թվերի քանակի անվերջ լինելու իրական պատճառը ($\mathbb{Z}(+,\cdot)$ օղակի հակադարձելի տարրերի խումբը վերջավոր է):

Ներկայումս գոյություն ունեն թեորեմ 7.1-ի բազմաթիվ ուշագրավ ապացուցումներ: Օրինակ, թեորեմ 7.1-ի հետևյալ ապացուցումն ունի տոպոլոգիական բնույթ:

Դիտարկենք $(\mathbb{Z};\tau)$ տոպոլոգիական տարածությունը, որտեղ τ-ն $\mathbb{Z}$-ի մնացքային տոպոլոգիան է, որում, ինչպես գիտենք (գլուխ 1), $x+(n)$ բազմությունները ($x\in\mathbb{Z}$, $n\in\mathbb{N}$) բաց են և փակ: Դիցուք պարզ թվերի քանակը վերջավոր է և դիցուք $p_1,p_2,\ldots,p_n$ բնական թվերը բոլոր պարզ թվերն են: Քանի որ տոպոլոգիական տարածության վերջավոր թվով փակ բազմությունների միավորումը նորից փակ բազմություն է, ապա

$$F=(p_1)\cup(p_2)\cup\ldots\cup(p_n)$$

բազմությունը կլինի փակ բազմություն և, հետևաբար, $\mathbb{Z}\setminus F$ լրացումը կլինի բաց բազմություն $(\mathbb{Z};\tau)$-ում: Սակայն, մյուս կողմից, հատկություն 6.1-ից բխում է, որ $\mathbb{Z}\setminus F=\{+1,-1\}$, որը հնարավոր չէ, որովհետև $(\mathbb{Z};\tau)$ տոպոլոգիական տարածության բոլոր ոչ դատարկ բաց բազմություններն անվերջ են: Հակասություն:

Հենվելով շարքի զուգամիտության գաղափարի վրա, Լ. Էյլերը (1748 թ.) տվել է թեորեմ 7.1-ի այլ ապացուցում, հետևյալ կերպ: Դիցուք պարզ թվերի քանակը վերջավոր է և դիցուք $p_1,p_2,\ldots,p_n$ բնական թվերը բոլոր պարզ թվերն են: Անվերջ նվազող երկրաչափական պրոգրեսիայի գումարի բանաձևով կունենանք՝

$$\frac{1}{1-\frac{1}{p_1}}=1+\frac{1}{p_1}+\frac{1}{p_1^2}+\cdots,$$
$$\frac{1}{1-\frac{1}{p_2}}=1+\frac{1}{p_2}+\frac{1}{p_2^2}+\cdots,$$
$$\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots$$
$$\frac{1}{1-\frac{1}{p_n}}=1+\frac{1}{p_n}+\frac{1}{p_n^2}+\cdots:$$

Քանի որ գրված զուգամետ թվային շարքերի անդամները դրական են (հետևաբար և շարքերը բացարձակ զուգամետ են), ապա դրանց կարելի է անդամ առ անդամ բազմապատկել (Կոշու ձևով) և արդյունքում կստանանք զուգամետ շարք՝

$$\prod_{i=1}^{n}\frac{1}{1-\frac{1}{p_i}}=\sum_{\alpha_1,\alpha_2,\ldots,\alpha_n}\frac{1}{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_n^{\alpha_n}},$$

որտեղ $\alpha_1, \alpha_2, \ldots, \alpha_n$-ը միմյանցից անկախ ստանում են բոլոր հնարավոր ոչ բացասական արժեքները: Ըստ ենթադրության, բոլոր պարզ թվերը սպառվում են $p_1, p_2, \ldots, p_n$ պարզ թվերով, հետևաբար, համաձայն թվաբանության հիմնական թեորեմի (թեորեմ 6.2), յուրաքանչյուր m բնական թիվ կհամընկնի ստացված թվային շարքի որևէ անդամի հայտարարի հետ: Քանի որ ստացված շարքը դրական անդամներով է, ապա (Ռիմանի թեորեմի համաձայն) դրա անդամների տեղափոխություններից շարքի զուգամիտությունը և գումարը չի փոխվի: Արդյունքում կստանանք $\sum\limits_{m=0}^{\infty} \frac{1}{m}$ հարմոնիկ շարքը, որը այսպիսով պետք է լինի զուգամետ և

$$\prod_{i=1}^{n} \frac{1}{1-\frac{1}{p_i}} = \sum_{m=0}^{\infty} \frac{1}{m};$$

Սակայն, ինչպես հայտնի է, $\sum\limits_{m=0}^{\infty} \frac{1}{m}$ հարմոնիկ շարքը տարամետ է: Ստացված հակասությունն ապացուցում է, որ պարզ թվերի քանակն անվերջ է:

Իրականում էյլերը դիտարկել է հետևյալ ֆունկցիան՝

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

կամայական $s > 1$ իրական թվի համար, որը այժմ կոչվում է էյլերի ձետա-ֆունկցիա: $s > 1$ դեպքում $\sum\limits_{n=1}^{\infty} \frac{1}{n^s}$ շարքը զուգամետ է (բխում է, օրինակ, շարքերի զուգամիտության ինտեգրալային հայտանիշից): Ընդհանուր դեպքում, եթե s-ը կոմպլեքս թիվ է, $\zeta(s)$ ֆունկցիան կոչվում է Ռիմանի ձետա-ֆունկցիա: Տեղի ունի հետևյալ նույնությունը, որից նույնպես հետևում է, որ պարզ թվերի քանակն անվերջ է:

էյլերի $\zeta(s)$ ձետա-ֆունկցիան բավարարում է հետևյալ նույնությանը՝

$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1},$$

որտեղ $s > 1$, իսկ p-ն փոփոխվում է բոլոր պարզ թվերի վրա, այսինքն

$s > 1$ դեպքում տեղի ունի հետևյալ հավասարությունը՝

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \left(1 - \frac{1}{5^s}\right)^{-1} \cdots,$$

որը կոչվում է Էյլերի նույնություն (կամ բանաձև)։

Իրոք՝

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots =$$

$$= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots + \frac{1}{2^s}\left(1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots\right) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots + \frac{1}{2^s}\zeta(s);$$

Հետևաբար՝

$$\zeta(s)\left(1 - \frac{1}{2^s}\right) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \cdots = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \cdots + \frac{1}{3^s}\zeta(s)\left(1 - \frac{1}{2^s}\right),$$

$$\zeta(s)\left(1 - \frac{1}{2^s}\right)\left(1 - \frac{1}{3^s}\right) = 1 + \frac{1}{5^s} + \frac{1}{7^s} + \cdots$$

և այսպես շարունակ։ Ի վերջո ստանում ենք՝

$$\zeta(s) \prod_p \left(1 - \frac{1}{p^s}\right) = 1$$

և

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} :$$

Եթե ստացված բանաձևում s-ը ձգտեցնենք 1-ի, ապա նույնության ձախ մասը կձգտի ∞։ Հետևաբար, պարզ թվերի քանակը չի կարող լինել վերջավոր, որովհետև այդ դեպքում հավասարության աջ մասը կձգտի վերջավոր թվի։

Թեորեմ 7.2 (Էյլեր, 1737 թ)։ *Բոլոր պարզ թվերի հակադարձների գումարից կազմված շարքը տարամետ է, այսինքն*

$$\sum_{p\text{-ն պարզ է}} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \cdots$$

շարքը տարամետ է։

Ապացուցում: Դիցուք m-ը կամայական բնական թիվ է, իսկ $p_1, p_2, \ldots, p_n$-ը բոլոր այն պարզ թվերն են, որոնք չեն գերազանցում m-ը՝

$$p_i \leqslant m, \quad i = 1, \ldots, n;$$

Ինչպես արդեն հայտնի է՝

$$\prod_{p_i \leqslant m} \frac{1}{1 - \frac{1}{p_i}} = \prod_{i=1}^{n} \frac{1}{1 - \frac{1}{p_i}} = \sum_{\alpha_1, \alpha_2, \ldots, \alpha_n} \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}};$$

Այս դեպքում $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ արտադրյալները կպարունակեն m-ը չգերազանցող բոլոր բնական թվերը, ինչպես նաև որոշ այլ բնական թվեր (սակայն ոչ բոլոր բնական թվերը, որովհետև թեորեմ 7.1-ի համաձայն, բոլոր պարզ թվերի քանակն անվերջ է): Հետևաբար՝

$$\prod_{p_i \leqslant m} \frac{1}{1 - \frac{1}{p_i}} > \sum_{k=1}^{m} \frac{1}{k}:$$

Եթե այստեղ $m \to \infty$, ապա անհավասարության աջ մասը ձգտում է տարամետ հարմոնիկ շարքին: Հետևաբար, ձախ մասում ստացվող

$$\prod_{i=1}^{\infty} \frac{1}{1 - \frac{1}{p_i}}$$

անվերջ արտադրյալը ևս կլինի տարամետ ($+\infty$ գումարով): Այդ դեպքում կլինի տարամետ նաև

$$-\sum_{i=1}^{\infty} \ln\left(1 - \frac{1}{p_i}\right)$$

շարքը ($+\infty$ գումարով): Նկատենք, որ $\ln\left(1 - \frac{1}{p_i}\right) < 0$:

Այնուհետև, քանի որ $\frac{1}{p_i} < 1$, ապա

$$-\ln\left(1 - \frac{1}{p_i}\right) =$$

$$= \frac{1}{p_i} + \frac{1}{2}\left(\frac{1}{p_i}\right)^2 + \frac{1}{3}\left(\frac{1}{p_i}\right)^3 + \cdots < \frac{1}{p_i} + \left(\frac{1}{p_i}\right)^2 + \left(\frac{1}{p_i}\right)^3 + \cdots = \frac{\frac{1}{p_i}}{1 - \frac{1}{p_i}};$$

Եթե $p_i > 2$, ապա $1 - \dfrac{1}{p_i} > \dfrac{1}{2}$ և հետևաբար՝

$$\frac{\frac{1}{p_i}}{1 - \frac{1}{p_i}} < \frac{\frac{1}{p_i}}{\frac{1}{2}} = 2\frac{1}{p_i};$$

Այսպիսով, $2 \cdot \sum_{i=1}^{\infty} \dfrac{1}{p_i}$ շարքի անդամները, սկսած երկրորդից, մեծ են $-\sum_{i=1}^{\infty} \ln\left(1 - \dfrac{1}{p_i}\right)$ շարքի համապատասխան անդամներից: Սակայն վերջին շարքը, ինչպես տեսանք, տարամետ է, հետևաբար կլինի տարամետ նաև $2 \cdot \sum_{i=1}^{\infty} \dfrac{1}{p_i}$ շարքը, իսկ վերջին շարքի տարամիտությունից բխում է նաև $\sum_{i=1}^{\infty} \dfrac{1}{p_i}$ շարքի տարամիտությունը: □

1860 թ. Ռիմանի կողմից ձևակերպվել է իր հայտնի վարկածը (հիպոթեզը), համաձայն որի $\zeta(s)$ Ռիմանի ձետա-ֆունկցիայի բոլոր այն $s = x + iy$ կոմպլեքս արմատները (զրոները), որոնց $x = Re\,(s)$ իրական մասերը պատկանում են $[0, 1]$ հատվածին, անպայման ընկած են $x = \dfrac{1}{2}$ ուղղի վրա: Այս պրոբլեմը, որպես կարևորագույններից մեկը, 1900 թ. ձևակերպվել է նաև Դ. Հիլբերթի կողմից՝ իր 23 չլուծված հանրահայտ պրոբլեմների շարքում:

$x = \dfrac{1}{2}$ ուղղի վրա արդեն հայտնաբերվել են (Գ. Հարդի) Ռիմանի ձետա-ֆունկցիայի անվերջ թվով կոմպլեքս արմատներ, սակայն մինչ այժմ Ռիմանի վարկածը չի ապացուցված (կամ հերքված):

n-րդ պարզ թիվը (ըստ մեծության) նշանակելով p_n-ով, կունենանք՝ $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\ldots$: Դիցուք $\psi(k) = p_1 \cdot p_2 \cdots p_k + 1$: k-ի տարբեր արժեքների դեպքում $\psi(k)$-ն կարող է լինել ինչպես պարզ, այնպես էլ բաղադրյալ: Սակայն մինչ այժմ հայտնի չէ վերջավոր է, թե՞ անվերջ $\psi(k)$ տեսքի պարզ (բաղադրյալ) բնական թվերի քանակը:

Հատկություն 7.1: *Տեղի ունի հետևյալ անհավասարությունը՝*

$$p_{n+1} < p_1 p_2 \cdots p_n,$$

որտեղ $n > 1$*:*

Ապացույց: Եթե $n > 1$, ապա $p_1p_2\cdots p_n - 1 > 1$ և հետևաբար (հատկություն 6.1) այն կբաժանվի որևէ p_k պարզ թվի վրա՝

$$p_1p_2\cdots p_n - 1 = p_k \cdot q,$$

որտեղ $q \geqslant 1$; Ակնհայտ է, որ այստեղ $k > n$, այսինքն p_k պարզ թիվը չի համընկնում $p_1, p_2, \ldots, p_n$ պարզ թվերից որևէ մեկի հետ: Այսպիսով՝ $n + 1 \leqslant k$,

$$p_{n+1} \leqslant p_k \leqslant p_k \cdot q = p_1p_2\cdots p_n - 1 < p_1p_2\cdots p_n : \qquad \square$$

Գնահատենք n-րդ p_n պարզ թվի մեծությունը:

Հատկություն 7.2: *Յուրաքանչյուր n բնական թվի համար տեղի ունի հետևյալ անհավասարությունը՝*

$$p_n \leqslant 2^{2^{n-1}},$$

ընդ որում հավասարությունը տեղի ունի միայն $n = 1$ դեպքում:

Ապացույց (վերհանգման եղանակ): $p_1 = 2^{2^0}$; Մնում է ապացուցել, որ

$$p_n < 2^{2^{n-1}},$$

որտեղ $n \geqslant 2$; Իրոք՝ $p_2 = 3 < 4 = 2^{2^1}$ և եթե

$$p_i < 2^{2^{i-1}}, \quad i = 2, 3, \ldots, n,$$

ապա, օգտվելով նախորդ հատկությունից, կունենանք՝

$$p_{n+1} < p_1p_2\cdots p_n < 2 \cdot 2^{2^1} \cdot 2^{2^2} \cdots 2^{2^{n-1}} = 2^{1+2+\cdots+2^{n-1}} = 2^{2^n-1} < 2^{2^n} : \quad \square$$

Հատկություն 7.3: *Տեղի ունի հետևյալ անհավասարությունը՝*

$$p_n > 2n,$$

որտեղ $n \geqslant 5$:

Ապացույց (վերհանգման եղանակ): $p_5 = 11 > 10 = 2 \cdot 5$; Ենթադրելով

$$p_i > 2i, \quad i = 5, 6, \ldots, n,$$

և օգտվելով $p_{n+1}-p_n \geqslant 2$ ակնհայտ անհավասարությունից, կունենանք՝

$$p_{n+1}-2n > 2,$$

կամ

$$p_{n+1} > 2+2n = 2(n+1) : \qquad \square$$

Միավորելով վերջին երկու հատկությունները, n-րդ պարզ թվի համար ստանում ենք հետևյալ գնահատականը՝

$$2n < p_n < 2^{2^{n-1}},$$

որտեղ $n \geqslant 5$; Ճիշտ է նաև $p_n < 2^n$ անհավասարությունը: Ավելի ճշգրիտ գնահատականներ են ստացվում Չեբիշևի հետևյալ արդյունքից. գոյություն ունեն այնպիսի $\alpha, \beta \in \mathbb{R}$ դրական հաստատուններ, որ $\alpha n \ln n < p_n < \beta n \ln n$:

Պարզ թվերի քանակի վերաբերյալ էվկլիդեսի պնդումն ունի մի շարք ընդհանրացումներ:

Նախ նկատենք, որ ինչպիսին էլ լինի $n \geqslant 1$ բնական թիվը, գոյություն ունեն միմյանց հաջորդող n հատ բաղադրյալ թվեր: Այդպիսին են, օրինակ,

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1)$$

բնական թվերը, որովհետև դրանցից առաջինը բաժանվում է 2-ի վրա, երկրորդը 3-ի վրա և այլն: Դեռ ավելին, նշված հատկությամբ օժտված հաջորդականությունների թիվն անվերջ է, որովհետև նշված հատկությանը բավարարում է նաև հետևյալ հաջորդականությունը՝

$$s(n+1)!+2, s(n+1)!+3, \ldots, s(n+1)!+(n+1)$$

ցանկացած $s = 2, 3, \ldots$ բնական թվերի դեպքում:

Հատկություն 7.4 (Բերթրան (1845 թ.), Չեբիշև (1852 թ.)): *Յուրաքանչյուր $n > 2$ բնական թվի համար, n և $n! = 1 \cdot 2 \cdots n$ թվերի միջև գոյություն ունի որևէ պարզ թիվ:*

Ապացույց: Եթե $n > 2$, ապա $n! - 1 > 1$ և հետևաբար այն ունի որևէ p պարզ բաժանարար: Քանի որ $p \leqslant n! - 1$, ապա $p < n!$; Ակնհայտ է, որ $p \leqslant n$ դեպքում $n!$-ը կբաժանվի p-ի վրա: Սակայն մեզ մոտ՝ $n! - 1 = pq$, այսինքն՝ $n! = pq + 1$, որտեղ $1 < p$, որը հակասում է $n! = p \cdot t$ պայմանին: Հետևաբար, $p > n$: Այսպիսով՝ $n < p < n!$, որտեղ p-ն պարզ թիվ է: $\square$

Հատկություն 7.5: *Եթե $a > 1$ և $n > 0$ բնական թվերի համար $(a^n + 1)$-ը պարզ թիվ է, ապա a-ն զույգ է, իսկ $n = 2^m$, որտեղ $m \geqslant 0$:*

Ապացուցում: Եթե a-ն կենտ է, ապա a^n-ը ևս կլինի կենտ, ուստի (a^n+1)-ը կլինի զույգ, մեծ 3-ից և հետևաբար ոչ պարզ: Այսպիսով a-ն զույգ է:

Եթե $n > 1$ բնական թիվը լինի կենտ, ապա

$$a^n + 1 = (a+1)\left(a^{n-1} - a^{n-2} + \cdots - a + 1\right), \quad 1 < a+1 < a^n + 1,$$

այսինքն՝ $(a^n + 1)$-ը կլինի բաղադրյալ: Ուստի $n > 1$ դեպքում n-ը կլինի զույգ թիվ: Դիցուք $n = 2^m \cdot q$, որտեղ $m \geqslant 1$ և q-ն կենտ է: Ապացուցենք, որ $q = 1$: Իրոք, եթե $q > 1$, ապա

$$a^n + 1 = a^{2^m \cdot q} + 1 = \left(a^{2^m}\right)^q + 1 = \left(a^{2^m} + 1\right)(\cdots),$$

որտեղ $1 < a^{2^m} + 1 < a^n + 1$, և հետևաբար $(a^n + 1)$-ը բաղադրյալ է:

Հակասություն: □

Հետևություն 7.1: *Եթե $2^n + 1$ տեսքի բնական թիվը պարզ է, ապա այն կլինի $2^{2^m} + 1$ տեսքի, $m \geqslant 0$:* □

Հանգում ենք Ֆերմայի թվի գաղափարին:

Յուրաքանչյուր $m \geqslant 0$ բնական թվի համար

$$F_m = 2^{2^m} + 1$$

տեսքի բնական թիվը կոչվում է **Ֆերմայի թիվ**:

Պ. Ֆերման սխալմամբ կարծել է, թե F_m թվերը բոլոր m բնական արժեքների դեպքում պարզ են: Սակայն այս պնդումը լինելով ճիշտ $m = 0, 1, 2, 3, 4$ արժեքների դեպքում, ճիշտ չէ արդեն $m = 5$ դեպքում (Լ. Էյլեր, 1732 թ.), որովհետև

$$\begin{aligned}
&F_0 = 2 + 1 = 3,\\
&F_1 = 2^{2^1} + 1 = 5,\\
&F_2 = 2^{2^2} + 1 = 17,\\
&F_3 = 2^{2^3} + 1 = 257,\\
&F_4 = 2^{2^4} + 1 = 65537
\end{aligned}$$

թվերը պարզ են, իսկ F_5-ը արդեն բաժանվում է 641-ի վրա: Իրոք՝

$$\begin{aligned}
&641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1,\\
&5^4 \cdot 2^{28} + 2^4 \cdot 2^{28} = 2^{28}\left(5^4 + 2^4\right),\\
&5^4 \cdot 2^{28} - 1 = \left(5^2 \cdot 2^{14} - 1\right)\left(5^2 \cdot 2^{14} + 1\right) =\\
&\quad = \left(5 \cdot 2^7 + 1\right)\left(5 \cdot 2^7 - 1\right)\left(5^2 \cdot 2^{14} + 1\right):
\end{aligned}$$

Հետևաբար, $\left(5^4 \cdot 2^{28} + 2^4 \cdot 2^{28}\right) - \left(5^4 \cdot 2^{28} - 1\right) = 2^{32} + 1 = F_5$ տարբերությունը ևս կբաժանվի 641-ի: $F_5 = 641 \cdot 6700417 = 641 \cdot \left(409^2 + 2556^2\right)$:

1880 թ. ապացուցվել է (Landry, Le Lasseur), որ F_6-ը բաղադրյալ է՝ ստանալով նաև դրա վերլուծությունը պարզ արտադրիչների: 1905 թ. ապացուցվել է (Morehead, Western) F_7-ի բաղադրյալ լինելը, որի վերլուծությունը պարզ արտադրիչների ստացվել է արդեն 1970 թ. (Brillhart, Morrison): 1909 թ. ապացուցվել է F_8-ի բաղադրյալ լինելը (Morehead, Western), որի վերլուծությունը պարզ արտադրիչների ստացվել է 1980 թ. (Brent, Pollard): F_9-ի վերլուծությունը պարզ արտադրիչների ստացվել է միայն 1990 թ. (Lenstra, Mannasse, Pollard), որը պարունակում է 155 թվանիշ:

F_{24}-ը այն ամենափոքր Ֆերմայի թիվն է, որի համար դեռևս հայտնի չէ նրա պարզ կամ բաղադրյալ լինելը:

Մինչ այժմ հայտնի չէ, թե m-ի ինչպիսի՞ արժեքի դեպքում F_m Ֆերմայի թիվը կլինի պարզ թիվ: Հետևյալ երկու խնդիրները նույնպես մնում են չլուծված. որոնք են այն F_m Ֆերմայի թվերը, որոնք չեն բաժանվում որևէ պարզ թվի քառակուսու վրա և վերջավոր է, թե՞ անվերջ բոլոր Ֆերմայի պարզ թվերի քանակը: Հատկապես վերջինս կարելի է համարել Ֆերմայի թվերի վերաբերյալ չլուծված հիմնական խնդիրը:

Բացի F_0, F_1, F_2, F_3 և F_4 Ֆերմայի պարզ թվերից, մինչ այժմ որևէ այլ Ֆերմայի պարզ թիվ չի հայտնաբերվել: Այդ պատճառով, շատ մաթեմատիկոսներ կարծում են թե բացի այս հինգ պարզ Ֆերմայի թվերից, ուրիշ պարզ Ֆերմայի թվեր գոյություն չունեն:

Ֆերմայի պարզ թվերը սերտորեն կապված են Գաուսի կողմից ապացուցված (1796 թ.) հետևյալ արդյունքի հետ. որպեսզի հնարավոր լինի կարկինի և քանոնի օգնությամբ կառուցել կանոնավոր n-անկյուն բազմանկյուն, անհրաժեշտ է և բավարար, որ կամ $n = 2^k$ կամ

$$n = 2^t \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_s,$$

որտեղ t-ն կամայական բնական թիվ է, իսկ $p_1, p_2, \ldots, p_s$-ը միմյանցից տարբեր պարզ Ֆերմայի թվեր են:

Պարզ թվերի հետ կապված են նաև մի շարք այլ հետաքրքրական պրոբլեմներ, որոնց ձևակերպումները լինելով դյուրին և գրավիչ, լուծումները մինչ այժմ հայտնի չեն: Օրինակ, 3 և 5, 5 և 7, 11 և 13, 17 և 19, $\ldots$ հաջորդական կենտ թվերի զույգերը պարզ թվերի զույգեր են, որոնք կոչվում են երկվորյակ պարզ թվեր: Սակայն մինչ այժմ հայտնի չէ վերջավոր է, թե՞ անվերջ այդպիսի պարզ թվերի զույգերի քանակը:

Մինչ այժմ հայտնի ամենամեծ հաջորդական կենտ պարզ թվերի զույգը՝

$$318032361 \cdot 2^{107001} \pm 1$$

թվերն են և հայտնաբերվել են 2001 թվականին (D. Underbakke, P. Carmody).

Վ. Բրունը (1919 թ.) ապացուցել է, որ եթե նույնիսկ հաջորդական կենտ պարզ թվերի զույգերի քանակը լինի անվերջ, ապա դրանց հակադարձներից կազմված

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\cdots$$

շարքի գումարը վերջավոր է և հավասար՝ $1.902160\ldots$, որը կոչվում է Բրունի հաստատուն: Որպեսզի $(n, n+2)$ զույգը լինի պարզ թվերի զույգ անհրաժեշտ է և բավարար, որ $(4((n-1)!+1)+n)$-ը բաժանվի $n(n+2)$-ի վրա (P. Clement, 1949).

Գոյություն ունի ավելի ընդհանուր վարկած, համաձայն որի տրված n զույգ բնական թվի դեպքում գոյություն ունեն անվերջ հատ այնպիսի p պարզ թվեր, որ $(p+n)$-ը ևս պարզ թիվ է:

Հեշտությամբ ձևակերպվում է նաև մեկ ուրիշ չլուծված հայտնի խնդիր՝ Գոլդբախի պրոբլեմը (1742 թ.). Կարելի է արդյոք 2-ից մեծ յուրաքանչյուր զույգ թիվ ներկայացնել երկու պարզ թվերի գումարի տեսքով: Օրինակ,
$4 = 2+2$, $6 = 3+3$, $8 = 5+3$, $10 = 5+5$, $\ldots$, $100 = 97+3$, $\ldots$: Այս ուղղությամբ ստացված հիմնական արդյունքները պատկանում են Լ. Գ. Շնիրելմանին և Ի. Մ. Վինոգրադովին: Գ. Հարդին (1877-1947) Գոլդբախի պրոբլեմը համարում էր մաթեմատիկայի ամենադժվարին խնդիրներից մեկը:

Հետաքրքրական է նաև հետևյալ ավելի ընդհանուր խնդիրը: Նկարագրել զույգ առ զույգ փոխադարձաբար պարզ a, b, c ամբողջ թվերի բոլոր այն եռյակները, որոնց համար

$$ax + by = c$$

Դիոֆանտյան հավասարումն ունի պարզ թվեր հանդիսացող x, y լուծումներ:

Հատկություն 7.6: *Եթե $a > 1$ և $n > 1$ բնական թվերի համար $(a^n - 1)$-ը պարզ թիվ է, ապա $a = 2$, իսկ n-ը հավասար է պարզ թվի:*

Ապացուցում: Քանի որ $(a^n - 1)$-ը պարզ թիվ է,

$$a^n - 1 = (a - 1)\left(a^{n-1} + a^{n-2} + \cdots + a + 1\right)$$

և երկրորդ արտադրիչը մեծ է 1-ից, ապա $a - 1 = 1$, հետևաբար $a = 1 + 1 = 2$: Իսկ եթե n-ը բաղադրյալ է՝ $n = s \cdot t$, $1 < s < n$, $1 < t < n$, ապա

$$2^n - 1 = 2^{st} - 1 = (2^s)^t - 1 = (2^s - 1)(\cdots),$$

որտեղ $1 < 2^s - 1 < 2^n - 1$, այսինքն $(2^n - 1)$-ը ևս կլինի բաղադրյալ: Հետևաբար, եթե $(2^n - 1)$-ը պարզ թիվ է, ապա n-ը ևս կլինի պարզ թիվ:
$\square$

Այսպիսով, հանգում ենք Մերսեննի (M. Mersenne) թվի գաղափարին. $M_n = 2^n - 1$ տեսքի բնական թիվը, որտեղ $n \geqslant 2$, կոչվում է **Մերսեննի թիվ**:

Հատկություն 7.6-ից բխում է, որ Մերսեննի M_n թվի պարզ լինելու անհրաժեշտ պայմանը n-ի պարզ լինելն է: Սակայն այս պայմանը բավարար չէ, որովհետև

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89 :$$

1644 թ. ֆրանսիացի մաթեմատիկոս Մ. Մերսեննը պնդում է, թե $2^n - 1$ տեսքի բոլոր պարզ թվերը ստացվում են n-ի հետևյալ արժեքների դեպքում՝

$$2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257 :$$

1772 թ. Էյլերն ապացուցում է, որ իրոք $2^{31} - 1 = 2147483647$ թիվը պարզ է: 1780 թ. Լուկասն ապացուցում է, որ $2^{127} - 1$ թիվը պարզ է, իսկ $2^{67} - 1$ թիվը՝ ոչ, որի վերլուծությունը պարզ արտադրիչների ստացել է Քոլը (F.N. Cole, 1903): 1883 թ. $2^{61} - 1$ թվի պարզ լինելը ապացուցել է Գ. Պերվուշինը, որն ապացուցել է նաև F_{12} և F_{23} Ֆերմայի թվերի բաղադրյալ լինելը: 1911-1914 թ.թ. Փաուերսը (R. E. Powers) ապացուցում է, որ $2^{89} - 1$ և $2^{107} - 1$ թվերը պարզ են, իսկ 1922-ին Կրայչիկը ապացուցում է, որ $2^{257} - 1$ թիվը պարզ չէ:

Ներկայումս (2002 թ.) հայտնի են ընդամենը 38 հատ Մերսեննի պարզ թվեր, որոնցից ամենամեծը $M_{6972593}$ թիվն է (N. Hajratwala,

G. Woltman, S. Kurowski), որը միաժամանակ հանդիսանում է նաև ներկայումս հայտնի ամենամեծ պարզ թիվը: Հայտնի են մեծ պարզ թվերի կիրառությունները գործարարության, բանկային և ֆինանսական հարցերի գաղտնագրության խնդիրներում:

Մինչ այժմ հայտնի չէ վերջավոր է, թե՞ անվերջ բոլոր Մերսեննի պարզ թվերի քանակը (բազմությունը):

Առանց ապացուցման նշենք նաև հետևյալ կարևոր հայտանիշը:

Թեորեմ 7.3 (Լուկաս (1876 թ.), Լեհմեր (1930 թ.)): *Դիցուք $M_n = 2^n - 1$, որտեղ $n \geqslant 3$ և պարզ է: Կազմենք հետևյալ L_i հաջորդականությունը, որը կոչվում է Լուկաս-Լեհմերի հաջորդականություն՝*

$$L_0 = 4, \ldots, L_{i+1} = \left(L_i^2 - 2\right) (mod\, M_n), \ldots$$

(այսինքն որպես L_{i+1} վերցվում է այն մնացորդը, որը ստացվում է $L_i^2 - 2$ թիվը M_n-ի վրա բաժանելուց):

M_n-ը կլինի պարզ թիվ այն և միայն այն դեպքում, երբ

$$L_{n-1} = 0 : \qquad \square$$

Օրինակ, Լուկաս-Լեհմերի հաջորդականությունը՝ $M_5 = 2^5 - 1$ թվի դեպքում կլինի 4, 14, 8, 0: Հետևաբար M_5-ը պարզ թիվ է, որովհետև $L_4 = 0$:

Ֆերմայի թվերի վերաբերյալ ապացուցենք հետևյալ հատկությունը, որից նույնպես բխում է, որ պարզ թվերի քանակն անվերջ է:

Հատկություն 7.7 (Պոյա): *Եթե $m \neq n$, ապա F_m և F_n Ֆերմայի թվերը փոխադարձաբար պարզ են՝*

$$(F_m, F_n) = 1 :$$

Ապացուցում: Եթե $m \neq n$, ապա կամ $m > n$ կամ $m < n$: Դիցուք $m > n$: Այդ դեպքում՝ $m = n + k$, որտեղ $k \geqslant 1$, և

$$F_m = 2^{2^m} + 1 = 2^{2^{n+k}} + 1 = 2^{2^n \cdot 2^k} + 1 = \left(2^{2^n}\right)^{2^k} + 1;$$

Ելնելով այս արտահայտությունից, նախ ապացուցենք, որ $(F_m - 2)$-ը բաժանվում է F_n-ի վրա:

$$F_m - 2 = \left(2^{2^n}\right)^{2^k} + 1 - 2 = \left(2^{2^n}\right)^{2^k} - 1 = \left(\left(2^{2^n}\right)^{2^{k-1}} - 1\right) \cdot \left(\left(2^{2^n}\right)^{2^{k-1}} + 1\right);$$

Եվս $k-1$ անգամ կիրառելով $a^2-b^2=(a-b)(a+b)$ հավասարությունը, կստանանք՝

$$F_m-2=\left(2^{2^n}+1\right)\left(2^{2^n}-1\right)\cdots\left(\left(2^{2^n}\right)^{2^{k-1}}+1\right)=F_n\cdot q;$$

Դիցուք $(F_m,F_n)=d$: Քանի որ (F_m-2)-ը բաժանվում է F_n-ի վրա, ապա (F_m-2)-ը կբաժանվի նաև d-ի վրա: Ուստի d-ի վրա կբաժանվի նաև 2-ը: Հետևաբար, $d=1$ կամ $d=2$: Բայց քանի որ Ֆերմայի թվերը կենտ են, ապա $d\neq 2$:

Այսպիսով, $d=1$ և $(F_m,F_n)=1$; Նույն եղանակով քննարկվում է նաև $m<n$ դեպքը: □

Տեղի ունի նաև հետևյալ ավելի ընդհանուր արդյունքը:

Թեորեմ 7.4 (Պոյա): *Յուրաքանչյուր ոչ զրոյական a ամբողջ թվի և կամայական $m\neq n$ բնական թվերի համար՝*

$$\left(a^{2^m}+1,a^{2^n}+1\right)=\begin{cases}1, & \text{եթե } a\text{-ն զույգ է},\\ 2, & \text{եթե } a\text{-ն կենտ >},\end{cases}$$

Ապացուցում: Նախորդ հատկության ապացուցման կրկնությունն է: □

Հետևյալ արդյունքը, պարզ թվերի քանակի վերաբերյալ էվկլիդեսի թեորեմի ամենահայտնի ընդհանրացումներից մեկն է:

Թեորեմ 7.5 (Լեժանդր, Դիրիխլե): *Եթե դրական անդամներով (անվերջ) թվաբանական պրոգրեսիայի առաջին անդամը և տարբերությունը փոխադարձաբար պարզ են, ապա այդ թվաբանական պրոգրեսիայում գոյություն ունեցող պարզ թվերի քանակն անվերջ է: Այսինքն, եթե $(s,l)=1$, ապա $s, s+l, s+2l, \ldots$ թվաբանական պրոգրեսիան պարունակում է անվերջ քանակի պարզ թվեր* [7]*:*

Ապացուցենք Լեժանդր-Դիրիխլեի թեորեմը մի շարք մասնավոր դեպքերում:

Հատկություն 7.8*: $4n+3$ տեսքի բոլոր բնական թվերի հաջորդականության մեջ $(n=0,1,2,\ldots)$ պարունակվում են անվերջ քանակի պարզ թվեր:*

[7] Այս թեորեմի մանրամասն ապացուցումը տե՛ս, օրինակ, հետևյալ գրքում՝ *Ж. П. Серр, Курс арифметики*, М., 1972 г.

Ապացույց: Յուրաքանչյուր $n > 0$ բնական թվի համապատասխան սահմանենք մի նոր M բնական թիվ հետևյալ կերպ՝

$$M = 4(n!) - 1 = 4(n! - 1) + 3 :$$

Հետևաբար M-ը պատկանում է տրված հաջորդականությանը: Մյուս կողմից, քանի որ $M > 1$, ապա M-ը վերածվում է պարզ թվերի արտադրյալի՝

$$M = p_1 \cdot p_2 \cdot \ldots \cdot p_s,$$

ընդ որում, այս վերլուծության մեջ գտնվող բոլոր p_i պարզ թվերը մեծ են n-ից, որովհետև հակառակ դեպքում՝ $p_i \leqslant n$ պարզ թիվը որպես արտադրիչ կմասնակցեր նաև $n! = 1{\cdot}2 \cdots n$ արտադրյալին և հետևաբար p_i-ն կլիներ բաժանարար նաև 1-ի համար, որովհետև

$$1 = 4(n!) - M,$$

որը հակասություն է:

Այժմ, օգտվելով մնացորդով բաժանման կանոնից (թեորեմ 1.1), բացահայտենք M-ի վերլուծությանը մասնակցող p_i պարզ թվերի տեսքը: Ցանկացած p բնական թվի համար տեղի ունի հետևյալ հավասարություններից որևէ մեկը՝

$$\begin{aligned} p &= 4k, \\ p &= 4k+1, \\ p &= 4k+2, \\ p &= 4k+3; \end{aligned}$$

Սակայն p պարզ թվի դեպքում առաջին հավասարությունը բացառվում է, իսկ երրորդ հավասարությունը տեղի կունենա միայն $p = 2$ դեպքում: Քանի որ M-ը կենտ է, ապա դրա p_i պարզ արտադրիչներից որևէ մեկը 2 լինել չի կարող: Այսպիսով, կամ $p_i = 4k+1$, կամ $p_i = 4k+3$: Եթե M-ի բոլոր p_i պարզ արտադրիչները լինեին $p_i = 4k+1$ տեսքի, ապա դրանց արտադրյալը ևս կլիներ $4k+1$ տեսքի, հետևաբար M-ը ևս կլիներ $4k+1$ տեսքի, որը տեղի չունի: Իրոք, եթե $M = 4k+1$, ապա կունենայինք

$$4m + 3 = 4k + 1,$$

որտեղից

$$2(k - m) = 1,$$

որը հակասություն է: Ուստի M-ի p_i պարզ արտադրիչներից որևէ մեկը կլինի $p_i = 4k + 3$ տեսքի: Այսպիսով, յուրաքանչյուր $n > 0$ բնական թվի համար գտանք այնպիսի $p_i > n$ պարզ թիվ, որը տրված հաջորդականության անդամ է: Հետևաբար, տրված հաջորդականության պարզ թիվ հանդիսացող անդամների քանակն անվերջ է: □

Հատկություն 7.9: *$6n + 5$ տեսքի բոլոր բնական թվերի հաջորդականության մեջ ($n = 0, 1, 2, \dots$) պարունակվում են անվերջ քանակի պարզ թվեր:*

Ապացուցում: Կրկնում ենք նախորդ հատկության ապացուցման քայլերը, վերցնելով՝

$$M = 6(n!) - 1 :$$ □

Հատկություն 7.10: *$3n + 2$ տեսքի բոլոր բնական թվերի հաջորդականության մեջ ($n = 0, 1, 2, \dots$) պարունակվում են անվերջ քանակի պարզ թվեր:*

*Ապացուցում:*Կրկնում ենք հատկություն 7.8-ի ապացուցման քայլերը, վերցնելով՝

$$M = 3(n!) - 1 :$$ □

Մի դիտողություն ևս՝ թեորեմ 7.5-ի կապակցությամբ: Նախ՝

$$s, s + l, s + 2l, \dots$$

թվաբանական պրոգրեսիան, որտեղ $(s, l) = 1$, անվանենք Լեժանդր-Դիրիխլեի թվաբանական պրոգրեսիա:

Օգտվելով թեորեմ 7.5-ից, կարելի է ապացուցել, որ ցանկացած վերջավոր թվով Լեժանդր-Դիրիխլեի թվաբանական պրոգրեսիաներ պարունակում են անվերջ թվով ընդհանուր պարզ թվեր:

Սակայն հայտնի չէ օժտված են արդյոք նույն հատկությամբ Լեժանդր-Դիրիխլեի բոլոր թվաբանական պրոգրեսիաները (որոնց բազմությունը հաշվելի է):

Հետաքրքրական է նաև հետևյալ արդյունքը:

Թեորեմ 7.6 (Ք. Գոլդբախ): *Եթե ամբողջ գործակիցներով $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n$ բազմանդամում $a_0 > 0$ և $n \geqslant 1$, ապա*

$$f(1), f(2), \dots, f(n), \dots$$

հաջորդականությունը պարունակում է անվերջ թվով բաղադրյալ անդամներ (բնական թվեր):

Ապացուցում: Կօգտվենք մաթեմատիկական անալիզի դասընթացում հեշտությամբ ապացուցվող փաստերից: Եթե $a_0 > 0$, ապա $\lim\limits_{x\to+\infty} f(x) = +\infty$ և հետևաբար գոյություն կունենա այնպիսի $x_1 \in \mathbb{R}$, որ $x > x_1$ դեպքում $f(x) > 1$: Գոյություն կունենա նաև այնպիսի $x_2 \in \mathbb{R}$, որ $x > x_2$ դեպքում $f'(x) > 0$: Այսպիսով, գոյություն կունենա այնպիսի $x_0 \in \mathbb{N}$ բնական թիվ, որ $x \geqslant x_0$ դեպքում $f(x) > 1$ և $f'(x) > 0$: Նշանակենք $f(x_0) = A$ և դիտարկենք $f(x_0 + At)$ ամբողջ և դրական արժեքները՝ $t = 1, 2, \ldots$ դեպքերում: Ապացուցենք, որ այս արժեքներից յուրաքանչյուրը բաղադրյալ թիվ է: Օգտվենք բազմանդամի Թեյլորի բանաձևից՝

$$f(x_0 + h) = f(x_0) + \frac{f'(x_0)}{1!}h + \frac{f''(x_0)}{2!}h^2 + \cdots + \frac{f^{(n)}(x_0)}{n!}h^n;$$

Ուստի՝

$$f(x_0 + At) = f(x_0) + f'(x_0) \cdot At + \frac{f''(x_0)}{2!}(At)^2 + \cdots + \frac{f^{(n)}(x_0)}{n!}(At)^n$$

և քանի որ աջ մասի բոլոր գումարելիները բաժանվում են A-ի վրա, ապա $f(x_0 + At)$-ն ևս կբաժանվի $A > 1$ բնական թվի վրա: Այսպիսով, $f(x_0+At)$ բնական թիվը բաղադրյալ է: Մնում է նկատել, որ t-ի տարբեր արժեքների դեպքում ստանում ենք տարբեր բաղադրյալ թվեր: Իրոք, համաձայն $f'(x) > 0$ պայմանի, $f(x)$ բազմանդամը $x \geqslant x_0$ դեպքում կլինի աճող, մասնավորապես՝

$$t_1 < t_2 \to x_0 + At_1 < x_0 + At_2 \to f(x_0 + At_1) < f(x_0 + At_2) : \qquad \square$$

Հետևություն 7.2 (Գոլդբախ): *Գոյություն չունի հաստատունից տարբեր ամբողջ գործակիցներով այնպիսի $f(x)$ բազմանդամ, որը x-ի յուրաքանչյուր բնական արժեքի դեպքում հավասար լինի պարզ թվի: Ավելի ճիշտ, գոյություն չունի հաստատունից տարբեր ամբողջ գործակիցներով այնպիսի բազմանդամ, որի բնական թիվ հանդիսացող յուրաքանչյուր արժեք հավասար լինի պարզ թվի:* $\square$

Սակայն հիշարժան են նաև հետևյալ արդյունքները.

ա) $x^2 + x + 17$ բազմանդամն ընդունում է պարզ արժեքներ, երբ $x = 0, 1, \ldots, 15$, մինչդեռ $x = 16$ դեպքում բազմանդամի արժեքը բաղադրյալ է (Էյլեր, 1772 թ.):

բ) $x^2 - x + 41$ բազմանդամն ընդունում է պարզ արժեքներ, երբ $x = 0, 1, \ldots, 40$, մինչդեռ $x = 41$ դեպքում բազմանդամի արժեքը բաղադրյալ է (Էյլեր):

գ) $x^2 + x + 41$ բազմանդամն ընդունում է պարզ արժեքներ, երբ $x = 0, \pm 1, \ldots, \pm 39, -40, -41$, մինչդեռ $x = 40$ դեպքում բազմանդամի արժեքը բաղադրյալ է (Էյլեր, Լեժանդր):

դ) $x^2 - 79x + 1601$ բազմանդամն ընդունում է պարզ արժեքներ, երբ $x = 0, 1, \ldots, 79$, մինչդեռ $x = 80$ դեպքում բազմանդամի արժեքը բաղադրյալ է (Է. Բ. Էսքոթթ, 1899 թ.):

ե) Դիրիխլեի թեորեմից (թեորեմ 7.5) կարելի է բխեցնել, որ յուրաքանչյուր n բնական թվի համապատասխան գոյություն ունի ամբողջ գործակիցներով այնպիսի $f(x)$ բազմանդամ, որ

$$f(1) < f(2) < \cdots < f(n)$$

և այդ թվերից յուրաքանչյուրը պարզ է:

Հիշատակենք նաև Հարդիի և Լիթթլվուդի հետևյալ պրոբլեմը՝ դրված 1922 թ.: Վերջավո՞ր է, թե՞ անվերջ $x^2 + 1$ բազմանդամի արժեքներ հանդիսացող պարզ թվերի քանակը, որտեղ $x \in \mathbb{N}$:

Եթե $\pi(x)$-ով նշանակենք x իրական թիվը չգերազանցող բոլոր պարզ թվերի քանակը, այսինքն

$$\pi(x) = \left|\{p \in \mathbb{N} |\ 1 < p \leqslant x \text{ և } p\text{-ն պարզ է } \}\right|,$$

ապա տեղի ունի հետևյալ հավասարությունը՝

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0,$$

որն առաջին անգամ ապացուցել է Լ. Էյլերը և նշանակում է, որ բավական «հեռվում», պարզ թվերը բաշխվում են շատ նոսր: Տեղի ունի նաև հետևյալ հավասարությունը՝

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1,$$

որն առաջին անգամ ապացուցվել է Հադամարի և Վալլե-Պուսսենի կողմից (1896 թ.): Այլ կերպ ասած, մեծ x-երի դեպքում $\pi(x)\ln x$ և x թվերը կարելի է համարել մոտավորապես հավասար՝

$$\pi(x) \approx \frac{x}{\ln x} :$$

Այս հավասարության ապացուցումը սովորաբար կատարվում է Ռիմանի ձետա-ֆունկցիայի միջոցով՝ կոմպլեքս անալիզի մեթոդներով, սակայն Ա. Սելբերգի և Պ. Էրդյոշի կողմից առաջարկվել է այս հավասարության ապացուցման նաև «տարրական» եղանակ (1949 թ.): Այնուհետև, նկատվել է նաև այս ապացուցման հետագա պարզեցումներ (Ա. Գ. Պոստնիկով, Ն. Պ. Ռոմանով):

Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ

1. Ապացուցել, որ յուրաքանչյուր $n > 1$ բնական թիվ կարելի է ներկայացնել $n = ab^2$ տեսքով, որտեղ $a, b \in \mathbb{N}$ և a-ն չի բաժանվում որևէ պարզ թվի քառակուսու վրա: Այստեղից բխեցնել, որ բոլոր պարզ թվերի քանակն անվերջ է:

   (Ցուցում. դիցուք $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ և $\alpha_i = 2\beta_i + r_i$, որտեղ $r_i = 0$ կամ 1; Ընդունելով՝ $a = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ և $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_m^{\beta_m}$ կունենանք՝ $n = a \cdot b^2$):

2. Ապացուցել, որ ցանկացած $n > 3$ բնական թվի համար, n և $2n - 2$ թվերի միջև գոյություն ունի գոնե մի պարզ թիվ (Չեբիշև, 1850թ.):

   Հետևաբար, ցանկացած $n > 1$ բնական թվի համար, n և $2n$ թվերի միջև գոյություն ունի գոնե մի պարզ թիվ (Բերթրան, 1845թ.):

3. Ապացուցել, որ ցանկացած $n > 5$ բնական թվի համար, n և $2n$ թվերի միջև գոյություն ունեն գոնե երկու միմյանցից տարբեր պարզ թվեր:

4. Ապացուցել, որ ցանկացած $n > 1$ բնական թվի համար, $n!$-ի կանոնական վերլուծության մեջ գոյություն ունի 1 ցուցիչով որևէ պարզ թիվ:

5. Ապացուցել, որ ցանկացած $n > 1$ բնական թվի համար, $n!$-ը չի հանդիսանում 1-ից մեծ բնական ցուցիչով որևէ բնական թվի աստիճան:

6. Ապացուցել, որ $p_{k+1} < 2p_k$, որտեղ p_i-ն i-րդ պարզ թիվն է: Դեռ ավելին $p_{k+2} < 2p_k$, եթե $k > 3$:

7. Ապացուցել, որ $p_{k+1} + p_{k+2} \leqslant p_1 p_2 \cdots p_k$, որտեղ $k \geqslant 3$:

8. Ապացուցել, որ $n > 2$ բնական թիվը չգերազանցող բոլոր պարզ թվերի արտադրյալը փոքր է 4^n-ից:

9. Վերհանգման եղանակով ապացուցել

$$p_{n+1} < p_1 + \cdots + p_n$$

անհավասարությունը, որտեղ p_i-ն i-րդ պարզ թիվն է, իսկ $n \geqslant 3$:

10. Ապացուցել, որ $F_m = 2^{2^m} + 1$ Ֆերմայի թիվը, որտեղ $m > 1$, հնարավոր չէ ներկայացնել երկու պարզ թվերի գումարի տեսքով:

11. Վերհանգման եղանակով ապացուցել, որ $m \geqslant 2$ դեպքում F_m ֆերմայի թիվը վերջանում է 7-ով:

12. Վերհանգման եղանակով ապացուցել, որ $m \geqslant 1$ դեպքում F_m ֆերմայի թիվն ունի $12k + 5$ տեսքը ($k \in \mathbb{N}$):

13. Ապացուցել, որ որևէ Ֆերմայի թիվ չի հանդիսանում բնական թվի քառակուսի:

14. Ապացուցել, որ որևէ Ֆերմայի թիվ չի հանդիսանում բնական թվի խորանարդ:

(Ցուցում. եթե $F_n = 2^{2^n} + 1 = (2k+1)^3$, ապա

$$2^{2^n} = 2k\left(4k^2 + 6k + 3\right),$$

որտեղ $4k^2 + 6k + 3$-ը կենտ թիվ է: Մնում է օգտվել թվաբանություն հիմնական թեորեմից):

15. Ապացուցել, որ $n \geqslant 1$ դեպքում F_n ֆերմայի թիվը օժտված է հետևյալ ներկայացումներով՝

$$F_n = F_0 \cdot F_1 \cdots F_{n-1} + 2,$$

$$F_n = F_{n-1}^2 - 2F_{n-1} + 2:$$

16. Ապացուցել, որ եթե a և b բնական թվերը փոխադարձաբար պարզ են, ապա
$$a, a+b, a+2b, \ldots, a+nb, \ldots$$
հաջորդականությունը (թվաբանական պրոգրեսիան) պարունակում է անվերջ թվով բաղադրյալ թվեր:

(Ցուցում. եթե $a+nb=p$ բնական թիվը պարզ է, ապա $a+(n+p)b$ թիվը կլինի բաղադրյալ: Մնում է օգտվել թեորեմ 7.5-ից):

17. Օգտվելով Լուկաս-Լեհմերի հաջորդականությունից ապացուցել, որ Մերսեննի M_7 թիվը պարզ է:

18. Ապացուցել, որ եթե s կոմպլեքս թվի համար $Re\,(s)>1$, ապա
$$\zeta(s)=\prod_p\left(1-\frac{1}{p^s}\right)^{-1},$$
որտեղ p-ն փոփոխվում է բոլոր պարզ թվերի վրա:

19. Ապացուցել, որ
$$\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s},$$
որտեղ $s>1$ (կոմպլեքս s-ի դեպքում $Re\,(s)>1$):

20. Ապացուցել, որ $\pi(x)\geqslant\ln(\ln x)$, եթե $x\geqslant 2$:

21. Ապացուցել, որ $\pi(x)\geqslant\log_4 x$, որտեղ $x\geqslant 1$:

22. Ապացուցել, որ գոյություն ունի այնպիսի $c_1>0$ հաստատուն (իրական թիվ), որ
$$\pi(x)<c_1\frac{x}{\ln x},\quad \text{եթե } x\geqslant 2: \quad \textit{(Չեբիշևի անհավասարություն)}$$

23. Ապացուցել, որ գոյություն ունի այնպիսի $c_2>0$ հաստատուն (իրական թիվ), որ
$$\pi(x)>c_2\frac{x}{\ln x},\quad \text{եթե } x\geqslant 2: \quad \textit{(Չեբիշևի անհավասարություն)}$$

24. Ապացուցել, որ ցանկացած $n \geqslant 14$ բնական թվի համար տեղի ունի
$$\pi(n) \leqslant \frac{1}{2}n - 1$$
անհավասարությունը:

25. Ելնելով $\zeta(2) = \dfrac{\pi^2}{6}$ թվի իռացիոնալությունից, ապացուցել պարզ թվերի քանակի անվերջ լինելը:

26. Դիցուք τ-ն $\mathbb{Z}$ բազմության մնացքային տոպոլոգիան է: Ապացուցել, որ ± 1-ը բոլոր պարզ թվերի հետ մեկտեղ կազմում է $(\mathbb{Z}; \tau)$ տոպոլոգիական տարածության փակ բազմություն:

Գ լ ու խ 8

ԻՐԱԿԱՆ ԹՎԻ ԱՄԲՈՂՋ ՄԱՍ: ԼԵԺԱՆԴՐԻ ԹԵՈՐԵՄԸ

x իրական թվի **ամբողջ մաս է** կոչվում այն ամենամեծ k ամբողջ թիվը, որը չի գերազանցում x-ը, այսինքն՝

$$k \leqslant x < k+1;$$

x իրական թվի ամբողջ մասը որոշվում է միարժեքորեն և սովորաբար նշանակվում է $[x]$-ով: Այսպիսով, x իրական թվի $[x]$ ամբողջ մասը այն ամբողջ թիվն է, որը բավարարում է հետևյալ պայմանին՝

$$[x] \leqslant x < [x]+1;$$

Կոմպյուտերային գիտության մեջ $[x]$-ը հաճախ նշանակվում է $\lfloor x \rfloor$-ով, իսկ $\lceil x \rceil$-ով նշանակվում է այն ամենափոքր s ամբողջ թիվը, որին չի գերազանցում x-ը, այսինքն՝ $s-1 < x \leqslant s$;

Այսպիսով՝

$$\lfloor x \rfloor = \max\left\{k \in \mathbb{Z} \mid \; k \leqslant x\right\},$$
$$\lceil x \rceil = \min\left\{k \in \mathbb{Z} \mid \; k \geqslant x\right\}:$$

Լեմմ 8.1: *Ցանկացած x իրական և k ամբողջ թվերի համար՝*

$$\lfloor x \rfloor = k \longleftrightarrow x-1 < k \leqslant x,$$

$$\lceil x \rceil = k \longleftrightarrow x \leqslant k < x+1;$$

Մասնավորապես, $\lfloor x \rfloor = \lceil x \rceil$ այն և միայն այն դեպքում, երբ x-ը ամբողջ թիվ է:

Ապացուցում: Ակնհայտ է:

Լեմմ 8.2: *Ցանկացած x իրական և n ամբողջ թվերի համար՝*

$$x < n \longleftrightarrow \lfloor x \rfloor < n,$$

$$n < x \longleftrightarrow n < \lceil x \rceil,$$

$$x \leqslant n \longleftrightarrow \lceil x \rceil \leqslant n,$$

$$n \leqslant x \longleftrightarrow n \leqslant \lfloor x \rfloor:$$

Ապացուցում: Ակնհայտ է: □

x իրական թվի **կոտորակային մաս է** կոչվում $x - [x]$ տարբերությունը, որը նշանակվում է $\{x\}$-ով՝

$$x - [x] = \{x\};$$

Հետևաբար՝ $0 \leqslant \{x\} < 1$ և $x = [x] + \{x\}$: Օրինակ՝

$$[6,3] = 6, \quad \{6,3\} = 0.3, \quad [-6,3] = -7,$$

$$\{-6,3\} = 0.7, \quad \lceil 6,3 \rceil = 7, \quad \lceil -6,3 \rceil = -6;$$

Լեմմ 8.3: *Եթե $a, b \in \mathbb{Z}$, $b > 0$ և (թեորեմ 1.1-ի համաձայն)՝*

$$a = bq + r, \qquad 0 \leqslant r < b,$$

ապա

$$\left[\frac{a}{b}\right] = q \ \ ;$$

$$\left\{\frac{a}{b}\right\} = \frac{r}{b} \ :$$

Ապացուցում: Իրոք՝

$$\frac{a}{b} = q + \frac{r}{b}\ , \qquad 0 \leqslant \frac{r}{b} < 1\ ,$$

$$\frac{a}{b} = q + 1 + \frac{r-b}{b}\ , \qquad -1 \leqslant \frac{r-b}{b} < 0\ \ :$$

Այսպիսով՝

$$q \leqslant \frac{a}{b} < q + 1$$

և, հետևաբար,

$$\left[\frac{a}{b}\right] = q,$$

$$\frac{r}{b} = \frac{a}{b} - q = \frac{a}{b} - \left[\frac{a}{b}\right] = \left\{\frac{a}{b}\right\} :$$

Կարելի էր վարվել նաև հետևյալ կերպ՝

$$\frac{a}{b} = \left[\frac{a}{b}\right] + \left\{\frac{a}{b}\right\},$$

$$a = b\left[\frac{a}{b}\right] + b\left\{\frac{a}{b}\right\},$$

որտեղ $0 \leqslant b\left\{\frac{a}{b}\right\} < b$, որովհետև $0 \leqslant \left\{\frac{a}{b}\right\} < 1$: Այժմ օգտվելով թեորեմ 1.1-ի միակության մասից, կունենանք՝

$$q = \left[\frac{a}{b}\right], \quad r = b\left\{\frac{a}{b}\right\},$$

որտեղից էլ՝

$$\frac{r}{b} = \left\{\frac{a}{b}\right\}: \qquad \square$$

Հատկություն 8.1: *Յանկացած m ամբողջ թվի և ցանկացած x իրական թվի համար՝ $[x+m] = [x] + m$:*

Ապացուցում: Իրոք, լեմմ 8.1-ի համաձայն՝

$$x + m - 1 < [x+m] \leqslant x + m,$$

$$x - 1 < [x+m] - m \leqslant x$$

և քանի որ $[x+m]-m$ թիվը ամբողջ է, ապա $[x+m]-m = [x]$, որտեղից՝ $[x+m] = [x] + m = [x] + [m]$: $\square$

Որպես հետևություն հանգում ենք հետևյալ արդյունքին:

Հետևություն 8.1: *Յանկացած m ամբողջ թվի և ցանկացած x իրական թվի համար $\{x+m\} = \{x\}$:*

Ապացուցում: Իրոք՝

$$\{x+m\} = x+m-[x+m] = x+m-[x]-m = x-[x] = \{x\} = \{x\}+\{m\}: \ \square$$

Հատկություն 8.2: *Յանկացած x և y իրական թվերի համար տեղի ունի հետևյալ անհավասարությունը՝*

$$[x+y] \geqslant [x] + [y]:$$

Ապացուցում: Քանի որ՝ $[x] \leqslant x$ և $[y] \leqslant y$, ապա $[x]+[y] \leqslant x+y$, այսինքն $[x]+[y]$-ը $x+y$-ին չգերազանցող ամբողջ թիվ է: Սակայն $[x+y]$-ը $x+y$-ին չգերազանցող ամենամեծ ամբողջ թիվն է, հետևաբար

$$[x]+[y] \leqslant [x+y]: \qquad \square$$

Հատկություն 8.3: *Ցանկացած $x_1, x_2, \ldots, x_n$ իրական թվերի համար տեղի ունի հետևյալ անհավասարությունը՝*

$$[x_1 + x_2 + \cdots + x_n] \geqslant [x_1] + [x_2] + \cdots + [x_n] :$$

Ապացուցում: Հեշտությամբ ստացվում է վերհանգման եղանակով: □

Հատկություն 8.4: *Դիցուք x-ը իրական, իսկ n-ը բնական թվեր են: Այն ամենամեծ a ամբողջ թիվը, որի n-պատիկը (այսինքն na-ն) չի գերազանցում x-ը, որոշվում է հետևյալ կերպ՝*

$$a = \left[\frac{x}{n}\right] :$$

Ապացուցում: Ըստ պայմանի՝

$$an \leqslant x < (a+1)n,$$

$$a \leq \frac{x}{n} < a + 1$$

և հետևաբար՝

$$a = \left[\frac{x}{n}\right] :$$ □

Որպես հետևանք ստանում ենք հետևյալ արդյունքը:

Հետևություն 8.2: *Ցանկացած x իրական և n բնական թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right] :$$

Ապացուցում: Քանի որ $[x]$-ի և x-ի միջև չկա որևէ ամբողջ թիվ, ապա այն ամենամեծ a ամբողջ թիվը, որի n-պատիկը չի գերազանցում $[x]$-ը, կլինի նաև այն ամենամեծ ամբողջ թիվը որի n-պատիկը չի գերազանցում x-ը: Այսպիսով, օգտվելով նախորդ հատկությունից, կունենանք՝

$$\left[\frac{x}{n}\right] = \left[\frac{[x]}{n}\right] :$$ □

Այժմ որոշենք այն ցուցիչը, որով $p \leqslant n$ պարզ թիվը մասնակցում է $n! = 1 \cdot 2 \cdots n$ արտադրյալի կանոնական վերլուծությանը:

Թեորեմ 8.1 (Լեժանդր, 1808 թ.): *Դիցուք $n \geqslant 2$ և $p \leqslant n$; Այն α ցուցիչը, որով p պարզ թիվը մասնակցում է $n!$-ի կանոնական վերլուծության մեջ, որոշվում է հետևյալ հավասարությամբ՝*

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right] = \sum_{i=1}^{k} \left[\frac{n}{p^i}\right],$$

որտեղ p^k-ը p-ի այն ամենամեծ աստիճանն է, որը չի գերազանցում n-ը $\left(p^k \leqslant n < p^{k+1}\right)$;

Ապացուցում: Նախ դժվար չէ որոշել k-ն.

$$p^k \leqslant n < p^{k+1},$$

$$k \ln p \leqslant \ln n < (k+1) \ln p,$$

$$k \leqslant \frac{\ln n}{\ln p} < (k+1),$$

$$k = \left[\frac{\ln n}{\ln p}\right];$$

Համաձայն հատկություն 8.4-ի, այն ամենամեծ ամբողջ թիվը, որի p-պատիկը չի գերազանցում n-ը, կլինի $\left[\frac{n}{p}\right]$ թիվը: Հետևաբար, $n!$-ի արտադրիչներ համարվող $1, 2, \ldots, n$ բնական թվերից p-ի վրա կբաժանվեն միայն հետևյալ թվերը՝

$$p, 2p, \ldots, \left[\frac{n}{p}\right] \cdot p,$$

որոնց քանակը հավասար է $\left[\frac{n}{p}\right]$-ին: Սակայն դրանց մեջ կան նաև այնպիսիները, որոնք բաժանվում են $p^2, \ldots, p^k$ աստիճանների վրա: Նշված թվերից p^2 վրա կբաժանվեն միայն հետևյալ թվերը՝

$$p^2, 2 \cdot p^2, \ldots, \left[\frac{n}{p^2}\right] \cdot p^2,$$

որոնց քանակը հավասար է $\left[\frac{n}{p^2}\right]$-ին, իսկ դրանցից p^3-ի վրա կբաժանվեն միայն հետևյալ թվերը՝

$$p^3, 2 \cdot p^3, \ldots, \left[\frac{n}{p^3}\right] \cdot p^3,$$

և այլն $,\ldots,p^k$-ի վրա կբաժանվեն միայն հետևյալ թվերը՝

$$p^k, 2\cdot p^k, \ldots, \left[\frac{n}{p^k}\right]\cdot p^k,$$

որոնց քանակը հավասար է $\left[\frac{n}{p^k}\right]$-ին:

Այսպիսով $n!$ արտադրյալի ընդամենը $\left[\frac{n}{p}\right]$ թվով արտադրիչներ բաժանվում են p-ի վրա, որոնցից ընդամենը $\left[\frac{n}{p^2}\right]$ թվով անդամներ բաժանվում են նաև p^2 վրա, $\left[\frac{n}{p^3}\right]$ թվով անդամներ բաժանվում են նաև p^3-ի վրա, $\ldots$, $\left[\frac{n}{p^k}\right]$ թվով անդամներ բաժանվում են նաև p^k-ի վրա: Ուստի, այդ $\left[\frac{n}{p}\right]$ թվով արտադրիչներից ընդամենը $\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]$ թվով անդամներ կբաժանվեն p-ի վրա, բայց չեն բաժանվի p^2 վրա, ընդամենը $\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]$ թվով անդամներ կբաժանվեն p^2 վրա, բայց չեն բաժանվի p^3-ի վրա, $\ldots$, ընդամենը $\left[\frac{n}{p^k}\right]$ թվով անդամներ կբաժանվեն p^k-ի վրա:

Հետևաբար, եթե $n!$-ը վերլուծենք պարզ թվերի արտադրյալի, այսինքն նրա բոլոր արտադրիչները վերլուծենք պարզ թվերի արտադրյալի, ապա p պարզ թիվը այդ վերլուծության մեջ կստացվի հետևյալ աստիճանով՝

$$\underbrace{p\ \cdots\ p}_{\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]}\cdot\underbrace{p^2\ \cdots\ p^2}_{\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]}\ \cdots\ \underbrace{p^{k-1}\ \cdots\ p^{k-1}}_{\left[\frac{n}{p^{k-1}}\right]-\left[\frac{n}{p^k}\right]}\cdot\underbrace{p^k\ \cdots\ p^k}_{\left[\frac{n}{p^k}\right]}=$$

$$=p^{\left[\frac{n}{p}\right]-\left[\frac{n}{p^2}\right]+2\left(\left[\frac{n}{p^2}\right]-\left[\frac{n}{p^3}\right]\right)+\cdots+(k-1)\left(\left[\frac{n}{p^{k-1}}\right]-\left[\frac{n}{p^k}\right]\right)+k\left[\frac{n}{p^k}\right]}=$$

$$=p^{\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^k}\right]}=p^{\sum\limits_{i=1}^{k}\left[\frac{n}{p^i}\right]};\qquad\square$$

Որպես հետևություն հանգում ենք հետևյալ արդյունքներին.

Հետևություն 8.3: *Եթե $n \geqslant 2$ և $p_1, p_2, \ldots, p_s$ պարզ թվերը n-ը չգերազանցող բոլոր պարզ թվերն են, ապա*

$$n! = p_1^{\sum\limits_{t=1}^{k_1}\left[\frac{n}{p_1^t}\right]} \cdot p_2^{\sum\limits_{t=1}^{k_2}\left[\frac{n}{p_2^t}\right]} \cdots p_s^{\sum\limits_{t=1}^{k_s}\left[\frac{n}{p_s^t}\right]},$$

որտեղ $p_i^{k_i} \leqslant n < p_i^{k_i+1}$, $i = 1, 2, \ldots, s$;

Ապացուցում: $n!$-ը չի կարող բաժանվել $n < p$ պարզ թվի վրա, որովհետև $n! = 1 \cdot 2 \cdots n$ արտադրյալի արտադրիչներից ոչ մեկը չի բաժանվում այդպիսի p-ի վրա: Մնում է օգտվել նախորդ թեորեմից: □

Օրինակ՝

$$6! = 2^{\left[\frac{6}{2}\right]+\left[\frac{6}{2^2}\right]} \cdot 3^{\left[\frac{6}{3}\right]} \cdot 5^{\left[\frac{6}{5}\right]} = 2^{3+1} \cdot 3^2 \cdot 5^1 = 2^4 \cdot 3^2 \cdot 5;$$

Հետևություն 8.4: *$n!$-ը չի բաժանվում 2^n-ի վրա:*

Ապացուցում: $n = 1$ դեպքում պնդումն ակնհայտ է: $n \geqslant 2$ դեպքում, համաձայն թեորեմ 8.1-ի, $n!$-ի կանոնական վերլուծության մեջ 2-ը որպես պարզ թիվ մասնակցում է հետևյալ ցուցիչով՝

$$\alpha = \left[\frac{n}{2}\right] + \left[\frac{n}{2^2}\right] + \cdots + \left[\frac{n}{2^k}\right] \leqslant \frac{n}{2} + \frac{n}{2^2} + \cdots + \frac{n}{2^k} =$$

$$= \frac{n}{2}\frac{\left(\left(\frac{1}{2}\right)^k - 1\right)}{\frac{1}{2} - 1} = n\left(1 - \left(\frac{1}{2}\right)^k\right) < n: \qquad \square$$

Հետևություն 8.5: *$(2n)!$-ն արդեն բաժանվում է 2^n-ի վրա:*

Ապացուցում:

$$\alpha = \left[\frac{2n}{2}\right] + \left[\frac{2n}{2^2}\right] + \cdots + \left[\frac{2n}{2^k}\right] = [n] + (\cdots) = n + (\cdots): \qquad \square$$

Կիրառություններում հաճախ օգտակար է լինում նաև x իրական թվի մոտակա ամբողջ թվի գաղափարը, որը կապված է $\lfloor x \rfloor$ և $\lceil x \rceil$ ֆունկցիաների հետ: x իրական թվի **մոտակա ամբողջ թիվը** նշանակվում է $[x]'$-ով և սահմանվում է հետևյալ կերպ՝

$$[x]' = \begin{cases} [x], & \textbf{եթե } [x] \leqslant x < [x] + \frac{1}{2}, \\ [x] + 1, & \textbf{եթե } [x] + \frac{1}{2} \leqslant x < [x] + 1: \end{cases}$$

Սահմանվում է նաև $\{x\}'$ ֆունկցիան հետևյալ կերպ՝

$$\{x\}' = x - [x]',$$

որը կոչվում է x իրական թվի **մոտակա կոտորակային մաս**: Ակնհայտ է, որ $|\{x\}'| \leqslant \frac{1}{2}$:

Վարժություններ և խնդիրներ

1. Եթե $f : \mathbb{R}_+ \to \mathbb{R}_+$ ֆունկցիան ($\mathbb{R}_+$-ը բոլոր ոչ բացասական կամ դրական թվերի բազմությունն է) չնվազող (մասնավորապես աճող) ու անընդհատ ֆունկցիա է և

$$f(x) \in \mathbb{N} \to x \in \mathbb{N},$$

ապա

$$[f([x])] = [f(x)] :$$

Մասնավորապես՝

ա) $\left[\sqrt[n]{[x]}\right] = [\sqrt[n]{x}]$, $n \in \mathbb{N}$, $x \in \mathbb{R}_+$;

բ) $[\log_a [x]] = [\log_a x]$, $a \in \mathbb{N}$, $a > 1$:

(Ցուցում. եթե $x \in \mathbb{N}$, ապա պնդումն ակնհայտ է: Եթե $x \notin \mathbb{N}$, ապա $[x] < x$: Հետևաբար, $f([x]) \leqslant f(x)$: Այնուհետև,

$[f([x])] \leqslant [f(x)] < f(x)$ (որովհետև $f(x)$-ը ամբողջ չէ);

Այստեղ ենթադրելով $[f([x])] < [f(x)]$ անհավասարությունը, ստանում ենք հակասություն: Իրոք, այդ դեպքում՝

$$[f([x])] + 1 \leqslant [f(x)] < f(x),$$

$$f([x]) < [f([x])] + 1 \leqslant [f(x)] < f(x);$$

Այժմ կարելի է կիրառել միջանկյալ արժեքի վերաբերյալ Բոլցանո-Կոշիի թեորեմը $[[x], x]$ հատվածի վրա. գոյություն կունենա այնպիսի $y \in [[x], x]$, որ $f(y) = [f(x)] \in \mathbb{N}$: Հետևաբար, $f(y) \in \mathbb{N}$ և $y \in \mathbb{N}$, ուստի՝ $y = [x]$ և $f(y) < f(y)$: Հակասություն):

2. Նախորդ խնդրի պայմաններում ստանալ բանաձև $\lceil f(\lceil x \rceil) \rceil$-ի հաշվման համար:

3. Ապացուցել հետևյալ հավասարությունները.

   ա) $\left[\sqrt[3]{[x]}\right] = [\sqrt[3]{x}]$;

   բ) $\left[\sqrt[2n+1]{[x]}\right] = [\sqrt[2n+1]{x}]$:

4. Ապացուցել, որ ցանկացած x, y իրական և $m \neq 0$ ամբողջ թվերի համար, $\left[\dfrac{x+y}{m}\right]$-ը հավասար է՝ $\left[\dfrac{x}{m}\right] + \left[\dfrac{y}{m}\right]$ կամ՝ $\left[\dfrac{x}{m}\right] + \left[\dfrac{y}{m}\right] + 1$:
   (Ցուցում. $\dfrac{x+y}{m} = \dfrac{x}{m} + \dfrac{y}{m} = \left[\dfrac{x}{m}\right] + \alpha + \left[\dfrac{y}{m}\right] + \beta$, որտեղ $0 \leqslant \alpha < 1$, $0 \leqslant \beta < 1$, $0 \leqslant \alpha + \beta < 2$: Հետևաբար, $\left[\dfrac{x+y}{m}\right] = \left[\dfrac{x}{m}\right] + \left[\dfrac{y}{m}\right] + [\alpha + \beta]$, որտեղ $[\alpha+\beta] = 0$ կամ 1):

5. Ապացուցել, որ ցանկացած x իրական թվի համար՝

$$[x] + [-x] = \begin{cases} 0, & \text{եթե } x \in \mathbb{Z}, \\ -1, & \text{եթե } x \notin \mathbb{Z}; \end{cases}$$

   (Ցուցում. եթե $x \in \mathbb{Z}$, ապա $[-x] = -[x]$, իսկ եթե $x \notin \mathbb{Z}$, ապա $[-x] = -[x] - 1$):

6. Ապացուցել, որ ցանկացած a և m բնական թվերի համար՝

$$\left[\frac{a}{m}\right] = \frac{a-r}{m},$$

   որտեղ $r = a(mod\, m)$:

7. Ապացուցել, որ եթե $p > 2$ բնական թիվը պարզ է, ապա

$$\left[\frac{p}{4}\right] = \begin{cases} \dfrac{p-1}{4}, & \text{եթե } p = 4q+1, \\[2ex] \dfrac{p-3}{4}, & \text{եթե } p = 4q+3: \end{cases}$$

8. Եթե m ամբողջ թիվը կենտ է, ապա

$$\left[\frac{m}{2}\right] = \frac{m-1}{2}:$$

9. Լուծել հետևյալ հավասարումները՝

$$\left[x^2\right] = 2,$$

$$\left[x^2\right] = x :$$

10. Ապացուցել, որ ցանկացած x իրական թվի համար՝

$$[x] + \left[x + \frac{1}{2}\right] = [2x];$$

(Ցուցում. $x = [x] + \alpha$, որտեղ $0 \leqslant \alpha < 1$):

11. Կառուցել հետևյալ ֆունկցիաների գրաֆիկները՝

$$y = \left[\frac{x}{2}\right],$$

$$y = \left[x^2\right],$$

$$y = [\cos x] :$$

12. Օգտվելով Լեժանդրի թեորեմից, ստանալ $11!$-ի կանոնական վերլուծությունը՝

$$11! = 2^8 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11 :$$

13. Գտնել այն ամենափոքր n բնական թիվը, որի դեպքում $n!$-ը բաժանվում է 5^7-ի վրա:

14. Դիցուք $m \in \mathbb{N}$: Գտնել m-ը չգերազանցող բոլոր բնական թվերի ամենափոքր ընդհանուր բազմապատիկը:

(Ցուցում. եթե m-ը չգերազանցող բոլոր պարզ թվերը նշանակենք՝ $p_1 < p_2 < \cdots < p_k \leqslant m$, իսկ

$$p_i^{x_i} \leqslant m < p_i^{x_i+1}, \quad x_i \in \mathbb{N} \ \left(x_i = \left[\frac{\ln m}{\ln p_i}\right]\right),$$

ապա որոնելի թիվը կլինի՝ $p_1^{x_1} \cdot p_2^{x_2} \cdots p_k^{x_k}$):

15. Օգտվելով նախորդ խնդրի արդյունքից և Չեբիշևի անհավասարությունից, ապացուցել որ գոյություն ունի այնպիսի $c > 0$ իրական թիվ, որ

$$[1, 2, \ldots, n] < c^n$$

ցանկացած n բնական թվի համար:

16. Ապացուցել հետևյալ հավասարությունը՝

$$\sum_{k=1}^{n} \mu(k) \left[\frac{n}{k}\right] = 1,$$

որտեղ μ-ն Մյոբիուսի ֆունկցիան է:

17. Ապացուցել, որ

$$\tau(1) + \tau(2) + \cdots + \tau(n) = \left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{n}\right],$$

որտեղ $\tau(n)$-ը n-ի բոլոր բնական բաժանարարների թիվն է:

18. Ապացուցել, որ

$$\sigma(1) + \sigma(2) + \cdots + \sigma(n) = 1 \cdot \left[\frac{n}{1}\right] + 2 \cdot \left[\frac{n}{2}\right] + \cdots + n \cdot \left[\frac{n}{n}\right],$$

որտեղ $\sigma(n)$-ը n-ի բոլոր բնական բաժանարարների գումարն է:

19. Եթե $n > 2$, ապա $\frac{2}{3}n < p \leqslant n$ պայմանին բավարարող p պարզ թիվը չի կարող լինել $\binom{2n}{n}$ բնական թվի բաժանարար:

20. Ապացուցել, որ $n < p < 2n$ պայմանին բավարարող p պարզ թիվը $\binom{2n}{n}$ բնական թվի կանոնական վերլուծության մեջ մասնակցում է 1 ցուցիչով:

21. Եթե $\binom{2n}{n}$ բնական թիվը բաժանվում է p պարզ թվի վրա և $p \geqslant \sqrt{2n}$, ապա p-ն $\binom{2n}{n}$-ի կանոնական վերլուծության մեջ մասնակցում է 1 ցուցիչով:

22. Ապացուցել, որ ցանկացած $n > 10$ բնական թվի համար, $n!$-ի կանոնական վերլուծության մեջ գոյություն ունեն 1 ցուցիչով միմյանցից տարբեր գոնե երկու պարզ թվեր:

23. Ապացուցել, որ $x > 0$ բնական թվի 2-ական համակարգում ունեցած ներկայացման երկարությունը համընկնում է $[\log_2 x]$-ի հետ:

Գ լ ու խ 9

ԷՅԼԵՐԻ ՖՈՒՆԿՑԻԱՆ: ԷՅԼԵՐԻ, ՖԵՐՄԱՅԻ, ԼՈՒԿԱՍԻ, ԳԱՈՒՍԻ, ՄՅՈԲԻՈՒՍԻ ԹԵՈՐԵՄՆԵՐԸ: ՊՍԵՎԴՈՊԱՐԶ ԹՎԵՐ: ԹՎԱԿԵՐՊ ԲԱԶՄՈՒԹՅՈՒՆՆԵՐ ԵՎ ԱՐՏԱԴՐՅԱԼԱՅԻՆ ՖՈՒՆԿՑԻԱՆԵՐ: ԿԱՏԱՐՅԱԼ ԵՎ p-ԱԴԻԿ ԹՎԵՐ

9.1. Էյլերի ֆունկցիայի սահմանումը, Էյլերի և Ֆերմայի թեորեմները: Պսևդոպարզ և լիովին պսևդոպարզ (Քարմայքլի) թվեր

Դիցուք m-ը ամբողջ և դրական թիվ է: $\varphi(m)$-ով կամ $\Phi(m)$-ով նշանակենք այն ամբողջ և դրական թվերի քանակը, որոնք չեն գերազանցում m-ը և փոխադարձաբար պարզ են դրա հետ, այսինքն՝

$$\varphi(m) = |\{x \in \mathbb{Z} \,|\, 1 \leqslant x \leqslant m,\, (x, m) = 1\}| :$$

Օրինակ, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$, $\varphi(6) = 2$, $\varphi(7) = 6, \ldots$

Այսպիսով, ստացվում է մի $\varphi : \mathbb{N} \to \mathbb{N}$ ֆունկցիա (արտապատկերում), որը բոլոր ամբողջ և դրական թվերի բազմությունն արտապատկերում է իր մեջ՝ հետևյալ կերպ. $m \to \varphi(m)$, $m \in \mathbb{N}$: Այդ ֆունկցիան կոչվում է **Էյլերի ֆունկցիա** (1760 թ.), կամ ավելի ճիշտ Էյլերի φ ֆունկցիա: Քանի, որ $\mathbb{N} \subseteq \mathbb{Z}$, ապա հաճախ Էյլերի $\varphi : \mathbb{N} \to \mathbb{N}$ ֆունկցիան օգտակար է դիտել նաև որպես $\varphi : \mathbb{N} \to \mathbb{Z}$ ֆունկցիա (տե՛ս 9.10, 9.12 թեորեմները):

Ակնհայտ է, որ $m \geqslant 2$ դեպքում՝ $\varphi(m) \leqslant m - 1$ և $m = p$ պարզ թվի համար՝ $\varphi(p) = p - 1$, որովհետև $1, 2, \ldots, p - 1$ թվերից յուրաքանչյուրը փոխադարձաբար պարզ է p-ի հետ, իսկ $(p, p) = p > 1$: Եվ հակառակը, եթե $\varphi(m) = m - 1$, ապա m-ը պարզ թիվ է:

Մինչ այժմ չի հայտնաբերվել այնպիսի m բաղադրյալ թվի օրինակ, որ $(m - 1)$-ը բաժանվի $\varphi(m)$-ի վրա (Լեհմերի խնդիրը, 1932 թ.): Մինչ այժմ չի լուծված նաև հետևյալ խնդիրը (Քարմայքլ, 1922 թ.). ցանկացած n բնական թվի համար գոյություն ունի արդյոք այնպիսի $m \neq n$ բնական թիվ, որ $\varphi(m) = \varphi(n)$:

$[a] \in \mathbb{Z}_m$ մնացքների դասը կոչվում է փոխադարձաբար պարզ m-ի հետ և գրվում է $([a], m) = 1$, եթե $[a]$ դասին պատկանող յուրաքանչյուր ամբողջ թիվ փոխադարձաբար պարզ է m-ի հետ:

Եթե $(a, m) = 1$, ապա (հատկություն 2.3) $([a], m) = 1$: Այսպիսով, $\varphi(m)$-ը հավասար է բոլոր այն մնացքների դասերի քանակին ըստ մոդուլ m-ի, որոնք փոխադարձաբար պարզ են m-ի հետ: Համաձայն հետևություն 3.5-ի, $\varphi(m)$-ը կլինի հավասար

$$[0], [1], \ldots, [m-1] \in \mathbb{Z}_m$$

հաջորդականության բոլոր հակադարձելի դասերի թվին:

Եթե $(a, m) = 1$, ապա համաձայն թեորեմ 3.1-ի, գոյություն կունենան այնպիսի $x, y \in \mathbb{Z}$ ամբողջ թվեր, որ $ax + my = 1$, կամ $ax \equiv 1 (mod\, m)$: Հետևյալ արդյունքը պնդում է, որ որպես նշված բաղդատման լուծում կարելի է վերցնել նաև $x = a^{\varphi(m)-1}$ թիվը:

Թեորեմ 9.1 (Էյլեր, 1760 թ.): *Եթե* $(a, m) = 1$, *ապա* $a^{\varphi(m)} \equiv 1 (mod\, m)$, *այսինքն* $a^{\varphi(m)} - 1$ *տարբերությունը բաժանվում է* m-*ի վրա:*

Ապացուցում: Եթե $a = 0$, ապա $m = 1$ և թեորեմն ակնհայտ է: Դիցուք $a \neq 0$ և դիցուք $[a_1], [a_2], \ldots, [a_k]$ դասերը միմյանցից տարբեր բոլոր այն մնացքների դասերն են ըստ մոդուլ m-ի, որոնք փոխադարձաբար պարզ են m-ի հետ, այսինքն՝ $k = \varphi(m)$: Դիտարկենք

$$[aa_1], [aa_2], \ldots, [aa_k]$$

մնացքների դասերը, որտեղ $(a, m) = 1$, $a \in \mathbb{Z}$: Հատկություն 3.1-ի համաձայն, այդ դասերից յուրաքանչյուրը նույնպես փոխադարձաբար պարզ է m-ի հետ և դրանք զույգ առ զույգ միմյանցից տարբեր են: Իրոք, եթե $aa_i \equiv aa_j (mod\, m)$, ապա, համաձայն հատկություն 3.8-ի, կստանայինք՝ $a_i \equiv a_j (mod\, m)$, որը հակասություն է:

Այսպիսով՝

$$\{[aa_1], \ldots, [aa_k]\} = \{[a_1], \ldots, [a_k]\}$$

և

$$[aa_1] \cdot [aa_2] \cdots [aa_k] = [a_1][a_2] \cdots [a_k],$$

$$[aa_1 \cdot aa_2 \cdots aa_k] = [a_1 \cdot a_2 \cdots a_k] :$$

Հետևաբար՝

$$[a^k a_1 a_2 \cdots a_k] = [a_1 a_2 \cdots a_k],$$

$$a^k a_1 a_2 \cdots a_k \equiv a_1 a_2 \cdots a_k (mod\, m) :$$

Քանի որ $a_1 a_2 \cdots a_k$ արտադրյալը փոխադարձաբար պարզ է m-ի հետ (հատկություն 3.2), ապա հատկություն 3.8-ի համաձայն, կունենանք՝

$$a^k \equiv 1 (mod\, m),$$

որտեղ $k = \varphi(m)$: □

Հետևություն 9.1 (Ֆերմայի փոքր թեորեմը, 1640 թ.): *Եթե p-ն պարզ թիվ է և a ամբողջ թիվը չի բաժանվում p-ի վրա, ապա*

$$a^{p-1} \equiv 1 (mod\, p) :$$

Ապացուցում: Ըստ տրված պայմանի՝ $(a, p) = 1$ և $\varphi(p) = p - 1$: Մնում է օգտվել թեորեմ 9.1-ից: □

Հաճախ Ֆերմայի փոքր թեորեմը ձևակերպվում է նաև հետևյալ կերպ. **ցանկացած p պարզ թվի և ցանկացած a ամբողջ թվի համար՝**

$$a^p \equiv a (mod\, p);$$

Եվ, հետևաբար, եթե $a^n \not\equiv a (mod\, n)$, ապա n-ը բաղադրյալ է: Իհարկե, այս ձևակերպումով Ֆերմայի փոքր թեորեմը բխում է նաև

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p (mod\, p), \quad a_1, a_2, \ldots, a_n \in \mathbb{Z},$$

բանաձևից, եթե վերցնենք՝ $a_1 = a_2 = \cdots = a_n = 1$ և $a_1 = a_2 = \cdots = a_n = -1$:

Ֆերմայի փոքր թեորեմից (վերհանգման եղանակով) բխում է ավելի ընդհանուր պնդում. **եթե p-ն պարզ թիվ է, ապա**

$$a^{p^k} \equiv a (mod\, p), \quad k \in \mathbb{N},\ a \in \mathbb{Z} :$$

Մենք նշեցինք էյլերի և Ֆերմայի փոքր թեորեմների ավանդական ապացուցումները: Սակայն, հաճախ Ֆերմայի փոքր թեորեմը կիրառվում է ֆունկցիաների (դինամիկ համակարգերի) անշարժ և պարբերական կետերը հետազոտելու համար (տես՝ W. E. Briggs,

W. L. Briggs, Anatomy of a Circle Map, Math. Magazine 72(1999), 166-175) և հակառակը, ելնելով $g_n : [0,1] \to [0,1]$, $n \in \mathbb{N}$ ֆունկցիաների՝

$$g_n(x) = \begin{cases} n \cdot x, & \text{եթե } 0 \leqslant x \leqslant \dfrac{1}{n}, \\ n \cdot x - j, & \text{եթե } \dfrac{j}{n} < x \leqslant \dfrac{j+1}{n}, \end{cases}$$

անշարժ և պարբերական կետերի հատկություններից, կարելի է բխեցնել էյլերի և Ֆերմայի փոքր թեորեմները (M. Frame, B. Johnson, J. Sauerberg, Fixed points and Fermat: A Dinamical Systems Approach to Number Theory, The American Mathematical Monthly, 2000, vol. 107, $\mathcal{N}$5, 422–428):

Ֆերմայի փոքր թեորեմի հակադարձը ճիշտ չէ:

Օրինակ, $3^{90} \equiv 1(mod\, 91)$, սակայն 91-ը բաղադրյալ թիվ է $(91 = 7 \cdot 13)$, կամ $2^{341} \equiv 2(mod\, 341)$, բայց $341 = 11 \cdot 31$: Ապացուցենք վերջին բաղդատումը, օգտվելով Ֆերմայի փոքր թեորեմից (նույն եղանակով ստուգվում է նաև առաջին բաղդատումը)՝

$$2^{341} \equiv \left(2^{10}\right)^{34} \cdot 2(mod\, 11) \equiv (1)^{34} \cdot 2(mod\, 11) \equiv 2(mod\, 11),$$

և

$$2^{341} \equiv \left(2^{30}\right)^{11} \cdot 2^{11}(mod\, 31) \equiv (1)^{11} \cdot 2^{11}(mod\, 31) \equiv 2^{11}(mod\, 31) \equiv$$

$$\equiv \left(2^{5}\right)^{2} \cdot 2(mod\, 31) \equiv (1)^{2} \cdot 2(mod\, 31) \equiv 2(mod\, 31) :$$

Այսպիսով, $2^{341} - 2$ տարբերությունը միաժամանակ բաժանվում է 11-ի և 31-ի (վրա), և քանի որ $(11, 31) = 1$, ապա (հատկություն 3.5) այն կբաժանվի նաև դրանց $11 \cdot 31 = 341$ արտադրյալի վրա, այսինքն՝

$$2^{341} \equiv 2(mod\, 341) :$$

Այս բաղդատումը, որ 1819 թ. ստացել է Ֆ. Սարյուսը (F. Sarrus), հետաքրքրական է նաև նրանով, որ այն ժխտում է նաև ավելի քան 2000 տարի առաջ Չինական մաթեմատիկոսների կողմից ձևակերպված հետևյալ վարկածը (ենթադրությունը). եթե $2^n \equiv 2(mod\, n)$, ապա n բնական թիվը պարզ է: Այս պնդումը 1680 թ. վերաձևակերպվել է նաև Լայբնիցի կողմից:

Հանգում ենք հետևյալ գաղափարին:

Դիցուք n-ը և a-ն բնական թվեր են, իսկ n-ը բաղադրյալ է: n բաղադրյալ թիվը կոչվում է **պսևդոպարզ ըստ** a **հենքի** (կամ a բնական թվի նկատմամբ), եթե

$$a^n \equiv a(mod\, n) :$$

n բնական թիվը կոչվում է **պսևդոպարզ**, եթե այն պսևդոպարզ է ըստ որևէ հենքի:

Այսպիսով, 341-ը պսևդոպարզ է ըստ 2 հենքի, որը հայտնաբերված առաջին պսևդոպարզ թիվն է: Նույն եղանակով ապացուցվում է, որ 561 և 645 թվերը նույնպես պսևդոպարզ են ըստ 2 հենքի: Ավելի դժվար է հայտնաբերել զույգ պսևդոպարզ թվեր: Առաջին այդպիսի թիվը՝ $161038 = 2 \cdot 73 \cdot 1103$ հայտնաբերվել է 1950 թ. Դ. Լեհմերի կողմից, որից հետո ապացուցվել է (N. G. W. H. Beeger, On Even Numbers m Dividing $2^m - 2$, American Mathematical Monthly, 58(1951), 553-555), որ բոլոր զույգ պսևդոպարզ թվերի քանակն անվերջ է: Նույնպիսի արդյունք տեղի ունի նաև կենտ պսևդոպարզ թվերի համար, որը բխում է նաև հետևյալ արդյունքից:

Հատկություն 9.1 (Ե. Մալո, 1903 թ.): *Եթե $n > 3$ բնական թիվը պսևդոպարզ է ըստ 2 հենքի, ապա այդպիսին է նաև $2^n - 1$ թիվը:*

Ապացուցում: Դիցուք n-ը պսևդոպարզ է ըստ 2 հենքի՝

$$2^n \equiv 2(mod\, n),$$

այսինքն՝ $2^n - 2 = nk$, որտեղ $k \in \mathbb{N}$, հետևաբար՝ $2^n - 1 = nk + 1$:

Քանի որ n-ը բաղադրյալ է, ապա այդպիսին կլինի նաև $2^n - 1$ թիվը, որովհետև՝

$$n = s \cdot t, \quad 1 < s < n \to 2^n - 1 = 2^{s \cdot t} - 1 = (2^s)^t - 1 = (2^s - 1)(\cdots);$$

Մնում է ապացուցել, որ

$$2^{2^n - 1} \equiv 2\,(mod\ (2^n - 1)) :$$

Իրոք՝

$$2^{2^n - 1} - 2 \equiv 2^{nk+1} - 2 = 2\left((2^n)^k - 1\right) = 2\,(2^n - 1)\,(\cdots) : \qquad \square$$

Բաղադրյալ n բնական թիվը կոչվում է *լիովին պսևդոպարզ* կամ *Քարմայքլի թիվ* (R. D. Carmichael, 1912), եթե n-ը պսևդոպարզ է $1 <$

$a < n$ և $(a, n) = 1$ պայմաններին բավարարող ցանկացած a բնական թվի նկատմամբ:

Օրինակ, 561-ը Քարմայքլի թիվ է (և սա ամենափոքր Քարմայքլի թիվն է): Իրոք, պահանջվում է ապացուցել, որ

$$a^{561} \equiv a(mod\, 561)$$

բոլոր այնպիսի a բնական թվերի համար, որ $1 < a < 561$ և $(a, 561) = 1$: Քանի որ $561 = 3 \cdot 11 \cdot 17$ և $(a, 561) = 1$, ապա $(a, 3) = 1$, $(a, 11) = 1$ և $(a, 17) = 1$: Ֆերմայի փոքր թեորեմի համաձայն՝

$$a^2 \equiv 1(mod\, 3),$$

$$a^{10} \equiv 1(mod\, 11),$$

$$a^{16} \equiv 1(mod\, 17),$$

այսինքն $a^2 - 1$ տարբերությունը բաժանվում է 3-ի, $\left(a^{10} - 1\right)$-ը՝ 11-ի, իսկ $\left(a^{16} - 1\right)$-ը՝ 17-ի վրա: Միաժամանակ՝

$$a^{561} - a = a\left(a^{560} - 1\right) = a\left[\left(a^{10}\right)^{56} - 1\right] = a\left(a^{10} - 1\right)(\ldots),$$

$$a^{561} - a = a\left[\left(a^{16}\right)^{35} - 1\right] = a\left(a^{16} - 1\right)(\ldots),$$

$$a^{561} - a = a\left[\left(a^{2}\right)^{280} - 1\right] = a\left(a^{2} - 1\right)(\ldots):$$

Այսպիսով, $a^{561} - a$ տարբերությունը միաժամանակ բաժանվում է 3, 11 և 17 (փոխադարձաբար) պարզ թվերից յուրաքանչյուրի վրա, հետևաբար, այն կբաժանվի նաև $561 = 3 \cdot 11 \cdot 17$ արտադրյալի վրա (հատկություն 3.6):

Հաջորդ Քարմայքլի թվերն են՝

$$1105 = 5 \cdot 13 \cdot 17,$$

$$1729 = 7 \cdot 13 \cdot 19,$$

$$2465 = 5 \cdot 17 \cdot 29,$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

Համեմատաբար վերջերս ապացուցվել է (Alford W. R., Granville A., Pomerance C., There are infinitely many Carmichael numbers, Ann. Math., 140, 1994, p. 703–722), որ բոլոր Քարմայքլի թվերի քանակն անվերջ է, իսկ n-ը չգերազանցող բոլոր Քարմայքլի թվերի քանակը $\leqslant \sqrt[7]{n^2}$:

Առանց ապացուցման մանրամասնությունների վրա կանգ առնելու նշենք նաև հետևյալ հայտանիշը. որպեսզի $n > 3$ բաղադրյալ թիվը լինի Քարմայքլի թիվ անհրաժեշտ է և բավարար, որ այն չբաժանվի որևէ պարզ թվի քառակուսու վրա և n-ի յուրաքանչյուր p պարզ բաժանարարի համար՝ $(p-1)$-ը լինի $(n-1)$-ի բաժանարար (A. Korselt): Մասնավորապես, այս հայտանիշից բխում է, որ յուրաքանչյուր Քայմայքլի թիվ կենտ է և հավասար է միմյանցից տարբեր առնվազն 3 հատ պարզ թվերի արտադրյալի: Իրոք, եթե n-ը Քարմայքլի թիվ է և $n = p_1 \cdot p_2 \cdots p_m$, որտեղ p_i-ն պարզ է $(i = 1, \ldots, n)$, $p_i \neq p_j$ $(i \neq j)$, ապա նախ $m \geqslant 2$, որովհետև n-ը բաղադրյալ թիվ է: Դիցուք $p_1 = 2$: Այդ դեպքում, համաձայն ձևակերպված հայտանիշի՝ $n - 1 = (p_2 - 1)t$: Հետևաբար, հավասարության աջ մասը կլինի զույգ թիվ, իսկ ձախ մասը՝ ոչ: Հակասություն: □

Իսկ, եթե $n = p_1 p_2$, որտեղ $p_1 < p_2$, ապա $0 < p_1 - 1 < p_2 - 1$ և

$$n - 1 = p_1 p_2 - 1 = (p_2 - 1)p_1 + p_1 - 1,$$

այսինքն, հայտանիշի համաձայն, $(p_1 - 1)$-ը կբաժանվի $(p_2 - 1)$-ի վրա: Հակասություն:

9.2. Ամբողջ թվի կարգ ըստ տրված հենքի: Լուկասի թեորեմը

Դիցուք $n > 0$ բնական թիվը և a ամբողջ թիվը փոխադարձաբար պարզ են: Ըստ Էյլերի թեորեմի՝ $a^{\varphi(n)} \equiv 1 (mod\, n)$: Այն ամենափոքր $k > 0$ բնական թիվը, որի համար $a^k \equiv 1 (mod\, n)$, կոչվում է **a-ի կարգ ըստ մոդուլ n-ի** (կամ ըստ n հենքի, հենաթվի) և նշանակվում է՝ $k = ord_n(a)$:

Ակնհայտ է, որ եթե $b \equiv a (mod\, n)$, ապա $ord_n(b) = ord_n(a)$:

Լեմմ 9.1: *Եթե $(a, n) = 1$, ապա տեղի ունեն հետևյալ պնդումները.*
1) Եթե $a^m \equiv 1 (mod\, n)$, ապա m-ը բաժանվում է $ord_n(a)$-ի վրա: Մասնավորապես, Էյլերի թեորեմից բխում է, որ $\varphi(n)$-ը բաժանվում է $ord_n(a)$-ի վրա;

2) $ord_n(a^m) = \dfrac{ord_n(a)}{(ord_n(a), m)}$: Մասնավորապես, $ord_n(a^m) = ord_n(a) \Longleftrightarrow (ord_n(a), m) = 1$;

3) Եթե $(b, n) = 1$ *և* $(ord_n(a), ord_n(b)) = 1$*, ապա*

$$ord_n(a \cdot b) = ord_n(a) \cdot ord_n(b);$$

4) Եթե $(b_i, n) = 1$*,* $i = 1, \ldots, k$ *և* $ord_n(b_1), \ldots, ord_n(b_k)$ *թվերը զույգ առ զույգ փոխադարձաբար պարզ են, ապա* $ord_n(b_1 \cdots b_k) = ord_n(b_1) \cdots ord_n(b_k)$*:*

Ապացուցում: 1) Եթե $a^m \equiv 1(mod\, n)$ և $k = ord_n(a)$, ապա ըստ մնացորդով բաժանման ալգորիթմի՝ $m = kq + r$, $0 \leqslant r < k$, և, հետևաբար, $a^m = a^{kq+r} = a^{kq}a^r = \left(a^k\right)^q a^r$, որտեղից՝ $a^r \equiv 1(mod\, n)$: Եթե այստեղ $r > 0$, ապա ստացված առնչությունը կհակասի կարգի սահմանմանը, հետևաբար $r = 0$ և $m = kq$:

2) Դիցուք $k = ord_n(a)$, $d = (k, m)$: Հետևաբար, $k = du$, $m = dv$ և

$$(a^m)^{\frac{k}{d}} = \left(a^k\right)^{\frac{m}{d}} \equiv 1(mod\, n);$$

Ենթադրելով որևէ $t > 0$ բնական թվի համար՝

$$(a^m)^t \equiv 1(mod\, n),$$

կունենանք՝ $a^{mt} \equiv 1(mod\, n)$ և ըստ 1) կետի mt-ն կբաժանվի k-ի վրա, այսինքն՝ $mt = ks$, որևէ $s \geqslant 1$ բնական թվի համար: Հետևաբար, $dvt = dus$, $vt = us$ և քանի որ $(u, v) = 1$, ապա t-ն կբաժանվի u-ի վրա: Ուստի $t \geqslant u = \dfrac{k}{d}$:

3) Եթե $k = ord_n(a)$, $s = ord_n(b)$, ապա

$$(ab)^{ks} = a^{ks} \cdot b^{ks} = \left(a^k\right)^s \cdot (b^s)^k \equiv 1(mod\, n):$$

Նախ ապացուցենք հետևյալ միջանկյալ փաստը:

Եթե $c \equiv a^i(mod\, n)$ և $c \equiv b^j(mod\, n)$, ապա $c \equiv 1(mod\, n)$: Իրոք, $c^k \equiv \left(a^k\right)^i(mod\, n) \equiv 1(mod\, n)$ և $c^s \equiv (b^s)^j(mod\, n) \equiv 1(mod\, n)$: Ուստի, համաձայն 1) կետի՝ k և s փոխադարձաբար պարզ թվերը կբաժանվեն $ord_n(c)$-ի վրա, այսինքն $ord_n(c) = 1$ և, հետևաբար, $c \equiv 1(mod\, n)$:

Դիցուք այժմ $(ab)^t \equiv 1(mod\, n)$, պահանջվում է ապացուցել, որ $t \geqslant k \cdot s$: Իրոք, $a^t b^t \equiv 1(mod\, n)$ և

$$a^t b^t b^{\varphi(n)t-t} \equiv b^{\varphi(n)\cdot t-t}(mod\, n),$$

$$a^t b^{\varphi(n)\cdot t} \equiv b^{\varphi(n)\cdot t-t}(mod\, n),$$

և, ըստ Էյլերի թեորեմի (թեորեմ 9.1),

$$a^t \equiv b^{t\varphi(n)-t}(mod\, n) :$$

Նշանակելով $c = a^t$, կունենանք՝

$$c \equiv a^t(mod\, n) \quad \text{և} \quad c \equiv b^{t\varphi(n)-t}(mod\, n);$$

Ուստի, համաձայն վերոհիշյալ միջանկյալ փաստի, $c \equiv 1(mod\, n)$: Մասնավորապես,

$$b^{t\varphi(n)-t} \equiv 1(mod\, n),$$

$$b^{t\varphi(n)-t} \cdot b^t \equiv b^t(mod\, n),$$

$$b^{t\varphi(n)} \equiv b^t(mod\, n),$$

$$\left(b^{\varphi(n)}\right)^t \equiv b^t(mod\, n),$$

$$1 \equiv b^t(mod\, n) :$$

Այսպիսով, $a^t \equiv 1(mod\, n)$, $b^t \equiv 1(mod\, n)$ և t-ն միաժամանակ կբաժանվի k-ի և s-ի վրա, ուստի նաև $k \cdot s$-ի վրա (հատկություն 3.5) և, հետևաբար, $t \geqslant k \cdot s$:

4) Ապացուցվում է վերհանգման եղանակով: □

Թեորեմ 9.2 (Լուկաս, 1891 թ.): *Եթե* $n \geqslant 3$ *բնական թվի համար գոյություն ունի այնպիսի* a *ամբողջ թիվ, որ*

$$a^{n-1} \equiv 1(mod\, n)$$

և $(n-1)$*-ի յուրաքանչյուր* p *պարզ բաժանարարի համար՝*

$$a^{\frac{n-1}{p}} \not\equiv 1(mod\, n),$$

ապա n*-ը պարզ թիվ է:*

Ապացուցում: $a^{n-1} \equiv 1(mod\, n)$ պայմանից բխում է (թեորեմ 3.1), որ $(a, n) = 1$, իսկ նախորդ լեմմի 1) կետի համաձայն, $(n-1)$-ը կբաժանվի $ord_n(a)$ կարգի վրա: Տրված $a^{\frac{n-1}{p}} \not\equiv 1(mod\, n)$ պայմանից բխում է, որ

$\dfrac{n-1}{p}$ բնական թիվը չի բաժանվում $k = ord_n(a)$ կարգի վրա, որովհետև հակառակ դեպքում կունենայինք՝ $\dfrac{n-1}{p} = k \cdot q$,

$$a^{\frac{n-1}{p}} = a^{kq} = \left(a^k\right)^q \equiv 1(mod\, n),$$

որը հակասություն է: Այսպիսով, $(n-1)$-ը բաժանվում է $k = ord_n(a)$-ի վրա, բայց $(n-1)$-ի յուրաքանչյուր p պարզ բաժանարարի համար, $\dfrac{n-1}{p}$ բնական թիվը չի բաժանվում $k = ord_n(a)$-ի վրա: Հետևաբար, (հատկություն 6.6) $n-1 = ord_n(a)$: Քանի որ $\varphi(n) \leqslant n-1$ և, համաձայն լեմմ 9.1-ի 1) կետի, $\varphi(n)$-ը բաժանվում է $ord_n(a) = n-1$ թվի վրա, ապա $\varphi(n) = n-1$, իսկ այստեղից էլ հետևում է, որ n-ը պարզ թիվ է: $\square$

Լուկասի թեորեմով կարելի է ապացուցել նաև $n = 2^{31}-1$ Մերսեննի թվի պարզ լինելը (էյլեր), ընտրելով $a = 7$, իսկ $n-1 = 2 \cdot 3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$:

Համանման եղանակով ապացուցվում են նաև հետևյալ երկու ավելի ընդհանուր արդյունքները:

Թեորեմ 9.3*: Դիցուք տրված է $n-1$ բնական թվի կանոնական վերլուծությունը պարզ արտադրիչների՝*

$$n - 1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} :$$

Եթե յուրաքանչյուր $i = 1, \ldots, k$ նշիչի համար գոյություն ունի այնպիսի a_i բնական թիվ, որ

$$a_i^{n-1} \equiv 1(mod\, n),$$

և

$$a_i^{\frac{n-1}{p_i}} \not\equiv 1(mod\, n),$$

ապա n-ը պարզ թիվ է:

Ապացուցում: Երկրորդ պայմանից բխում է (թեորեմ 3.1), որ $(a_i, n) = 1$ և $(n-1)$-ը բաժանվում է $ord_n(a_i) = m_i$-ի վրա (լեմմ 9.1): Երրորդ պայմանից հետևում է, որ $\dfrac{n-1}{p_i}$ բնական թիվը չի բաժանվում $m_i = ord_n(a_i)$ կարգի վրա: Ուստի, m_i-ն բաժանվում է $p_i^{\alpha_i}$-ի վրա: Դիցուք՝

$$b_1 = a_1^{\frac{m_1}{p_1^{\alpha_1}}}, \ldots, b_k = a_k^{\frac{m_k}{p_k^{\alpha_k}}}, \quad a = b_1 \cdot b_2 \cdots b_k :$$

Հետևաբար, համաձայն լեմմ 9.1-ի 2) հատկության՝

$$ord_n(b_1) = p_1^{\alpha_1}, \ldots, ord_n(b_k) = p_k^{\alpha_k}$$

և, համաձայն լեմմ 9.1-ի 4) հատկության, կունենանք՝

$$ord_n(a) = ord_n(b_1 \cdot b_2 \cdots b_k) = ord_n(b_1) \cdot ord_n(b_2) \cdots ord_n(b_k) =$$

$$= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_k^{\alpha_k} = n - 1,$$

այսինքն՝ $ord_n(a) = n - 1$: Այնուհետև կրկնում ենք թեորեմ 9.2-ի ապացուցման շարունակությունը: □

Հետևյալ արդյունքն ունի ավելի ընդհանուր բնույթ:

Թեորեմ 9.4: *Դիցուք $n - 1 = F_1 R_1$, որտեղ $(F_1, R_1) = 1$, և դիցուք F_1-ի յուրաքանչյուր p_i պարզ բաժանարարի համար գոյություն ունի այնպիսի a_i բնական թիվ, որ*

$$a_i^{n-1} \equiv 1(mod\, n), \quad \left(a_i^{\frac{n-1}{p_i}} - 1, n\right) = 1 :$$

Այդ դեպքում, եթե $F_1 > \sqrt{n}$, ապա n-ը պարզ թիվ է (Brillhart J., Lehmer D. H., Selfridge J. L., New primality criteria and factorizations of $2^m \pm 1$, Math. Comput., 1975, v. 29, № 130, p. 620-647):[8]

Անցնենք էյլերի ֆունկցիայի հատկությունների հանգամանալից ուսումնասիրությանը:

9.3. Էյլերի ֆունկցիայի հատկությունները

Հատկություն 9.2: *Ցանկացած p պարզ թվի և կամայական $n \geqslant 1$ բնական թվի համար*

$$\varphi\left(p^n\right) = p^n - p^{n-1} :$$

Մասնավորապես $\varphi\left(p^n\right)$-ը զույգ թիվ է, եթե $n \geqslant 2$:

[8]Այստեղ $\sqrt{n}$-ը կարելի է փոխարինել ավելի փոքր թվով՝ $(\frac{n}{2})^{\frac{1}{3}}$-ով:

Ապացուցում: Դիտարկենք

$$1, 2, \ldots, p^n$$

հաջորդականությունը և պարզենք այդ հաջորդականության այն անդամների քանակը, որոնք փոխադարձաբար պարզ են p^n-ի հետ: Դրա համար բավական է պարզել այդ հաջորդականության այն անդամների քանակը, որոնք բաժանվում են p-ի վրա, այսինքն ունեն $l \cdot p$ տեսքը, որտեղ $l \cdot p \leqslant p^n$: Այն ամենամեծ ամբողջ l թիվը, որի p-պատիկը չի գերազանցում p^n-ը, կլինի p^{n-1} թիվը (որը բխում է նաև հատկություն 8.3-ից): Այսպիսով,

$$1, 2, \ldots, p^n$$

հաջորդականության $1 \cdot p, 2 \cdot p, \ldots, p^{n-1} \cdot p$ անդամների քանակը, որոնք բաժանվում են p-ի վրա ճիշտ հավասար է p^{n-1}-ի: Ուստի, այդ շարքի մնացած բոլոր անդամները կլինեն փոխադարձաբար պարզ p^n-ի հետ: Հետևաբար՝

$$\varphi\left(p^n\right) = p^n - p^{n-1} : \qquad \square$$

Այժմ անցնենք էյլերի ֆունկցիայի, այսպես կոչված, **արտադրյալային հատկության** ձևակերպմանը և ապացուցմանը.

Թեորեմ 9.5 (Չինական թեորեմ): *Եթե $m, n \geqslant 1$ բնական թվերը փոխադարձաբար պարզ են, ապա*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n),$$

այսինքն՝ էյլերի ֆունկցիան արտադրյալային է:

Ապացուցում: Պահանջվում է ապացուցել, որ $1, 2, \ldots, m \cdot n$ հաջորդականության մեջ $m \cdot n$ -ի հետ փոխադարձաբար պարզ անդամների քանակը հավասար է $\varphi(m) \cdot \varphi(n)$-ին: Ապացուցման համար 1-ից մինչև $m \cdot n$ բնական թվերը դասավորենք ըստ հետևյալ աղյուսակի՝

1	2	3	$\cdots$	m
$m+1$	$m+2$	$m+3$	$\cdots$	$m+m=2m$
$2m+1$	$2m+2$	$2m+3$	$\cdots$	$2m+m=3m$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
$(n-1)m+1$	$(n-1)m+2$	$(n-1)m+3$	$\cdots$	nm

Աղյուսակի առաջին սյունակի թվերը պատկանում են $\mathbb{Z}_m$-ի $[1]$ դասին (տարրին), երկրորդ սյունակի թվերը՝ $\mathbb{Z}_m$-ի $[2]$ դասին, և այլն, վերջին սյունակի թվերը պատկանում են $\mathbb{Z}_m$-ի $[0]$ դասին: $\varphi(m)$-ը հավասար է $1, 2, \ldots, m$ հաջորդականության բոլոր այն թվերի քանակին, որոնք փոխադարձաբար պարզ են m-ի հետ, կամ՝

$$[0], [1], \ldots, [m-1] \in \mathbb{Z}_m$$

հաջորդականության բոլոր հակադարձելի դասերի թվին: Նույնը վերաբերվում է $\varphi(n)$-ին և $\varphi(n \cdot m)$-ին: Միաժամանակ $1 \leqslant a \leqslant mn$ թիվը կլինի փոխադարձաբար պարզ mn-ի հետ այն և միայն այն դեպքում, երբ a-ն փոխադարձաբար պարզ է m, n բնական թվերից յուրաքանչյուրի հետ (հատկություն 3.1): Նկատենք, որ աղյուսակի յուրաքանչյուր սյունակ պարունակում է n հատ թվեր, որոնք զույգ առ զույգ բաղդատելի չեն ըստ մոդուլ n-ի: Իրոք, եթե $im+k \equiv jm+k (mod\, n)$, ապա $(i-j)m \equiv 0 (mod\, n)$, այսինքն $(i-j)m$ արտադրյալը բաժանվում է n-ի վրա: Ուստի, հատկություն 3.4-ի համաձայն, $(i-j)$-ն կբաժանվի n-ի վրա, որտեղ $|i-j| < n$, որովհետև $0 \leqslant i,\ j < n$, և, հետևաբար, $i - j = 0$, $i = j$: Այսպիսով, աղյուսակի յուրաքանչյուր սյունակում կպարունակվի $\varphi(n)$ հատ թվեր, որոնք փոխադարձաբար պարզ են n-ի հետ: Սակայն, ինչպես նկատեցինք, աղյուսակում գոյություն ունի ճիշտ $\varphi(m)$ հատ սյունակներ, որոնց բոլոր թվերը փոխադարձաբար պարզ են m-ի հետ: Հետևաբար, հենց այդ սյունակներում էլ կգտնվեն աղյուսակի բոլոր այն a թվերը, որոնք միաժամանակ փոխադարձաբար պարզ են m-ի և n-ի հետ: Արդյունքում, այդպիսի a թվերի քանակը ստացվում է հավասար $\varphi(n) \cdot \varphi(m)$-ի:

Երկրորդ ապացուցում: Այս ապացուցումը հենվում է Չինական թեորեմի (թեորեմ 3.5) վրա: $[x] \in \mathbb{Z}_m$ տարրը նշանակենք նաև $[x]_m$-ով և դիտարկենք

$$\mathbb{Z}_m \times \mathbb{Z}_n = \{(u, v) \mid u \in \mathbb{Z}_m, v \in \mathbb{Z}_n\}$$

դեկարտյան արտադրյալը, որում բազմապատկման գործողությունը հասկացվում է ըստ համապատասխան բաղադրիչների արտադրյալի՝

$$(u_1, v_1) \cdot (u_2, v_2) = (u_1 u_2, v_1 v_2):$$

Այս արտադրյալ գործողությունը զուգորդական է և օժտված $([1]_m, [1]_n)$ միավորով: Ակնհայտ է, որ

$$(u_1, v_1) \cdot (u_2, v_2) = (u_2, v_2) \cdot (u_1, v_1) = ([1]_m, [1]_n)$$

այն և միայն այն դեպքում, երբ

$$\begin{cases} u_1u_2 = u_2u_1 = [1]_m, \\ v_1v_2 = v_2v_1 = [1]_n; \end{cases}$$

Այսինքն $(u, v) \in \mathbb{Z}_m \times \mathbb{Z}_n$ տարրը կլինի հակադարձելի այն և միայն այն դեպքում, երբ $u \in \mathbb{Z}_m$ և $v \in \mathbb{Z}_n$ տարրերը հակադարձելի են: Հետևաբար, բոլոր $(u, v) \in \mathbb{Z}_m \times \mathbb{Z}_n$ հակադարձելի տարրերի թիվը հավասար է $\varphi(m) \cdot \varphi(n)$-ի: Մնում է համոզվել, որ $\mathbb{Z}_{m \cdot n}$-ի բոլոր հակադարձելի տարրերի թիվը, այսինքն $\varphi(m \cdot n)$-ը, հավասար է $\mathbb{Z}_m \times \mathbb{Z}_n$-ի բոլոր հակադարձելի տարրերի թվին: $\mathbb{Z}_{m \cdot n}$ և $\mathbb{Z}_m \times \mathbb{Z}_n$ բազմությունների կարգերը հավասար են: Այդ բազմությունների միջև կառուցենք այնպիսի բիեկտիվ արտապատկերում, որը մակածում է բիեկտիվ արտապատկերում հակադարձելի տարրերի համապատասխան բազմությունների միջև:

$\mathbb{Z}_{m \cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n$ արտապատկերումը սահմանենք հետևյալ կերպ՝

$$[x]_{m \cdot n} \to ([x]_m, [x]_n) :$$

Նախ այս համապատասխանեցումը արտապատկերում է, որովհետև եթե $[x]_{m \cdot n} = [y]_{m \cdot n}$, ապա $x - y/m \cdot n$, հետևաբար, $x - y/m$ և $x - y/n$, այսինքն $[x]_m = [y]_m$ և $[x]_n = [y]_n$:

Արտապատկերման ինյեկտիվությունը. եթե

$$([x]_m, [x]_n) = ([y]_m, [y]_n) ,$$

ապա $[x]_m = [y]_m$, $[x]_n = [y]_n$ և $x - y/m$, $x - y/n$: Հետևաբար, $x - y/m \cdot n$ (հատկություն 3.5) և $[x]_{m \cdot n} = [y]_{m \cdot n}$:

Արտապատկերման սյուրեկտիվությունը. ցանկացած $a, b \in \mathbb{Z}$ ամբողջ թվերի համար գոյություն ունի այնպիսի $x \in \mathbb{Z}$, որ $([a]_m, [b]_n) = ([x]_m, [x]_n)$, որովհետև, համաձայն թեորեմ 3.5-ի,

$$\begin{cases} x \equiv a (mod\, m), \\ x \equiv b (mod\, n) \end{cases}$$

համակարգն ունի լուծում:

Մնում է նկատել, որ $[x]_{m \cdot n}$-ը կլինի հակադարձելի այն և միայն այն դեպքում, երբ $[x]_m$-ը և $[x]_n$-ը հակադարձելի են, որովհետև x-ը կլինի փոխադարձաբար պարզ mn-ի հետ այն և միայն այն դեպքում, երբ x-ը փոխադարձաբար պարզ է m-ի և n-ի հետ (հատկություն 3.1): Այսպիսով, կառուցված $\mathbb{Z}_{m\cdot n} \to \mathbb{Z}_m \times \mathbb{Z}_n$ բիեկտիվ արտապատկերումը մակածում է բիեկտիվ արտապատկերում $\mathbb{Z}_{m\cdot n}$-ի և $\mathbb{Z}_m \times \mathbb{Z}_n$-ի հակադարձելի տարրերի բազմությունների միջև[9]: □

Հատկություն 9.3: *Եթե* $a_1, a_2, \ldots, a_n$ *բնական թվերը զույգ առ զույգ փոխադարձաբար պարզ են, ապա*

$$\varphi(a_1 \cdot a_2 \cdots a_n) = \varphi(a_1) \cdot \varphi(a_2) \cdots \varphi(a_n),$$

որտեղ $n \geqslant 2$:

Ապացուցում (վերհանգման եղանակ): $n = 2$ դեպքում պնդումն արդեն ապացուցված է: Ենթադրելով պնդումը ճիշտ n-ից քիչ թվով անդամներ ունեցող և զույգ առ զույգ փոխադարձաբար պարզ բնական թվերի հաջորդականությունների համար ու օգտվելով նախորդ հատկությունից, կունենանք՝

$$\varphi(a_1 \cdot a_2 \cdots a_n) = \varphi\left((a_1 \cdot a_2 \cdots a_{n-1})a_n\right) =$$

$$= \varphi(a_1 \cdot a_2 \cdots a_{n-1}) \cdot \varphi(a_n) = \varphi(a_1) \cdot \varphi(a_2) \cdots \varphi(a_{n-1}) \cdot \varphi(a_n),$$

որովհետև a_n-ը, համաձայն հատկություն 3.2-ի, կլինի փոխադարձաբար պարզ նաև $a_1 \cdot a_2 \cdots a_{n-1}$ արտադրյալի հետ: □

Հետևյալ արդյունքը հնարավորություն է տալիս ցանկացած n բնական թվի համար որոշել Էյլերի ֆունկցիայի $\varphi(n)$ արժեքը, արտահայտելով նրան n-ով և n-ի կանոնական վերլուծությանը մասնակցող պարզ թվերով:

Թեորեմ 9.6: *Եթե* $n \geqslant 2$ *բնական թիվն ունի*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

կանոնական վերլուծությունը, ապա

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) = n \sum_{n/d, d>0} \frac{\mu(d)}{d},$$

[9] Տես նաև ավելի ընդհանուր թեորեմ 19.21-ի ապացուցումը:

որտեղ μ-ն Մյոբիուսի ֆունկցիան է (գլուխ 6): Մասնավորապես՝

ա) $\varphi(n)$-ը զույգ թիվ է, եթե $n > 2$;

բ) Եթե m-ը n բնական թվի բնական բաժանարարն է, ապա $\varphi(m)$ -ը կլինի $\varphi(n)$-ի բաժանարարը:

Ապացուցում: Ակնհայտ է, որ

$$n_1 = p_1^{\alpha_1}, n_2 = p_2^{\alpha_2}, \ldots, n_k = p_k^{\alpha_k}$$

թվերը զույգ առ զույգ փոխադարձաբար պարզ են և $n = n_1 \cdot n_2 \cdots n_k$; Հետևաբար, համաձայն նախորդ հատկության, կունենանք՝

$$\varphi(n) = \varphi(n_1) \cdot \varphi(n_2) \cdots \varphi(n_k) = \varphi\left(p_1^{\alpha_1}\right) \cdot \varphi\left(p_2^{\alpha_2}\right) \cdots \varphi\left(p_k^{\alpha_k}\right),$$

որտեղից, ըստ հատկություն 9.3-ի, կստանանք՝

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) =$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) =$$

$$= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right);$$

Մնում է կիրառել թեորեմ 6.4-ը, իսկ ա) և բ) պնդումները բխում են ապացուցված հավասարությունից: □

Ապացուցենք նաև հետևյալ ընդհանուր արդյունքը:

Հատկություն 9.4: *Ցանկացած m և n բնական թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)},$$

որտեղ $d = (m, n)$:

Ապացուցում: Եթե $m = 1$ կամ $n = 1$, ապա գրված հավասարությունը ակնհայտորեն ճիշտ է: Դիցուք $m > 1$ և $n > 1$: Հնարավոր է երկու դեպք:

1) m և n բնական թվերի կանոնական վերլուծությունները չեն պարունակում ընդհանուր պարզ թվեր; Այդ դեպքում $(m,n) = 1$ և պնդվող հավասարությունը համընկնում է թեորեմ 9.5-ի հետ:

2) m և n բնական թվերի կանոնական վերլուծություններն ունեն ընդհանուր պարզ թվեր: Դիցուք m-ը և n-ը ունեն հետևյալ կանոնական վերլուծությունները՝

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t},$$

$$n = q_1^{\delta_1} q_2^{\delta_2} \cdots q_t^{\delta_t} l_1^{\gamma_1} l_2^{\gamma_2} \cdots l_s^{\gamma_s},$$

որտեղ $q_1, q_2, \ldots, q_t$ պարզ թվերը մասնակցում են երկու կանոնական վերլուծություններին: Այդ դեպքում,

$$m \cdot n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1+\delta_1} \cdots q_t^{\beta_t+\delta_t} \cdot l_1^{\gamma_1} \cdots l_s^{\gamma_s},$$

$$d = (m,n) = q_1^{\min\{\beta_1,\delta_1\}} \cdot q_2^{\min\{\beta_2,\delta_2\}} \cdots q_t^{\min\{\beta_t,\delta_t\}}$$

և, հետևաբար, համաձայն նախորդ թեորեմի, կունենանք՝

$$\begin{aligned}\varphi(m \cdot n) &= m \cdot n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \left(1 - \frac{1}{q_1}\right) \cdots \\ &\qquad \cdots \left(1 - \frac{1}{q_t}\right) \left(1 - \frac{1}{l_1}\right) \cdots \left(1 - \frac{1}{l_s}\right) = \\ &= m \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_t}\right) \times \\ &\qquad \times n \left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_t}\right) \left(1 - \frac{1}{l_1}\right) \cdots \left(1 - \frac{1}{l_s}\right) \times \\ &\qquad \times \frac{d}{d\left(1 - \frac{1}{q_1}\right) \cdots \left(1 - \frac{1}{q_t}\right)} = \varphi(m) \cdot \varphi(n) \cdot \frac{d}{\varphi(d)};\end{aligned}$$

□

Հաշվի առնելով նաև $n \cdot m = (n,m) \cdot [n,m]$ հավասարությունը (հետևություն 4.2), հանգում ենք հետևյալ արդյունքին:

Հետևություն 9.2: *Ցանկացած m և n բնական թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$\varphi(n) \cdot \varphi(m) = \varphi\left((n,m)\right) \cdot \varphi\left([n,m]\right)\ ^{10}\ :$$

[10]Մասնավորապես, Г.А. Кудреватов, *Сборник задач по теории чисел,* М., 1970,խնդրագրքի 146-րդ խնդրի պնդումը տեղի չունի:

Ապացույց: Մի կողմից (հատկություն 9.4)՝

$$\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)\cdot\frac{d}{\varphi(d)},\quad d=(n,m),$$

մյուս կողմից՝

$$\varphi(n\cdot m)=\varphi((n,m)\cdot[n,m])=$$

$$\varphi((n,m))\cdot\varphi([n,m])\cdot\frac{(n,m)}{\varphi((n,m))}=(n,m)\cdot\varphi([n,m]);$$

Հետևաբար,

$$\varphi(n)\cdot\varphi(m)\cdot\frac{d}{\varphi(d)}=(n,m)\cdot\varphi([n,m]),$$

$$\varphi(n)\cdot\varphi(m)\cdot\frac{1}{\varphi(d)}=\varphi([n,m]),$$

$$\varphi(n)\cdot\varphi(m)=\varphi((n,m))\cdot\varphi([n,m]):\qquad\square$$

Հետևյալ հատկությունը կոչվում է Գաուսի նույնություն:

Թեորեմ 9.7 (Գաուս): *Եթե $d_1,d_2,\ldots,d_k$ թվերը կամայական $n>1$ բնական թվի բոլոր բնական բաժանարարներն են, ապա՝*

$$\varphi(d_1)+\varphi(d_2)+\cdots+\varphi(d_k)=n;\quad \text{(Գաուսի նույնությունը)}$$

Համառոտ՝ $\sum\limits_{n/d,d>0}\varphi(d)=n$*:*

Ապացույց: Դիցուք

$$n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_m^{\alpha_m}$$

վերլուծությունը տրված $n>1$ բնական թվի կանոնական վերլուծությունն է, որտեղ $p_1,p_2,\ldots,p_m$-ը միմյանցից տարբեր պարզ թվեր են: Համաձայն հատկություն 6.6-ի, n-ի յուրաքանչյուր $d\geqslant 1$ բնական բաժանարար ունի

$$d=p_1^{\beta_1}\cdot p_2^{\beta_2}\cdots p_m^{\beta_m}$$

տեսքը, որտեղ $0\leqslant\beta_1\leqslant\alpha_1$, $0\leqslant\beta_2\leqslant\alpha_2$, $\ldots$, $0\leqslant\beta_m\leqslant\alpha_m$: Հետևաբար, եթե $d_1,d_2,\ldots,d_k$-ն n-ի բոլոր հնարավոր բնական բաժանարարներն են, ապա

$$\left(1+p_1+p_1^2+\cdots+p_1^{\alpha_1}\right)\cdot\left(1+p_2+p_2^2+\cdots+p_2^{\alpha_2}\right)\cdots$$

$$\cdots\left(1+p_m+p_m^2+\cdots+p_m^{\alpha_m}\right)=d_1+d_2+\cdots+d_k,$$

իսկ օգտվելով հատկություն 9.3-ից բխող

$$\varphi\left(p_1^{\beta_1}\right)\cdot\varphi\left(p_2^{\beta_2}\right)\cdots\varphi\left(p_m^{\beta_m}\right)=\varphi\left(p_1^{\beta_1}\cdot p_2^{\beta_2}\cdots p_m^{\beta_m}\right)$$

հավասարությունից, կստանանք՝

$$\begin{gathered}\left(\varphi(1)+\varphi\left(p_1\right)+\varphi\left(p_1^2\right)+\cdots\right.\\ \left.+\varphi\left(p_1^{\alpha_1}\right)\right)\cdot\left(\varphi(1)+\varphi\left(p_2\right)+\varphi\left(p_2^2\right)+\cdots+\varphi\left(p_2^{\alpha_2}\right)\right)\cdots\\ \cdots\left(\varphi(1)+\varphi\left(p_m\right)+\varphi\left(p_m^2\right)+\cdots+\varphi\left(p_m^{\alpha_m}\right)\right)=\varphi\left(d_1\right)+\varphi\left(d_2\right)+\cdots+\varphi\left(d_k\right);\end{gathered}$$

Միաժամանակ, համաձայն հատկություն 9.2-ի՝

$$\begin{gathered}\varphi(1)+\varphi\left(p_i\right)+\varphi\left(p_i^2\right)+\cdots+\varphi\left(p_i^{\alpha_i}\right)=\\ =1+\left(p_i-1\right)+\left(p_i^2-p_i\right)+\cdots+\left(p_i^{\alpha_i}-p_i^{\alpha_i-1}\right)=p_i^{\alpha_i};\end{gathered}$$

Այսպիսով՝

$$p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdots p_m^{\alpha_m}=\varphi\left(d_1\right)+\varphi\left(d_2\right)+\cdots+\varphi\left(d_k\right),$$

այսինքն՝

$$n=\varphi\left(d_1\right)+\varphi\left(d_2\right)+\cdots+\varphi\left(d_k\right):$$

Երկրորդ ապացուցում: Կարելի է տալ թեորեմ 9.7-ի նաև հետևյալ տարրական ապացուցումը: Դիտարկենք $\frac{1}{n},\frac{2}{n},\ldots,\frac{n-1}{n},\frac{n}{n}$ կոտորակները (ռացիոնալ թվերը), որոնց քանակը հավասար է n-ի: Յուրաքանչյուր $\frac{s}{n}$ կոտորակ, որտեղ $1\leqslant s\leqslant n$, կրճատելով (s,n)-ով կստանանք $\frac{a_1}{b_1},\frac{a_2}{b_2},\ldots,\frac{a_{n-1}}{b_{n-1}},\frac{a_n}{b_n}$ կոտորակները, որտեղ $(a_i,b_i)=1$, $i=1,\ldots,n$ (հետևություն 3.1):

Այստեղ $b_1,b_2,\ldots,b_{n-1},b_n$ բնական թվերը n-ի բաժանարարներ են: Ընդ որում n-ի յուրաքանչյուր d բնական բաժանարար $b_1,b_2,\ldots,b_{n-1},b_n$ թվերի շարքում կհանդիպի, այն էլ $\varphi(d)$ անգամ: Իրոք, եթե $n=d\cdot d'$ և $1\leqslant l\leqslant d$, $(l,d)=1$, ապա $l\cdot d'\leqslant d\cdot d'=n$ և $\frac{l\cdot d'}{n}=\frac{l\cdot d'}{d\cdot d'}=\frac{l}{d}$:

Քանի որ դիտարկվող կոտորակների թիվը հավասար է n-ի, ապա՝

$$n=\sum_{n/d,d>0}\varphi(d):$$

Թեորեմն ապացուցված է[11]: □

Թեորեմ 9.8: *Եթե $d_1, d_2, \ldots, d_k$ թվերը կամայական $n > 1$ բնական թվի բոլոր բնական բաժանարարներն են, ապա Մյոբիուսի μ ֆունկցիայի (գլուխ 6) համար տեղի ունի հետևյալ հավասարությունը՝*

$$\mu(d_1) + \mu(d_2) + \cdots + \mu(d_k) = 0;$$

Համառոտ՝ $\sum\limits_{n/d, d>0} \mu(d) = 0$*:*

Ապացուցում: Քանի որ համաձայն թեորեմ 6.3-ի Մյոբիուսի μ ֆունկցիան ևս արտադրյալային է, ապա կարելի է կրկնել նախորդ թեորեմի առաջին ապացուցումը՝ հաշվի առնելով

$$\mu(1) + \mu(p_i) + \mu\left(p_i^2\right) + \cdots + \mu\left(p_i^{\alpha_i}\right) = 1 + (-1) + 0 + \cdots + 0 = 0$$

հավասարությունը: □

9.4. Թվակերպ բազմություններ և արտադրյալային ֆունկցիաներ: τ և σ ֆունկցիաները: Կատարյալ թվեր

Էյլերի և Մյոբիուսի ֆունկցիաների մի շարք հատկություններ բնական ճանապարհով կարելի է ընդհանրացնել: Այդ նպատակով նախ ներմուծենք թվակերպ բազմության ընդհանուր հասկացությունը, ապա դրա հիման վրա նաև արտադրյալային ֆունկցիայի ընդհանուր գաղափարը:

Ոչ դատարկ Q բազմությունը կոչվում է **թվակերպ բազմություն**, եթե դրա մեջ սահմանված են գումարման՝ $+$ և բազմապատկման՝ $\cdot$ այնպիսի գործողություններ, որոնք բավարարում են հետևյալ պայմաններին (աքսիոմներին).

1. Գումարման և բազմապատկման գործողությունները զուգորդական են, այսինքն՝

$$(x + y) + z = x + (y + z),$$

$$(x \cdot y) \cdot z = x \cdot (y \cdot z)$$

ցանկացած $x, y, z \in Q$ տարրերի համար:

[11] Ելնելով թեորեմ 9.7-ի երկրորդ ապացուցումից, կարելի է ստանալ էյլերի φ ֆունկցիայի արտադրյալային հատկության նոր ապացուցում (տես՝ վարժություն 21-ը այս գլխի վերջում և դրա լուծման ցուցումը):

2. Գումարման և բազմապատկման գործողությունները տեղափոխական են, այսինքն՝
$$x + y = y + x,$$
$$x \cdot y = y \cdot x$$
ցանկացած $x, y \in Q$ տարրերի համար:

3. Գումարման և բազմապատկման գործողություններից յուրաքանչյուրն օժտված է միավորով: Այդ միավորներից յուրաքանչյուրը որոշվում է միարժեքորեն, ըստ որում, գումարման միավորը կոչվում է զրո և նշանակվում է 0-ով, իսկ բազմապատկման միավորը՝ մեկ և նշանակվում է 1-ով, այսինքն՝
$$x + 0 = 0 + x = x,$$
$$x \cdot 1 = 1 \cdot x = x$$
ցանկացած $x \in Q$ տարրի համար: Ենթադրվում է նաև, որ $0 \neq 1$ և $x \cdot 0 = 0$ հավասարությունը՝ ցանկացած $x \in Q$ տարրի համար:

4. Բազմապատկման և գումարման գործողությունները կապված են բաշխական (կամ բաշխականության) օրենքով (նույնությամբ), այսինքն՝
$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
ցանկացած $x, y, z \in Q$ տարրերի համար:

   Սովորաբար բաշխական օրենքը համառոտ գրվում է այսպես՝ $x(y + z) = xy + xz$:

Օրինակ, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}_n$ բազմությունները[12] թվակերպ բազմություններ են:

Եթե Q_1 և Q_2 բազմությունները թվակերպ բազմություններ են, ապա $Q_1 \times Q_2 = \{(a, b) \,|\; a \in Q_1, b \in Q_2\}$ բազմությունը (դեկարտյան արտադրյալը) վերածվում է թվակերպ բազմության, եթե սահմանենք՝
$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 \cdot a_2, b_1 \cdot b_2) :$$

[12] Այստեղ ենթադրվում է, որ $0 \in \mathbb{N}$:

Թվակերպ բազմության x, y տարրերի համար $(x + y)$-ը և $(x \cdot y)$-ը համապատասխանաբար կոչվում են x, y տարրերի գումար և արտադրյալ: Օգտվելով փակագծերից կարելի է կազմել թվակերպ բազմության վերջավոր թվով ցանկացած տարրերի գումարը և արտադրյալը՝ $x + (y + z)$, $x \cdot ((y \cdot z) \cdot u)$, ...

Գումարման և բազմապատկման գործողությունների զուգորդականությունից բխում է (թեորեմ 1.3), որ թվակերպ բազմության կամայական $x_1, \ldots, x_n$ տարրերի հաջորդականությունից փակագծերի տարբեր դասավորությամբ կազմված բոլոր գումարները (արտադրյալները) միմյանց հավասար են և այդ պատճառով այդ գումարներից (արտադրյալներից) յուրաքանչյուրը կարելի է գրել առանց փակագծերի դասավորության՝ $x_1 + x_2 + \cdots + x_n$ (համապատասխանաբար՝ $x_1 \cdot x_2 \cdots x_n$): Վերհանգման եղանակով դժվար չէ ապացուցել նաև հետևյալ ընդհանրացված բաշխական օրենքը (նույնությունը)՝

$$x(y_1 + \cdots + x_n) = xy_1 + \cdots + xy_n :$$

Դիցուք Q-ն թվակերպ բազմություն է: $\theta : \mathbb{N} \to Q$ ֆունկցիան կոչվում է զրոյական, եթե $\theta(x) = 0$ բոլոր $x \in \mathbb{N}$ բնական թվերի համար: Հակառակ դեպքում, $\theta : \mathbb{N} \to Q$ ֆունկցիան կոչվում է ոչ զրոյական և գրվում է՝ $\theta \neq 0$:

$\theta : \mathbb{N} \to Q$ ֆունկցիան կոչվում է **արտադրյալային**, եթե այն բավարարում է հետևյալ պայմաններին՝

ա) $\theta(1) = 1$ (և, հետևաբար, $\theta \neq 0$);

բ) $\theta(n \cdot m) = \theta(n) \cdot \theta(m)$, որտեղ $(n, m) = 1$, $n, m \in \mathbb{N}$:

Օրինակ, $\theta : \mathbb{N} \to Q$ ֆունկցիան, որտեղ ցանկացած $x \in \mathbb{N}$ բնական թվի համար՝ $\theta(x) = 1$, կլինի արտադրյալային: Եթե $Q = \mathbb{R}$, $t \in \mathbb{R}$ և $\theta(x) = x^t$ ցանկացած $x \in \mathbb{N}$ բնական թվի համար, ապա θ-ն արտադրյալային ֆունկցիա է: Էյլերի և Մյոբիուսի ֆունկցիաները արտադրյալային են ($Q = \mathbb{Z}$):

Եթե պայմանավորվենք Q թվակերպ բազմության մեջ նշանակել՝

$$I(k) = \underbrace{1 + 1 + \cdots + 1}_{k} = k \circ 1, \quad k \in \mathbb{N}, \text{ [13]}$$

[13] $\circ$ նշանը չշփոթել Q թվակերպ բազմության $\cdot$ բազմապատկման գործողության հետ:

ապա կստանանք $I : \mathbb{N} \to Q$ արտադրյալային ֆունկցիան: Ընդհանուր դեպքում, կամայական $\alpha : \mathbb{N} \to \mathbb{N}$ արտադրյալային ֆունկցիային համապատասխան սահմանելով $\theta_\alpha : \mathbb{N} \to Q$ ֆունկցիան, հետևյալ կերպ՝

$$\theta_\alpha(n) = \alpha(n) \circ 1,$$

կստանանք արտադրյալային ֆունկցիա: Իրոք, $\theta_\alpha(1) = 1$ և եթե $(n, m) = 1$, ապա

$$\theta_\alpha(n \cdot m) = \alpha(n \cdot m) \circ 1 = (\alpha(n) \cdot \alpha(m)) \circ 1 =$$
$$= (\alpha(n) \circ 1) \cdot (\alpha(m) \circ 1) = \theta_\alpha(n) \cdot \theta_\alpha(m) :$$

Մասնավորապես, եթե որպես α վերցնենք էյլերի φ ֆունկցիան, ապա համապատասխան θ_φ ֆունկցիան կկոչվի **էյլերի թվակերպ ֆունկցիա**:

Եթե Q-ն կամայական թվակերպ բազմություն է, իսկ

$$\theta(n) = \begin{cases} 0, & \text{երբ } n\text{-ը բաժանվում է որևէ } p \\ & \text{պարզ թվի քառակուսու վրա ,} \\ 1, & \text{հակառակ դեպքում,} \end{cases}$$

ապա կառուցված $\theta : \mathbb{N} \to Q$ ֆունկցիան կլինի արտադրյալային: Ավելի ընդհանուր է հետևյալ արտադրյալային ֆունկցիայի օրինակը. սևեռենք որևէ $a \in Q$ տարր և սահմանենք $\theta_a : \mathbb{N} \to Q$ ֆունկցիան հետևյալ կերպ՝

$$\theta_a(n) = \begin{cases} 1, & \text{երբ } n = 1, \\ a^k, & \text{երբ } n = p_1 \cdots p_k, \text{ որտեղ բոլոր } p_i \text{ թվերը} \\ & \text{միմյանցից տարբեր պարզ թվեր են,} \\ 0, & \text{երբ } n\text{-ը բաժանվում է որևէ } p \\ & \text{պարզ թվի քառակուսու վրա :} \end{cases}$$

Հեշտությամբ ստուգվում է, որ սահմանված $\theta_a : \mathbb{N} \to Q$ ֆունկցիան արտադրյալային է (տես թեորեմ 6.3-ի ապացուցումը): θ_a-ից, $a = 1$ դեպքում, ստանում ենք նախորդ օրինակը, իսկ $Q = \mathbb{Z}$ և $a = -1$ դեպքում՝ Մյոբիուսի ֆունկցիան: Այս պատճառով, $\theta_a : \mathbb{N} \to Q$ արտադրյալային ֆունկցիան բնական է անվանել **Մյոբիուսի ընդհանրացված ֆունկցիա**:

Հատկություն 9.5: *Դիցուք Q-ն թվակերպ բազմություն է: Եթե $\theta : \mathbb{N} \to Q$ ֆունկցիան արտադրյալային է, ապա տեղի ունեն հետևյալ հատկությունները՝*

1) $\theta(1) = 1$*;*

2) Եթե $a_1, a_2, \ldots, a_m \in \mathbb{N}$ *բնական թվերը զույգ առ զույգ փոխադարձաբար պարզ են, ապա*

$$\theta(a_1 \cdot a_2 \cdots a_m) = \theta(a_1) \cdot \theta(a_2) \cdots \theta(a_m),$$

որտեղ $m \geqslant 2$*:*

Ապացույց: Ըստ արտադրյալային ֆունկցիայի սահմանման՝ $\theta(1) = 1$: 2) հատկությունն ապացուցվում է վերհանգման եղանակով: □

Հետևություն 9.3*: Դիցուք Q-ն թվակերպ բազմություն է: Որպեսզի $\theta : \mathbb{N} \to Q$ ֆունկցիան լինի արտադրյալային անհրաժեշտ է և բավարար, որ տեղի ունենան հետևյալ երկու պայմանները՝*

1°) $\theta(1) = 1$*:*

2°) $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ *կանոնական վերլուծությամբ օժտված ցանկացած* $n > 1$ *բնական թվի համար՝*

$$\theta(n) = \theta\left(p_1^{\alpha_1}\right) \cdot \theta\left(p_2^{\alpha_2}\right) \cdots \theta\left(p_m^{\alpha_m}\right):$$

Ապացույց: Անհրաժեշտությունը բխում է նախորդ հատկությունից: Ապացուցենք բավարարությունը:

Դիցուք $a, b \in \mathbb{N}$ և $(a, b) = 1$: Հետևաբար, a, b բնական թվերը կունենան հետևյալ կանոնական վերլուծությունները՝

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

$$b = p_{k+1}^{\alpha_{k+1}} \cdots p_s^{\alpha_s},$$

որտեղ $p_i \neq p_j$, $i, j = 1, \ldots, s$, $i \neq j$: Այժմ 2°) պայմանի համաձայն՝

$$\theta\left(a \cdot b\right) = \theta\left(p_1^{\alpha_1} \cdots p_s^{\alpha_s}\right) = \theta\left(p_1^{\alpha_1}\right) \cdots \theta\left(p_k^{\alpha_k}\right) \cdot \theta\left(p_{k+1}^{\alpha_{k+1}}\right) \cdots \theta\left(p_s^{\alpha_s}\right) =$$

$$= \theta\left(p_1^{\alpha_1} \cdots p_k^{\alpha_k}\right) \cdot \theta\left(p_{k+1}^{\alpha_{k+1}} \cdots p_s^{\alpha_s}\right) = \theta(a) \cdot \theta(b); \qquad \square$$

Ստացված հայտանիշը տալիս է արտադրյալային ֆունկցիաների կառուցման ընդհանուր եղանակը: Որևէ $\theta : \mathbb{N} \to Q$ արտադրյալային ֆունկցիա կառուցելու համար նախ պետք է սահմանել $\theta(1) = 1$, ապա ցանկացած p պարզ թվի և ցանկացած k բնական թվի համար սահմանել $\theta\left(p^k\right)$-ը՝ որպես Q թվակերպ բազմության կամայական տարր: Որից հետո, ցանկացած $n > 1$ բնական թվի համար, որտեղ $n = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, սահմանում ենք՝

$$\theta(n) = \theta\left(p_1^{\alpha_1}\right) \cdots \theta\left(p_t^{\alpha_t}\right):$$

Համաձայն հետևություն 9.3-ի, θ-ն կլինի արտադրյալային ֆունկցիա:

Հաջորդ հատկությունը հնարավորություն է ընձեռում տրված արտադրյալային ֆունկցիաների միջոցով ստանալ նոր արտադրյալային ֆունկցիաներ:

Հատկություն 9.6: *Դիցուք Q-ն թվակերպ բազմություն է: Եթե $\theta_1, \theta_2, \ldots, \theta_n : \mathbb{N} \to Q$ ֆունկցիաները արտադրյալային են, ապա $\theta : \mathbb{N} \to Q$ ֆունկցիան, որը սահմանվում է հետևյալ կերպ՝*

$$\theta(x) = \theta_1(x) \cdot \theta_2(x) \cdots \theta_n(x), \quad x \in \mathbb{N},$$

ևս կլինի արտադրյալային:

Ապացուցում (վերհանգման եղանակ): Եթե $n = 2$, ապա $\theta(1) = \theta_1(1) \cdot \theta_2(1) = 1 \cdot 1 = 1$: Այնուհետև, եթե $(a, b) = 1$, ապա

$$\theta(a \cdot b) = \theta_1(a \cdot b) \cdot \theta_2(a \cdot b) = \theta_1(a)\theta_1(b) \cdot \theta_2(a)\theta_2(b) =$$

$$= \theta_1(a)\theta_2(a) \cdot \theta_1(b)\theta_2(b) = \theta(a) \cdot \theta(b);$$

Կատարենք վերհանգման ենթադրություն և դիտարկենք $\theta(x) = \theta_1(x) \cdots \theta_n(x)$, $x \in \mathbb{N}$, ֆունկցիան: Ըստ վերհանգման ենթադրության

$$\theta'(x) = \theta_1(x) \cdots \theta_{n-1}(x)$$

ֆունկցիան կլինի արտադրյալային, ուստի արտադրյալային կլինի նաև $\theta(x) = \theta'(x) \cdot \theta_n(x)$ ֆունկցիան: $\square$

Հատկություն 9.7: *Դիցուք Q-ն թվակերպ բազմություն է և $a \in Q$: Եթե $d_1, \ldots, d_k$ թվերը կամայական $n > 1$ բնական թվի բոլոր բնական բաժանարարներն են և $n = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$, ապա ցանկացած $\theta : \mathbb{N} \to Q$ արտադրյալային ֆունկցիայի համար՝*

$$\theta\left(d_1\right) + \cdots + \theta\left(d_k\right) = \left(1 + \theta\left(p_1\right) + \cdots + \theta\left(p_1^{\alpha_1}\right)\right) \cdots \left(1 + \theta\left(p_m\right) + \cdots + \theta\left(p_m^{\alpha_m}\right)\right):$$

Մասնավորապես, Մյոբիուսի ընդհանրացված ֆունկցիայի համար կունենանք՝

$$\theta_a(d_1)+\cdots+\theta_a(d_k)=(1+a)^m\ :$$

Այսպիսով՝

$$\sum_{n/d,d>0}\theta_a(d)=\begin{cases}1, & \text{եթե }\ n=1,\\ (1+a)^m, & \text{եթե }\ n>1\ \text{ և }\ n=p_1^{\alpha_1}\cdots p_m^{\alpha_m}\ :\end{cases}$$

Ապացուցում: Թեորեմ 9.7-ի ապացուցման սկզբնամասի դատողությունների կրկնությունն է: □

Հաջորդ հատկության ապացուցման մեջ նշվում է հատկություն 9.7-ի կիրառության երկու դեպք:

Ցանկացած $n\in\mathbb{N}$ բնական թվի համար $\tau(n)$-ով նշանակենք n-ի բոլոր բնական բաժանարարների քանակը, իսկ $\sigma(n)$-ով նշանակենք n-ի բոլոր բնական բաժանարարների գումարը: Ստանում ենք $\tau:\mathbb{N}\to\mathbb{N}$ և $\sigma:\mathbb{N}\to\mathbb{N}$ հանրահայտ ֆունկցիաները:

Օրինակ՝

$$\begin{array}{lllll}\tau(1)=1, & \tau(2)=2, & \tau(3)=2, & \tau(4)=3, & \ldots\\ \sigma(1)=1, & \sigma(2)=1+2=3, & \sigma(3)=1+3=4, & \sigma(4)=1+2+4=7, & \ldots\end{array}$$

Հատկություն 9.8*:* *$n=p_1^{\alpha_1}\cdots p_m^{\alpha_m}$ կանոնական վերլուծությամբ օժտված ցանկացած $n>1$ բնական թվի համար՝*

$$\tau(n)=(1+\alpha_1)\,(1+\alpha_2)\cdots(1+\alpha_m)\,,$$

$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdots\frac{p_m^{\alpha_m+1}-1}{p_m-1}\ :$$

Ապացուցում: Սահմանենք $\theta_1:\mathbb{N}\to\mathbb{N}$ և $\theta_2:\mathbb{N}\to\mathbb{N}$ արտապատկերումները հետևյալ կերպ՝ $\theta_1(x)=1$ և $\theta_2(x)=x$ ցանկացած x բնական թվի համար: Ակնհայտ է, որ θ_1, θ_2 ֆունկցիաները արտադրյալային են և եթե $d_1,\ldots,d_k$ թվերը n-ի բոլոր բնական բաժանարարներն են, ապա օգտվելով հատկություն 9.7-ից կունենանք՝

$$\tau(n)=k=\underbrace{1+1\cdots+1}_{k}=\theta_1\left(d_1\right)+\cdots+\theta_1\left(d_k\right)=$$

$$=\left(1+\theta_1\left(p_1\right)+\cdots+\theta_1\left(p_1^{\alpha_1}\right)\right)\cdots\left(1+\theta_1\left(p_m\right)+\cdots+\theta_1\left(p_m^{\alpha_m}\right)\right)=$$

$$= (1+\alpha_1)\cdots(1+\alpha_m)\,;$$

$$\sigma(n) = d_1 + \cdots + d_k = \theta_2(d_1) + \cdots + \theta_2(d_k) =$$

$$= \left(1+\theta_2(p_1)+\cdots+\theta_2\left(p_1^{\alpha_1}\right)\right)\cdots\left(1+\theta_2(p_m)+\cdots+\theta_2\left(p_m^{\alpha_m}\right)\right) =$$

$$= \left(1+p_1+\cdots+p_1^{\alpha_1}\right)\cdots\left(1+p_m+\cdots+p_m^{\alpha_m}\right) = \frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdots\frac{p_m^{\alpha_m+1}-1}{p_m-1};$$

□

Օրինակ, $\tau(120) = \tau\left(2^3\cdot 3^1\cdot 5^1\right) = (1+3)(1+1)(1+1) = 16;$ $\sigma(120) = \dfrac{2^4-1}{2-1}\cdot\dfrac{3^2-1}{3-1}\cdot\dfrac{5^2-1}{5-1} = 15\cdot 4\cdot 6 = 360$:

Հետևություն 9.4: $\tau(p^\alpha) = \alpha+1$, $\sigma(p^\alpha) = \dfrac{p^{\alpha+1}-1}{p-1}$ *և, հետևաբար,*

$$\tau\left(p_1^{\alpha_1}\cdots p_m^{\alpha_m}\right) = \tau\left(p_1^{\alpha_1}\right)\cdots\tau\left(p_m^{\alpha_m}\right),$$

$$\sigma\left(p_1^{\alpha_1}\cdots p_m^{\alpha_m}\right) = \sigma\left(p_1^{\alpha_1}\right)\cdots\sigma\left(p_m^{\alpha_m}\right),$$

այսինքն, համաձայն հետևություն 9.4-ի, τ և σ ֆունկցիաները կլինեն արտադրյալային: □

Հետևյալ խնդիրը մինչ այժմ չի լուծված. գոյություն ունեն արդյոք անվերջ թվով բնական թվերի այնպիսի (m,n) զույգեր, որ $\varphi(m) = \sigma(n)$: Օրինակ՝ $\varphi(780) = \sigma(105)$:

n բնական թիվը կոչվում է **կատարյալ**, եթե $\sigma(n) = 2n$:

Օրինակ, 6-ը կատարյալ թիվ է, որովհետև $\sigma(6) = 1+2+3+6 = 12 = 2\cdot 6$:

Հետևյալ արդյունքը համարժեք ձևով ներկայացված է Էվկլիդեսի «Սկզբունքներ» աշխատության մեջ (գիրք IX):

Հատկություն 9.9 (Արխիդաս, Էվկլիդես): *Եթե* 2^n-1 *թիվը պարզ է, ապա* $2^{n-1}(2^n-1)$ *արտադրյալը կատարյալ թիվ է:*

Ապացուցում: 2^{n-1}-ի բաժանարարներն են՝ $1, 2, 2^2, \ldots, 2^{n-1}$ թվերը, իսկ 2^n-1 թվի բաժանարարներն են՝ 1, 2^n-1 թվերը, քանի որ (2^n-1)-ը պարզ է: Այսպիսով, 2^{n-1} և 2^n-1 թվերի միակ ընդհանուր բաժանարարը հավասար է 1-ի: Այսինքն այդ թվերը փոխադարձաբար պարզ են, որը բխում է նաև փոխադարձաբար պարզության հայտանիշից՝

$$2^{n-1}x + (2^n-1)\,y = 1,$$

եթե $x = 2$, $y = -1$: Հետևաբար՝

$$\sigma\left(2^{n-1}\left(2^n-1\right)\right) = \sigma\left(2^{n-1}\right)\sigma\left(2^n-1\right) =$$

$$= \left(1+2+2^2+\cdots+2^{n-1}\right)\left(\left(2^n-1\right)+1\right) =$$

$$= \frac{2^n-1}{2-1}\cdot 2^n = \left(2^n-1\right)2^n = 2\cdot 2^{n-1}\left(2^n-1\right) : \qquad \square$$

Հատկություն 9.9-ի ապացուցումից մոտ 2000 տարի հետո Լ. Էյլերի կողմից ապացուցվել է հետևյալ հակադարձ պնդումը:

Թեորեմ 9.9 (Էյլեր): *Յուրաքանչյուր* $m > 0$ *զույգ կատարյալ թիվ ունի հետևյալ տեսքը՝*

$$2^{n-1}\left(2^n-1\right), \quad n \geqslant 2,$$

որտեղ 2^n-1 *թիվը պարզ է:*

Ապացուցում: Դիցուք $m = 2^k\cdot t$, որտեղ $k, t\in\mathbb{N}$, $k\geqslant 1$ և t-ն կենտ է: Հետևաբար, $\left(2^k, t\right) = 1$ և

$$\sigma(m) = \sigma\left(2^k\cdot t\right) = \sigma\left(2^k\right)\cdot\sigma(t) =$$

$$= \left(1+2+2^2+\cdots+2^k\right)\cdot\sigma(t) = \frac{2^{k+1}-1}{2-1}\cdot\sigma(t) = \left(2^{k+1}-1\right)\sigma(t);$$

Քանի որ m-ը կատարյալ է, ապա $\sigma(m) = 2m = 2\left(2^k\cdot t\right) = 2^{k+1}\cdot t$: Ուստի՝

$$\left(2^{k+1}-1\right)\sigma(t) = 2^{k+1}\cdot t$$

և, քանի որ $\left(2^{k+1}-1, 2^{k+1}\right) = 1$, ապա $\sigma(t)$-ն կբաժանվի 2^{k+1}-ի վրա (հատկություն 3.4), այսինքն՝

$$\sigma(t) = 2^{k+1}\cdot l, \quad l\in\mathbb{N};$$

Այսպիսով,

$$\left(2^{k+1}-1\right)\cdot 2^{k+1}\cdot l = 2^{k+1}\cdot t$$

կամ

$$\left(2^{k+1}-1\right)l = t :$$

Այժմ ապացուցենք, որ $l = 1$: Ենթադրելով հակառակը, ստանանք հակասություն: Դիցուք $l > 1$: Այդ դեպքում, օգտվելով վերջին հավասարությունից կարող ենք ասել, որ t-ն օժտված է առնվազն երեք միմյանցից տարբեր դրական բաժանարարներով՝ 1, t, l: Հետևաբար՝

$$\sigma(t) \geqslant 1 + t + l;$$

Սակայն մյուս կողմից՝

$$\sigma(t) = 2^{k+1} \cdot l = \left(2^{k+1} - 1\right) l + l = t + l;$$

Հակասություն: Այսպիսով $l = 1$,

$$t = 2^{k+1} - 1,$$

$$\sigma(t) = 2^{k+1} = t + 1,$$

այսինքն՝ t-ի միակ բնական բաժանարարներն են 1 և t թվերը: Հետևաբար, $t = 2^{k+1} - 1$ թիվը պարզ է, իսկ

$$m = 2^k \cdot t = 2^k \left(2^{k+1} - 1\right) : \qquad \square$$

Այսպիսով, զույգ կատարյալ թվերը կապված են

$$M_n = 2^n - 1$$

տեսքի պարզ թվերի հետ, որոնց 7-րդ գլխում մենք անվանել ենք Մերսեննի թվեր: Եվ մինչ այժմ հայտնի են ընդամենը 38 հատ զույգ կատարյալ թվեր, որոնք համապատասխանում են 38 հատ հայտնի Մերսեննի պարզ թվերին: Առաջին 5 զույգ կատարյալ թվերն են՝ 6, 28, 496, 8128 և 33550336 թվերը, որոնք համապատասխանում են $n = 2, 3, 5, 7, 13$ պարզ թվերին: Առաջին 4 կատարյալ թվերը հայտնի են եղել դեռևս անտիկ աշխարհում (Nichomachus, Introductio Arithmeticae):

Մինչ այժմ հայտնի չէ վերջավոր է թե անվերջ բոլոր կատարյալ թվերի քանակը:

Մինչ այժմ հայտնի չէ գոյություն ունի արդյոք որևէ կենտ կատարյալ թիվ: Այս խնդիրն այժմ համարվում է թվերի տեսության ամենահայտնի չլուծված պրոբլեմներից մեկը:

Կատարյալ թվի սահմանման հետ կապված նշենք նաև, որ մինչ այժմ հայտնի չէ ունի արդյոք $\sigma(n) = 2n+1$ հավասարումը որևէ բնական լուծում ($n \in \mathbb{N}$):

9.5. Ֆունկցիաների Դիրիխլեի արտադրյալ: Մյոբիուսի թեորեմը շրջման վերաբերյալ

Դիցուք Q-ն թվակերպ բազմություն է: Կասենք, որ Q-ն օժտված է -1-ով կամ՝ $-1 \in Q$ հատկությամբ, եթե գոյություն ունի միարժեքորեն որոշվող այնպիսի $x \in Q$ տարր, որ $1 + x = 0$, որտեղ 0-ն և 1-ը Q-ի զրոն և մեկն են[14]:

Այս հավասարման միարժեքորեն որոշվող լուծումը սովորաբար նշանակվում է՝ $x = -1$: Այսպիսով՝ $1 + (-1) = 0$: Օրինակ, $\mathbb{Z}_n$ թվակերպ բազմության դեպքում՝ $-1 = [n-1]$:

Եթե $-1 \in Q$, ապա սահմանելով

$$-x = (-1) \cdot x$$

և

$$x - y = x + (-y), \quad x, y \in Q,$$

գործողությունը, կունենանք՝

$$a(x - y) = a(x + (-1)y) = ax + a(-1)y = ax + (-1)ay = ax - ay,$$

$$x - x = x + (-x) = x + (-1)x = 1x + (-1)x = (1 + (-1))x = 0x = 0,$$

որտեղ $a, x, y \in Q$: Այսինքն տեղի ունեն հետևյալ նույնությունները՝ $a(x - y) = ax - ay$ և $x - x = 0$: $-1 \in Q$ հատկությամբ օժտված թվակերպ բազմությունները կոչվում են նաև օղակներ, որոնց ուսումնասիրությունը կշարունակվի գլուխ 19-ում:

Եթե Q-ն թվակերպ բազմություն է՝ օժտված $-1 \in Q$ հատկությամբ, ապա կարելի է սահմանել հետևյալ $\mu : \mathbb{N} \to Q$ ֆունկցիան, որը կոչվում է **Մյոբիուսի թվակերպ ֆունկցիա**՝

$$\mu(n) = \begin{cases} 1, & \text{երբ } n = 1, \\ (-1)^k, & \text{երբ } n = p_1 \cdots p_k, \text{ որտեղ բոլոր } p_i \text{ թվերը} \\ & \text{պարզ են և միմյանցից տարբեր,} \\ 0, & \text{երբ } n\text{-ը բաժանվում է որևէ } p \\ & \text{պարզ թվի քառակուսու վրա :} \end{cases}$$

Այսպիսով, $\mu = \theta_a$, որտեղ $a = -1$:

[14] x-ի միակությունն էական չէ:

Եթե $Q = \mathbb{Z}$, ապա Մյոբիուսի թվակերպ ֆունկցիան համընկնում է Մյոբիուսի ֆունկցիայի հետ (գլուխ 6): Եթե $Q = \mathbb{Z}_2$, ապա $-1 = 1$, որովհետև $1 + 1 = 0$, և Մյոբիուսի թվակերպ ֆունկցիան այս դեպքում կունենա հետևյալ տեսքը՝

$$\mu(n) = \begin{cases} 0, & \text{երբ } n\text{-ը բաժանվում է որևէ } p \\ & \text{պարզ թվի քառակուսու վրա }, \\ 1, & \text{հակառակ դեպքում:} \end{cases}$$

Դժվար չէ ապացուցել հետևյալ երկու հատկությունները.

1) Մյոբիուսի թվակերպ ֆունկցիան արտադրյալային է, այսինքն՝

$$\mu(n \cdot m) = \mu(n) \cdot \mu(m),$$

որտեղ $(n, m) = 1$, $n, m \in \mathbb{N}$ (տես թեորեմ 6.3-ի ապացուցումը);

2) Եթե $d_1, d_2, \ldots, d_k$ թվերը կամայական $n > 1$ բնական թվի բոլոր բնական բաժանարարներն են, ապա Մյոբիուսի թվակերպ ֆունկցիայի համար տեղի ունի հետևյալ հավասարությունը՝

$$\mu(d_1) + \mu(d_2) + \cdots + \mu(d_k) = 0$$

(տես թեորեմ 9.8-ի ապացուցումը և հատկություն 9.7-ը): Այսպիսով՝

$$\sum_{n/d, d>0} \mu(d) = \begin{cases} 1, & \text{եթե } n = 1, \\ 0, & \text{եթե } n > 1: \end{cases}$$

Ըստ որում, այս հատկությամբ $\mu : \mathbb{N} \to Q$ ֆունկցիան որոշվում է միարժեքորեն (տես թեորեմ 9.13-ը):

Դիցուք Q-ն կամայական թվակերպ բազմություն է: Երկու $f : \mathbb{N} \to Q$, $g : \mathbb{N} \to Q$ ֆունկցիաների **Դիրիխլեի** $f \circ g : \mathbb{N} \to Q$ **արտադրյալը** սահմանվում է հետևյալ կերպ՝

$$f \circ g(n) = \sum_{n/d, d>0} f(d) g\left(\frac{n}{d}\right), \quad n \in \mathbb{N},$$

այսինքն՝ գումարը հաշվվում է ըստ n-ի բոլոր $d_1, \ldots, d_k$ բնական բաժանարարների՝

$$f \circ g(n) = f(d_1) g\left(\frac{n}{d_1}\right) + f(d_2) g\left(\frac{n}{d_2}\right) + \cdots + f(d_k) g\left(\frac{n}{d_k}\right),$$

կամ կարելի է գրել՝

$$f \circ g(n) = \sum_{\substack{d_1 \cdot d_2 = n \\ d_1 > 0, d_2 > 0}} f(d_1)g(d_2) = g \circ f(n) :$$

Հեշտությամբ ստուգվում է նաև Դիրիխլեի արտադրյալի զուգորդականության հատկությունը (նույնությունը)՝ $(f \circ g) \circ h = f \circ (g \circ h)$, որովհետև

$$(f \circ g) \circ h(n) = f \circ (g \circ h)(n) = \sum_{\substack{d_1 d_2 d_3 = n \\ d_1 > 0, d_2 > 0, d_3 > 0}} f(d_1)g(d_2)h(d_3)$$

ցանկացած $f, g, h : \mathbb{N} \to Q$ արտապատկերումների (ֆունկցիաների) համար:

Ներմուծենք $I_0, I_1 : \mathbb{N} \to Q$ ֆունկցիաները հետևյալ կերպ՝

$$I_1(n) = 1, \quad n \in \mathbb{N},$$

$$I_0(n) = \begin{cases} 1, & \text{եթե } n = 1, \\ 0, & \text{եթե } n > 1; \end{cases}$$

I_0 ֆունկցիան երբեմն կոչվում է նաև Դիրակի ֆունկցիա և նշանակվում է δ_1-ով:

Ցանկացած $f : \mathbb{N} \to Q$ ֆունկցիայի համար տեղի ունի հետևյալ հավասարությունը՝

$$f \circ I_0 = I_0 \circ f = f,$$

որը բխում է Դիրիխլեի արտադրյալի սահմանումից:

Լեմմ 9.2: *Եթե Q-ն թվակերպ բազմություն է՝ օժտված $-1 \in Q$ հատկությամբ, ապա*

$$\mu \circ I_1 = I_1 \circ \mu = I_0,$$

որտեղ $\mu : \mathbb{N} \to Q$ ֆունկցիան Մյոբիուսի թվակերպ ֆունկցիան է:

Ապացուցում: Իրոք՝

$$\mu \circ I_1(n) = \sum_{n/d, d>0} \mu(d) = \begin{cases} 1, & \text{եթե } n = 1, \\ 0, & \text{եթե } n > 1 \end{cases} = I_0(n) : \qquad \square$$

Թեորեմ 9.10 (Մյոբիուսի թեորեմը (բանաձևը) շրջման կամ հակադարձման վերաբերյալ): *Դիցուք Q-ն թվակերպ բազմություն է՝ օժտված $-1 \in Q$ հատկությամբ: $f, g : \mathbb{N} \to Q$ ֆունկցիաների համար տեղի ունի $f = g \circ I_1$ հավասարությունը այն և միայն այն դեպքում, երբ $g = f \circ \mu$: Այլ կերպ ասած՝*

$$f(n) = \sum_{n/d, d>0} g(d) \longleftrightarrow g(n) = \sum_{n/d, d>0} f(d)\mu\left(\frac{n}{d}\right) = \sum_{n/d, d>0} \mu(d) f\left(\frac{n}{d}\right) :$$

Ապացուցում: Եթե $f = g \circ I_1$, ապա համաձայն լեմմ 9.2-ի կունենանք՝

$$f \circ \mu = (g \circ I_1) \circ \mu = g \circ (I_1 \circ \mu) = g \circ I_0 = g;$$

Եվ հակառակը, եթե $g = f \circ \mu$, ապա

$$g \circ I_1 = (f \circ \mu) \circ I_1 = f \circ (\mu \circ I_1) = f \circ I_0 = f : \qquad \square$$

Թեորեմ 9.11*: Դիցուք Q-ն թվակերպ բազմություն է: Եթե $f, g : \mathbb{N} \to Q$ ֆունկցիաները արտադրյալային են, ապա դրանց $F = f \circ g$ Դիրիխլեի արտադրյալը ևս կլինի արտադրյալային:*

Ապացուցում: Եթե $(m, n) = 1$, ապա

$$m \cdot n/d \longleftrightarrow d = d_1 \cdot d_2,$$

որտեղ $d > 0$, $d_1 > 0$, $d_2 > 0$, m/d_1, n/d_2, $(d_1, d_2) = 1$, $\left(\frac{m}{d_1}, \frac{n}{d_2}\right) = 1$: Հետևաբար՝

$$F(m \cdot n) = f \circ g(m \cdot n) = \sum_{mn/d} f(d) g\left(\frac{mn}{d}\right) =$$

$$= \sum_{m/d_1, n/d_2} f(d_1 d_2) g\left(\frac{mn}{d_1 d_2}\right) = \sum_{m/d_1, n/d_2} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) =$$

$$= \left(\sum_{m/d_1} f(d_1) g\left(\frac{m}{d_1}\right)\right)\left(\sum_{n/d_2} f(d_2) g\left(\frac{n}{d_2}\right)\right) = F(m)F(n) : \qquad \square$$

Թեորեմ 9.12: *Դիցուք Q-ն թվակերպ բազմություն է՝ օժտված $-1 \in Q$ հատկությամբ, $f : \mathbb{N} \to Q$, իսկ*

$$F(n) = \sum_{n/d, d>0} f(d);$$

Այդ դեպքում, f-ը կլինի արտադրյալային այն և միայն այն դեպքում, երբ F-ը արտադրյալային է:

Ապացույց: Եթե f-ը արտադրյալային է, ապա դիտարկելով նաև $I_1(n) = 1$, $n \in \mathbb{N}$, արտադրյալային ֆունկցիան, կունենանք՝ $F = f \circ I_1$, որովհետև

$$F(n) = \sum_{n/d, d>0} f(d) = \sum_{n/d, d>0} f(d) \cdot 1 = \sum_{n/d, d>0} f(d) \cdot I_1\left(\frac{n}{d}\right) = f \circ I_1(n), \quad n \in \mathbb{N};$$

Հետևաբար, համաձայն թեորեմ 9.11-ի, F-ը կլինի արտադրյալային:

Եվ հակառակը, եթե $F = f \circ I_1$ և F-ը արտադրյալային է, ապա համաձայն թեորեմ 9.10-ի՝ $f = F \circ \mu$, որտեղ μ Մյոբիուսի թվակերպ ֆունկցիան ևս արտադրյալային է և, հետևաբար, ըստ թեորեմ 9.11-ի, f-ը կլինի արտադրյալային: □

Թեորեմ 9.13 (Մյոբիուսի թվակերպ ֆունկցիայի միակության վերաբերյալ): *Եթե Q-ն թվակերպ բազմություն է՝ օժտված $-1 \in Q$ հատկությամբ և $g : \mathbb{N} \to Q$ ֆունկցիայի համար տեղի ունի*

$$\sum_{n/d, d>0} g(d) = \begin{cases} 1, & \text{եթե } n = 1, \\ 0, & \text{եթե } n > 1 \end{cases} = I_0(n)$$

հավասարությունը, ապա $g(n) = \mu(n)$ բոլոր $n \in \mathbb{N}$ բնական թվերի համար, այսինքն՝ $g = \mu$:

Ապացույց: Թեորեմ 9.10-ի համաձայն՝

$$g(n) = \sum_{n/d, d>0} \mu(d) I_0\left(\frac{n}{d}\right) = \mu(n) :$$

Հետևություն 9.5: *Եթե Q-ն թվակերպ բազմություն է՝ օժտված $-1 \in Q$ հատկությամբ, ապա $g : \mathbb{N} \to Q$ ֆունկցիան կլինի հավասար Մյոբիուսի $\mu : \mathbb{N} \to Q$ թվակերպ ֆունկցիային այն և միայն այն դեպքում, երբ*

$$\sum_{n/d, d>0} g(d) = I_0(n)$$

ցանկացած $n \in \mathbb{N}$ *բնական թվի համար:* □

9.6. Ամբողջ p-ադիկ թվեր

Դիցուք p-ն պարզ թիվ է: Ամբողջ թվերի

$$\{x_n\} = \{x_0, x_1, \ldots, x_n, \ldots\}$$

հաջորդականությունը, որտեղ

$$x_n \equiv x_{n-1} \, (mod \, p^n) \, , \quad n \geqslant 1,$$

կոչվում է **ամբողջ p-ադիկ թիվ**: Երկու $\{x_n\}$ և $\{x'_n\}$ ամբողջ p-ադիկ թվեր կոչվում են **հավասար** և գրվում է՝ $\{x_n\} = \{x'_n\}$, եթե

$$x_n \equiv x'_n \left(mod \, p^{n+1} \right) , \quad n \geqslant 0 :$$

Հակառակ դեպքում, տրված երկու ամբողջ p-ադիկ թվերը կոչվում են **ոչ հավասար** և գրվում է՝ $\{x_n\} \neq \{x'_n\}$:

Այս եղանակով սահմանված հավասարության գաղափարը ակնհայտորեն բավարարում է համարժեքության երեք պայմաններին.

ա) $\{x_n\} = \{x_n\}$, (ռեֆլեքսիվություն)

բ) $\{x_n\} = \{y_n\} \to \{y_n\} = \{x_n\}$, (համաչափություն կամ սիմետրիկություն)

գ)$\{x_n\} = \{y_n\}, \{y_n\} = \{z_n\} \to \{x_n\} = \{z_n\}$: (փոխանցականություն)

Սովորաբար բոլոր ամբողջ p-ադիկ թվերի բազմությունը նշանակվում է $\mathcal{O}_p$-ով:

Յուրաքանչյուր x ամբողջ թվի համապատասխանեցվում է $\{x, x, \ldots, x, \ldots\}$ ամբողջ p-ադիկ թիվը, որը նշանակվում է $\{x\}$ -ով: Եթե $x \neq y$, ապա $\{x\} \neq \{y\}$, որովհետև հակառակ դեպքում կունենայինք՝

$$x \equiv y (mod \, p^n)$$

բոլոր $n \geqslant 1$ բնական թվերի համար: Ուստի $x - y / p^n$, որտեղ բավական մեծ n-երի դեպքում՝ $|x - y| < p^n$ և հետևաբար (հատկություն 7°, գլուխ 1), $x - y = 0$ կամ $x = y$:

Այսպիսով, բոլոր ամբողջ թվերի $\mathbb{Z}$ բազմությունը կարելի է ընդունել (դիտել) որպես բոլոր ամբողջ p-ադիկ թվերի $\mathcal{O}_p$ բազմության մաս՝ $\mathbb{Z} \subseteq \mathcal{O}_p$ ցանկացած p պարզ թվի դեպքում:

Ամբողջ թվերի սովորական թվաբանական գործողությունները բնական եղանակով տարածվում են ամբողջ p-ադիկ թվերի վրա՝ հետևյալ կերպ:

$\{x_n\}$ և $\{y_n\}$ ամբողջ p-ադիկ թվերի **գումար** և **արտադրյալ** են կոչվում $\{x_n + y_n\}$ և $\{x_n y_n\}$ հաջորդականությունները, որոնց համար $\{x_n\}$ և $\{y_n\}$ ամբողջ p-ադիկ թվերը համապատասխանաբար կոչվում են գումարելիներ և արտադրիչներ: Նախ նկատենք, որ ամբողջ p-ադիկ թվերի գումարը և արտադրյալը նորից ամբողջ p-ադիկ թվեր են և որոշվում են միարժեքորեն, այսինքն՝ $x_n + y_n \equiv x_{n-1} + y_{n-1} (mod\, p^n)$, $x_n y_n \equiv x_{n-1} y_{n-1} (mod\, p^n)$, $\{x_n + y_n\} = \{x'_n + y'_n\}$ և $\{x_n y_n\} = \{x'_n y'_n\}$, եթե $\{x_n\} = \{x'_n\}$ և $\{y_n\} = \{y'_n\}$:

Իրոք, եթե $\{x_n\} = \{x'_n\}$ և $\{y_n\} = \{y'_n\}$, ապա $x_n \equiv x'_n (mod\, p^{n+1})$ և $y_n \equiv y'_n (mod\, p^{n+1})$: Ուստի, $x_n + y_n \equiv x'_n + y'_n \left(mod\, p^{n+1}\right)$ և $x_n y_n \equiv x'_n y'_n \left(mod\, p^{n+1}\right)$ բոլոր $n \geqslant 0$ բնական թվերի համար: Այսպիսով՝

$$\{x_n + y_n\} = \{x'_n + y'_n\} \quad \text{և} \quad \{x_n y_n\} = \{x'_n y'_n\}$$

համաձայն ամբողջ p-ադիկ թվերի հավասարության սահմանման:

Այնուհետև՝ $(x_n + y_n) - (x_{n-1} + y_{n-1}) = (x_n - x_{n-1}) + (y_n - y_{n-1})$,

$$x_n y_n - x_{n-1} y_{n-1} = x_n y_n - x_{n-1} y_n + x_{n-1} y_n - x_{n-1} y_{n-1} =$$

$$= y_n (x_n - x_{n-1}) + x_{n-1} (y_n - y_{n-1}) :$$

Հեշտությամբ ստուգվում են նաև, որ ամբողջ p-ադիկ թվերի գումարը և արտադրյալը տեղափոխական են, զուգորդական են, կապված են բաշխական նույնությամբ, օժտված են միարժեքորեն որոշվող $\{0\}$ և $\{1\}$ միավորներով: Ընդ որում, յուրաքանչյուր $\{x_n\}$ ամբողջ p-ադիկ թվի համար գոյություն ունի միարժեքորեն որոշվող այնպիսի $\{x'_n\}$ ամբողջ p-ադիկ թիվ, որ

$$\{x_n\} + \{x'_n\} = \{0\} :$$

Ակնհայտ է, որ $x'_n = -x_n$: $\{x'_n\}$-ը կոչվում է $\{x_n\}$-ի հակադիր ամբողջ p-ադիկ թիվ և նշանակվում է $-\{x_n\}$-ով: Այսպիսով՝ $-\{x_n\} = \{-x_n\}$: Ակնհայտ է նաև, որ $-(-\alpha) = \alpha$, $(-\alpha)\beta = \alpha(-\beta) = -(\alpha\beta)$, որտեղ $\alpha, \beta \in \mathcal{O}_p$:

Այնուհետև, սովորական եղանակով սահմանվում է նաև ամբողջ p-ադիկ թվերի բաժանման գաղափարը. կասենք որ $\alpha = \{x_n\}$ ամբողջ

p-ադիկ թիվը **բաժանվում է** $\beta = \{y_n\}$ ամբողջ p-ադիկ թվի վրա, եթե գոյություն ունի այնպիսի $\gamma = \{z_n\}$ ամբողջ p-ադիկ թիվ, որ $\alpha = \beta \cdot \gamma$: Այս դեպքում α-ն կոչվում է բաժանելի, իսկ β-ն (ինչպես նաև γ-ն) բաժանարար: Ամբողջ p-ադիկ թիվը կոչվում է **հակադարձելի**, եթե այն 1-ի բաժանարար է:

Թեորեմ 9.14: *Որպեսզի $\alpha = \{x_n\}$ ամբողջ p-ադիկ թիվը լինի հակադարձելի անհրաժեշտ է և բավարար, որ $x_0 \not\equiv 0(mod p)$: Մասնավորապես, $x \in \mathbb{Z}$ ամբողջ թիվը կլինի հակադարձելի ամբողջ p-ադիկ թիվ այն և միայն այն դեպքում, երբ $x \not\equiv 0(mod\, p)$:*

Ապացուցում: Անհրաժեշտություն: Դիցուք $\alpha = \{x_n\}$ ամբողջ p-ադիկ թիվը հակադարձելի է, այսինքն գոյություն ունի այնպիսի $\beta = \{y_n\}$ ամբողջ p-ադիկ թիվ, որ $\alpha \cdot \beta = 1$, այսինքն՝

$$x_n y_n \equiv 1\, (mod\, p^n)\,, \quad n = 0, 1, \ldots :$$

Մասնավորապես, $x_0 y_0 \equiv 1\, (mod\, p^n)$ և հետևաբար $x_0 \not\equiv 0\, (mod\, p^n)$:

Բավարարություն: Դիցուք $\{x_n\}$ ամբողջ p-ադիկ թվի մեջ՝ $x_0 \not\equiv 0\, (mod\, p)$: Ամբողջ p-ադիկ թվի սահմանման համաձայն՝ $x_n \equiv x_{n-1}\, (mod\, p^n)$ ցանկացած $n \geqslant 1$ բնական թվի համար: Ուստի՝

$$x_1 \equiv x_0\, (mod\, p)\,,$$

$$x_2 \equiv x_1\, (mod\, p)\,,$$

$$\cdots\cdots\cdots\cdots$$

$$x_n \equiv x_{n-1}\, (mod\, p) :$$

Հետևաբար, $x_n \equiv x_0\, (mod p)$ և քանի որ $x_0 \not\equiv 0\, (mod p)$, ապա $x_n \not\equiv 0\, (mod\, p)$ և $(x_n, p) = 1$: Ուստի, համաձայն հատկություն 3.2-ի, $\left(x_n, p^{n+1}\right) = 1$, այսինքն (թեորեմ 3.1) գոյություն կունենան այնպիսի y_n և t_{n+1} ամբողջ թվեր, որ

$$x_n y_n + p^{n+1} t_{n+1} = 1,$$

$$x_n y_n - 1 = p^{n+1}\left(-t_{n+1}\right),$$

այսինքն՝

$$x_n y_n \equiv 1\, \left(mod\, p^{n+1}\right),$$

որտեղից՝

$$x_{n-1}y_{n-1} \equiv 1\,(mod\,p^n)$$

և

$$x_n y_n \equiv 1\,(mod\,p^n)\;:$$

Այսպիսով, $x_n y_n \equiv x_{n-1}y_{n-1}\,(mod\,p^n)$ և քանի որ $x_n \equiv x_{n-1}\,(mod\,p^n)$ և

$$x_n y_n - x_{n-1}y_{n-1} = x_n y_n - x_n y_{n-1} + x_n y_{n-1} - x_{n-1}y_{n-1} =$$

$$= x_n(y_n - y_{n-1}) + y_{n-1}(x_n - x_{n-1}),$$

ապա $y_n \equiv y_{n-1}\,(mod\,p^n)$, այսինքն $\{y_n\}$ հաջորդականությունը հանդիսանում է p-ադիկ թիվ և $\{x_n\}\cdot\{y_n\} = 1$: □

Թեորեմ 9.15*: Յուրաքանչյուր $\alpha \neq 0$ ամբողջ p-ադիկ թիվ միարժեքորեն ներկայացվում է*

$$\alpha = p^m \cdot \varepsilon$$

տեսքով, որտեղ $\mathcal{E}$ -ը հակադարձելի ամբողջ p-ադիկ թիվ է, իսկ $m \geqslant 0$:

Ապացուցում: **Ներկայացման գոյությունը:** Եթե α-ն հակադարձելի ամբողջ p-ադիկ թիվ է, ապա $\alpha = p^m \cdot \varepsilon$ հավասարությունը կլինի ճիշտ՝ $m = 0$ և $\varepsilon = \alpha$ դեպքում: Դիցուք $\alpha = \{x_n\}$ ամբողջ p-ադիկ թիվը հակադարձելի չէ, այսինքն, համաձայն թեորեմ 9.14-ի , $x_0 \equiv 0\,(mod\,p)$: Քանի որ նաև $\alpha \neq 0$, ապա ամբողջ p-ադիկ թվերի հավասարության սահմանման համաձայն՝ $x_n \equiv 0\left(mod\,p^{n+1}\right)$ բաղդատումը տեղի չի ունենա բոլոր $n \geqslant 0$ բնական թվերի դեպքում: Ենթադրենք m-ը այն ամենափոքր բնական թիվն է, որի համար

$$x_m \not\equiv 0\left(mod\,p^{m+1}\right)\;:$$

Հետևաբար՝

$$x_{m-1} \equiv 0\,(mod\,p^m)$$

և քանի որ ամբողջ p-ադիկ թվի սահմանման համաձայն՝

$$x_{m+s} \equiv x_{m-1}\,(mod\,p^m)\,, \quad s \geqslant 0,$$

ապա

$$x_{m+s} \equiv 0\,(mod\,p^m)\,,$$

այսինքն x_{m+s}-ը բաժանվում է p^m-ի վրա: Դիտարկելով $\dfrac{x_{m+s}}{p^m} = y_s$ ամբողջ թիվը, կունենանք՝

$$p^m y_s - p^m y_{s-1} = x_{m+s} - x_{m+s-1} \equiv 0 \left(mod\, p^{m+s}\right),$$

$$p^m \left(y_s - y_{s-1}\right) = p^{m+s} \cdot t_s, \quad t_s \in Z,$$

այսինքն $y_s \equiv y_{s-1} \left(mod\, p^s\right)$, $s \geqslant 0$ և հետևաբար ամբողջ թվերի $\{y_s\} = \varepsilon$ հաջորդականությունը հանդիսանում է ամբողջ p-ական թիվ: Քանի որ $y_0 = \dfrac{x_m}{p^m}$ և $x_m \not\equiv 0 \left(mod\, p^{m+1}\right)$, ապա $\dfrac{x_m}{p^m} \not\equiv 0 \left(mod\, p\right)$, այսինքն $y_0 \not\equiv 0 \left(mod\, p\right)$: Հետևաբար, թեորեմ 9.14-ի համաձայն, $\mathcal{E}$-ը կլինի հակադարձելի ամբողջ p-ադիկ թիվ: Ի վերջո,

$$p^m y_s = x_{m+s} \equiv x_s \left(mod\, p^{s+1}\right)$$

բաղդատումից բխում է

$$p^m \cdot \varepsilon = \alpha$$

հավասարությունը:

Ներկայացման միակությունը: Դիցուք ոչ զրոյական $\alpha = \{x_n\}$ ամբողջ p-ադիկ թիվն ունի նաև $\alpha = p^k \cdot \delta$ ներկայացումը, որտեղ δ-ն հակադարձելի ամբողջ p-ադիկ թիվ է, իսկ $k \geqslant 0$: Եթե $\delta = \{z_n\}$, ապա $\{p^m y_s\} = \left\{p^k z_s\right\}$ և ամբողջ p-ադիկ թվերի հավասարության սահմանման համաձայն՝

$$p^m y_s \equiv p^k z_s \left(mod\, p^{s+1}\right), \quad s \geqslant 0:$$

Մասնավորապես, $p^m y_m \equiv p^k z_m \left(mod\, p^{m+1}\right)$ և $p^m y_{s+k} \equiv p^k z_{s+k} \left(mod\, p^{s+k+1}\right)$: Սակայն $\alpha = p^m \cdot \varepsilon$ ներկայացման ժամանակ, m-ը ընտրվեց որպես այն ամենափոքր բնական թիվը, որի համար $x_m \not\equiv 0 \left(mod\, p^{m+1}\right)$: Միաժամանակ, երկու ամբողջ p-ադիկ թվերի հավասարության սահմանումից ունենք՝

$$p^m y_m \equiv x_m \left(mod\, p^{m+1}\right):$$

Այսպիսով, $p^k z_m \not\equiv 0 \left(mod\, p^{m+1}\right)$ և հետևաբար՝ $k \leqslant m$: Այժմ $p^m y_{s+k} \equiv p^k z_{s+k} \left(mod\, p^{s+k+1}\right)$ բաղդատումը կրճատելով p^k-ով, կունենանք՝

$$p^{m-k} y_{s+k} \equiv z_{s+k} \left(mod\, p^{s+1}\right):$$

Միաժամանակ, համաձայն ամբողջ p-ադիկ թվի սահմանման՝

$$z_{s+k} \equiv z_s \left(mod\, p^{s+1}\right),$$

և հետևաբար՝

$$p^{m-k} y_{s+k} \equiv z_s \left(mod\, p^{s+1}\right),$$

որտեղից $m-k>0$ անհավասարությունը հանգեցնում է $z_s \equiv 0(mod\, p)$, $s \geqslant 0$ բաղդատմանը, որը հակասում է թեորեմ 9.14-ին: Այսպիսով, $m-k=0$ և $m=k$: Որից հետո, վերոհիշյալ

$$p^m y_{s+k} \equiv p^k z_{s+k} \left(mod\, p^{s+k+1}\right)$$

բաղդատումից հանգում ենք

$$y_{s+k} \equiv z_{s+k} \left(mod\, p^{s+1}\right)$$

բաղդատմանը, իսկ այնուհետև ($k=0$ դեպքում) նաև

$$y_s \equiv z_s \left(mod\, p^{s+1}\right)$$

բաղդատմանը, որը հենց նշանակում է $\varepsilon = \delta$ հավասարությունը: □

Թեորեմ 9.16*: Երկու ոչ զրոյական ամբողջ p-ադիկ թվերի արտադրյալը նորից ոչ զրոյական ամբողջ p-ադիկ թիվ է:*

Ապացուցում: Եթե $\alpha \neq 0$ և $\beta \neq 0$, ապա նախորդ թեորեմի համաձայն, գոյություն կունենան այնպիսի m և k բնական թվեր, որ

$$\alpha = p^m \varepsilon, \quad \beta = p^k \delta,$$

որտեղ ε և δ ամբողջ p-ադիկ թվերը հակադարձելի են, այսինքն գոյություն ունեն այնպիսի ε' և δ' ամբողջ p-ադիկ թվեր, որ $\varepsilon \cdot \varepsilon' = 1$ և $\delta \cdot \delta' = 1$: Եթե այժմ $\alpha \cdot \beta = 0$, ապա

$$p^m \varepsilon \cdot p^k \delta = 0,$$

$$p^{m+k} \varepsilon\delta \cdot \varepsilon'\delta' = 0 \cdot \varepsilon'\delta',$$

$$p^{m+k} \cdot \varepsilon\varepsilon' \cdot \delta\delta' = 0,$$

$$p^{m+k} = 0,$$

որը հնարավոր չէ՝ որպես երկու ամբողջ p-ադիկ թվերի հավասարություն: Ստացված հակասությունն ապացուցում է թեորեմ 9.16-ը: □

Հատկություն 9.10: *Որպեսզի ոչ զրոյական $\alpha = p^m \cdot \varepsilon$ ամբողջ p-ադիկ թիվը բաժանվի ոչ զրոյական $\beta = p^n \cdot \delta$ ամբողջ p-ադիկ թվի վրա անհրաժեշտ է և բավարար, որ $m \geqslant n$ (այստեղ ε-ը և δ-ն հակադարձելի ամբողջ p-ադիկ թվեր են):*

Ապացուցում: Բավարարություն: Եթե $\alpha = p^m \cdot \varepsilon$, $\beta = p^n \cdot \delta$ և $m \geqslant n$, ապա

$$\alpha = p^n \cdot \delta \cdot p^{m-n} \cdot \varepsilon \cdot \delta' = \beta \cdot \gamma,$$

որտեղ $\delta \cdot \delta' = 1$, իսկ $\gamma = p^{m-n} \cdot \varepsilon \cdot \delta' \in \mathcal{O}_p$:

Անհրաժեշտություն: Եթե $\alpha = \beta \cdot \gamma$, ապա $\gamma \neq 0$ և հետևաբար $\gamma = p^k \cdot \sigma$, որտեղ σ-ն հակադարձելի է, իսկ $k \geqslant 0$ (թեորեմ 9.15): Հետևաբար,

$$p^m \cdot \varepsilon = p^n \delta \cdot p^k \tau = p^{n+k} \cdot \delta\tau$$

և այժմ թեորեմ 9.15-ի միակության մասից կբխի $m = n + k$ հավասարությունը, որտեղից էլ՝ $m \geqslant n$ անհավասարությունը: □

Հատկություն 9.11: *Որպեսզի ոչ զրոյական $\alpha = \{x_n\}$ ամբողջ p-ադիկ թիվը բաժանվի p^k-ի վրա, անհրաժեշտ է և բավարար, որ*

$$x_n \equiv 0 \left(mod\, p^{n+1}\right), \quad n = 0, 1, \ldots, k-1 :$$

Ապացուցում: Եթե $\alpha \neq 0$, ապա թեորեմ 9.15-ի համաձայն՝ $\alpha = p^m \cdot \varepsilon$, որտեղ m-ը այն ամենափոքր ոչ բացասական ամբողջ թիվն է, որի համար՝

$$x_m \not\equiv 0 \left(mod\, p^{m+1}\right) :$$

Մյուս կողմից, նախորդ հատկության համաձայն, որպեսզի α-ն բաժանվի p^k-ի վրա, անհրաժեշտ է և բավարար, որ $m \geqslant k$, այսինքն՝

$$x_0 \equiv 0 \left(mod\, p\right),$$

$$x_1 \equiv 0 \left(mod\, p^2\right),$$

$$\ldots \ldots \ldots$$

$$x_{k-1} \equiv 0 \left(mod\, p^k\right) :$$ □

Անցնենք երկու ամբողջ p-ադիկ թվերի բաղդատման գաղափարին: Նախ ներմուծենք երկու ամբողջ p-ադիկ թվերի **տարբերության** (հանման) գաղափարը, հետևյալ կերպ՝

$$\alpha - \beta = \alpha + (-\beta) :$$

Այսպիսով,

$$\alpha - \alpha = 0$$

և

$$\alpha(\beta - \gamma) = \alpha\beta - \alpha\gamma :$$

Դիցուք տրված են α, β, γ ամբողջ p-ադիկ թվերը, որտեղ $\gamma \neq 0$: α և β ամբողջ p-ադիկ թվերը կոչվում են **բաղդատելի** ըստ γ հենքի (մոդուլի), եթե $\alpha - \beta$ տարբերությունը բաժանվում է γ-ի վրա: Այդ դեպքում, գրվում է՝

$$\alpha \equiv \beta (mod\, \gamma) :$$

Ակնհայտ է, որ սահմանված «$\equiv$» հարաբերությունը համարժեքության հարաբերություն է:

$$[\alpha] = \{x \in \mathcal{O}_p |\, x \equiv \alpha (mod\, \gamma)\} \subseteq \mathcal{O}_p$$

ենթաբազմությունը կոչվում է α-ի մնացքների դաս ըստ γ-ի:

$$[\alpha] = [\beta] \longleftrightarrow \alpha \equiv \beta (mod\, \gamma) :$$

Քանի որ ոչ զրոյական $\alpha - \beta$ ամբողջ p-ադիկ թիվը կբաժանվի ոչ զրոյական $\gamma = p^n \cdot \varepsilon$ ամբողջ p-ադիկ թվի վրա այն և միայն այն դեպքում, երբ $\alpha - \beta$-ն կբաժանվի p^n-ի վրա, ապա որպես ամբողջ p-ադիկ թվերի բաղդատման հենք (մոդուլ) կարելի է ընդունել p^n-ը:

Հատկություն 9.12: *Դիցուք $n \geqslant 1$ և p-ն պարզ թիվ է: Յուրաքանչյուր ամբողջ p-ադիկ թիվ բաղդատելի է որևէ ամբողջ թվի հետ ըստ p^n հենքի: Երկու ամբողջ թվեր կլինեն բաղդատելի որպես ամբողջ p-ադիկ թվեր ըստ p^n հենքի այն և միայն այն դեպքում, երբ դրանք բաղդատելի են ըստ p^n հենքի որպես ամբողջ թվեր: Մասնավորապես, $\mathcal{O}_p$ բազմության բոլոր մնացքների դասերի քանակը ըստ p^n հենքի կլինի հավասար p^n-ի:*

Ապացուցում: Նախ ապացուցենք առաջին պնդումը: Դիցուք $\alpha \in \mathcal{O}_p$ և դիցուք $\alpha = \{x_n\}$: Դիտարկենք $x_{n-1} \in \mathbb{Z}$ ամբողջ թվին համապատասխանող $\beta = \{x_{n-1}, x_{n-1}, \ldots, x_{n-1}, \ldots\}$ ամբողջ p-ադիկ թիվը և ապացուցենք $\alpha \equiv \beta (mod\, p^n)$ բաղդատումը: Քանի որ՝

$$\alpha - \beta = \{x_0 - x_{n-1}, x_1 - x_{n-1}, \ldots\}$$

ապա համաձայն հատկություն 9.11-ի, պահանջվում է ապացուցել

$$x_k - x_{n-1} \equiv 0 \left(mod\, p^{k+1} \right), \quad k = 0, 1, \ldots, n-1$$

բաղդատումները: Նշված բաղդատումը ակնհայտորեն ճիշտ է $k = n-1$ դեպքում, իսկ $k = n-2$ դեպքում բխում է $x_{n-1} \equiv x_{n-2} \left(mod\, p^{n-1} \right)$ բաղդատումից, որը տեղի ունի համաձայն ամբողջ p-ադիկ թվի սահմանման: Դիցուք $k = n-3$: Քանի որ

$$x_{n-1} \equiv x_{n-2} \left(mod\, p^{n-1} \right),$$

$$x_{n-2} \equiv x_{n-3} \left(mod\, p^{n-2} \right),$$

ապա $x_{n-1} \equiv x_{n-2} \left(mod\, p^{n-2} \right)$ և $x_{n-3} \equiv x_{n-1} \left(mod\, p^{n-2} \right)$, այսինքն $x_{n-3} - x_{n-1} \equiv 0 \left(mod\, p^{n-2} \right)$: Եվ այսպես շարունակ ...

Այժմ ապացուցենք հատկության երկրորդ պնդումը: Դիցուք $x, y \in \mathbb{Z}$, $x - y \neq 0$, $\alpha = \{x\}$, $\beta = \{y\}$: Ակնհայտ է, որ եթե երկու ամբողջ թվեր բաղդատելի են $\mathbb{Z}$-ում, ապա նրանք բաղդատելի են նաև $\mathcal{O}_p$-ում, որովհետև եթե $x - y = t \cdot z$, ապա $\{x - y\} = \{t \cdot z\}$, $\{x\} - \{y\} = \{t\} \cdot \{z\}$: Բավական է այժմ ապացուցել, որ եթե α, β ամբողջ p-ադիկ թվերը բաղդատելի են $\mathcal{O}_p$-ում, ապա x, y-ը կլինեն բաղդատելի նաև $\mathbb{Z}$-ում, այսինքն եթե

$$\alpha - \beta = p^n \cdot \tau,$$

որտեղ $\tau \in \mathcal{O}_p$, ապա $x - y = p^n \cdot z$, որտեղ $z \in \mathbb{Z}$:

Իրոք, դիցուք $x - y = p^m \cdot a$, որտեղ $a \in \mathbb{Z}$ և a-ն չի բաժանվում p-ի վրա, այսինքն $a \not\equiv 0 (mod\, p)$: Հետևաբար, $\{x - y\} = \{p^m \cdot a\}$, $\{x\} - \{y\} = \{p^m\} \cdot \{a\}$, այսինքն $\alpha - \beta = p^m \cdot \sigma$, որտեղ $\sigma = \{a\}$ և համաձայն թեորեմ 9.14-ի, σ-ն հակադարձելի է: Այսպիսով,

$$p^m \cdot \sigma = p^n \cdot \tau,$$

$$p^m = p^n \cdot \tau\sigma',$$

որտեղ $\sigma \cdot \sigma' = 1$: Հատկություն 9.10-ի համաձայն, այժմ կստանանք՝ $m \geqslant n$: Այսպիսով, $m - n \geqslant 0$ և

$$x - y = p^m \cdot a = p^n \cdot p^{m-n} \cdot a = p^n \cdot z,$$

որտեղ $z = p^{m-n} \cdot a \in \mathbb{Z}$: □

9.7. p-ադիկ թվեր

Դիցուք p-ն պարզ թիվ է: (α, p^k) տեսքի յուրաքանչյուր զույգ, որտեղ α-ն ամբողջ p-ադիկ թիվ է ($\alpha \in \mathcal{O}_p$), $k \geqslant 0$, կոչվում է p-ադիկ թիվ: Երկու (α, p^k) և (β, p^m) p-ադիկ թվեր կոչվում են հավասար, եթե ($\mathcal{O}_p$-ում) տեղի ունի հետևյալ հավասարությունը՝ $\alpha \cdot p^m = \beta \cdot p^k$: Սովորաբար (α, p^k) զույգը ներկայացվում (գրվում) է կոտորակային տեսքով՝ $\dfrac{\alpha}{p^k}$, իսկ բոլոր p-ադիկ թվերի բազմությունը նշանակվում է $\mathbb{R}_p$-ով:

Յուրաքանչյուր α ամբողջ p-ադիկ թիվ նույնականացվում է $\dfrac{\alpha}{p^0} = \dfrac{\alpha}{1}$ p-ադիկ թվի հետ և հետևաբար բոլոր ամբողջ p-ադիկ թվերի բազմությունը ընդունվում է որպես բոլոր p-ադիկ թվերի $\mathbb{R}_p$ բազմության մաս՝ $\mathcal{O}_p \subseteq \mathbb{R}_p$:

Գումարման և բազմապատկման գործողությունները $\mathbb{R}_p$-ում սահմանվում են բնական եղանակով՝

$$\frac{\alpha}{p^k} + \frac{\beta}{p^m} = \frac{\alpha p^m + \beta p^k}{p^{k+m}},$$

$$\frac{\alpha}{p^k} \cdot \frac{\beta}{p^m} = \frac{\alpha\beta}{p^{k+m}}:$$

Դժվար չէ համոզվել, որ երկու p-ադիկ թվերի գումարը և արտադրյալը որոշվում են միարժեքորեն, այսինքն

$$\frac{\alpha}{p^k} + \frac{\beta}{p^m} = \frac{\alpha'}{p^{k'}} + \frac{\beta'}{p^{m'}}$$

և

$$\frac{\alpha}{p^k} \cdot \frac{\beta}{p^m} = \frac{\alpha'}{p^{k'}} \cdot \frac{\beta'}{p^{m'}},$$

եթե $\dfrac{\alpha}{p^k} = \dfrac{\alpha'}{p^{k'}}$, $\dfrac{\beta}{p^m} = \dfrac{\beta'}{p^{m'}}$: Իրոք, $\alpha p^{k'} = \alpha' p^k$, $\beta p^{m'} = \beta' p^m$ և հետևաբար $\alpha\beta \cdot p^{k'+m'} = \alpha'\beta' p^{k+m}$,

$$\alpha p^{k'+m+m'} = \alpha' p^{k+m+m'},$$

$$\beta p^{m'+k+k'} = \beta' p^{m+k+k'},$$

$$\alpha p^{k'+m+m'} + \beta p^{m'+k+k'} = \alpha' p^{k+m+m'} + \beta' p^{m+k+k'},$$

$$\left(\alpha p^m + \beta p^k\right) p^{k'+m'} = \left(\alpha' p^{m'} + \beta' p^{k'}\right) p^{k+m} :$$

Հեշտությամբ ստուգվում են նաև, որ p-ադիկ թվերի գումարը և արտադրյալը տեղափոխական են, զուգորդական են, կապված են բաշխական նույնությամբ, օժտված են միարժեքորեն որոշվող $\frac{0}{p^0}$ և $\frac{1}{p^0}$ միավորներով: Ընդ որում, յուրաքանչյուր $\frac{\alpha}{p^k}$ p-ադիկ թվի համար գոյություն ունի միարժեքորեն որոշվող այնպիսի u p-ադիկ թիվ, որ

$$\frac{\alpha}{p^k} + u = \frac{0}{p^0} :$$

Ակնհայտ է, որ $u = \frac{-\alpha}{p^k}$: Այս p-ադիկ թիվը կոչվում է $\frac{\alpha}{p^k}$ p-ադիկ թվի հակադիր և նշանակվում է $-\frac{\alpha}{p^k}$-ով: Այսպիսով՝ $-\frac{\alpha}{p^k} = \frac{-\alpha}{p^k}$:

Այնուհետև, յուրաքանչյուր $\frac{\alpha}{p^k} \neq \frac{0}{p^0}$ p-ադիկ թիվ հակադարձելի է, այսինքն գոյություն ունի միարժեքորեն որոշվող այնպիսի v p-ադիկ թիվ, որ

$$\frac{\alpha}{p^k} \cdot v = \frac{1}{p^0} :$$

Իրոք, եթե $\frac{\alpha}{p^k} \neq \frac{0}{p^0}$, ապա $\alpha \neq 0$ և (թեորեմ 9.15) $\alpha = p^s \cdot \varepsilon$, որտեղ ε-ը հակադարձելի ամբողջ p-ադիկ թիվ է և $\varepsilon \cdot \varepsilon' = 1$, որտեղ $\varepsilon' \in \mathcal{O}_p$: Այդ դեպքում, $v = \frac{\varepsilon'}{p^{s-k}}$, եթե $s \geqslant k$, և $v = p^{k-s} \cdot \varepsilon'$, եթե $k \geqslant s$: v-ի միակությունը բխում է արտադրյալ գործողության զուգորդականությունից և այն կոչվում է $\frac{\alpha}{p^k}$ p-ադիկ թվի հակադարձ և նշանակվում է՝ $v = \left(\frac{\alpha}{p^k}\right)^{-1}$:

Թեորեմ 9.17*: Յուրաքանչյուր ոչ զրոյական μ p-ադիկ թիվ միարժեքորեն ներկայացվում է*

$$\mu = p^m \cdot \varepsilon$$

տեսքով, որտեղ $m \in \mathbb{Z}$, իսկ ε-ը հակադարձելի ամբողջ p-ադիկ թիվ է:

Ապացուցում: Դիցուք $\mu = \dfrac{\alpha}{p^k}$, որտեղ $\alpha \in \mathcal{O}_p$ և $\alpha \neq 0$: Համաձայն թեորեմ 9.15-ի՝ $\alpha = p^n \cdot \varepsilon$, որտեղ $n \geqslant 0$, իսկ ε-ը հակադարձելի ամբողջ p-ադիկ թիվ է: Նշանակելով՝ $m = n - k$, կունենանք $m \in \mathbb{Z}$ և $\dfrac{\alpha}{p^k} = p^m \cdot \varepsilon$՝ համաձայն երկու p-ադիկ թվերի հավասարության սահմանման: Այժմ ապացուցենք ներկայացման միակությունը: Դիցուք $\mu = p^m \cdot \varepsilon$ և $\mu = p^{m'} \cdot \varepsilon'$, որտեղ $m, m' \in \mathbb{Z}$ և $\varepsilon, \varepsilon'$-ը հակադարձելի ամբողջ p-ադիկ թվեր են: Ապացուցենք $m = m'$ և $\varepsilon = \varepsilon'$ հավասարությունները: Դիցուք $m \neq m'$ և դիցուք $m < m'$: Այդ դեպքում, կունենանք $m' - m > 0$ և

$$p^m \cdot \varepsilon = p^{m'} \cdot \varepsilon',$$

$$p^{m'-m} \cdot \varepsilon' = p^0 \cdot \varepsilon,$$

որը հակասում է թեորեմ 9.15-ի միակության մասին:

Այսպիսով $m' = m$ հավասարությունն ապացուցված է, և օգտվելով

$$p^m \cdot \varepsilon = p^m \cdot \varepsilon'$$

հավասարությունից, ստանում ենք նաև $\varepsilon = \varepsilon'$ հավասարությունը: □

Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ

1. Ապացուցել, որ եթե $\{x_n\}$-ը ամբողջ p-ադիկ թիվ է, ապա $\{-x_n\}$-ը ևս կլինի ամբողջ p-ադիկ թիվ (p-ն կամայական պարզ թիվ է):

2. Ապացուցել, որ յուրաքանչյուր $\dfrac{\alpha}{p^k}$ p-ադիկ թվի համար տեղի ունի հետևյալ ներակայացումը՝

$$\frac{\alpha}{p^k} = \alpha \cdot (p^k)^{-1} :$$

3. Ապացուցել, որ գոյություն չունի այնպիսի $x \in \mathbb{R}_p$, $x \neq 1$, որ $x^p = 1$, որտեղ p-ն կենտ պարզ թիվ է:

4. Գտնել՝

   ա) 2-ի կարգը ըստ մոդուլ 11-ի;

   բ) 3-ի կարգը ըստ մոդուլ 10-ի;

   գ) 8-ի կարգը ըստ մոդուլ 15-ի:

5. Ապացուցել, որ $7 \cdot 23 \cdot 41 = 6601$-ը Քարմայքլի թիվ է:

6. Ձևակերպել և ապացուցել Գաուսի նույնությունը (թեորեմ 9.7) էյլերի թվակերպ ֆունկցիայի համար:

7. Ապացուցել, որ $\varphi(n^2) = n \cdot \varphi(n)$, որտեղ φ-ն էյլերի ֆունկցիան է:

   Այնուհետև ապացուցել, որ կամայական Q թվակերպ բազմության համար՝
$$\theta_\varphi(n^2) = I(n) \cdot \theta_\varphi(n),$$
   որտեղ $\theta_\varphi : \mathbb{N} \to Q$ ֆունկցիան էյլերի թվակերպ ֆունկցիան է, իսկ $I(n) = n \circ 1$:

8. Եթե $n = 2^{2k+1}$, որտեղ $k \geqslant 1$, ապա $\varphi(n)$-ը հանդիսանում է բնական թվի քառակուսի: Հետևաբար, գոյություն ունեն անվերջ թվով այնպիսի n բնական թվեր, որոնց համար $\varphi(n)$-ը բնական թվի քառակուսի է:

9. Լուծել $41x \equiv 53(mod\,62)$ համասարումը՝ օգտվելով էյլերի թեորեմից ($\varphi(62) = 30, (41, 62) = 1$):

10. Ապացուցել, որ
$$\varphi(2n) = \begin{cases} \varphi(n), & \text{եթե } n\text{-ը կենտ է}, \\ \\ 2\varphi(n), & \text{եթե } n\text{-ը զույգ է}, \end{cases}$$
    որտեղ φ-ն էյլերի ֆունկցիան է: Ձևակերպել և ապացուցել համապատասխան արդյունքը նաև էյլերի թվակերպ ֆունկցիայի համար:

11. Ապացուցել, որ $f(n) = n^2 \cdot \sigma(n) \cdot \varphi(n)$ ֆունկցիան արտադրյալային է:

12. Ապացուցել, որ եթե $(m, n) = 1$, $m, n \in \mathbb{N}$, ապա $m^{\varphi(n)} + n^{\varphi(m)} \equiv 1(mod\,mn)$, որտեղ φ-ն էյլերի ֆունկցիան է:

13. Ապացուցել, որ $\sigma(m) = 2m - 1$ հավասարումն ունի անվերջ թվով բնական լուծումներ:

    (Ցուցում. $m = 2^n$, $n \in \mathbb{N}$): Այդպիսի $m > 0$ բնական թվերը երբեմն կոչվում են **գրեթե-կատարյալ**:

14. Ապացուցել, որ եթե n-ը կատարյալ թիվ է և $d_1, d_2, \ldots, d_k$ բնական թվերը n-ի բոլոր բնական բաժանարարներն են, ապա
$$\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} = 2 :$$

15. Ապացուցել, որ եթե $n_1, n_2, \ldots, n_m$ բնական թվերը միմյանցից տարբեր զույգ կատարյալ թվեր են, ապա
$$\varphi(n_1 n_2 \cdots n_m) = 2^{m-1}\varphi(n_1)\varphi(n_2)\cdots\varphi(n_m) :$$

16. $n > 0$ բնական թիվը կոչվում է **գերկատարյալ**, եթե $\sigma(\sigma(n)) = 2n$: Օրինակ, 16-ը գերկատարյալ թիվ է: Ապացուցել, որ $2^m - 1$ թիվը կլինի պարզ այն և միայն այն դեպքում, երբ 2^{m-1} թիվը գերկատարյալ է:

    Սակայն մինչ այժմ որևէ կենտ գերկատարյալ բնական թիվ չի հայտնաբերվել:

17. Ապացուցել, որ ցանկացած n բնական թվի համար՝
$$(d_1 \cdot d_2 \cdots d_k)^2 = n^{\tau(n)},$$
որտեղ $d_1 < d_2 < \cdots < d_k$ թվերը n-ի բոլոր բնական բաժանարարներն են: Մասնավորապես, $d_1 \cdot d_2 \cdots d_k = \sqrt{n^{\tau(n)}}$:

    (Ցուցում. $\tau(n) = k$,
$$n = \begin{cases} d_1 d_k = d_2 d_{k-1} = \cdots = d_k d_1, \\ \qquad \text{եթե } k = 2t, \\ d_1 d_k = d_2 d_{k-1} = \cdots = d_{t-1}d_{t+1} = d_t^2 = d_{t+1}d_{t-1} = \cdots = d_k d_1, \\ \qquad \text{եթե } k = 2t-1, \end{cases}$$
և
$$\begin{aligned}(d_1 \cdot d_2 \cdots d_k)^2 &= (d_1 \cdot d_2 \cdots d_k)(d_1 \cdot d_2 \cdots d_k) = \\ &= (d_1 d_k)(d_2 d_{k-1})\cdots(d_k d_1) = \underbrace{n \cdot n \cdots n}_{k} = n^k \quad) :\end{aligned}$$

18. Ապացուցել, որ եթե $(n-1)$-ը բաժանվում է $\varphi(n)$-ի վրա ($n > 1$), ապա $n = p_1 p_2 \cdots p_k$, որտեղ $p_1, p_2, \ldots, p_k$ թվերը միմյանցից տարբեր պարզ թվեր են, այսինքն՝ n բնական թիվը էվկլիդեսյան է:

(Ցուցում. եթե $n = p^2 m$, $m \in \mathbb{N}$, որտեղ p-ն որևէ պարզ թիվ է, ապա, համաձայն թեորեմ 9.6-ի, $\varphi(n)$-ը կբաժանվի p-ի վրա: Հետևաբար, $(n-1)$-ը կբաժանվի p-ի վրա՝

$$n-1 = pq,\ p^2m-1 = pq,\ p(pm-q) = 1,$$

որը հակասություն է: Մնում է օգտվել թվաբանության հիմնական թեորեմից):

Սակայն ինչպես նշել ենք, մինչ այժմ չի լուծված հետևյալ խնդիրը (Լեհմեր, 1932 թ.). ապացուցել (կամ հերքել), որ եթե $(n-1)$-ը բաժանվում է $\varphi(n)$-ի վրա, ապա $n > 1$ բնական թիվը պարզ է, այսինքն՝ $\varphi(n) = n-1$:

19. Դիցուք Q-ն թվակերպ բազմություն է՝ օժտված $-1 \in Q$ հատկությամբ, իսկ $f : \mathbb{N} \to Q$ ֆունկցիան արտադրյալային է: Ապացուցել, որ $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m} > 1$ բնական թվի համար՝

$$\sum_{n/d, d>0} \mu(d) f(d) = \prod_{i=1}^{m} \left(1 - f(p_i)\right),$$

որտեղ μ-ն Մյոբիուսի թվակերպ ֆունկցիան է:

(Ցուցում. հավասարության ձախ մասը n-ից կախված արտադրյալային ֆունկցիա է, հետևաբար հավասարությունը բավական է ապացուցել $m = 1$ դեպքում):

20. Ապացուցել σ և τ ֆունկցիաների արտադրյալային հատկությունը՝ օգտվելով թեորեմ 9.12-ից:

21. Օգտվելով թեորեմ 9.7-ի երկրորդ ապացուցումից և թեորեմ 9.12-ից, ստանալ Էյլերի φ ֆունկցիայի արտադրյալային հատկությունը և

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_m}\right)$$

հավասարությունը՝ օգտվելով նաև թեորեմ 9.10-ից և թեորեմ 6.4-ից, որտեղ $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} > 1$:

(Ցուցում. քանի որ $n = \sum\limits_{n/d, d>0} \varphi(d)$, ապա $I(n) = \sum\limits_{n/d, d>0} \varphi(d)$, որտեղ $I(n) = n$ ֆունկցիան արտադրյալային է: Համաձայն թեորեմ

9.10-ի $\varphi(n) = \sum\limits_{n/d, d>0} \mu(d) I\left(\frac{n}{d}\right) = n \sum\limits_{n/d, d>0} \frac{\mu(d)}{d}$: Մնում է կիրառել թեորեմ 6.4-ը):

22. Ապացուցել, որ
$$\sum_{n/d, d>0} \mu\left(\frac{n}{d}\right) \tau(n) = 1 :$$
(Ցուցում. $\tau(n) = \sum\limits_{n/d, d>0} I_1(d)$, որտեղ $I_1(n) = 1$, $n \in \mathbb{N}$: Մնում է օգտվել թեորեմ 9.10-ից):

23. Ապացուցել, որ
$$\sum_{n/d, d>0} \mu\left(\frac{n}{d}\right) \sigma(d) = n :$$
(Ցուցում. $\sigma(n) = \sum\limits_{n/d, d>0} I(d)$, որտեղ $I(n) = n$, $n \in \mathbb{N}$: Մնում է օգտվել թեորեմ 9.10-ից):

24. Ապացուցել հետևյալ հավասարությունը՝
$$\varphi(n) = \sum_{n/d, d>0} \mu\left(\frac{n}{d}\right) \cdot d :$$
(Ցուցում. ըստ թեորեմ 9.7-ի՝ $I(n) = \sum\limits_{n/d, d>0} \varphi(d)$, որտեղ $I(n) = n$, $n \in \mathbb{N}$: Մնում է օգտվել թեորեմ 9.10-ից):

25. Դիցուք $k \in \mathbb{Z}$, $k \geqslant 0$: Սահմանենք $\varphi_k : \mathbb{N} \to \mathbb{N}$ ֆունկցիան հետևյալ կերպ՝
$$\varphi_k(n) = \sum_{1 \leqslant d \leqslant n, (d,n)=1} d^k, \qquad n \in \mathbb{N} :$$
Ակնհայտ է, որ $\varphi_0(n) = \varphi(n)$, որտեղ φ-ն էյլերի ֆունկցիան է: Ապացուցել Գաուսի նույնության (թեորեմ 9.7) հետևյալ ընդհանրացումը՝
$$\sum_{n/d, d>0} \frac{\varphi_k(d)}{d^k} = \frac{1^k + 2^k + \cdots + n^k}{n^k} :$$

26. Յուրաքանչյուր $n > 0$ բնական թվի համար գոյություն ունեն արդյոք այնպիսի a և b բնական թվեր, որ

$$\varphi(a) + \varphi(b) = 2n,$$

որտեղ φ-ն էյլերի ֆունկցիան է:

Էրդյոշի և Մոզերի կողմից դրված այս խնդիրը դեռևս չի լուծված:

27. Դիցուք $n = p_1 p_2 \cdots p_m$, որտեղ $p_1, p_2, \ldots, p_m$-ը միմյանցից տարբեր պարզ թվեր են: Ապացուցել $\tau(n) = 2^m$ հավասարությունը:

28. Ապացուցել $\tau(n) \leqslant 2\sqrt{n}$ անհավասարությունը:

29. Ապացուցել $\tau(n) \leqslant \tau\left(2^n - 1\right)$ անհավասարությունը:

30. Ապացուցել $\tau(mn) \leqslant \tau(m)\tau(n)$ անհավասարությունը:

31. Դիցուք $n \in \mathbb{N}$: Ապացուցել հետևյալ հավասարությունը՝

$$\left(\sum_{n/d, d>0} \tau(d)\right)^2 = \sum_{n/d, d>0} (\tau(d))^3 :$$

32. Ապացուցել $n \leqslant \sigma(n) \leqslant n^2$ անհավասարությունները:

(Ցուցում. $\sigma(n) \leqslant 1 + 2 + \cdots + n = \dfrac{1+n}{2} \cdot n = \dfrac{n+n^2}{2} \leqslant n^2$):

33. Դիցուք $n \in \mathbb{N}$: Ապացուցել հետևյալ հավասարությունը՝

$$\frac{\sigma(n)}{n} = \sum_{n/d, d>0} \frac{1}{d} :$$

34. Դիցուք $n \in \mathbb{N}$: Ապացուցել հետևյալ անհավասարությունը՝

$$\frac{\sigma(n!)}{n!} \geqslant \sum_{i=1}^{n} \frac{1}{i} :$$

35. Դիցուք $n, k \in \mathbb{N}$: Սահմանենք՝

$$\sigma_k(n) = \sum_{n/d, d>0} d^k :$$

Ապացուցել, որ $\sigma_k : \mathbb{N} \to \mathbb{N}$ ֆունկցիան արտադրյալային է ($\sigma_1(n) = \sigma(n)$):

36. Գտնել բոլոր այն n բնական թվերը, որոնց համար՝

$$\varphi(n) + \sigma(n) = n\tau(n) :$$

Այս խնդիրը մինչ այժմ չի լուծված:

37. Օգտվելով թեորեմ 9.6-ից ապացուցել, որ պարզ թվերի քանակն անվերջ է:

(Ցուցում. Դիցուք պարզ թվերի քանակը վերջավոր է և $p_1, p_2, \ldots, p_n$-ը բոլոր պարզ թվերն են, իսկ $m = p_1 \cdot p_2 \cdots p_n$: Թեորեմ 9.6-ի համաձայն՝

$$\varphi(m) = (p_1 - 1)(p_2 - 1) \cdots (p_n - 1) :$$

Սակայն, մյուս կողմից, էյլերի φ ֆունկցիայի սահմանման համաձայն՝ $\varphi(m) = 1$, որովհետև յուրաքանչյուր $t > 1$ բնական թիվ ունի պարզ բաժանարար (հատկություն 6.1), որը այդ դեպքում կհամընկնի $p_1, p_2, \ldots, p_n$ պարզ թվերից որևէ մեկի հետ և, հետևաբար, $(t, m) \neq 1$: Ուստի՝

$$(p_1 - 1)(p_2 - 1) \cdots (p_n - 1) = 1,$$

որը հակասություն է, որովհետև հավասարության ձախ մասը, ակնհայտորեն, մեծ է մեկից):

38. Նկարագրել Մյոբիուսի թվակերպ ֆունկցիան՝ $Q = \mathbb{Z}_3$ թվակերպ բազմության դեպքում:

39. Նկարագրել Մյոբիուսի ընդհանրացված ֆունկցիաները $Q = \mathbb{Z}_2$ թվակերպ բազմության դեպքում:

40. Նկարագրել Մյոբիուսի ընդհանրացված ֆունկցիաները $Q = \mathbb{Z}_3$ թվակերպ բազմության դեպքում:

41. Նկարագրել Մյոբիուսի թվակերպ ֆունկցիան՝ $Q = \mathbb{Z}_4$ թվակերպ բազմության դեպքում:

42. Նկարագրել Մյոբիուսի ընդհանրացված ֆունկցիաները $Q = \mathbb{Z}_4$ թվակերպ բազմության դեպքում:

43. Նկարագրել Մյոբիուսի թվակերպ ֆունկցիան՝ $Q = \mathbb{Z}_2 \times \mathbb{Z}_2$ թվակերպ բազմության դեպքում:

Գ լ ու խ 10

ԵՐԿՐՈՐԴ ԱՍՏԻՃԱՆԻ ԲԱՂԴԱՏՈՒՄՆԵՐ: ՔԱՌԱԿՈՒՍԱՅԻՆ ՄՆԱՑՔ ԵՎ ՈՉ-ՄՆԱՑՔ: ԼԵԺԱՆԴՐԻ ՊԱՅՄԱՆԱՆՇԱՆ

10.1. Քառակուսային մնացք և ոչ-մնացք

Դիտարկենք $x^n \equiv a(mod\, m)$ բաղդատումը, որտեղ $a \in \mathbb{Z}$, $m \in \mathbb{N}$ և $(a, m) = 1$: Այն կոչվում է n-րդ աստիճանի երկանդամ բաղդատում: Եթե այս բաղդատումն ունի ամբողջ թվերի $\mathbb{Z}$ բազմությանը պատկանող լուծում, ապա a-ն կոչվում է **n-րդ աստիճանի մնացք ըստ m-ի**: Հակառակ դեպքում, a-ն կոչվում է n-րդ աստիճանի **ոչ-մնացք** ըստ m-ի: $n = 2$ դեպքում, n-րդ աստիճանի մնացքը (ոչ-մնացքը) ըստ m-ի կոչվում է **քառակուսային մնացք** (ոչ-մնացք) ըստ m-ի:

Օրինակ, 4-ը քառակուսային մնացք է ըստ 7-ի, իսկ 3-ը քառակուսային ոչ-մնացք է ըստ 7-ի, որովհետև $x^2 \equiv 4(mod\, 7)$ բաղդատումն ունի ամբողջ լուծում ($x = 2$), իսկ $x^2 \equiv 3(mod\, 7)$ բաղդատումը՝ ոչ:

Այստեղ հիմնականում կուսումնասիրվեն քառակուսային մնացքներ և ոչ-մնացքներ ըստ $p \neq 2$ պարզ թվերի:

Ակնհայտ է, որ եթե $x_0 \in \mathbb{Z}$ ամբողջ թիվը լուծում է n-րդ աստիճանի վերոհիշյալ երկանդամ բաղդատման համար, ապա $[x_0] \in \mathbb{Z}_m$ մնացքների դասը ևս կլինի լուծում դրա համար, այսինքն $[x_0]$-ին պատկանող յուրաքանչյուր ամբողջ թիվ լուծում է նշված բաղդատման համար:

Թեորեմ 10.1: *Եթե $a \in \mathbb{Z}$ ամբողջ թիվը չի բաժանվում $p \neq 2$ պարզ թվի վրա, այսինքն $(a, p) = 1$, ապա $x^2 \equiv a(mod\, p)$ բաղդատումը կամ չունի ամբողջ լուծում, կամ նրա լուծում հանդիսացող մնացքների դասերի թիվը ճիշտ հավասար է 2-ի:*

Ապացուցում: Մի կողմից, համաձայն թեորեմ 6.6-ի, $x^2 \equiv a(mod\, p)$ բաղդատման լուծում հանդիսացող մնացքների դասերի թիվը չի գերազանցում 2-ը: Դիցուք a-ն քառակուսային մնացք է ըստ տրված $p \neq 2$ պարզ թվի, այսինքն գոյություն ունի այնպիսի $x_1 \in \mathbb{Z}$ ամբողջ թիվ, որ $x_1^2 \equiv a(mod\, p)$: Քանի որ $(-x_1)^2 = x_1^2$, ապա $(-x_1)^2 \equiv a(mod\, p)$: Մնում է ապացուցել, որ $-x_1 \not\equiv x_1(mod\, p)$: Իրոք, եթե $x_1 \equiv -x_1(mod\, p)$, ապա $2x_1 \equiv 0(mod\, p)$, այսինքն $2x_1$-ը բաժանվում է p-ի վրա և համաձայն հատկություն 6.3-ի, կամ 2-ն է բաժանվում p-ի վրա, կամ x_1-ը: Սակայն $p \neq 2$ պայմանից բխում է, որ $p > 2$ և հետևաբար 2-ը չի կարող բաժանվել p-ի վրա: Իսկ եթե x_1-ը բաժանվի p-ի վրա, այսինքն՝ $x_1 \equiv 0(mod\, p)$, ապա $x_1^2 \equiv 0(mod\, p)$ և հետևաբար՝ $a \equiv 0(mod\, p)$, այսինքն a-ն կբաժանվի p-ի վրա, որը հակասում է տրված պայմանին: □

Դիցուք $a \in \mathbb{Z}$, $m \in \mathbb{N}$ և $(a, m) = 1$: $[a] \in \mathbb{Z}_m$ մնացքների դասը կոչվում է քառակուսային մնացք (ոչ-մնացք) ըստ m-ի, եթե $[a]$-ին պատկանող յուրաքանչյուր ամբողջ թիվ քառակուսային մնացք (ոչ-մնացք) է ըստ m-ի: Ակնհայտ է, որ եթե a ամբողջ թիվը քառակուսային մնացք է ըստ m-ի, ապա $[a] \in \mathbb{Z}_m$ մնացքների դասը ևս կլինի քառակուսային մնացք ըստ m-ի: Իրոք, եթե $(a, m) = 1$, $x^2 \equiv a(mod\, m)$ բաղդատումը ունի ամբողջ լուծում և $b \equiv a(mod\, m)$, ապա $(b, m) = 1$ և $x^2 \equiv b(mod\, m)$ բաղդատումը կունենա նույն ամբողջ լուծումը: Հետևաբար, եթե a ամբողջ թիվը քառակուսային ոչ-մնացք է ըստ m-ի, ապա $[a] \in \mathbb{Z}_m$ մնացքների դասը ևս կլինի քառակուսային ոչ-մնացք ըստ m-ի:

Թեորեմ 10.2: *$[1], [2], \ldots, [p-1] \in \mathbb{Z}_p$ մնացքների դասերից ճիշտ $\frac{p-1}{2}$ հատը կլինի քառակուսային մնացք ըստ $p \neq 2$ պարզ թվի և հետևաբար, ճիշտ $\frac{p-1}{2}$ հատը կլինի քառակուսային ոչ-մնացք ըստ այդ p-ի:*

Ապացուցում: Քանի որ $[-x] = [p - x]$, ապա $[-1] = [p - 1]$, $[-2] = [p - 2]$, $\ldots$, $\left[-\frac{p-1}{2}\right] = \left[p - \frac{p-1}{2}\right] = \left[\frac{p+1}{2}\right] = \left[\frac{p-1}{2} + 1\right]$ և $\{[1], [2], \ldots, [p-1]\} = \left\{[1], \ldots, \left[\frac{p-1}{2}\right], \left[-\frac{p-1}{2}\right], \ldots, [-1]\right\}$ և հետևաբար $x^2 \equiv a(mod\, p)$ բաղդատումը կունենա ամբողջ լուծում այն և միայն այն դեպքում, երբ $a \equiv x^2(mod\, p)$, որտեղ $x = \pm 1, \pm 2, \ldots, \pm\frac{p-1}{2}$, կամ $x = 1, 2, \ldots, \frac{p-1}{2}$, որովհետև $x^2 = (-x)^2$: Մնում է ապացուցել, որ $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ բնական թվերը զույգ առ զույգ միմյանց հետ բաղդատելի չեն: Իրոք, եթե $1 \leqslant k < l \leqslant \frac{p-1}{2}$ և $k^2 \equiv l^2(mod\, p)$, ապա

$$x^2 \equiv k^2(mod\, p)$$

բաղդատումը կունենա $x = -k, k, l, -l$ լուծումները, որոնք միմյանց հետ բաղդատելի չեն ըստ p-ի, իսկ սա հակասում է թեորեմ 6.6-ին: $\square$

Այժմ ակնհայտ է դառնում, թե ինչու վերոհիշյալ $x^2 \equiv 3(mod\,7)$ բաղդատումը չունի ամբողջ լուծում: Որովհետև այս դեպքում՝ $p = 7$, $\dfrac{p-1}{2} = 3$, $a = 3$, սակայն $a \not\equiv x^2(mod\,7)$, $x = 1, 2, 3$ դեպքերում:

Թեորեմ 10.3 (Էյլերի հայտանիշը): *Եթե* $a \in \mathbb{Z}$ *ամբողջ թիվը չի բաժանվում* $p \neq 2$ *պարզ թվի վրա, ապա* $x^2 \equiv a(mod\,p)$ *բաղդատումը*

ա) կունենա ամբողջ լուծում այն և միայն այն դեպքում, երբ $a^{\frac{p-1}{2}} \equiv 1(mod\,p)$ *և*

բ) չի ունենա ամբողջ լուծում այն և միայն այն դեպքում, երբ $a^{\frac{p-1}{2}} \equiv -1(mod\,p)$*:*

Ապացուցում: Ֆերմայի փոքր թեորեմի (հետևություն 9.1) համաձայն՝ $a^{p-1} \equiv 1(mod\,p)$ կամ $a^{p-1} - 1 \equiv 0(mod\,p)$: Քանի որ $\left(\dfrac{p-1}{2}\right) \cdot 2 = p - 1$. ապա այստեղից կունենանք՝

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(mod\,p)$$

կամ $\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right)$ արտադրյալը բաժանվում է p պարզ թվի վրա: Հետևաբար, կամ առաջին արտադրիչն է բաժանվում p-ի վրա, կամ՝ երկրորդ (սակայն երկու արտադրիչները միաժամանակ p-ի վրա բաժանվել չեն կարող, որովհետև այդ դեպքում միմյանցից հանելով կստանայինք, որ 2-ը բաժանվում է p-ի վրա, որը հնարավոր չէ, որովհետև $p > 2$): Առաջին դեպքում կունենանք՝

$$a^{\frac{p-1}{2}} \equiv 1(mod\,p),$$

իսկ երկրորդ դեպքում՝

$$a^{\frac{p-1}{2}} \equiv -1(mod\,p):$$

Մնում է ապացուցել, որ առաջին դեպքը տեղի կունենա այն և միայն այն դեպքում, երբ a-ն քառակուսային մնացք է ըստ p-ի: Հետևաբար, երկրորդ դեպքը տեղի կունենա այն և միայն այն դեպքում, երբ a-ն քառակուսային ոչ-մնացք է ըստ p-ի:

Դիցուք a-ն քառակուսային մնացք է ըստ p-ի, այսինքն $x^2 \equiv a(mod\,p)$ բաղդատումը օժտված է x_1 ամբողջ լուծումով, այսինքն $x_1^2 \equiv a(mod\,p)$, կամ $a \equiv x_1^2(mod\,p)$, որտեղ $(x_1, p) = 1$ (որովհետև, եթե x_1-ը (հետևաբար և x_1^2-ն) բաժանվեր p-ի վրա, ապա a-ն ևս կբաժանվեր p-ի վրա, որը հակասում է թեորեմի պայմանին): Ուստի՝

$$a^{\frac{p-1}{2}} \equiv \left(x_1^2\right)^{\frac{p-1}{2}} (mod\,p),$$

$$a^{\frac{p-1}{2}} \equiv x_1^{p-1}(mod\,p),$$

$$a^{\frac{p-1}{2}} \equiv 1(mod\,p)$$

համաձայն Ֆերմայի փոքր թեորեմի:

Այսինքն, յուրաքանչյուր քառակուսային մնացք ըստ $p \neq 2$ պարզ թվի հանդիսանում է $x^{\frac{p-1}{2}} \equiv 1(mod\,p)$ բաղդատման լուծում: Այսպիսով, համաձայն թեորեմ 10.2-ի, ստանում ենք նշված բաղդատման լուծում հանդիսացող առնվազն $\dfrac{p-1}{2}$ հատ մնացքների դասեր: Մյուս կողմից, համաձայն թեորեմ 6.7-ի, $\dfrac{p-1}{2}$ աստիճան ունեցող բաղդատումը (ըստ p պարզ հենքի) չի կարող ուրիշ լուծումներ ունենալ, այսինքն մնացած $\dfrac{p-1}{2}$ հատ քառակուսային ոչ-մնացք հանդիսացող մնացքների դասերը $x^{\frac{p-1}{2}} \equiv 1(mod\,p)$ բաղդատման լուծումներ չեն: Հետևաբար, քառակուսային ոչ-մնացք հանդիսացող յուրաքանչյուր a ամբողջ թիվ չի բավարարի $x^{\frac{p-1}{2}} \equiv 1(mod\,p)$ բաղդատմանը, այլ կբավարարի $x^{\frac{p-1}{2}} \equiv -1(mod\,p)$ բաղդատմանը: $\square$

10.2. Լեժանդրի պայմանանշանը

Դիցուք $a \in \mathbb{Z}$, իսկ p-ն կենտ պարզ թիվ է ($p \neq 2$) և դիցուք a-ն չի բաժանվում p-ի վրա, այսինքն $(a, p) = 1$: a թվի **Լեժանդրի պայմանանշանը** ըստ p պարզ թվի նշանակվում է $\left(\dfrac{a}{p}\right)$ ձևով (որտեղ a-ն կոչվում է պայմանանշանի համարիչ, իսկ p-ն՝ հայտարար) և սահմանվում է հետևյալ կերպ՝

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{եթե } a\text{-ն քառակուսային մնացք է ըստ } p\text{-ի}, \\ -1, & \text{եթե } a\text{-ն քառակուսային ոչ-մնացք է ըստ } p\text{-ի}: \end{cases}$$

Այսինքն, $\left(\dfrac{a}{p}\right)=1$ այն և միայն այն դեպքում, երբ $x^2 \equiv a(mod\, p)$ բաղդատումն ունի ամբողջ լուծում, և $\left(\dfrac{a}{p}\right)=-1$ այն և միայն այն դեպքում, երբ $x^2 \equiv a(mod\, p)$ բաղդատումը չունի ամբողջ լուծում: *Օրինակ,* ըստ սահմանման՝ $\left(\dfrac{4}{7}\right)=1$, իսկ $\left(\dfrac{3}{7}\right)=-1$:

Օգտվելով Լեժանդրի պայմանանշանից, Էյլերի հայտանիշը (թեորեմ 10.3) կարելի է վերաձևակերպել հետևյալ կերպ:

Թեորեմ 10.4 (Էյլերի բանաձևը): *Եթե* $a \in \mathbb{Z}$ *ամբողջ թիվը չի բաժանվում* $p \neq 2$ *պարզ թվի վրա, ապա*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)(mod\, p),$$

կամ՝

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(mod\, p):$$

□

Օրինակ, օգտվելով այս բանաձևից, հաշվենք $\left(\dfrac{3}{7}\right)$-ը, այսինքն պարզենք, թե $\left(\dfrac{3}{7}\right)=\pm 1$ արժեքներից որն է ճիշտ.

$$\left(\frac{3}{7}\right) \equiv 3^{\frac{7-1}{2}}(mod\, 7),$$

$$3^{\frac{7-1}{2}} = 3^3 = 27 \equiv -1(mod\, 7),$$

այսինքն՝ $\left(\dfrac{3}{7}\right) \equiv -1(mod\, 7)$ և հետևաբար $\left(\dfrac{3}{7}\right)=-1$, որովհետև $1 \not\equiv -1(mod\, 7)$:

Հատկություն 10.1: *Եթե* p*-ն կենտ պարզ թիվ է, իսկ* $a, b \in \mathbb{Z}$ *ամբողջ թվերը չեն բաժանվում* p*-ի վրա, ապա՝*

1) $\left(\dfrac{1}{p}\right)=1$;

2) $\left(\dfrac{a^2}{p}\right)=1$;

3) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, *եթե* $a \equiv b(mod\, p)$;

4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{եթե} \quad p \equiv 1(mod\, 4), \\ -1, & \text{եթե} \quad p \equiv 3(mod\, 4); \end{cases}$

5) $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$;

Մասնավորապես, երկու քառակուսային մնացքների (ոչ-մնացքների) արտադրյալը նորից քառակուսային մնացք է, իսկ քառակուսային մնացքի և քառակուսային ոչ-մնացքի արտադրյալը քառակուսային ոչ-մնացք է ;

6) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$;

7) $\left(\frac{a_1 \cdot a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right) \cdot \left(\frac{a_2}{p}\right) \cdot \left(\frac{a_n}{p}\right)$,

եթե $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ *ամբողջ թվերը չեն բաժանվում* p*-ի վրա; Մասնավորապես,*

$$\left(\frac{a^n}{p}\right) = \left(\frac{a}{p}\right)^n :$$

Ապացուցում: 2) -ը ակնհայտ է, որովհետև $x^2 \equiv a^2(mod\, p)$ բաղդատումն ունի $x = a$ ամբողջ լուծումը: 2) -ից, $a = 1$ դեպքում, բխում է 1) -ը: 3) -ը նույնպես ակնհայտ է, որովհետև, եթե $a \equiv b(mod\, p)$, ապա $x^2 \equiv a(mod\, p)$ բաղդատումը կունենա ամբողջ լուծում այն և միայն այն դեպքում, երբ $x^2 \equiv b(mod\, p)$ բաղդատումը կունենա ամբողջ լուծում: Ապացուցենք 4)-ը: Համաձայն Էյլերի բանաձևի (թեորեմ 10.4),

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(mod\, p),$$

որտեղ $\left(\frac{-1}{p}\right) = \pm 1$ և $(-1)^{\frac{p-1}{2}} = \pm 1$: Բայց քանի որ $1 \not\equiv (-1)(mod\, p)$, ապա

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} :$$

6) -ը բխում է 5) -ից և 2) -ից: Ապացուցենք 5) -ը: Նորից օգտվելով Էյլերի բանաձևից, կունենանք՝

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} (mod\, p),$$

որտեղ՝

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) (mod\, p),$$

այսինքն՝

$$\left(\frac{a \cdot b}{p}\right) \equiv \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) (mod\, p) :$$

Հաշվի առնելով $\left(\frac{ab}{p}\right) = \pm 1$ և $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \pm 1$ արժեքները, հանգում ենք պահանջվող հավասարությանը՝

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) :$$

7)-րդ հատկությունն ապացուցվում է վերհանգման եղանակով: □

Դիցուք p-ն կենտ պարզ թիվ է և $a \in \mathbb{Z}$ ամբողջ թիվը չի բաժանվում p-ի վրա: Համաձայն թվաբանության հիմնական թեորեմի՝

$$a = \pm 2^{\alpha_0} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

որտեղ $p_!, p_2, \ldots, p_n$ պարզ թվերը p-ից տարբեր կենտ թվեր են, իսկ $\alpha_0, \alpha_1, \ldots, \alpha_n$-ը ոչ բացասական ամբողջ թվեր են: Օգտվելով հատկություն 10.1-ի 7) -րդ հատկությունից, կունենանք՝

$$\left(\frac{a}{p}\right) = \left(\frac{\pm 1}{p}\right) \cdot \left(\frac{2}{p}\right)^{\alpha_0} \cdot \left(\frac{p_1}{p}\right)^{\alpha_1} \cdots \left(\frac{p_n}{p}\right)^{\alpha_n} :$$

Այսպիսով, $\left(\frac{a}{p}\right)$-ն հաշվելու համար, բավական է ունենալ $\left(\frac{\pm 1}{p}\right)$, $\left(\frac{2}{p}\right)$ և $\left(\frac{q}{p}\right)$ արժեքները, որտեղ q-ն ևս կենտ պարզ թիվ է և $q \neq p$: Սակայն $\left(\frac{a}{p}\right)$-ն կարելի է հաշվել նաև անմիջական եղանակով, օգտվելով Գաուսի կողմից ապացուցված հետևյալ արդյունքից:

Լեմմ 10.1 (Գաուսի լեմմը): *Եթե* p*-ն կենտ պարզ թիվ է, իսկ* $a \in \mathbb{Z}$ *ամբողջ թիվը չի բաժանվում* p*-ի վրա, ապա*

$$\left(\frac{a}{p}\right) = (-1)^n,$$

որտեղ n*-ը* $[a], [2a], [3a], \ldots, \left[\frac{(p-1)}{2}a\right] \in \mathbb{Z}_p$ *մնացքների դասերում եղած այն դրական ամենափոքր ամբողջ թվերի քանակն է, որոնք մեծ են* $\frac{p}{2}$*-ից:*

Ապացույց: Դիցուք $r_1, r_2, \ldots, r_n$-ը $[a]$, $[2a]$, $[3a]$, $\ldots$, $\left[\frac{(p-1)}{2}a\right] \in \mathbb{Z}_p$ մնացքների դասերում եղած այն դրական և ամենափոքր ամբողջ թվերն են, որոնք մեծ են $\frac{p}{2}$-ից և դիցուք $s_1, s_2, \ldots, s_m$-ը այդ մնացքների դասերում եղած այն ոչ բացասական փոքրագույն ամբողջ թվերն են, որոնք փոքր են $\frac{p}{2}$-ից (կենտ p պարզ թվի համար $\frac{p}{2}$-ը ամբողջ թիվ չէ): Քանի որ p-ն պարզ թիվ է և ըստ պայմանի a-ն չի բաժանվում p-ի վրա, ապա $2a, 3a, \ldots, \frac{(p-1)}{2}a$ թվերից ոչ մեկը չի բաժանվի p-ի վրա (հատկություն 6.3) և հետևաբար՝ $s_i \neq 0$, $i = 1, 2, \ldots, m$: Ակնհայտ է նաև, որ

$$r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_m$$

ոչ զրոյական ամբողջ թվերի քանակը կլինի հավասար դիտարկվող $[a]$, $[2a]$, $[3a]$, $\ldots$, $\left[\frac{(p-1)}{2}a\right] \in \mathbb{Z}_p$ մնացքների դասերի քանակին, որը հավասար է՝ $\frac{p-1}{2}$: Այժմ դիտարկենք հետևյալ ամբողջ թվերը, որոնց քանակը նույնպես $\frac{p-1}{2}$- է՝

$$p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m$$

և ապացուցենք, որ սրանք հենց 1-ից մինչև $\frac{p-1}{2}$-ը եղած բոլոր բնական թվերն են: Դիցուք $p = 2k + 1$, $k \in N$:

Քանի որ $0 < s_i < \frac{p}{2} = k + \frac{1}{2}$, ապա $0 < s_i < k + \frac{1}{2}$, այսինքն $1 \leqslant s_i \leqslant k = \frac{p-1}{2}$: Քանի որ $p > r_j > \frac{p}{2}$, $-p < -r_j < -\frac{p}{2}$, ապա $p-p<p-r_j<p-\dfrac{p}{2}$, $0<p-r_j<\dfrac{p}{2}=k+\dfrac{1}{2}$, այսինքն $1\leqslant p-r_j\leqslant k=\dfrac{p-1}{2}$: Այժմ բավական է ապացուցել, որ դիտարկվող հաջորդականության կամայական երկու անդամներ բաղդատելի չեն ըստ p հենաթվի (մոդուլի): Իրոք, նախ առաջին n ամբողջ թվերի մեջ չկան միմյանց հետ բաղդատելի երկու թվեր, որովհետև, եթե $p-r_i\equiv p-r_j(mod\,p)$, որտեղ $i\neq j$, ապա $r_i\equiv r_j(mod\,p)$, որտեղ $r_i\equiv k_ia(mod\,p)$, $r_j\equiv k_ja(mod\,p)$, $1\leqslant k_i,k_j\leqslant\dfrac{p-1}{2}$, $k_i\neq k_j$ և հետևաբար $ak_i\equiv ak_j(mod\,p)$: Սակայն, քանի որ a-ն չի բաժանվում p-ի վրա, ապա այստեղից, հատկություն 3.8-ի համաձայն, կունենանք՝ $k_i\equiv k_j(mod\,p)$, որը հնարավոր չէ: Համանման եղանակով ստուգվում է, որ դիտարկվող հաջորդականության վերջին m անդամների մեջ չկան միմյանց հետ բաղդատելի երկու թվեր, ինչպես նաև առաջին n ամբողջ թվերից որևէ մեկը բաղդատելի չէ վերջին m ամբողջ թվերից որևէ մեկի հետ:

Այսպիսով,

$$p-r_1,p-r_2,\ldots,p-r_n,s_1,s_2,\ldots,s_m$$

ամբողջ թվերը հանդիսանում են 1-ից մինչև $\dfrac{p-1}{2}$-ը եղած բոլոր բնական թվերը՝ գրված որևէ հերթականությամբ: Մասնավորապես,

$$(p-r_1)(p-r_2)\cdots(p-r_n)s_1s_2\cdots s_m=1\cdot2\cdot3\cdots\frac{p-1}{2}=\left(\frac{p-1}{2}\right)!,$$

$$(p-r_1)(p-r_2)\cdots(p-r_n)s_1s_2\cdots s_m\equiv\left(\frac{p-1}{2}\right)!(mod\,p),$$

$$(-1)^nr_1r_2\cdots r_ns_1s_2\cdots s_m\equiv\left(\frac{p-1}{2}\right)!(mod\,p);$$

Օգտվելով r_i և s_j թվերի սահմանումներից, կունենանք՝

$$(-1)^na(2a)(3a)\cdots\left(\frac{p-1}{2}\right)a\equiv\left(\frac{p-1}{2}\right)!(mod\,p),$$

կամ՝

$$(-1)^na^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv\left(\frac{p-1}{2}\right)!(mod\,p),$$

և քանի որ $\left(\dfrac{p-1}{2}\right)$!-ը չի բաժանվում p պարզ թվի վրա (որովհետև, եթե $1 \leqslant k \leqslant \dfrac{p-1}{2}$ և $k = p \cdot t$, որտեղ $t \in \mathbb{N}$, ապա $p \geqslant 2k+1$ և $k = pt \geqslant (2k+1)t$, որտեղից $k(1-2t) \geqslant t$ և ստացված անհավասարության ձախ մասը բացասական է, իսկ աջ մասը դրական), ապա, նորից թեորեմ 3.2-ի համաձայն,

$$(-1)^n a^{\frac{p-1}{2}} \equiv 1 (mod\, p),$$

կամ՝

$$a^{\frac{p-1}{2}} \equiv (-1)^n (mod\, p)$$

և համաձայն էյլերի բանաձևի (թեորեմ 10.4), կունենանք՝

$$\left(\frac{a}{p}\right) \equiv (-1)^n (mod\, p) :$$

Այստեղից, քանի որ $\left(\dfrac{a}{p}\right) = \pm 1$ և $(-1)^n = \pm 1$, կունենանք՝

$$\left(\frac{a}{p}\right) = (-1)^n : \qquad \square$$

Հետևություն 10.1: *Եթե p-ն կենտ պարզ թիվ է, իսկ a-ն կենտ ամբողջ թիվ է և չի բաժանվում p-ի վրա, ապա $\left(\dfrac{a}{p}\right) = (-1)^N$, որտեղ $N = \sum_{j=1}^{\frac{p-1}{2}} \left[\dfrac{ja}{p}\right]$:*

Ապացուցում: Ինչպես և Գաուսի լեմմի ապացուցման ժամանակ, դիցուք $r_1, r_2, \ldots, r_n$ ամբողջ թվերը $[a]$, $[2a]$, $[3a]$, $\ldots$, $\left[\dfrac{p-1}{2} \cdot a\right]$ մնացքների դասերում պարունակվող բոլոր այն փոքրագույն դրական թվերն են, որոնք մեծ են $\dfrac{p}{2}$-ից, իսկ $s_1, s_2, \ldots, s_m$ ամբողջ թվերը բոլոր այն ոչ բացասական փոքրագուն դրական թվերն են, որոնք պարունակվում են նույն մնացքների դասերում և փոքր են $\dfrac{p}{2}$-ից: Այսինքն r_i և s_k թվերը ստացվում են որպես մնացորդներ, երբ ja-ն բաժանվում է p-ի վրա.

$$ja = p \cdot q_j + t_j, \qquad 1 \leqslant t_j < p,$$

որտեղ $j = 1, 2, \ldots, \frac{p-1}{2}$, $t_j = r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_m$: Համաձայն լեմմ 8.3-ի՝

$$q_j = \left[\frac{ja}{p}\right]:$$

Հետևաբար՝

$$ja = p\left[\frac{ja}{p}\right] + t_j$$

և

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \sum_{i=1}^{n} r_i + \sum_{k=1}^{m} s_k:$$

Ինչպես տեսանք Գաուսի լեմմի ապացուցման ժամանակ, $p-r_1, p-r_2, \ldots, p-r_n, s_1, s_2, \ldots, s_m$ ամբողջ թվերը հանդիսանում են 1-ից մինչև $\frac{p-1}{2}$-ը եղած բոլոր ամբողջ թվերի հետ: Հետևաբար,

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{n}(p - r_j) + \sum_{k=1}^{m} s_k = pn - \sum_{j=1}^{n} r_j + \sum_{j=1}^{m} s_j:$$

Հաշվի առնելով այս հավասարությունները, կստանանք՝

$$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] - pn + 2\sum_{j=1}^{n} r_j,$$

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] - pn + 2\sum_{j=1}^{n} r_j:$$

Քանի որ $(a-1)$-ը բաժանվում է 2-ի, ապա

$$\sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] - pn \equiv 0(mod\,2)$$

և քանի որ այստեղ p-ն չի բաժանվում 2-ի, ապա (հետևություն 6.4)՝

$$\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] - n \equiv 0(mod\,2),$$

կամ

$$N = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right] \equiv n(mod\, 2) :$$

Հետևաբար, $n = N + 2k$, $k \in \mathbb{Z}$ և համաձայն Գաուսի լեմմի՝

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{N+2k} = (-1)^N \cdot (-1)^{2k} = (-1)^N : \qquad \square$$

Օրինակ, օգտվելով Գաուսի լեմմից, հաշվենք $\left(\frac{6}{13}\right)$-ը: Այստեղ՝ $a = 6$, $p = 13$, $\frac{p}{2} = 6,5$ և համապատասխան մնացքների դասերն են՝ $[6]$, $[2{\cdot}6]$, $\ldots$, $\left[\frac{p-1}{2}\cdot 6\right] = [6\cdot 6]$:

Քանի որ՝

$$6 \equiv 6(mod\, 13),$$

$$2\cdot 6 = 12 \equiv 12(mod\, 13),$$

$$3\cdot 6 = 18 \equiv 5(mod\, 13),$$

$$4\cdot 6 = 24 \equiv 11(mod\, 13),$$

$$5\cdot 6 = 30 \equiv 4(mod\, 13),$$

$$6\cdot 6 = 36 \equiv 10(mod\, 13),$$

ապա դիտարկվող մնացքների դասերում եղած փոքրագույն դրական թվերն են՝ 6, 12, 5, 11, 4 և 10 թվերը, որոնցից $\frac{p}{2}$-ից մեծ են՝ 12, 11 և 10 թվերը: Այսպիսով, $n = 3$ և համաձայն Գաուսի լեմմի՝ $\left(\frac{6}{13}\right) = (-1)^3 = -1$, այսինքն $x^2 \equiv 6(mod\, 13)$ բաղդատումը չունի ամբողջ լուծում:

Թեորեմ 10.5*: Եթե p-ն կենտ պարզ թիվ է, ապա*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{եթե } p \equiv 1(mod\, 8) \text{ կամ } p \equiv 7(mod\, 8), \\ -1, & \text{եթե } p \equiv 3(mod\, 8) \text{ կամ } p \equiv 5(mod\, 8) : \end{cases}$$

Ապացուցում: Համաձայն Գաուսի լեմմի՝ $\left(\dfrac{2}{p}\right) = (-1)^n$, որտեղ n-ը $[2]$, $[2\cdot 2]$, $[3\cdot 2]$, $\ldots$, $\left[\dfrac{(p-1)}{2}\cdot 2\right] \in \mathbb{Z}_p$ մնացքների դասերում եղած այն դրական և փոքրագույն ամբողջ թվերի քանակն է, որոնք մեծ են $\dfrac{p}{2}$-ից: Քանի որ $\dfrac{p-1}{2}\cdot 2 = p-1 < p$, ապա $[2]$, $[2\cdot 2]$, $[3\cdot 2]$, $\ldots$, $\left[\dfrac{(p-1)}{2}\cdot 2\right]$ մնացքների դասերում եղած փոքրագույն դրական ամբողջ թվերը հենց 2, $2\cdot 2$, $3\cdot 2$, $\ldots$, $\dfrac{(p-1)}{2}\cdot 2$ բնական թվերն են: Այդ պատճառով, բավական է այժմ պարզել, թե նշված մնացքների դասերի ներկայացուցիչներից քանիսն են մեծ $\dfrac{p}{2}$-ից: Հաշվի առնելով

$$k\cdot 2 < \frac{p}{2} \longleftrightarrow k < \frac{p}{4}$$

պայմանը, նախ կարող ենք ասել, որ 2, $2\cdot 2$, $3\cdot 2$, $\ldots$, $\dfrac{(p-1)}{2}\cdot 2$ բնական թվերի շարքում $\dfrac{p}{2}$-ից փոքր դրական թվերի քանակը կլինի հավասար այն ամենամեծ k բնական թվին, որը փոքր է $\dfrac{p}{4}$-ից, այսինքն $k = \left[\dfrac{p}{4}\right]$: Հետևաբար, նշված թվերի շարքում կպարունակվեն $\dfrac{p-1}{2} - \left[\dfrac{p}{4}\right]$ քանակի այնպիսի բնական թվեր, որոնք մեծ են $\dfrac{p}{2}$-ից: Այսպիսով, $n = \dfrac{p-1}{2} - \left[\dfrac{p}{4}\right]$ և համաձայն Գաուսի լեմմի, կունենանք՝

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left[\frac{p}{4}\right]}:$$

Թեորեմ 10.5-ի առաջին հավասարության ապացուցման համար, մնում է այժմ ապացուցել

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8} (mod\, 2)$$

բաղդատումը, որտեղ կենտ p պարզ թիվը բավարարում է հետևյալ պայմաններից որևէ մեկին՝

ա) $p \equiv 1 (mod\, 8)$,

բ) $p \equiv 7(mod\, 8)$,

գ) $p \equiv 3(mod\, 8)$,

դ) $p \equiv 5(mod\, 8)$:

Իրոք, եթե $p \equiv 1(mod\, 8)$, ապա $p = 8k+1$, $k \in \mathbb{Z}$ և

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] = \frac{8k+1-1}{2} - \left[\frac{8k+1}{4}\right] = 4k - 2k = 2k \equiv 0(mod\, 2),$$

$$\frac{p^2-1}{8} = \frac{(8k+1)^2-1}{8} = 8k^2 + 2k \equiv 0(mod\, 2),$$

այսինքն ա) դեպքում՝

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8}(mod\, 2) :$$

Նույն արդյունքին ենք հանգում նաև բ), գ) և դ) դեպքերում: Մասնավորապես,

$$\frac{p^2-1}{8} \equiv \begin{cases} 0(mod\, 2), & \text{եթե } p \equiv 1(mod\, 8) \text{ կամ } p \equiv 7(mod\, 8), \\ 1(mod\, 2), & \text{եթե } p \equiv 3(mod\, 8) \text{ կամ } p \equiv 5(mod\, 8), \end{cases}$$

որտեղից և բխում է թեորեմ 10.5-ի երկրորդ հավասարությունը: □

Հետևյալ արդյունքն առաջին անգամ նկատվել է Էյլերի (1772 թ.) և Լեժանդրի (1785 թ.) կողմից, սակայն խիստ ապացուցվել է Գաուսի (1796 թ.) կողմից: Գաուսից հետո, այն վերաապացուցվել է ավելի քան 190 տարբեր եղանակներով և ընդհանրացվել է Յակոբիի, Կումմերի, Դ. Հիլբերթի, Է. Արթինի, Հասսեի, Շաֆարևիչի, Վոստոկովի կողմից (F. Lemmermeyer, Reciprocity Laws, Springer-Verlag, Berlin, 2000)[15]:

Թեորեմ 10.6 (քառակուսային մնացքների փոխադարձության օրենքը): *Եթե p-ն և q-ն միմյանցից տարբեր կենտ պարզ թվեր են, ապա*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} 1, & \text{եթե } p \equiv 1(mod\, 4) \text{ կամ } q \equiv 1(mod\, 4), \\ -1, & \text{եթե } p \equiv 3(mod\, 4) \text{ և } q \equiv 3(mod\, 4) : \end{cases}$$

[15]Ծագումով հայազգի Էմիլ Արթինը (1898-1962) XX դարի ամենախոշոր մաթեմատիկոսներից մեկն է և համարվում է հանրահաշվի և թվերի տեսության դասականներից մեկը:

Հետևաբար, եթե $p \equiv 1(mod\, 4)$, *կամ* $q \equiv 1(mod\, 4)$, *ապա* $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$, *իսկ եթե* $p \equiv 3(mod\, 4)$ *և* $q \equiv 3(mod\, 4)$, *ապա* $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$*:*

Ապացուցում: Համաձայն հետևություն 10.1-ի,

$$\left(\frac{q}{p}\right) = (-1)^{N_1}, \quad \text{որտեղ} \quad N_1 = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{j \cdot q}{p}\right],$$

$$\left(\frac{p}{q}\right) = (-1)^{N_2}, \quad \text{որտեղ} \quad N_2 = \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{j \cdot p}{q}\right];$$

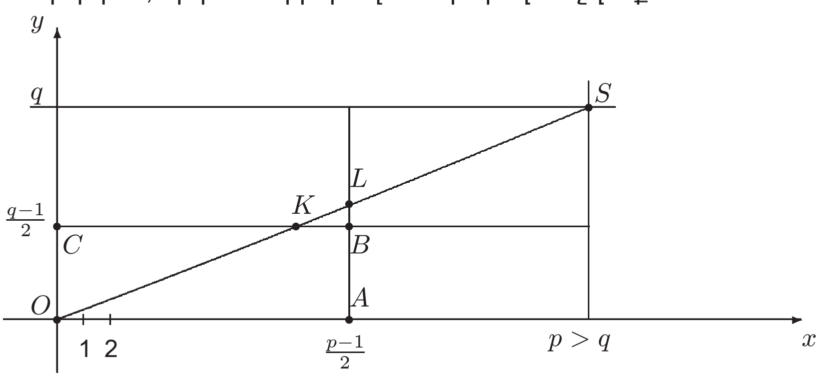
Հետևաբար,

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{N_2} \cdot (-1)^{N_1} = (-1)^{N_1+N_2} :$$

Այժմ ապացուցենք, որ

$$N_1 + N_2 = \frac{p-1}{2} \cdot \frac{q-1}{2} :$$

Այդ նպատակով (ենթադրելով $p > q$), ուղղանկյուն դեկարտյան համակարգում, երկու տարբեր եղանակներով հաշվենք $OABC$



ուղղանկյան ներսում գտնվող այն կետերի թիվը, որոնց կոորդինատները ամբողջ թվեր են (առանց OA և OC հատվածների վրա գտնվող նմանատիպ կետերի): Այդպիսի կետերը կոչվում են ամբողջ կետեր: Մի կողմից դրանց թիվը հավասար է՝ $\frac{p-1}{2}\cdot\frac{q-1}{2}$:

OS ուղղի անկյունային գործակիցն է՝ $\frac{q}{p}$: Հետևաբար, L կետի օրդինատը կլինի հավասար՝

$$y=\frac{q}{p}\cdot\frac{p-1}{2}=\frac{q}{2}-\frac{q}{2p}$$

և քանի որ $\frac{q}{p}<1$, ապա

$$\frac{q-1}{2}<\frac{q}{2}-\frac{q}{2p}<\frac{q}{2}<\frac{q+1}{2}=\frac{q-1}{2}+1,$$

այսինքն L կետի օրդինատը գտնվում է երկու հաջորդական ամբողջ թվերի միջև: Հետևաբար, ամբողջ կետերի թիվը OAL եռանկյան մեջ կլինի նույնը ինչ որ $OABK$ սեղանի մեջ: Այնուհետև նկատենք, որ բացի սկզբնակետից, OL ուղղի վրա չկան ուրիշ ամբողջ կետեր, որովհետև $x=1,2,\ldots,\frac{p-1}{2}$ դեպքում, $y=\frac{q}{p}x$-ը չի դառնում ամբողջ թիվ:

OAL եռանկյան մեջ եղած բոլոր որոնելի ամբողջ կետերի թիվը կլինի հավասար՝

$$\left[\frac{q\cdot 1}{p}\right]+\left[\frac{q\cdot 2}{p}\right]+\cdots+\left[\frac{q}{p}\cdot\frac{p-1}{2}\right]=\sum_{j=1}^{\frac{p-1}{2}}\left[\frac{qj}{p}\right]=N_1,$$

եթե հաշվումը կատարենք ըստ $x=1$, $x=2$, ..., $x=\frac{p-1}{2}$ ուղիղների: Համանման եղանակով, OKC եռանկյան մեջ եղած բոլոր որոնելի ամբողջ կետերի թիվը կլինի հավասար՝

$$\left[\frac{p\cdot 1}{q}\right]+\left[\frac{q\cdot 2}{q}\right]+\cdots+\left[\frac{p}{2}\cdot\frac{q-1}{2}\right]=\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{j\cdot p}{q}\right]=N_2:$$

Այսպիսով, հավասարեցնելով երկու տարբեր եղանակներով $OABC$ ուղղանկյան ներսում գտնվող ամբողջ կետերի թիվը, կունենանք՝

$$N_1+N_2=\frac{p-1}{2}\cdot\frac{q-1}{2}:$$

Վարժություններ և խնդիրներ

1. Դիցուք p-ն կենտ պարզ թիվ է, $a \in \mathbb{Z}$ ամբողջ թիվը չի բաժանվում p-ի վրա և դիցուք a-ն քառակուսային մնացք է ըստ p-ի: Ապացուցել, որ $-a$-ն ևս կլինի քառակուսային մնացք ըստ p-ի այն և միայն այն դեպքում, երբ $p \equiv 1(mod\, 4)$:

2. Դիցուք p-ն կենտ պարզ թիվ է և $a, b \in \mathbb{Z}$ ամբողջ թվերը չեն բաժանվում p-ի վրա: Ապացուցել, որ կամ բոլոր

$$x^2 \equiv a(mod\, p),$$

$$x^2 \equiv b(mod\, p),$$

$$x^2 \equiv ab(mod\, p)$$

բաղդատումներն օժտված են ամբողջ լուծումներով, կամ դրանցից միայն մեկն է օժտված ամբողջ լուծումով:

3. Դիցուք p-ն կենտ պարզ թիվ է, $a \in \mathbb{Z}$ ամբողջ թիվը չի բաժանվում p-ի վրա: Ապացուցել, որ $x^2 \equiv a(mod\, p^n)$, $n > 1$ բաղդատումը կունենա ամբողջ լուծում այն և միայն այն դեպքում, երբ a-ն քառակուսային մնացք է ըստ p-ի:

4. Ապացուցել, որ ցանկացած a ամբողջ և ցանկացած n բնական թվերի համար գոյություն ունեն անվերջ թվով այնպիսի p պարզ թվեր, որոնց նկատմամբ a-ն հանդիսանում է n-րդ աստիճանի մնացք:

5. Օգտվելով Էյլերի բանաձևից, հաշվել Լեժանդրի հետևյալ պայմանանշանները՝ $\left(\dfrac{3}{5}\right)$, $\left(\dfrac{-4}{11}\right)$, $\left(\dfrac{-6}{11}\right)$:

6. Օգտվելով Գաուսի լեմմից, հաշվել Լեժանդրի հետևյալ պայմանանշանները՝ $\left(\dfrac{5}{11}\right)$, $\left(\dfrac{12}{13}\right)$, $\left(\dfrac{2}{41}\right)$:

7. Դիցուք p-ն կենտ պարզ թիվ է և $a \in \mathbb{Z}$ ամբողջ թիվը չի բաժանվում p-ի վրա: Ապացուցել հետևյալ հավասարությունը՝

$$\left(\frac{a}{p}\right) + \left(\frac{2a}{p}\right) + \left(\frac{3a}{p}\right) + \cdots + \left(\frac{(p-1)a}{p}\right) = 0 :$$

8. Դիցուք p-ն կենտ պարզ թիվ է: Ապացուցել հետևյալ հավասարությունը՝

$$\left(\frac{1\cdot 2}{p}\right)+\left(\frac{2\cdot 3}{p}\right)+\left(\frac{3\cdot 4}{p}\right)+\cdots+\left(\frac{(p-2)(p-1)}{p}\right)=-1:$$

9. Դիցուք p-ն կենտ պարզ թիվ է, իսկ c ամբողջ թիվը քառակուսային մնացք է ըստ p հենքի: Ապացուցել, որ գոյություն ունեն երկու տարբեր p-ադիկ թվեր, որոնց քառակուսիները հավասար են c-ի:

10. Դիցուք p-ն պարզ թիվ է և $p \equiv 1 (mod\, 4)$: Ապացուցել հետևյալ հավասարությունը՝

$$\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right)=0:$$

11. Դիցուք n-ը մեկից մեծ կենտ բնական թիվ է օժտված $n = p_1^{k_1}\cdot p_2^{k_2}\cdots p_r^{k_r}$ կանոնական վերլուծությամբ և դիցուք $a\in\mathbb{Z}$, $(a,n) = 1$ (և հետևաբար նաև $(a,p_i) = 1$, $i = 1,2,\ldots,k$): a ամբողջ թվի **Յակոբիի պայմանշանը** ըստ n բնական թվի նշանակվում է $\left(\frac{a}{n}\right)$-ով և սահմանվում է հետևյալ կերպ՝

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p_1}\right)^{k_1}\cdot\left(\frac{a}{p_2}\right)^{k_2}\cdots\left(\frac{a}{p_r}\right)^{k_r},$$

որտեղ $\left(\frac{a}{p_i}\right)$ թիվը a ամբողջ թվի Լեժանդրի պայմանանշանն է ըստ p_i պարզ թվի:

Ապացուցել Յակոբիի պայմանանշանի հետևյալ հատկությունները.

(a) $\left(\frac{a}{n}\right)=\left(\frac{a'}{n}\right)$, եթե $a\equiv a'(mod\, n)$;

(b) $\left(\frac{1}{n}\right)=1$;

(c) $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$;

(d) $\left(\frac{a_1\cdot a_2\cdots a_s}{n}\right)=\left(\frac{a_1}{n}\right)\cdot\left(\frac{a_1}{n}\right)\cdots\left(\frac{a_s}{n}\right)$, որտեղ $(a_i,n)=1$, $i = 1,2,\ldots,s$;

(e) $\left(\dfrac{a_1\cdot a_2\cdots a_s}{n}\right)=\left(\dfrac{a_1}{n}\right)\cdot\left(\dfrac{a_1}{n}\right)\cdots\left(\dfrac{a_s}{n}\right)$, որտեղ $(a,n_i)=1$, $i=1,2,\ldots,s$;

(f) $\left(\dfrac{2}{n}\right)=(-1)^{\frac{n^2-1}{2}}$;

(g) $\left(\dfrac{m}{n}\right)\cdot\left(\dfrac{n}{m}\right)=(-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}$, որտեղ m,n-ը մեկից մեծ և կենտ փոխադարձաբար պարզ բնական թվեր են:

12. Եթե $\left(\dfrac{a}{n}\right)=-1$, ապա $x^2\equiv a(mod\, n)$ բաղդատումը չունի ամբողջ լուծում: Հետևաբար, եթե $x^2\equiv a(mod\, n)$ բաղդատումն ունի ամբողջ լուծում, ապա $\left(\dfrac{a}{n}\right)=1$:

Գ լ ու խ 11

ԹՎԵՐԻ ՏԵՍՈՒԹՅԱՆ ԿԻՐԱՌՈՒԹՅՈՒՆԸ ԳԱՂՏՆԱԳՐՈՒԹՅԱՆ ՄԵՋ (ԿՐԻՊՏՈԳՐԱՖԻԱՅՈՒՄ)

Համակարգչային (կոմպյուտերային) գիտության և նրա կիրառությունների ամենակարևոր խնդիրներից մեկը տեղեկատվության և դրանց փոխանակումների գաղտնիության ապահովումն է:

$A, B, \ldots$ կազմակերպությունների, ֆիրմաների, բանկերի, անձերի, $\ldots$ միջև տեղեկատվության գաղտնի փոխանակում (գաղտնի նամակագրություն, գաղտնագրություն) կազմակերպելու համար կարելի է վարվել հետևյալ կերպ: $A, B, \ldots$ կողմերը ընտրում են մի բավական մեծ p պարզ թիվ այնպես, որ $\varphi(p) = p-1$ բնական թվի վերլուծությունը պարզ արտադրիչների արտադրյալի հայտնի է, կամ դժվար չէ գտնել: Հետևաբար, կարելի է հաշվել և օգտվել նաև $\varphi(p-1)$ թվից, որտեղ φ-ն էյլերի ֆունկցիան է: Հաջորդ քայլում կողմերից յուրաքանչյուրը մյուսներից անկախ ընտրում է մի բնական թիվ, որը փոխադարձաբար պարզ է $\varphi(p) = p-1$ բնական թվի հետ: Դիցուք ընտրված բնական թվերն են՝ $a, b, \ldots$ Այնուհետև, A կողմը գտնում է α բնական թիվն այնպես, որ

$$a \cdot \alpha \equiv 1 (mod\, \varphi(p)) \quad 0 < \alpha < p-1; \tag{11.1}$$

Ըստ որում, ինչպես հայտնի է թեորեմ 3.3-ից, α-ն որոշվում է միարժեքորեն և համաձայն էյլերի թեորեմի (թեորեմ 9.1),

$$\alpha = a^{\varphi(p-1)-1} (mod\, (p-1)) :$$

Իրոք, համաձայն թեորեմ 1.1-ի՝

$$a^{\varphi(p-1)-1} = (p-1) \cdot q + \alpha, \quad 0 < \alpha < p-1$$

(այստեղ $\alpha \neq 0$, որովհետև $\left(a^{\varphi(p-1)-1}, p-1\right) = 1$, քանի որ $(a, p-1) = 1$ (հատկություն 3.2)): Հետևաբար,

$$a \cdot \alpha = a \left(a^{\varphi(p-1)-1} - (p-1)q \right) = a^{\varphi(p-1)} - a(p-1)q \equiv 1 (mod\, \varphi(p)),$$

որովհետև

$$a^{\varphi(p-1)} \equiv 1 (mod\, (p-1)),$$

$$a(p-1)q \equiv 0(mod\,(p-1)) :$$

Համանման եղանակով B կողմը գտնում է այնպիսի β բնական թիվ, որ

$$b \cdot \beta \equiv 1(mod\,\varphi(p)), \quad 0 < \beta < p-1 : \tag{11.2}$$

Այս դեպքում, a և α թվերը կոչվում են A կողմի **գաղտնի բանալիներ**, իսկ b և β թվերը՝ B կողմի գաղտնի բանալիներ (համապատասխանաբար առաջին և երկրորդ):

Դիցուք A կողմը որոշել է m բնական թիվն ուղարկել B կողմին, որտեղ $0 < m < p-1$ (հակառակ դեպքում m-ը տրոհվում է մասերի): Այդ նպատակով A կողմը m թիվը նախ գաղտնագրում է իր առաջին գաղտնի բանալիի միջոցով՝ հետևյալ կերպ. m թիվը փոխարինվում է m^a-ը p-ի վրա բաժանելուց ստացվող մնացորդով, այսինքն՝

$$m_1 = m^a(mod\,p) \tag{11.3}$$

թվով և ստացված m_1 թիվը հաղորդվում է B կողմին: B կողմը ստանալով m_1 թիվը, իր հերթին գաղտնագրում է այն իր առաջին գաղտնի բանալիի միջոցով, այսինքն m_1 թիվը փոխարինվում է

$$m_2 = m_1^b(mod\,p) \tag{11.4}$$

թվով և ստացված m_2 թիվը ետ է ուղարկվում A կողմին: A կողմը ստանալով m_2 թիվը, այժմ այն ծածկագրում է իր երկրորդ գաղտնի բանալիի միջոցով և արդյունքում ստանում է հետևյալ

$$m_3 = m_2^\alpha(mod\,p) \tag{11.5}$$

թիվը և նորից ստացված m_3 թիվն ուղարկում է B կողմին: Վերջինս ստանալով m_3 թիվը գաղտնազերծում է այն՝ իր երկրորդ գաղտնի բանալիի օգնությամբ, այսինքն ստանում է

$$m_4 = m_3^\beta(mod\,p) \tag{11.6}$$

թիվը, որը պարզվում է հավասար է հենց m բնական թվին:

Ապացուցում: Համաձայն (11.3), (11.4) և (11.5) հավասարությունների և Ֆերմայի փոքր թեորեմի (հետևություն 9.1)՝

$$m_4 \equiv m^{ab\alpha\beta}(mod\,p), \quad m^{ab\alpha\beta} \equiv m^{ab\alpha\beta(mod\,\varphi(p))}(mod\,p)$$

և, հետևաբար,

$$m_4 \equiv m^{ab\alpha\beta(mod\,\varphi(p))}(mod\,p):$$

Իրոք, դիցուք $r = ab\alpha\beta(mod\,(p-1))$, այսինքն $ab\alpha\beta = k(p-1)+r$, որտեղ $0 \leqslant r < p-1$: Այդ դեպքում՝

$$m^{ab\alpha\beta} = m^{k(p-1)+r} = m^{k(p-1)} \cdot m^r = \left(m^{p-1}\right)^k \cdot m^r \equiv m^r(mod\,p);$$

Մյուս կողմից, համաձայն (11.1) և (11.2) բաղդատումների՝

$$ab\alpha\beta \equiv 1(mod\,\varphi(p)),$$

կամ

$$1 = ab\alpha\beta(mod\,\varphi(p)):$$

Հետևաբար՝

$$m_4 \equiv m(mod\,p)$$

և, քանի որ $0 < m, m_4 < p$, ապա $|m_4 - m| < p$ և $m_4 - m = 0$, $m_4 = m$:

Գաղտնագրության շարադրված համակարգը (եղանակը) կոչվում է գաղտնագրություն՝ **առանց գաղտնի բանալիների հաղորդման** (իմացության, փոխանակման):

Գաղտնագրության հաջորդ եղանակը կոչվում է **բաց բանալիով** (կամ բանալիներով) գաղտնագրություն (W. Diffie, M.E. Hellman, *New directions in crytography*, IEEE Trans. Inform. Theory, vol. II-22, 11, 1976, p. 644–654; J.H. Ellis, *The possibility of secure non-secret digital encryption*, CESG Report, January 1970), որի էությունը կայանում է հետևյալում:

A և B կողմերից յուրաքանչյուրը, մեկը մյուսից անկախ, ընտրում է երկու մեծ պարզ թվեր, կազմում դրանց արտադրյալը, հայտնի բանաձևով (հատկություն 9.3) որոշում Էյլերի ֆունկցիայի արժեքը այդ արտադրյալի վրա, այնուհետև ընտրում այնպիսի մի բնական թիվ, որը փոխադարձաբար պարզ է ստացված Էյլերի ֆունկցիայի արժեքի հետ և փոքր է դրանից: Համառոտ՝

$$A:\ p_1, p_2,\ \ r_A = p_1 \cdot p_2,\ \ \varphi(r_A),\ \ (a, \varphi(r_A)) = 1,\ \ 0 < a < \varphi(r_A),$$

$$B:\ q_1, q_2,\ \ r_B = q_1 \cdot q_2,\ \ \varphi(r_B),\ \ (b, \varphi(r_B)) = 1,\ \ 0 < b < \varphi(r_B):$$

Այնուհետև, տպագրվում է այսպես կոչված հեռախոսային (համակարգչային կամ ինտերնետային) գրքույկ, որն ունի հետևյալ տեսքը՝

$$\boxed{\begin{array}{l} A:\ r_A,\ \ a \\ B:\ r_B,\ \ b \end{array}}\quad ,$$

որը հասանելի է բոլոր նրանց, ովքեր մտադրված են գաղտնի հաղորդագրություն ուղարկելու A, B կողմերին:

r_A և a բնական թվերը կոչվում են A կողմի **բաց բանալիներ**, իսկ r_B և b բնական թվերը՝ B կողմի բաց բանալիներ:

Հաջորդ քայլում, կողմերից յուրաքանչյուրը գտնում է իր գաղտնի բանալին՝ հետևյալ կերպ: A և B կողմերը գտնում են α և β գաղտնի թվերն այնպես, որ

$$a \cdot \alpha \equiv 1(mod\,\varphi(r_A)), \quad 0 < \alpha < \varphi(r_A),$$

$$b \cdot \beta \equiv 1(mod\,\varphi(r_B)), \quad 0 < \beta < \varphi(r_B) :$$

α և β թվերը կոչվում են համապատասխանաբար A և B կողմերի **գաղտնի բանալիներ**:

Դիցուք A կողմը որոշել է m գաղտնի թիվն ուղարկել B կողմին, որտեղ $0 < m < r_B$ և $(m, r_B) = 1$: Այդ նպատակով, նախ A-ն գաղտնագրում է m-ը՝ B-ի բաց բանալիի օգնությամբ, հետևյալ կերպ՝

$$m_1 = m^b(mod\,r_B) :$$

Այնուհետև, ստացված m_1 բնական թիվն ուղարկվում է B-ին: B-ն ստանալով m_1-ը, իր գաղտնի բանալիի օգնությամբ գաղտնազերծում է այն, այսինքն՝ ստանում է

$$m_2 = m_1^{\beta}(mod\,r_B)$$

թիվը, որը պարզվում է հավասար է հենց m բնական թվին:

Ապացույց: Քանի որ $(m, r_B) = 1$, ապա Էյլերի թեորեմի համաձայն (թեորեմ 9.1), կունենանք՝

$$m_2 \equiv m^{b\beta}(mod\,r_B) \equiv m^{b\beta(mod\,\varphi(r_B))}(mod\,r_B) :$$

Մյուս կողմից, քանի որ

$$1 \equiv b \cdot \beta(mod\,\varphi(r_B)),$$

ապա

$$1 = b \cdot \beta (mod\, \varphi(r_B));$$

Հետևաբար՝

$$m_2 \equiv m (mod\, r_B)$$

և, քանի որ $0 < m, m_2 < r_B$, ապա $|m_2 - m| < r_B$ և $m_2 - m = 0$, $m_2 = m$:

Քանի որ գաղտնագրության նշված եղանակում (ալգորիթմում) ուղարկող A կողմի տվյալները չեն կիրառվում (օգտագործվում), ապա ստացող B կողմը չի կարող տեղեկանալ թե ով է գաղտնի տեղեկատվության հեղինակը: Գաղտնագրության հետևյալ համակարգը, որը կոչվում է **էլեկտրոնային** (համակարգչային, ինտերնետային) **ստորագրություն**, արդեն զերծ է նշված թերությունից:

Գաղտնագրության նախորդ եղանակի հեռախոսային գրքույկը և A, B կողմերի համապատասխան α, β գաղտնի բանալիները ունենալու դեպքում, դիցուք A կողմը մտադիր է m գաղտնի թիվն ուղարկել B կողմին, որտեղ $m < r_A$ և $(m, r_A) = 1$:

Դիցուք՝ $0 < r_A \leqslant r_B$ և $(m^\alpha (mod\, r_A), r_B) = 1$:

A կողմը m-ը նախ գաղտնագրում է իր գաղտնի բանալիի օգնությամբ, ստանալով հետևյալ թիվը՝

$$m_1 = m^\alpha (mod\, r_A),$$

ապա՝ նաև B կողմի բաց բանալիի օգնությամբ՝

$$m_2 = m_1^b (mod\, r_B) :$$

Այնուհետև, B կողմը ստանալով m_2 բնական թիվը, գաղտնազերծում է այն երկու քայլով՝ հետևյալ կերպ: Նախ B-ն օգտվում է իր β գաղտնի բանալիից և ստանում հետևյալ թիվը՝

$$m_3 = m_2^\beta (mod\, r_B),$$

իսկ այնուհետև նաև A-ի բաց բանալիից՝ ստանալով

$$m_4 = m_3^a (mod\, r_A)$$

թիվը: Արդյունքում ստացվում է $m_4 = m$ ուղարկված թիվը:

Ապացուցում: Քանի որ $(m_1, r_B) = 1$, կունենանք՝

$$m_3 \equiv m_1^{b\beta} (mod\, r_B), \quad m_1^{b\beta} \equiv m_1^{b\beta (mod\, \varphi(r_B))} (mod\, r_B) :$$

Այսպիսով,

$$m_3 \equiv m_1^{b\beta(mod\,\varphi(r_B))}(mod\,r_B)\;:$$

Քանի որ, $b\beta(mod\,\varphi(r_B)) = 1$, ապա

$$m_3 \equiv m_1(mod\,r_B),$$

որտեղ $0 < m_3 < r_B$, $0 < m_1 < r_A \leqslant r_B$: Ուստի՝ $m_3 = m_1$:

Այնուհետև, քանի որ $m_3 = m_1$, և $(m, r_A) = 1$, ապա նորից էյլերի թեորեմի համաձայն՝

$$m_4 = m_1^a(mod\,r_A),\; m_1^a \equiv m^{a\alpha}(mod\,r_A),\; m^{a\alpha} \equiv m^{a\alpha(\mod \varphi(r_A))}(mod\,r_A)\;:$$

Հետևաբար, $m_4 \equiv m^{a\alpha(\mod \varphi(r_A))}(mod\,r_A)$, որտեղ $a\alpha(\mod \varphi(r_A)) = 1$:

Այսպիսով՝ $m_4 \equiv m(mod\,r_A)$, որտեղ $0 < m_4, m < r_A$: Ուստի՝ $m_4 = m$:

Վարժություններ և խնդիրներ

1. Դիցուք A և B բանկերը որոշել են ստեղծել (ունենալ) գաղտնի կապ՝ առանց գաղտնի բանալիների հաղորդման: Եվ դիցուք այդ նպատակով նրանք ընտրել են $p = 23$ պարզ թիվը: Այնուհետև, A բանկը ընտրել է $a = 5$ թիվը, իսկ B բանկը՝ $b = 7$ թիվը: Գտնել A և B բանկերի գաղտնի բանալիները:

2. Դիցուք A և B բանկերը որոշել են ստեղծել բաց բանալիներով գաղտնագրություն և դիցուք նրանք մեկը մյուսից անկախ ընտրել են $p_1 = 7$, $p_2 = 23$ և $q_1 = 11$, $q_2 = 17$ պարզ թվերի զույգերը: Այնուհետև, A-ն ընտրում է $a = 7$, իսկ B-ն՝ $b = 9$ թվերը: Գտնել համապատասխան հեռախոսային (ինտերնետային) գրքույկը և կողմերից յուրաքանչյուրի գաղտնի բանալին:

Գ լ ու խ 12

ԳԱՂԱՓԱՐ ԹՎԵՐԻ ՏԵՍԱ-ԲԱԶՄԱՅԻՆ ԵՎ ԱՔՍԻՈՄԱՅԻՆ ԿԱՌՈՒՑՈՒՄՆԵՐԻ ՎԵՐԱԲԵՐՅԱԼ

12.1. Տեսա-բազմային մոտեցում

Նախորդ վերնագրերում զարգացված թվերի տեսությունը չի կարող համարվել թվերի տեսության (կամ թվաբանության) խիստ կառուցում: Ինչը պայմանավորված է ոչ միայն բնական թվի հասկացության ճշգրիտ սահմանման բացակայությամբ, այլև դրանց գումարման և բազմապատկման գործողությունների սահմանումների բացակայությամբ, հետևաբար, նաև այդ գործողությունների տեղափոխական, զուգորդական, բաշխական և այլ հատկությունների լիարժեք հիմնավորումների բացակայությամբ: Այդ ամենի հետ առնչվելիս մենք հենվում էինք այն պատկերացումների վրա, որոնք ստեղծվում են մաթեմատիկայի դպրոցական դասընթացից կամ առօրյա կյանքից:

Բնական թվի սահմանման պարզագույն եղանակներից մեկն ունի տեսա-բազմային բնույթ և առաջարկվել է Գ. Ֆրեգեի կողմից, XIX դարի վերջին՝ որպես վերջավոր բազմության հզորություն: Ըստ որում, վերջավոր է կոչվում այն բազմությունը, որը հավասարազոր չէ իրենից տարբեր իր որևէ ենթաբազմությանը: Մասնավորապես, դատարկ բազմությունը կլինի վերջավոր: Դատարկ բազմության հզորությունն ընդունվում է որպես «զրո» բնական թիվ և նշանակվում է 0-ով, մեկ տարրանի ցանկացած բազմության հզորությունն ընդունվում է որպես «մեկ» բնական թիվ և նշանակվում է 1-ով, երկու տարրանի ցանկացած բազմության հզորությունն ընդունվում է որպես «երկու» բնական թիվ և նշանակվում է 2-ով, և այսպես շարունակ:

Ենթադրվում է, որ ցանկացած երկու վերջավոր բազմությունների համար գոյություն ունի դրանցից որևէ մեկը մյուսի մեջ տանող ինյեկտիվ (ներդրող) արտապատկերում:

Դիցուք $[A]$-ն A վերջավոր բազմության հզորությունն է: Երկու $m = [A]$ և $n = [B]$ բնական թվեր կոչվում են հավասար և գրվում է $m = n$, եթե հավասարազոր են համապատասխան A և B բազմությունները՝ $A \sim B$, այսինքն գոյություն ունի որևէ $\alpha : A \to B$ բիեկտիվ (փոխմիարժեք) արտապատկերում: Հակառակ դեպքում, m և n բնական թվերը կոչվում են **ոչ հավասար** և գրվում է $m \neq n$: Բիեկտիվ արտապատկերումների հատկություններից բխում է, որ բնական թվերի հավասարության սահմանված հասկացությունն օժտված է համարժեքության երեք հատկություններով՝

ա) $m = m$ ցանկացած m բնական թվի համար (առինքնություն կամ ռեֆլեքսիվություն);

բ) $m = n \to n = m$ (համաչափություն կամ սիմետրիկություն);

գ) $m = n,\ n = k \to m = k$ (փոխանցականություն կամ տրանզիտիվություն):

$m = [A]$ բնական թիվը կոչվում է **փոքր** $n = [B]$ բնական թվից և գրվում է $m < n$, եթե գոյություն ունի այնպիսի $\alpha : A \to B$ ինյեկտիվ արտապատկերում, որը բիեկտիվ չէ, այսինքն գոյություն ունի այնպիսի $B' \subseteq B$ ենթաբազմություն, որ $B' \neq B$ և $A \sim B'$: Եթե $m < n$, ապա n-ը կոչվում է **մեծ** m-ից[16]: Այնուհետև, $m = [A]$ բնական թիվը կոչվում է **փոքր** կամ հավասար $n = [B]$ բնական թվից և գրվում է $m \leqslant n$, եթե $m < n$ կամ $m = n$, այսինքն եթե գոյություն ունի որևէ $\alpha : A \to B$ ինյեկտիվ արտապատկերում:

Սահմանված «$\leqslant$» հարաբերությունը բավարարում է մասնակի կարգի սահմանման բոլոր երեք պայմաններին, իսկ «$<$» հարաբերությունը բավարարում է փոխանցականության պայմանին: «$\leqslant$» հարաբերության հակասիմետրիկությունը բխում է Կանտոր-Շրյոդեր-Բեռնշտայնի թեորեմից (թեորեմ 0.17):

Եթե $m = [A]$ և $n = [B]$, ապա սահմանվում է՝ $m \cdot n = [A \times B]$, իսկ եթե նաև $A \cap B = \emptyset$, ապա սահմանվում է՝ $m + n = [A \cup B]$: $m \cdot n$-ը կոչվում է m և n բնական թվերի **արտադրյալ**, իսկ $m + n$-ը՝ դրանց **գումար**: m-ը և n-ը կոչվում են $m \cdot n$ արտադրյալի արտադրիչներ, իսկ $m + n$ գումարի՝ գումարելիներ: Բնական թվերի սահմանված արտադրյալը և գումարը ըստ արտադրիչների որոշվում են միարժեքորեն: Իրոք, եթե $A \sim A'$ և $B \sim B'$, ապա $A \times B \sim A' \times B'$, իսկ եթե նաև $A \cap B = \emptyset$ և $A' \cap B' = \emptyset$, ապա $A \cup B \sim A' \cup B'$: Բնական թվերի գումարի և արտադրյալի տրված սահմանման համաձայն՝

$$[A \cup B] = [A] + [B], \quad \text{եթե} \quad A \cap B = \emptyset,$$

[16] Ենթադրվում է, որ գոյություն ունի $\alpha : \emptyset \to B$ ինյեկտիվ արտապատկերում, որը $B = \emptyset$ դեպքում ենթադրվում է բիեկտիվ:

$$[A \times B] = [A] \cdot [B] :$$

Քանի որ՝

$$A \cup \emptyset = A,$$

$$A \cup B = B \cup A,$$

$$A \cup (B \cup C) = (A \cup B) \cup C,$$

$$A \times (B \cup C) = (A \times B) \cup (A \times C),$$

$$A \times B \sim B \times A,$$

$$A \times (B \times C) \sim (A \times B) \times C,$$

$$A \times \{b\} \sim A,$$

$$A \times \emptyset = \emptyset,$$

ապա՝

$$m + 0 = m,$$

$$m + n = n + m,$$

$$m + (n + k) = (m + n) + k,$$

$$m(n + k) = mn + mk,$$

$$m \cdot n = n \cdot m,$$

$$m \cdot (n \cdot k) = (m \cdot n) \cdot k,$$

$$m \cdot 1 = m,$$

$$m \cdot 0 = 0$$

ցանկացած m, n, k բնական թվերի համար:

Դիցուք $m = [A]$ և $n = [B]$ բնական թվերի համար $m \leqslant n$, այսինքն գոյություն ունի որևէ $\alpha : A \to B$ ինյեկտիվ արտապատկերում: Այդ դեպքում, սահմանվում է n և m բնական թվերի տարբերությունը, հետևյալ կերպ՝ $n - m = [B \setminus \alpha(A)]$: Տրված n, m բնական թվերի $n - m$ տարբերությունը որոշվում է միարժեքորեն, եթե այն գոյություն ունի (այսինքն, եթե $m \leqslant n$): Իրոք, եթե տրված են A, B, A' և B' վերջավոր բազմությունները և $\alpha : A \to B$, $\beta : A' \to B'$ ինյեկտիվ արտապատկերումները, որտեղ $A \sim A'$ և $B \sim B'$, ապա

$$B \setminus \alpha(A) \sim B' \setminus \beta(A') :$$

Եթե $m \leqslant n$ և $n-m=k$, ապա n-ը կոչվում է նվազելի, m-ը՝ հանելի, իսկ k-ն՝ տարբերություն և $n = m + k$: Իրոք, եթե $m = [A]$, $n = [B]$, $k = [B \setminus \alpha(A)]$, որտեղ $\alpha : A \to B$ արտապատկերումն ինյեկտիվ է, ապա

$$B = \alpha(A) \cup (B \setminus \alpha(A)),$$

որտեղ $\alpha(A) \cap (B \setminus \alpha(A)) = \emptyset$, $A \sim \alpha(A)$ և հետևաբար՝

$$n = [B] = [\alpha(A) \cup (B \setminus \alpha(A))] =$$

$$= [\alpha(A)] + [(B \setminus \alpha(A))] = [A] + [B \setminus \alpha(A)] = m + k :$$

Այսինքն, եթե $m \leqslant n$, ապա $(n-m)+m = n$:

Ակնհայտ է նաև, որ ցանկացած m, n բնական թվերի համար $m \leqslant m+n$ և $(m+n)-n = m$: Եթե $n \neq 0$, ապա $m < m+n$; Մասնավորապես, նշանակելով $m' = m+1$ և անվանելով նրան m-ի հաջորդը, կունենանք $m < m'$ և

$$m' = n' \longrightarrow m = n :$$

Ըստ որում, 0-ն չի հանդիսանում որևէ բնական թվի հաջորդը, իսկ ցանկացած $n \neq 0$ բնական թիվ հանդիսանում է որևէ բնական թվի հաջորդը՝ $n = (n-1)+1 = (n-1)'$, որտեղ $n \geqslant 1$:

Այսպիսով, $0 < 1 < 2 < 3 < \ldots < n < n+1 < \ldots$ և, հետևաբար, սահմանված բնական թվերը կարելի է դասավորել առանցքի վրա՝ ըստ աճման: Ցանկացած երկու m և n բնական թվերի համար տեղի ունի հետևյալ առնչություններից միայն մեկը՝ $m < n$, $m = n$, $m > n$: Բնական թվերի յուրաքանչյուր ոչ դատարկ K ենթաբազմություն կունենա փոքրագույն տարր, այսինքն՝ այնպիսի $k_0 \in K$ տարր, որը փոքր է կամ հավասար K-ի բոլոր թվերից: Հետևաբար, սահմանված բնական թվերի համար տեղի կունենա նաև վերհանգման սկզբունքը:

12.2. Աքսիոմային մոտեցում

Թվաբանության խիստ կառուցման հետևյալ աքսիոմային (աքսիոմատիկ) եղանակը՝ բազմության և արտապատկերման գաղափարների միջոցով, տրվել են (XIX դարի վերջին, XX դարի սկզբին) Պեանոյի (1891թ.) և Դեդեկինդի (1901թ.) կողմից:

Կամայական ոչ դատարկ P բազմությունը կոչվում է բնական թվերի բազմություն, եթե տրված է մի $\sigma : P \to P$ արտապատկերում (ֆունկցիա), որը բավարարում է հետևյալ երեք պայմաններին (Պեանոյի աքսիոմներին).

(P_1) $\sigma(m) = \sigma(n) \to m = n$, որտեղ $m, n \in P$ (այսինքն σ-ն ինյեկտիվ է);

(P_2) գոյություն ունի P-ի այնպիսի տարր, որը նշանակվում է 0-ով (և կարդացվում է «զրո») և որի համար գոյություն չունի այնպիսի $n \in P$, որ $0 = \sigma(n)$ (այսինքն 0-ն չունի նախապատկեր);

(P_3) (Վերիանգման աքսիոմ): Եթե $M \subseteq P$ ենթաբազմությունն օժտված է հետևյալ երկու հատկություններով՝

ա) $0 \in M$,

բ) $n \in M \to \sigma(n) \in M$,

ապա $M = P$:

Այդ դեպքում, P-ի տարրերն անվանվում են **բնական թվեր**, իսկ σ արտապատկերումը՝ հաջորդին անցնելու գործողություն, նշանակելով $\sigma(n) = n'$ (ըստ որում n'-ը կոչվում է n-ի հաջորդը):

Զրոյի միակությունը բխում է հետևյալ հատկությունից:

Հատկություն 12.1: *Զրոյից տարբեր P-ի յուրաքանչյուր տարր հանդիսանում է նրա որևէ տարրի հաջորդը:*

Ապացուցում: Եթե M-ը կազմված է 0-ից և P-ի բոլոր այն տարրերից, որոնցից յուրաքանչյուրը P-ի որևէ տարրի հաջորդն է, ապա M-ը բավարարում է (P_3)-ի ա) և բ) պայմաններին և, հետևաբար, $M = P$; Այսպիսով, P-ի յուրաքանչյուր տարր կամ հավասար է 0-ի, կամ նրա որևէ տարրի հաջորդն է: □

Զրոյի միակությունը հաստատելուց հետո, P-ի մեջ ներմուծվում են «մեկը» (նշանակումը՝ 1), «երկուսը» (նշանակումը՝ 2), «երեքը» (նշանակումը՝ 3) և այլ բնական թվերը՝ հետևյալ կերպ.

$$\begin{aligned}
&1 = 0', \\
&2 = 1' = (0')' = 0'', \\
&3 = 2' = (0'')' = 0''', \\
&\quad\vdots
\end{aligned}$$

Այսպիսով, ստանում ենք $0, 1, 2, 3, \ldots$ բնական թվերի շարքը, որոնցով սպառվում է P-ն: Իրոք՝

$$M = \{0, 1, 2, 3, \ldots\} \subseteq P,$$

և M-ը բավարարում է (P_3) աքսիոմի ա) և բ) պայմաններին և, հետևաբար, $M = P$:

Վերհանգման աքսիոմից անմիջապես բխում է նաև վերհանգման հետևյալ սկզբունքը (եղանակը). n-ից կախված $A(n)$ պնդումը ճիշտ է բոլոր $n \in P$ արժեքների դեպքում, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա$_1$) $A(n)$ պնդումը ճիշտ է $n = 0$ դեպքում;

բ$_1$) $A(n)$-ի ճիշտ լինելուց բխում է $A(n')$-ի ճիշտ լինելը՝ ցանկացած $n \in P$ տարրի դեպքում:

Իրոք, եթե

$$M = \{n \in P \mid A(n)\text{-ը ճիշտ է}\},$$

ապա M-ը բավարարում է (P_3) աքսիոմի ա) և բ) պահանջներին և, հետևաբար, $M = P$, այսինքն՝ $A(n)$ պնդումը ճիշտ է բոլոր $n \in P$ արժեքների համար:

Այս դեպքում վերհանգման սկզբունքը (եղանակը) կոչվում է նաև վերհանգման սկզբունք (եղանակ) ըստ n-ի, կամ համառոտ՝ վերհանգում ըստ n-ի:

Օգտվելով (P_1) – (P_3) աքսիոմներից, բնական թվերի P բազմության մեջ ներմուծվում են գումարման և բազմապատկման գործողությունները, «փոքրի» և «մեծի» գաղափարները և ապացուցվում են բոլոր այն հիմնական հատկությունները, որոնք հայտնի են թվաբանությունից (դպրոցական դասընթացից):

Սկսենք գումարի և արտադրյալի (բազմապատկման) սահմանումներից՝

$$\begin{aligned} a+0 &= a, & a\cdot 0 &= 0,\\ a+b' &= (a+b)', & a\cdot b' &= ab+a \end{aligned}$$

ցանկացած $a, b \in P$ տարրերի համար:

Օրինակներ: 1) $2+2 = 2+1' = (2+1)' = (2+0') = ((2+0)')' = (2') = 3' = 4$;

2) $5+4 = 5+3' = (5+3)' = (5+2')' = ((5+2)')' = ((5+1')')' = (((5+1)')')' = (((5+0')')')' = ((((5+0)')')')' = (((5')')')' = ((6')')' = (7')' = 8' = 9$;

3) $a' = (a+0)' = a+0' = a+1$:

4) Վերհանգման եղանակով ապացուցվում է $a' = 1 + a$ հավասարությունը: Հետևաբար, $a + 1 = 1 + a$:

Այստեղ տեղին է վերհիշել հետևյալ հայտնի խոսքերը, որ «Եգիպտացիների և Բաբելոնցիների կողմից ամբողջ, ռացիոնալ և իռացիոնալ թվերի ներմուծումից ավելի քան 6000 տարի հետո, մաթեմատիկոսները 19-րդ դարի 90-ական թվականներին վերջապես ապացուցեցին, որ $2 + 2 = 4$»:

Վերհանգման եղանակով կարելի է նաև ապացուցել սահմանված գումարման և բազմապատկման գործողությունների գոյությունը և միակությունը:

Հատկություն 12.2: *Բնական թվերի գումարը զուգորդական է և տեղափոխական, այսինքն՝*

$$a + (b + c) = (a + b) + c \quad \text{(զուգորդականություն)}$$

և

$$a + b = b + a \quad \text{(տեղափոխականություն)}$$

ցանկացած $a, b, c \in P$ տարրերի համար:

Ապացուցում: Ապացուցենք զուգորդականությունը, դիտելով նրան որպես հատկություն՝ կախված c փոփոխականից: Սևեռենք կամայական $c \in P$ տարր և $A(c)$-ով նշանակենք հետևյալ հատկությունը

$$\forall a \in P,\ \forall b \in P \quad (a + (b + c) = (a + b) + c) :$$

Պահանջվում է ապացուցել, որ $A(c)$-ն ճիշտ է ցանկացած $c \in P$ տարրի համար: Ապացուցման համար կիրառենք վերհանգման սկզբունքը ըստ c-ի:

$A(0)$-ն ճիշտ է, որովհետև

$$a + (b + 0) = (a + b) + 0 :$$

Այժմ ենթադրենք, թե $A(c)$-ն ճիշտ է, այսինքն ցանկացած $a, b \in P$ տարրերի համար

$$a + (b + c) = (a + b) + c$$

և ապացուցենք, որ ճիշտ է նաև $A(c')$-ը, այսինքն՝

$$a + (b + c') = (a + b) + c'$$

կամայական $a, b \in P$ տարրերի դեպքում:

Իրոք,

$$a + (b + c') = a + (b + c)' = (a + (b + c))' = ((a + b) + c)' = (a + b) + c';$$

Զուգորդականությունն ապացուցված է: Ապացուցենք տեղափոխականությունը:

Նախ ապացուցենք տեղափոխականությունը $b = 0$ դեպքում: Այդ պատճառով

$$a + 0 = 0 + a$$

հատկությունը նշանակենք $B(a)$-ով և կիրառենք վերհանգման սկզբունքը՝ ըստ a-ի: $B(0)$-ն ճիշտ է, որովհետև $0 + 0 = 0 + 0$; Ենթադրելով $B(a)$-ն ճիշտ, ապացուցենք, որ այդ դեպքում ճիշտ կլինի նաև $B(a')$-ը.

$$a' + 0 = a' = (a + 0)' = (0 + a)' = 0 + a' :$$

Այժմ սևեռենք կամայական $b \in P$ տարր և

$$\forall a \in P \quad (a + b = b + a)$$

հատկությունը նշանակենք $C(b)$-ով: $C(0)$-ն ինչպես տեսանք ճիշտ է: Ենթադրելով, որ $C(b)$-ն ճիշտ է, ապացուցենք $C(b')$-ի ճիշտ լինելը.

$$a + b' = (a + b)' = (b + a)' = b + a' = b + (1 + a) = (b + 1) + a =$$

$$= (b + 0') + a = (b + 0)' + a = b' + a$$

ցանկացած $a \in P$ տարրի համար:

Հատկություն 12.3*: Բնական թվերի արտադրյալը և գումարը կապված են ձախ և աջ բաշխական հատկություններով, այսինքն՝*

$$a(b + c) = ab + ac, \quad (\text{ձախ բաշխականություն})$$

$$(a + b)c = ac + bc \quad (\text{աջ բաշխականություն})$$

կամայական $a, b, c \in P$ տարրերի համար:

Ապացույց: Եթե $A(c)$-ով նշանակենք

$$\forall a \in P,\ \forall b \in P \quad (a(b+c) = ab + ac)$$

հատկությունը, որտեղ $c \in P$, ապա $A(0)$-ն, ակնհայտորեն, կլինի ճիշտ: Ենթադրելով $A(c)$-ի ճիշտ լինելը, այժմ ստանանք նաև $A(c')$-ի ճիշտ լինելը.

$$a(b+c') = a(b+c)' = a(b+c)+a = (ab+ac)+a = ab+(ac+a) = ab+ac'$$

ցանկացած $a, b \in P$ տարրերի համար:

Համանման եղանակով ապացուցվում է նաև աջ բաշխականությունը: □

Հատկություն 12.4*: Բնական թվերի արտադրյալը զուգորդական է և տեղափոխական, այսինքն՝*

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$

և

$$a \cdot b = b \cdot a$$

կամայական $a, b, c \in P$ տարրերի համար:

Ապացույց: Դիցուք $c \in P$: Եթե $A(c)$-ով նշանակենք

$$\forall a \in P,\ \forall b \in P \quad (a \cdot (b \cdot c) = (a \cdot b) \cdot c)$$

հատկությունը, ապա $A(0)$-ն, ակնհայտորեն, կլինի ճիշտ է: Ենթադրելով $A(c)$-ի ճիշտ լինելը, ստանանք նաև $A(c')$-ի ճիշտ լինելը (օգտվելով հատկություն 12.3-ից).

$$a \cdot (b \cdot c') = a \cdot (b \cdot c + b) = a(bc) + ab = (ab)c + ab = (ab) \cdot c'$$

ցանկացած $a, b \in P$ տարրերի համար:

Ապացուցենք արտադրյալի տեղափոխականությունը: Նախ վերհանգման եղանակով հեշտությամբ ստուգվում են $a \cdot 0 = 0 \cdot a$ և $a \cdot 1 = 1 \cdot a$ հավասարությունները: Այնուհետև, եթե $B(b)$-ով նշանակենք

$$\forall a \in P \quad (a \cdot b = b \cdot a)$$

հատկությունը, որտեղ $b \in P$, ապա $B(0)$-ն ճիշտ է, իսկ $B(b)$-ի ճիշտ լինելուց բխում է նաև $B(b')$-ի ճիշտ լինելը, որովհետև հաշվի առնելով աջ բաշխականությունը, կունենանք՝

$$a \cdot b' = ab + a = ab + a \cdot 1 = ba + 1 \cdot a = (b+1)a = b' \cdot a$$

ցանկացած $a \in P$ տարրի համար: Այսպիսով, ըստ վերհանգման սկզբունքի, $B(b)$-ն ճիշտ է կամայական $b \in P$ տարրի համար: Ուստի, արտադրյալի տեղափոխականությունը ևս ապացուցված է: □

Այժմ անցնենք «փոքրի» և «մեծի» հասկացություններին:

Եթե a և b բնական թվերի համար գոյություն ունի այնպիսի $k \neq 0$ բնական թիվ, որ $b = a + k$, ապա կասենք, որ a-ն փոքր է b-ից և կգրենք՝ $a < b$: a-ն կոչվում է փոքր կամ հավասար b-ից և գրվում է $a \leqslant b$, եթե $a < b$ կամ $a = b$: Եթե $a < b$, ապա b-ն կոչվում է մեծ a-ից և գրվում է նաև $b > a$, իսկ եթե $a \leqslant b$, ապա b-ն կոչվում է մեծ կամ հավասար a-ից և գրվում է նաև $b \geqslant a$:

Եթե $a \neq 0$, ապա $a > 0$, որովհետև $a = 0 + a$ (այստեղ $k = a$): Ակնհայտ է նաև, որ $n < n + 1 = n'$ և, հետևաբար, $0 < 1 < 2 < 3 < \cdots < n < n + 1 < \cdots$:

Եթե $a \geqslant b$, ապա a և b բնական թվերի **տարբերություն** (հանում) է կոչվում այն $k \in P$ բնական թիվը, որի համար $a = b + k$: Հետևյալ հատկությունից բխում է երկու բնական թվերի տարբերության միակությունը (եթե այն գոյություն ունի):

Հատկություն 12.5:
$$a + c = b + c \to a = b,$$

որտեղ $a, b, c \in P$*:*

Ապացուցում: Կիրառենք վերհանգման եղանակը հետևյալ $A(c)$ հատկության նկատմամբ՝

$$\forall a \in P,\ \forall b \in P \quad (a + c = b + c \to a = b):$$

Ակնհայտորեն $A(0)$-ն ճիշտ է, որովհետև

$$a + 0 = b + 0 \to a = b:$$

Ենթադրելով $A(c)$-ի ճիշտ լինելը, ապացուցենք $A(c')$-ի ճիշտ լինելը.

$$a + c' = b + c' \to (a + c)' = (b + c)' \to a + c = b + c \to a = b; \qquad \square$$

Հատկություն 12.5-ից բխում է նաև, որ $a < a$ անհավասարությունը տեղի չունի, եթե $a \in P$:

Եթե $a \geqslant b$, ապա a և b բնական թվերի միարժեքորեն որոշվող տարբերությունը նշանակվում է $a - b$ ձևով: Այսպիսով՝ $b + (a - b) = a$: Մասնավորապես, $a - a = 0$:

Եթե $a \neq 0$, ապա $a > 0$ և համաձայն հատկություն 12.1-ի, գոյություն ունի այնպիսի $b \in P$, որ $b' = a$: Այսպիսով՝ $b + 1 = a$ և հետևաբար $a \geqslant 1$ և $a - 1 = b \geqslant 0$:

Եթե $a < b$, ապա $b = a + k$, $k \neq 0$, որտեղից $k - 1 \geqslant 0$ և $b = a + (1 + (k - 1)) = (a + 1) + (k - 1)$, այսինքն $a' = a + 1 \leqslant b$:

Հատկություն 12.6*:*

(1) Եթե $a < b$ և $b < c$, ապա $a < c$; (փոխանցականություն)

(2) Եթե $a \leqslant b$ և $b \leqslant c$, ապա $a \leqslant c$; (փոխանցականություն)

(3) Եթե $a \leqslant b$ և $b \leqslant a$, ապա $a = b$; (հակասիմետրիկություն կամ հակահամաչափություն)

(4) $a \leqslant a$ ցանկացած $a \in P$ տարրի համար: (առինքնություն)

Այսպիսով, «$\leqslant$» հարաբերությունը մասնակի կարգ >՝ որոշված P բազմության վրա:

Ապացուցում: (1) Եթե $a < b$, ապա $b = a + k$, որտեղ $k \neq 0$: Եթե $b < c$, ապա $c = b + s$, որտեղ $s \neq 0$: Հետևաբար, $c = (a + k) + s = a + (k + s)$, որտեղ $k + s \neq 0$: Իրոք, եթե $s \neq 0$, ապա համաձայն հատկության 12.1-ի գոյություն ունի այնպիսի $t \in P$, որ $t' = s$: Հետևաբար՝

$$k + s = k + t' = (k + t)' \neq 0$$

(համաձայն (P_2) աքսիոմի):

(2)-ը և (4)-ը ակնհայտ են: Ապացուցենք (3)-ը:

Եթե $a = b + k$ և $b = a + s$, ապա $a = (a + s) + k = a + (s + k)$: Այստեղից, համաձայն հատկություն 12.5-ի՝ $s + k = 0$, որտեղից բխում է $s = 0$ և $k = 0$ (որովհետև հակառակ դեպքում, ինչպես և քիչ առաջ, կունենայինք $s + k \neq 0$): Այսպիսով՝ $a = b$: □

Հատկություն 12.7*: Կամայական a և b բնական թվերի համար տեղի ունի հետևյալ առնչություններից միայն մեկը՝ $a < b$, $a = b$, $a > b$:*

Ապացուցում: Հատկություն 12.5-ից և 12.6-ից բխում է, որ նշված առնչություններից որևէ երկուսը միաժամանակ տեղի ունենալ չեն կարող: Այժմ ապացուցենք, որ տեղի կունենա նշված առնչություններից որևէ մեկը: $A(b)$-ով նշանակենք հետևյալ հատկությունը՝

$$\forall a \in P \ \ (a = b \text{ կամ } \exists k \in P\backslash\{0\}(a + k = b) \text{ կամ } \exists s \in P\backslash\{0\}(a = b + s))\,,$$

որտեղ $b \in P$: Այժմ վերհանգման եղանակով ապացուցենք, որ $A(b)$-ն ճիշտ է ցանկացած $b \in P$ տարրի համար: $A(0)$-ն ճիշտ է, որովհետև, եթե $b = 0$, ապա ցանկացած a-ի համար կամ $a = 0$, կամ $a \neq 0$: Եթե $a \neq 0$, ապա $a = 0 + s$, որտեղ $s = a \neq 0$: Հետևաբար, եթե $b = 0$, ապա տեղի ունի $A(b)$-ի առաջին կամ երրորդ առնչությունը: Այժմ ենթադրելով $A(b)$-ի ճիշտ լինելը, ապացուցենք $A(b')$-ի ճիշտ լինելը: Իրոք, եթե $a = b$, ապա $a + 1 = a' = b'$ (տեղի ունի $A(b')$-ի երկրորդ առնչությունը): Եթե $a+k = b$, ապա $(a+k)' = b'$ և հետևաբար $a'+k = b'$, այսինքն $a + (1 + k) = b'$ (տեղի ունի $A(b')$-ի երկրորդ առնչությունը): Իսկ եթե $a = b + s$, ապա $a' = (b + s)' = (s + b)' = s + b' = b' + s$; Այստեղ հնարավոր են հետևյալ ենթադեպքերը: ա) $s = 1$; Այս դեպքում համաձայն (P_1) աքսիոմի կունենանք՝ $a = b'$ (տեղի ունի $A(b')$-ի առաջին առնչությունը): բ) $s \neq 1$; Այս դեպքում, համաձայն հատկություն 12.1-ի գոյություն կունենա այնպիսի $t \neq 0$, որ $t' = s$: Հետևաբար՝

$$a' = b' + s = b' + t' = (b' + t)'$$

և համաձայն (P_1) աքսիոմի՝ $a = b' + t$, որտեղ $t \neq 0$ (տեղի ունի $A(b')$-ի երրորդ առնչությունը): □

Հետևություն 12.1: *Կամայական a և b բնական թվերի համար կամ $a \leqslant b$ կամ $b \leqslant a$:* □

Հատկություն 12.8: *Բնական թվերի P բազմության յուրաքանչյուր ոչ դատարկ $K \subseteq P$ ենթաբազմություն ունի փոքրագույն տարր, այսինքն այնպիսի $k_0 \in K$ տարր, որը փոքր է կամ հավասար K-ի բոլոր տարրերից: (Այլ կերպ՝ բնական թվերի բազմությունը լիովին կարգավորված բազմություն է:)*

Ապացուցում: Ենթադրելով հակառակը, ստանանք հակասություն: Դիցուք ոչ դատարկ $K \subseteq P$ ենթաբազմությունը չունի փոքրագույն տարր: Այդ դեպքում, հետևյալ հատկությունը

$$a \in K \to b \leqslant a$$

նշանակելով $A(b)$-ով, որտեղ $b \in P$, վերհանգման եղանակով ապացուցենք, որ $A(b)$-ն ճիշտ է բոլոր $b \in P$ տարրերի համար: Իրոք, $A(0)$-ն ակհայտորեն ճիշտ է: Ենթադրելով $A(b)$-ի ճիշտ լինելը, ապացուցենք $A(b')$-ի ճիշտ լինելը: քանի որ $A(b)$-ն ենթադրել ենք ճիշտ, ապա

$$a \in K \to b \leqslant a;$$

Հետևաբար $b \notin K$ և $b \neq a$, հակառակ դեպքում b-ն կլիներ K-ի փոքրագույն տարրը: Ուստի

$$a \in K \to b < a,$$

հետևաբար

$$a \in K \to b' = b + 1 \leqslant a$$

և $A(b')$-ը ճիշտ է: Այսպիսով $A(b)$-ն ճիշտ է բոլոր $b \in P$ տարրերի համար:

Այժմ ստանանք հակասությունը: Քանի որ $K \neq \emptyset$, ապա գոյություն ունի $a \in K : A(b)$ բանաձևի մեջ վերցնելով $b = a' = a + 1$ կունենանք՝

$$a \in K \to a + 1 \leqslant a,$$

այսինքն a բնական թվի համար ստանում ենք $a + 1 \leqslant a$, որը հակասություն է: Իրոք, հաշվի առնելով նաև $a \leqslant a + 1$ պայմանը, կունենանք՝ $a + 1 = a$: □

Ի վերջո ապացուցենք, որ բնական թվերի բազմությունը որոշվում է միարժեքորեն, այսպես կոչված, իզոմորֆիզմի ճշտությամբ:

Դիցուք P-ն և P^*-ը բնական թվերի կամայական երկու բազմություններ են, այսինքն՝ դրանց համար գոյություն ունեն այնպիսի $\sigma : P \to P$ և $\sigma^* : P^* \to P^*$ արտապատկերումներ, որ տեղի ունեն Պեանոյի երեք աքսիոմները՝ ինչպես P, այնպես էլ P^* բազմությունների համար: P և P^* բնական թվերի բազմությունները կոչվում են **նույնածև** կամ **իզոմորֆ** և գրվում է՝ $P \simeq P^*$, եթե գոյություն ունի այնպիսի $\varphi : P \to P^*$ բիեկտիվ (փոխմիարժեք) արտապատկերում, որ տեղի ունեն հետևյալ երկու պայմանները.

ա) յուրաքանչյուր $x \in P$ տարրի համար

$$\varphi[\sigma(x)] = \sigma^*[\varphi(x)],$$

բ) $\varphi(0) = 0^*$;

Այդ դեպքում, $\varphi : P \to P^*$ բիեկտիվ (փոխմիարժեք) արտապատկերումը կոչվում է **իզոմորֆիզմ** կամ **նույնածնություն**:

Հատկություն 12.9: *Բնական թվերի կամայական երկու P և P^* բազմություններ իզոմորֆ են:*

Ապացուցում: Դիցուք $P = \{0, 1, 2, \ldots\}$ և $P^* = \{0^*, 1^*, 2^*, \ldots\}$: Սահմանելով $\varphi : P \to P^*$ բիեկտիվ արտապատկերումը հետևյալ կերպ՝

$$\varphi(0) = 0^*, \ \ \varphi(1) = 1^*, \ \ \varphi(2) = 2^*, \ \ \ldots$$

վերհանգման եղանակով, հեշտությամբ ստուգվում է իզոմորֆիզմի

$$\varphi[\sigma(x)] = \sigma^*[\varphi(x)]$$

պայմանը: □

Այսպիսով իզոմորֆիզմի ճշտությամբ բնական թվերի բազմությունը (շարքը) որոշվում է միարժեքորեն: Ընդ որում, φ իզոմորֆիզմն այստեղ նույնիսկ միակն է, այսինքն, եթե $\varphi : P \to P^*$ և $\varphi_1 : P \to P^*$ արտապատկերումները իզոմորֆիզմներ են, ապա $\varphi(x) = \varphi_1(x)$ յուրաքանչյուր $x \in P$ տարրի դեպքում: Իրոք, $\varphi(0) = 0^* = \varphi_1(0)$: Դիցուք $\varphi(a) = \varphi_1(a)$, $a \in P$: Այդ դեպքում $\sigma^*[\varphi(a)] = \sigma^*[\varphi_1(a)]$ և հետևաբար $\varphi[\sigma(a)] = \varphi_1[\sigma(a)]$, այսինքն $\varphi(a') = \varphi_1(a')$: Ուստի վերհանգման սկզբունքի համաձայն $\varphi(x) = \varphi_1(x)$ բոլոր $x \in P$ տարրերի համար:

Ընդհանուր դեպքում, ոչ դատարկ P բազմությունը $\sigma : P \to P$ արտապատկերման (ֆունկցիայի) հետ մեկտեղ (կամ նկատմամբ) կոչվում է նաև **դինամիկ (շարժուն) համակարգ** և նշանակվում է $P(\sigma)$-ով: Վերջիններիս հետազոտությունը հետաքրքրական է ոչ միայն թվերի տեսության տեսանկյունից, այլև հանրահաշվական գիտության և նրա կիրառությունների տեսանկյունից:

Վարժություններ և խնդիրներ

1. Ապացուցել, որ ցանկացած $a \in P$ բնական թվի համար՝ $a \cdot 1 = a$:
2. Ապացուցել, որ ցանկացած $a \in P$, $a \neq 0$ բնական թվի համար՝ $a = \underbrace{1 + \cdots + 1}_{a}$:

3. Ապացուցել, որ ցանկացած $a, b \in P$, $b \neq 0$ բնական թվերի համար՝

$$a \cdot b = \underbrace{a + \cdots + a}_{b} :$$

4. Ապացուցել, որ ցանկացած $a, b \in P$ բնական թվերի համար՝

$$b \neq 0 \rightarrow a \neq a + b :$$

5. Ապացուցել, որ ցանկացած $a, b \in P$ բնական թվերի համար՝ $a+b \neq 0$, եթե $a \neq 0$ կամ $b \neq 0$: Հետևաբար, եթե $a + b = 0$, ապա $a = 0$ և $b = 0$:

6. Ապացուցել, որ ցանկացած $a, b \in P$ բնական թվերի համար՝

$$a \neq 0,\ b \neq 0 \rightarrow a \cdot b \neq 0 :$$

7. Ապացուցել, որ ցանկացած $a, b, c \in P$ բնական թվերի համար՝

$$a \cdot c = b \cdot c \rightarrow a = b,$$

որտեղ $c \neq 0$:

8. Ապացուցել, որ ցանկացած $a, b, c \in P$ բնական թվերի համար տեղի ունեն հետևյալ հավասարությունները (նույնությունները).

$$(a + b) - b = a,$$

$$a - (b - c) = (a + c) - b,$$

$$a - (b + c) = (a - b) - c,$$

$$(a + b) - c = (a - c) + b,$$

$$(a + b) - c = a + (b - c),$$

$$(a + b) - (c + d) = (a - c) + (b - d),$$

$$(a - b) - (c - d) = (a - c) - (b - d) :$$

9. Ապացուցել, որ ցանկացած $a, b, c \in P$ բնական թվերի համար՝

$$a < b \rightarrow a + c < b + c :$$

10. Ապացուցել, որ ցանկացած $a, b, c \in P$, $c \neq 0$ բնական թվերի համար՝

$$a < b \longrightarrow a \cdot c < b \cdot c \,:$$

11. Ապացուցել, որ ցանկացած $a, b, c \in P$ բնական թվերի համար՝

$$a \leqslant b,\ b < c \longrightarrow a < c,$$

$$a < b,\ b \leqslant c \longrightarrow a < c \,:$$

Մաս Բ

Դասական – գծային հանրահաշիվ

Գ լ ու խ 13

ՏԵՂԱԴՐՈՒԹՅՈՒՆՆԵՐ ԵՎ ՏԵՂԱՓՈԽՈՒԹՅՈՒՆՆԵՐ

13.1. Զույգ և կենտ տեղադրություններ

$\alpha : A \to A$ տեսքի յուրաքանչյուր փոխմիարժեք (բիեկտիվ) արտապատկերում կոչվում է A **բազմության տեղադրություն**: A բազմության բոլոր տեղադրությունների բազմությունը ընդունված է նշանակել S_A-ով: n-տարրանի $A = \{1, 2, \ldots, n\}$ բազմության յուրաքանչյուր տեղադրություն կոչվում է նաև n**-րդ աստիճանի տեղադրություն**, կամ համառոտ՝ n-տեղադրություն: n-րդ աստիճանի բոլոր տեղադրությունների բազմությունը նշանակվում է S_n-ով: Հայտնի է, որ $|S_n| = n!$ (հետևություն 0.8):

Կասենք, որ (i, j) թվազույգը (կամ զույգը), որտեղ $i, j \in \{1, \ldots, n\}$, $i \neq j$, հանդիսանում (կատարում) է **կարգի խախտում** $\alpha \in S_n$ տեղադրության նկատմամբ (մեջ), եթե $i < j$, բայց $\alpha(i) > \alpha(j)$: Եթե (i, j) թվազույգը կատարում է կարգի խախտում $\alpha \in S_n$ տեղադրության նկատմամբ, ապա (i, j)-ն կանվանենք նաև (α-ի) կարգի խախտում, կամ կարգի խախտում α-ում: $(i, i + 1)$ տեսքի կարգի խախտումը կոչվում է **տարրական**:

Եթե $\alpha \in S_n$ տեղադրության նկատմամբ կարգի խախտում կատարող բոլոր թվազույգերի թիվը նշանակենք $I(\alpha)$-ով, ապա $(-1)^{I(\alpha)}$ աստիճանը կոչվում է α **տեղադրության նշան** և նշանակվում է՝

$$sgn\,(\alpha) = (-1)^{I(\alpha)};$$

Այսպիսով, սահմանված է $sgn : S_n \to \{1, -1\}$ արտապատկերումը, որը կոչվում է նաև **զույգության ֆունկցիա**:

n-րդ աստիճանի α տեղադրությունը կոչվում է **զույգ**, եթե նրա նշանը հավասար է 1-ի՝ $sgn\,(\alpha) = 1$, այսինքն՝ կամ α-ի նկատմամբ կարգի խախտում կատարող թվազույգեր չկան ($I(\alpha) = 0$), կամ դրանց քանակը հավասար է զույգ թվի: n-րդ աստիճանի α տեղադրությունը կոչվում է **կենտ**, եթե $sgn\,(\alpha) = -1$, այսինքն՝ α-ի նկատմամբ կարգի խախտում կատարող թվազույգերի քանակը կենտ թիվ է:

Օրինակ,

$$\varepsilon = \begin{pmatrix} 1, 2, \ldots, n \\ 1, 2, \ldots, n \end{pmatrix}$$

նույնական արտապատկերումը զույգ տեղադրություն է, որովհետև չկա նրա նկատմամբ կարգի խախտում կատարող որևէ թվազույգ: Ճիշտ է նաև հակառակը, եթե չկա $\alpha \in S_n$ տեղադրության նկատմամբ կարգի խախտում կատարող որևէ թվազույգ, ապա α-ն նույնական արտապատկերումն է: Իրոք, ապացուցենք $\alpha(1) = 1$, $\alpha(2) = 2$, …, $\alpha(n) = n$ հավասարությունները: Եթե $\alpha(1) = k > 1$, ապա α-ի սյուրեկտիվության համաձայն գոյություն կունենա այնպիսի $i > 1$ բնական թիվ, որ $\alpha(i) = 1$: Ուստի, $(1, i)$ թվազույգը կարգի խախտում է: Հակասություն: Հետևաբար՝ $\alpha(1) = 1$: Որից հետո, համանման եղանակով, ստացվում են նաև մնացած հավասարությունները: Այսպիսով՝

$$I(\alpha) = 0 \longleftrightarrow \alpha = \varepsilon;$$

$\alpha \in S_n$ տեղադրությունը կոչվում է **դիրքափոխություն**, եթե գոյություն ունեն այնպիսի $i, j \in \{1, \ldots, n\}$, $i \neq j$, թվեր, որ

$$\alpha(i) = j,$$

$$\alpha(j) = i,$$

$$\alpha(x) = x$$

բոլոր $x \in \{1, \ldots, n\}$, $x \neq i, j$ թվերի համար: Այդ դեպքում համառոտ գրվում է $\alpha = (i, j)$: Եթե $\alpha = (i, i+1)$, ապա այդպիսի դիրքափոխությունը կոչվում է **տարրական**:

Յուրաքանչյուր α դիրքափոխության հակադարձ տեղադրությունը համընկնում է իր հետ՝ $\alpha^{-1} = \alpha$, որովհետև $\alpha \cdot \alpha = \varepsilon$:

Հատկություն 13.1: *Յուրաքանչյուր $\alpha = (i, j)$ դիրքափոխություն կենտ տեղադրություն է, որովհետև նրա կարգի խախտումների քանակը հավասար է $2(j - i) - 1$ կենտ թվին ($i < j$):*

Ապացուցում: Պնդումն ակնհայտ է տարրական դիրքափոխության համար: Իրոք, եթե $j = i + 1$-ի, այսինքն՝

$$\alpha = \begin{pmatrix} 1, \ldots, i-1, i, i+1, i+2, \ldots, n \\ 1, \ldots, i-1, i+1, i, i+2, \ldots, n \end{pmatrix},$$

ապա α-ի նկատմամբ միակ կարգի խախտում կատարող թվազույգը $(i, i+1)$ զույգն է:

Անցնենք ընդհանուր դեպքին: Դիցուք $\alpha = (i,j)$, որտեղ $i < j$ և $j - i > 1$, այսինքն՝

$$\alpha = \begin{pmatrix} 1,\ldots,i-1,i,i+1,\ldots,j-1,j,j+1,\ldots,n \\ 1,\ldots,i-1,j,i+1,\ldots,j-1,i,j+1,\ldots,n \end{pmatrix};$$

Այս դեպքում α-ի նկատմամբ կարգի խախտում կատարող բոլոր թվազույգերն են՝

$$(i,i+1),\ldots,(i,j-1),(i,j),$$

$$(i+1,j),\ldots,(j-1,j),$$

որոնց թիվը կենտ է և հավասար է՝

$$(j-i)+(j-1-i) = 2(j-i)-1 : \qquad \square$$

Օրինակ, $\alpha = (1,8)$ դիրքափոխության բոլոր կարգի խախտումների քանակը հավասար է՝ $2(8-1)-1 = 13$:

Թեորեմ 13.1*: Նույնական (միավոր) արտապատկերումից տարբեր յուրաքանչյուր n-րդ աստիճանի տեղադրություն կամ դիրքափոխություն է, կամ վերածվում է դիրքափոխությունների արտադրյալի: Դեռ ավելին, նույնական արտապատկերումից տարբեր յուրաքանչյուր $\alpha \in S_n$ տեղադրության կամ տարրական դիրքափոխություն է, կամ վերածվում է $I(\alpha)$ թվով տարրական դիրքափոխությունների արտադրյալի:*

Ապացուցում: Բավական է ապացուցել թեորեմի երկրորդ մասը: Դիցուք $\alpha \in S_n$, $\alpha \neq \varepsilon$: Հետևաբար, $n > 1$ և $I(\alpha) \geqslant 1$, այսինքն՝ α-ում գոյություն ունի կարգի խախտում: Այդ դեպքում, α-ում գոյություն կունենա նաև տարրական կարգի խախտում: Իրոք, դիցուք α-ում գոյություն ունի որևէ (i,j) կարգի խախատում, բայց գոյություն չունի որևէ տարրական կարգի խախտում: Ուստի՝

$$i < j \longrightarrow i < i+1 < \cdots < j-1 < j \longrightarrow$$

$$\longrightarrow \alpha(i) < \alpha(i+1) < \cdots < \alpha(j-1) < \alpha(j) \longrightarrow \alpha(i) < \alpha(j),$$

որը հակասում է (i,j) թվազույգի ընտրությանը:

Այսպիսով, α-ում գոյություն ունի որևէ տարրական կարգի խախտում, այսինքն՝ որևէ $(i,i+1)$ տեսքի կարգի խախտում:

Այժմ նկատենք, որ

$$\alpha = \begin{pmatrix} 1, \ldots, n \\ a_1, \ldots, a_n \end{pmatrix}$$

տեղադրությունը ձախից բազմապատկել որևէ $\beta = (i, i+1)$ տարրական դիրքափոխությամբ նշանակում է α-ի երկրորդ տողում տեղափոխել a_i և a_{i+1} տարրերը, այսինքն՝

$$\beta \cdot \alpha = \begin{pmatrix} 1, \ldots, i-1, i, i+1, i+2, \ldots, n \\ a_1, \ldots, a_{i-1}, a_{i+1}, a_i, a_{i+2}, \ldots, a_n \end{pmatrix},$$

որովհետև՝

$(\beta \cdot \alpha)i = \alpha(\beta i) = \alpha(i+1) = a_{i+1}$,

$(\beta \cdot \alpha)(i+1) = \alpha(\beta(i+1)) = \alpha(i) = a_i$,

$(\beta \cdot \alpha)x = \alpha(\beta x) = \alpha(x)$,

եթե $x \neq i, i+1$; Արդյունքում՝

$$I(\beta{\cdot}\alpha) = \begin{cases} I(\alpha)+1, & \text{եթե } (i, i+1) \text{ թվազույգը } \alpha\text{-ի կարգի խախտում չէ,} \\ I(\alpha)-1, & \text{հակառակ դեպքում;} \end{cases} \tag{13.1}$$

Հետևաբար, եթե (i_1, i_1+1) թվազույգը α-ի որևէ տարրական կարգի խախտում է, ապա α-ն ձախից բազմապատկելով համապատասխան $\alpha_1 = (i_1, i_1+1)$ դիրքափոխությամբ, ստանում ենք մի նոր $\alpha_1 \cdot \alpha$ տեղադրություն, որի մեջ (i_1, i_1+1) թվազույգն արդեն կարգի խախտում չէ և արդյունքում $\alpha_1{\cdot}\alpha$ տեղադրության կարգի խախտումների թիվը կլինի մեկով պակաս քան α-ի կարգի խախտումների թիվը՝

$$I(\alpha_1 \cdot \alpha) = I(\alpha) - 1 :$$

Եթե այստեղ $\alpha_1 \cdot \alpha \neq \varepsilon$, այսինքն՝ $I(\alpha) - 1 \neq 0$, ապա կրկնելով կատարված քայլը, գտնում ենք մի այնպիսի նոր $\alpha_2 = (i_2, i_2+1)$ տարրական դիրքափոխություն, որ

$$I(\alpha_2\alpha_1\alpha) = I(\alpha_1\alpha) - 1 = I(\alpha) - 2$$

և այսպես շարունակ: Քանի որ յուրաքանչյուր քայլից հետո ստացված արտադրյալ տեղադրության կարգի խախտումների թիվը մեկով պակաս է նախորդ քայլում ունեցած տեղադրության կարգի խախտումների թվից, ապա ի վերջո $k = I(\alpha)$ թվով քայլերից հետո կգտնենք այնպիսի $\alpha_1, \ldots, \alpha_k$ տարրական դիրքափոխություններ, որ

$$I(\alpha_k \cdot \alpha_{k-1} \cdots \alpha_1 \cdot \alpha) = 0,$$

այսինքն՝ $\alpha_k \cdot \alpha_{k-1} \cdots \alpha_1 \cdot \alpha = \varepsilon$: Այստեղից, քանի որ $\alpha_i^{-1} = \alpha_i$ այսինքն՝ դիրքափոխության հակադարձը ինքն է, ապա

$$\alpha = \alpha_1^{-1} \cdot \alpha_2^{-1} \cdots \alpha_k^{-1} = \alpha_1 \cdot \alpha_2 \cdots \alpha_k,$$

որտեղ $k = I(\alpha)$: □

Հետևություն 13.1: *Նույնական (միավոր) արտապատկերումից տարբեր յուրաքանչյուր զույգ տեղադրություն վերածվում է զույգ թվով դիրքափոխությունների արտադրյալի: Դեռ ավելին, նույնական արտապատկերումից տարբեր յուրաքանչյուր զույգ տեղադրություն վերածվում է զույգ թվով տարրական դիրքափոխությունների արտադրյալի:* □

Հետևություն 13.2: *Յուրաքանչյուր կենտ տեղադրություն կամ դիրքափոխություն է կամ վերածվում է կենտ թվով դիրքափոխությունների արտադրյալի: Դեռ ավելին, յուրաքանչյուր կենտ տեղադրություն կամ տարրական դիրքափոխություն է, կամ վերածվում է կենտ թվով տարրական դիրքափոխությունների արտադրյալի:* □

Հակառակ պնդումները հասկանալի դարձնելու համար նախ պիտի ստանանք տեղադրությունների արտադրյալի նշանի որոշման կանոնը: Մինչ այդ դիտարկենք օրինակ:

Օրինակ, եթե $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix}$, ապա α-ի նկատմամբ կարգի խախտում կատարող թվազույգերն են՝ $(1,4)$, $(2,3)$, $(2,4)$, $(2,5)$, $(3,4)$, այսինքն՝ $I(\alpha) = 5$ և α -ն կենտ է: Միաժամանակ հաշվելով հետևյալ արտադրյալները՝ ըստ տարրական կարգի խախտումների, կունենանք.

$$(2,3) \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix},$$

$$(3,4) \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix},$$

$$(2,3)\cdot\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix},$$

$$(1,2)\cdot\begin{pmatrix}1&2&3&4&5\\2&1&3&5&4\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix},$$

$$(4,5)\cdot\begin{pmatrix}1&2&3&4&5\\1&2&3&5&4\end{pmatrix}=\varepsilon:$$

Հետևաբար՝

$$\begin{pmatrix}1&2&3&4&5\\2&5&3&1&4\end{pmatrix}=(2,3)\cdot(3,4)\cdot(2,3)\cdot(1,2)\cdot(4,5);$$

α տեղադրության այս վերլուծությունը համապատասխանում է թեորեմ 13.1-ի ապացուցմանը: Սակայն դա α-ի միակ վերլուծությունը չէ ըստ դիրքափոխությունների արտադրյալի: Օրինակ՝

$$\begin{pmatrix}1&2&3&4&5\\2&5&3&1&4\end{pmatrix}=(1,2)\cdot(1,5)\cdot(1,4):$$

Հետևաբար, հարց է ծագում նաև, թե ինչ կապ գոյություն ունի միևնույն α տեղադրության տարբեր վերլուծությունների միջև: Այս և տեղադրությունների արտադրյալի նշանի կանոնը միմյանց հետ սերտորեն կապված են: Ի վերջո պարզվում է, որ միևնույն α տեղադրության բոլոր վերլուծություններում դիրքափոխությունների թվի զույգությունը նույնն է, իսկ $I(\alpha)$-ն տարրական դիրքափոխությունների այն փոքրագույն (մինիմալ) թիվն է, որոնց արտադրյալին հավասար է տրված α-ն: Սկսենք վերջին պնդման հիմնավորումից: □

Թեորեմ 13.2 (մինիմալության կամ օպտիմալության վերաբերյալ): *Եթե* $\alpha\in S_n$, $\alpha\neq\varepsilon$ *և*

$$\alpha=\beta_1\cdots\beta_m,$$

որտեղ β_j *տեղադրությունները տարրական դիրքափոխություններ են, ապա* $m\geqslant I(\alpha)$, *իսկ* $m-I(\alpha)\geqslant 0$ *տարբերությունը զույգ թիվ է:*

Ապացուցում: Եթե $\alpha=\beta_1\cdots\beta_m$, ապա $\beta_m\cdots\beta_1\alpha=\varepsilon$: Համաձայն (13.1) բանաձևի, α տեղադրությունը ձախից որևէ β տարրական դիրքափոխությամբ բազմապատկելուց α-ի կարգի խախտումների թիվը կամ 1-ով ավելանում է, կամ 1-ով պակասում: Դիցուք t հատ ձախից բազմապատկված β_i տարրական դիրքափոխություններ 1-ով ավելացնում են եղած կարգի խախտումների թիվը, իսկ մնացած $m-t$ հատ β_j տարրական դիրքափոխությունները 1-ով պակասեցնում են եղած կարգի խախտումների թիվը: Այդ դեպքում՝

$$I\left(\beta_m \cdots \beta_1 \alpha\right) = I(\varepsilon),$$

$$I(\alpha) + t - (m-t) = 0,$$

$$m - I(\alpha) = 2t \geqslant 0 : \qquad \square$$

Թեորեմ 13.3: *Կամայական $\alpha, \beta \in S_n$ տեղադրությունների համար*

$$sgn\,(\alpha \cdot \beta) = sgn\,(\alpha) \cdot sgn\,(\beta) :$$

Ապացուցում: Առանց ընդհանրությունը խախտելու կարող ենք ենթադրել, որ $\alpha \neq \varepsilon$ (որովհետև $\alpha = \varepsilon$ դեպքում պնդումն ակնհայտորեն ճիշտ է): Քննարկենք երկու դեպք:

ա) $\alpha = (i, i+1)$; Այս դեպքում, համաձայն (13.1) բանաձևի՝

$$I(\alpha \cdot \beta) = \begin{cases} I(\beta) + 1, & \textbf{եթե}\ \ \beta(i) < \beta(i+1), \\ I(\beta) - 1, & \textbf{եթե}\ \ \beta(i) > \beta(i+1), \end{cases}$$

և, հետևաբար,

$$sgn\,(\alpha \cdot \beta) = (-1)^{I(\alpha \cdot \beta)} = (-1)^{I(\beta) \pm 1} = (-1)^{\pm 1} \cdot (-1)^{I(\beta)} =$$

$$= (-1) \cdot (-1)^{I(\beta)} = sgn\,(\alpha) \cdot sgn\,(\beta);$$

բ) Ընդհանուր դեպքում, համաձայն թեորեմ 13.1-ի, α տեղադրությունը վերածելով $k = I(\alpha)$ թվով տարրական դիրքափոխությունների արտադրյալի, կունենանք՝

$$\alpha = \alpha_1 \cdots \alpha_k$$

և աստիճանաբար օգտվելով նախորդ դեպքից ու հատկություն 13.1-ից, կունենանք՝

$$sgn\,(\alpha \cdot \beta) = sgn\,(\alpha_1 \cdots \alpha_k \cdot \beta) = sgn\,(\alpha_1) \cdot sgn\,(\alpha_2 \cdots \alpha_k \cdot \beta) =$$

$$= (-1) \cdot sgn\,(\alpha_2 \cdots \alpha_k \cdot \beta) = (-1)^2 \cdot sgn\,(\alpha_3 \cdots \alpha_k \cdot \beta) =$$

$$\cdots = (-1)^{I(\alpha)} \cdot sgn\,(\beta) = sgn\,(\alpha) \cdot sgn\,(\beta) : \qquad \square$$

Հետևություն 13.3: *Կամայական $\alpha \in S_n$ տեղադրության համար՝ $sgn\,\alpha = sgn\,(\alpha^{-1})$, այսինքն՝ α-ն զույգ է (կենտ է) այն և միայն այն դեպքում, երբ զույգ է (կենտ է) α^{-1}-ը:*

Ապացուցում: $1 = sgn\,\varepsilon = sgn\,(\alpha \cdot \alpha^{-1}) = sgn\,(\alpha) \cdot sgn\,(\alpha^{-1})$: □

Հետևություն 13.4: *Վերջավոր թվով կամայական $\alpha_1, \ldots, \alpha_m \in S_n$ տեղադրությունների համար՝*

$$sgn\,(\alpha_1 \cdots \alpha_m) = sgn\,(\alpha_1) \cdots sgn\,(\alpha_m) :$$

Ապացուցում: Վերիանգման եղանակով: □

Հետևություն 13.5: *Երկու (կամ ընդհանրապես վերջավոր թվով) n-րդ աստիճանի զույգ տեղադրությունների արտադրյալը զույգ տեղադրություն է: Երկու (կամ ընդհանրապես զույգ թվով) n-րդ աստիճանի կենտ տեղադրությունների արտադրյալը զույգ տեղադրություն է: Կենտ թվով n-րդ աստիճանի կենտ տեղադրությունների արտադրյալը կենտ տեղադրություն է: Որպեսզի տեղադրությունը լինի զույգ (կենտ) անհրաժեշտ է և բավարար, որ այն վերածվի զույգ (համապատասխանաբար կենտ) թվով դիրքափոխությունների արտադրյալի:* □

n-րդ աստիճանի բոլոր զույգ տեղադրությունների բազմությունը սովորաբար նշանակվում է $\mathbb{A}_n$-ով:

Հատկություն 13.2: *n-րդ աստիճանի զույգ և կենտ տեղադրությունների քանակները հավասար են ($n > 1$), այսինքն՝ $|\mathbb{A}_n| = |S_n \setminus \mathbb{A}_n| = \dfrac{n!}{2}$;*

Ապացուցում: Պահանջվում է կառուցել որևէ

$$f : \mathbb{A}_n \longrightarrow S_n \setminus \mathbb{A}_n, \quad n > 1,$$

բիեկտիվ (փոխմիարժեք) արտապատկերում: Յուրաքանչյուր $\alpha \in \mathbb{A}_n$ զույգ տեղադրության համար սահմանենք

$$f(\alpha) = \alpha \cdot (1, 2) \in S_n \setminus \mathbb{A}_n;$$

Ակնհայտ է, որ f-ը ինյեկտիվ (ներդրող) է՝

$$f(\alpha_1) = f(\alpha_2) \longrightarrow \alpha_1 = \alpha_2,$$

որովհետև՝

$$\alpha_1\cdot(1,2) = \alpha_2\cdot(1,2) \longrightarrow \alpha_1\cdot(1,2)\cdot(1,2)^{-1} = \alpha_2\cdot(1,2)\cdot(1,2)^{-1} \longrightarrow \alpha_1 = \alpha_2 :$$

f-ը նաև սյուրեկտիվ (վերադրող) է, այսինքն՝ յուրաքանչյուր $\beta \in S_n\setminus \mathbb{A}_n$ կենտ տեղադրության համար գոյություն ունի այնպիսի $\alpha \in \mathbb{A}_n$ զույգ տեղադրություն, որ $f(\alpha) = \beta$: Իրոք, ընտրելով $\alpha = \beta\cdot(1,2)$, կունենանք՝ $\alpha \in \mathbb{A}_n$ և

$$f(\alpha) = \alpha\cdot(1,2) = \beta\cdot(1,2)\cdot(1,2) = \beta\cdot\varepsilon = \beta : \qquad \square$$

13.2. Տեղափոխություններ, դրանց արտադրյալը

Անցնենք տեղափոխության գաղափարին:

Բնական թվերի $(i_1, i_2, \ldots, i_n)$ կարգավորված n-յակը (հաջորդականությունը) կոչվում է n**-րդ աստիճանի տեղափոխություն** կամ համառոտ՝ n**-տեղափոխություն**, եթե գոյություն ունի այնպիսի $\alpha \in S_n$ տեղադրություն, որ $\alpha(1) = i_1$, $\alpha(2) = i_2$, ..., $\alpha(n) = i_n$: Այս $\alpha \in S_n$ տեղադրությունը որոշվում է միարժեքորեն և այդ պատճառով կարելի է գրել $(i_1, i_2, \ldots, i_n) = [\alpha]$: $i_1, i_2, \ldots, i_n$ թվերը կոչվում են $(i_1, i_2, \ldots, i_n)$ n**-տեղափոխության տարրեր**:

Երկու n-տեղափոխությունների արտադրյալը սահմանվում է հետևյալ կերպ՝

$$[\alpha]\cdot[\beta] = [\alpha\cdot\beta] :$$

Ակնհայտ է, որ n-տեղափոխությունների արտադրյալը զուգորդական է, այսինքն՝

$$([\alpha]\cdot[\beta])\cdot[\gamma] = [\alpha]\cdot([\beta]\cdot[\gamma]) :$$

$[\alpha]$ n-տեղափոխությունը կոչվում է զույգ (կենտ), եթե $\alpha \in S_n$ տեղադրությունը զույգ (կենտ) է:

Զույգ և կենտ տեղադրությունների վերաբերյալ ապացուցված բոլոր հիմնական արդյունքները հեշտությամբ տարածվում են զույգ և կենտ n-տեղափոխությունների վրա: Մասնավորապես, երկու (կամ վերջավոր թվով) զույգ n-տեղափոխությունների արտադրյալը զույգ n-տեղափոխություն է:

n-տեղափոխությունների արտադրյալի սահմանումից բխում է, որ

$$[\alpha]\cdot[\varepsilon] = [\varepsilon]\cdot[\alpha] = [\alpha]$$

և եթե $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = \varepsilon$, ապա

$$[\alpha] \cdot \left[\alpha^{-1}\right] = \left[\alpha^{-1}\right] \cdot [\alpha] = [\varepsilon],$$

որտեղ $[\varepsilon] = (1, 2, \ldots, n)$: Այլ կերպ, բոլոր n-տեղափոխությունների բազմությունն ունի միավոր և նրա յուրաքանչյուր տարր հակադարձելի է:

Բոլոր n-տեղափոխությունների բազմությունը կնշանակենք $\mathbb{P}_n$-ով, իսկ բոլոր զույգ n-տեղափոխությունների բազմությունը՝ $\mathbb{T}_n$-ով:

Կասենք, որ (i_k, i_s) թվազույգը հանդիսանում (կատարում) է **կարգի խախտում** $(i_1, i_2, \ldots, i_n)$ n-տեղափոխության մեջ, եթե $k < s$, բայց $i_k > i_s$: Եթե $(i_1, i_2, \ldots, i_n) = [\alpha]$ n-տեղափոխության մեջ կարգի խախտում հանդիսացող բոլոր թվազույգերի քանակը նշանակենք $I[\alpha]$-ով, ապա $I[\alpha] = I(\alpha)$, որովհետև (i_k, i_s) թվազույգը կատարում է կարգի խախտում $[\alpha]$ n-տեղափոխության մեջ այն և միայն այն դեպքում, երբ (k, s) թվազույգը կատարում է կարգի խախտում $\alpha \in S_n$ տեղադրության նկատմամբ: Հետևաբար,

$$(-1)^{I[\alpha]} = (-1)^{I(\alpha)} \ :$$

(i_k, i_{k+1}) տեսքի կարգի խախտումը կոչվում է **տարրական**:

1) Բոլոր n-տեղափոխությունների քանակը հավասար է $n!$-ի, այսինքն՝ բոլոր n-տեղադրությունների քանակին: □

2) Բոլոր զույգ n-տեղափոխությունների քանակը հավասար է բոլոր կենտ n-տեղափոխությունների քանակին ($n \geqslant 2$): □

3) Եթե n-տեղափոխության մեջ նրա կամայական երկու տարրերի տեղերը փոխենք, ապա դրանից կփոխվի նրա զույգությունը, այսինքն՝ կենտ n-տեղափոխությունը կդառնա զույգ, իսկ զույգը՝ կենտ:

Ապացույց: Եթե $(i_1, \ldots, i_k, \ldots, i_s \ldots, i_n) = [\alpha]$, ապա $(i_1, \ldots, i_s, \ldots, i_k \ldots, i_n) = [\beta \cdot \alpha] = [\beta] \cdot [\alpha]$, որտեղ $\beta = (k, s)$, և $sgn(\beta \cdot \alpha) = sgn(\beta) \cdot sgn(\alpha) = -sgn(\alpha)$: □

4) Յուրաքանչյուր $[\alpha]$ n-տեղափոխություն կարող է ստացվել կամայական $[\beta]$ n-տեղափոխությունից, վերջինիս մեջ նրա մի քանի (հարևան) տարրերի տեղերը փոխելով:

Ապացույց: Եթե $\gamma = \alpha \cdot \beta^{-1} \in S_n$, ապա $\gamma \cdot \beta = \alpha$, $[\gamma \cdot \beta] = [\alpha]$ և $[\gamma] \cdot [\beta] = [\alpha]$: Մնում է օգտվել թեորեմ 13.1-ից և $\gamma \in S_n$ տեղադրությունը վերածել տարրական դիրքափոխությունների արտադրյալի՝ $\gamma = \gamma_1 \cdots \gamma_l$; Ուստի՝

$$[\gamma_1] \cdots [\gamma_l] \cdot [\beta] = [\alpha] \ : \qquad \square$$

13.3. Շրջուն (ցիկլային) տեղադրություններ

$x \in A$ տարրը կոչվում է $\alpha \in S_A$ **տեղադրության շարժուն կետ** (տարր), եթե $\alpha(x) \neq x$: Հակառակ դեպքում, $x \in A$ տարրը կոչվում է $\alpha \in S_A$ **տեղադրության անշարժ կետ** ($\alpha(x) = x$): $\alpha \in S_A$ տեղադրության բոլոր շարժուն կետերի բազմությունը կնշանակենք $mob(\alpha)$-ով՝

$$mob(\alpha) = \{x \in A \,|\alpha(x) \neq x\} \subseteq A;$$

Ակնհայտ է, որ

$$mob(\alpha) = \emptyset \longleftrightarrow \alpha = \varepsilon :$$

$\alpha, \beta \in S_A$ տեղադրությունները կոչվում են **անկախ**, եթե նրանց շարժուն կետերի բազմությունները չեն հատվում, այսինքն՝

$$mob(\alpha) \cap mob(\beta) = \emptyset :$$

Հատկություն 13.3: *1) $mob(\alpha)$-ն կայուն (ինվարիանտ) է α-ի նկատմամբ, այսինքն՝*

$$x \in mob(\alpha) \longrightarrow \alpha(x) \in mob(\alpha);$$

2) $mob(\alpha^{-1}) = mob(\alpha)$:

Ապացուցում: 1) Դիցուք $mob(\alpha) \neq \emptyset$ և $x \in mob(\alpha)$: Ապացուցենք, որ $\alpha(x) \in mob(\alpha)$: Ենթադրելով հակառակը, ստանում ենք հակասություն: Իրոք, $\alpha(\alpha x) = \alpha(x)$ պայմանից, α-ի ինյեկտիվության համաձայն, կունենանք՝

$$\alpha(x) = x,$$

որը հակասում է $x \in mob(\alpha)$ պայմանին:

2) $\alpha(x) = x \longleftrightarrow \alpha^{-1}(\alpha x) = \alpha^{-1}(x) \longleftrightarrow x = \alpha^{-1}(x)$; Այսպիսով, յուրաքանչյուր $x \in A$ տարրի համար՝

$$x \notin mob(\alpha) \longleftrightarrow x \notin mob(\alpha^{-1});$$

Հետևաբար՝

$$mob(\alpha^{-1}) = mob(\alpha) : \qquad \square$$

Հետևություն 13.6: *Եթե $mob(\alpha) \neq \emptyset$, ապա $mob(\alpha)$-ն առնվազն երկու տարրանի է:*

Ապացուցում: Եթե $mob(\alpha) \neq \emptyset$, ապա գոյություն ունի $a \in mob(\alpha)$: Հետևաբար, ըստ հատկություն 13.3-ի, $\alpha(a) \in mob(\alpha)$, որտեղ $\alpha(a) \neq a$, այսինքն՝ $mob(\alpha)$-ն կլինի առնվազն երկու տարրանի: □

Հատկություն 13.4: *Եթե A բազմության α և β տեղադրություններն անկախ են, այսինքն՝ $mob(\alpha) \cap mob(\beta) = \emptyset$, ապա*

1) $\alpha \cdot \beta = \beta \cdot \alpha$*;*

2) $mob(\alpha \cdot \beta) = mob(\alpha) \cup mob(\beta)$*;*

Ապացուցում: 1) Ապացուցենք $(\alpha \cdot \beta)x = (\beta \cdot \alpha)x$ հավասարությունը յուրաքանչյուր $x \in A$ տարրի համար: Եթե $x \in mob(\alpha)$, ապա համաձայն հատկություն 13.3-ի $\alpha(x) \in mob(\alpha)$: Հետևաբար, ըստ α-ի ու β-ի անկախության պայմանի, $x, \alpha(x) \notin mob(\beta)$, այսինքն՝ $\beta(x) = x$, $\beta(\alpha x) = \alpha(x)$ և

$$(\alpha \cdot \beta)x = \beta(\alpha x) = \alpha(x), \tag{13.2}$$

$$(\beta \cdot \alpha)x = \alpha(\beta x) = \alpha(x); \tag{13.3}$$

Համանման եղանակով քննարկվում է նաև $x \in mob(\beta)$ դեպքը: Իսկ $x \notin mob(\alpha) \cup mob(\beta)$ դեպքում պնդումն ակնհայտ է, որովհետև այս դեպքում $x \notin mob(\alpha)$ և $x \notin mob(\beta)$, այսինքն՝ $\alpha(x) = x$ և $\beta(x) = x$, հետևաբար՝

$$(\alpha \cdot \beta)x = \beta(\alpha x) = \beta(x) = x,$$

$$(\beta \cdot \alpha)x = \alpha(\beta x) = \alpha(x) = x;$$

2) Եթե $x \notin mob(\alpha) \cup mob(\beta)$, ապա ինչպես տեսանք $(\alpha \cdot \beta)x = x$, այսինքն՝ $x \notin mob(\alpha \cdot \beta)$: Ուստի, եթե $x \in mob(\alpha \cdot \beta)$, ապա $x \in mob(\alpha) \cup mob(\beta)$: Ճիշտ է նաև հակառակը, եթե $x \in mob(\alpha) \cup mob(\beta)$, ապա $x \in mob(\alpha \cdot \beta)$: Իրոք, դիցուք $x \in mob(\alpha)$: Այդ դեպքում, համաձայն (13.2) հավասարության՝ $(\alpha \cdot \beta)x = \alpha(x) \neq x$, այսինքն՝ $x \in mob(\alpha \cdot \beta)$: Համանման եղանակով ապացուցում ենք նաև, որ եթե $x \in mob(\beta)$, ապա $x \in mob(\alpha \cdot \beta)$: □

Հետևություն 13.7: *Եթե A բազմության $\alpha_1, \alpha_2, \ldots, \alpha_n$ տեղադրությունները զույգ առ զույգ անկախ են, այսինքն՝ $mob(\alpha_i) \cap mob(\alpha_j) = \emptyset$, արտեղ $i \neq j$ և $i, j \in \{1, \ldots, n\}$, ապա*

$$mob(\alpha_1 \cdot \alpha_2 \cdots \alpha_n) = mob(\alpha_1) \cup mob(\alpha_2) \cup \cdots \cup mob(\alpha_n) :$$

Ապացույց (վերհանգման եղանակ): $n = 2$ դեպքում պնդումն ապացուցված է: Ենթադրենք թե n-ից քիչ թվով և զույգ առ զույգ անկախ տեղադրությունների համար պնդումը ճիշտ է: Այդ դեպքում՝

$$mob(\alpha_1 \cdot \alpha_2 \cdots \alpha_{n-1}) = mob(\alpha_1) \cup mob(\alpha_2) \cup \cdots \cup mob(\alpha_{n-1})$$

և, հետևաբար, $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ արտադրյալը և α_n-ը կլինեն անկախ: Ուստի՝

$$mob(\alpha_1 \cdot \alpha_2 \cdots \alpha_n) = mob\left((\alpha_1 \cdot \alpha_2 \cdots \alpha_{n-1}) \cdot \alpha_n\right) =$$

$$= mob(\alpha_1 \cdot \alpha_2 \cdots \alpha_{n-1}) \cup mob(\alpha_n) =$$

$$= mob(\alpha_1) \cup \cdots \cup mob(\alpha_{n-1}) \cup mob(\alpha_n) : \qquad \square$$

$\alpha \in S_n$ տեղադրությունը $(n > 1)$ կոչվում է **շրջուն** (ցիկլային), եթե գոյություն ունեն զույգ առ զույգ միմյանցից տարբեր այնպիսի $i_1, i_2, \ldots, i_k$ բնական թվեր $(k > 1)$, որ $1 \leqslant i_1, i_2, \ldots, i_k \leqslant n$ և

$$\alpha(i_1) = i_2,$$

$$\alpha(i_2) = i_3,$$

$$\vdots$$

$$\alpha(i_{k-1}) = i_k,$$

$$\alpha(i_k) = i_1,$$

իսկ $\alpha(x) = x$ յուրաքանչյուր $x \neq i_1, \ldots, i_k$ բնական թվի համար $(1 \leqslant x \leqslant n)$:

Այդ դեպքում $\alpha \in S_n$ շրջուն տեղադրությունը նշանակվում է

$$\alpha = (i_1, i_2, \ldots, i_k)$$

ձևով: Ակնհայտ է, որ եթե $\alpha = (i_1, i_2, \ldots, i_k)$, ապա

$$mob(\alpha) = \{i_1, i_2, \ldots, i_k\} = \left\{i_1, \alpha(i_1), \ldots, \alpha^{k-1}(i_1)\right\} =$$

$$= \left\{i_2, \alpha(i_2), \ldots, \alpha^{k-1}(i_2)\right\} = \cdots = \left\{i_k, \alpha(i_k), \ldots, \alpha^{k-1}(i_k)\right\},$$

իսկ k-ն կոչվում է α շրջուն տեղադրության երկարություն: Ակնհայտ է նաև, որ այդ դեպքում

$$\alpha^k = \underbrace{\alpha \cdots \alpha}_{k} = \varepsilon$$

և մասնավորապես $\alpha^{-1} = \alpha^{k-1}$; Շրջուն տեղադրության հակադարձը ևս շրջուն տեղադրություն է, որովհետև եթե $\alpha = (i_1, i_2, \ldots, i_k)$, ապա $\alpha^{-1} = (i_k, i_{k-1}, \ldots, i_2, i_1)$: Յուրաքանչյուր շրջուն տեղադրություն կամ դիրքափոխություն է կամ հանդիսանում է դիրքափոխությունների արտադրյալ: Ավելի ճիշտ, 2 երկարությամբ շրջուն տեղադրությունը դիրքափոխություն է, իսկ մնացած դեպքերում $(k > 2)$՝

$$(i_1, i_2, \ldots, i_k) = (i_1, i_2) \cdot (i_1, i_3) \cdots (i_1, i_k),$$

որի ստուգումը նույնպես հեշտությամբ կատարվում է որպես երկու արտապատկերումների հավասարություն: Օրինակ, ձախ մասում i_2-ը արտապատկերվում է i_3-ին, իսկ աջ մասի առաջին արտապատկերումով i_2-ը նախ արտապատկերվում է i_1-ին, երկրորդ արտապատկերումով ստացված i_1-ը արտապատկերվում է i_3-ին, որը աջ մասի մնացած բոլոր արտապատկերումներով չի փոխվում: Այսպիսով, աջ մասի արտադրյալի արդյունքում i_2-ը նույնպես արտապատկերվեց i_3-ին:

Մասնավորապես, $\alpha = (i_1, i_2, \ldots, i_k)$ շրջուն տեղադրությունը կլինի զույգ այն և միայն այն դեպքում, երբ k-ն կենտ է (կամ $k-1$ թիվը զույգ է):

Թեորեմ 13.4: *Նույնական (միավոր) արտապատկերումից տարբեր յուրաքանչյուր $\alpha \in S_n$ տեղադրություն կամ շրջուն է, կամ վերածվում է վերջավոր թվով (զույգ առ զույգ) անկախ շրջուն տեղադրությունների արտադրյալի: Ընդ որում, այդ վերլուծությունը արտադրիչների տեղափոխելիության ճշտությամբ որոշվում է միարժեքորեն:*

Ապացուցում: $\alpha \neq \varepsilon$ տեղադրության վերլուծության գոյությունը ապացուցենք վերիանգման եղանակով՝ ըստ $m_\alpha = |mob(\alpha)| \geqslant 2$ բնական թվի (տես հետևություն 13.6-ը): Եթե $m_\alpha = 2$, այսինքն՝ $mod(\alpha) = \{i_2, i_2\}$, ապա ակնհայտորեն α-ն կլինի դիրքափոխություն՝ $\alpha = (i_1, i_2)$, որը 2 երկարությամբ շրջուն տեղադրություն է:

Դիցուք $m > 2$ և դիցուք վերլուծության գոյությունը ճիշտ է բոլոր այն $\alpha \in S_n$ և $\alpha \neq \varepsilon$ տեղադրությունների համար, որ $2 \leqslant m_\alpha < m$: Դիցուք այժմ $\alpha \in S_n$, $\alpha \neq \varepsilon$ տեղադրության համար $m_\alpha = m$:

Դիտարկենք որևէ $a \in mob(\alpha) \neq \emptyset$ տարր: Քանի որ

$$a, \alpha(a), \alpha^2(a), \ldots, \alpha^i(a), \ldots$$

հաջորդականության բոլոր տարրերը պատկանում են $mob(\alpha)$ վերջավոր բազմությանը (հատկություն 13.3), ապա նշված հաջորդականության տարրերի մեջ կլինեն համընկնումներ: Դիցուք $a, \alpha(a), \ldots, \alpha^{k-1}(a)$ տարրերը զույգ առ զույգ միմյանցից տարբեր են, իսկ հաջորդ $\alpha^k(a)$ տարրը հավասար է նախորդ տարրերից որևէ մեկին: Այդ դեպքում, նախ $k > 1$, որովհետև $\alpha(a) \neq a$, իսկ $\alpha^k(a) = a$: Իրոք, եթե $\alpha^k(a) = \alpha^l(a)$, որտեղ $k > l > 0$, ապա $\alpha^{-1}\left(\alpha^k(a)\right) = \alpha^{-1}\left(\alpha^l(a)\right)$ և $\alpha^{k-1}(a) = \alpha^{l-1}(a)$, որը հակասում է k-ի ընտրությանը: Հետևաբար, վերոհիշյալ հաջորդականությունը կլինի հետևյալ տեսքի՝

$$a, \alpha(a), \ldots, \alpha^{k-1}(a), a, \alpha(a), \ldots, \alpha^{k-1}(a), a, \ldots$$

Ներմուծելով հետևյալ շրջուն տեղադրությունը՝

$$\alpha_1 = \left(a, \alpha(a), \ldots, \alpha^{k-1}(a)\right)$$

և կազմելով $\beta_1 = \alpha_1^{-1} \cdot \alpha$ արտադրյալը նկատում ենք, որ $a, \alpha(a), \ldots, \alpha^{k-1}(a)$ տարրերը β_1 տեղադրության համար անշարժ կետեր են և $mob(\beta_1) = mob(\alpha) \setminus \left\{a, \alpha(a), \ldots, \alpha^{k-1}(a)\right\}$: Եթե $mob(\beta_1) = \emptyset$, ապա $\beta_1 = \varepsilon$ և $\alpha = \alpha_1$: Եթե $mob(\beta_1) \neq \emptyset$, ապա $|mob(\beta_1)| = m_\alpha - k < m$ և վերհանգման ենթադրության համաձայն կամ β_1-ը շրջուն տեղադրություն է, կամ այն վերածվում է անկախ շրջուն տեղադրությունների արտադրյալի՝

$$\beta_1 = \alpha_2 \cdots \alpha_t;$$

Հետևաբար,

$$\alpha = \alpha_1\beta_1 = \alpha_1\alpha_2 \cdots \alpha_t,$$

ընդ որում, $t > 1$ դեպքում $\alpha_1, \ldots, \alpha_t$ շրջուն տեղադրությունները կլինեն (զույգ առ զույգ) անկախ, որովհետև համաձայն հետևություն 13.7-ի՝

$$mob(\alpha_2) \cup \cdots \cup mob(\alpha_t) = mob(\beta_1),$$

իսկ քանի որ $mob(\alpha_1) = \left\{a, \alpha(a), \ldots, \alpha^{k-1}(a)\right\}$ և $mob(\beta_1) \cap \left\{a, \alpha(a), \ldots, \alpha^{k-1}(a)\right\} = \emptyset$, ապա $mob(\alpha_1) \cap mob(\alpha_i) = \emptyset$, որտեղ $i = 2, \ldots, t$;

Թեորեմի գոյության մասն ապացուցված է: Մնում է ապացուցել միակությունը:

Դիցուք միևնույն $\alpha \in S_n$ տեղադրությունն ունի երկու վերլուծություններ՝ ըստ անկախ շրջուն տեղադրությունների արտադրյալի՝

$$\alpha = \alpha_1 \cdots \alpha_t,$$

$$\alpha = \beta_1 \cdots \beta_s :$$

Ապացուցենք, որ $t = s$ և գոյություն ունեն զույգ առ զույգ միմյանցից տարբեր այնպիսի $j_1, \ldots, j_t \in \{1, \ldots, t\}$ համարներ, որ $\alpha_1 = \beta_{j_1}, \ldots, \alpha_t = \beta_{j_t}$:

Դիցուք $t \neq s$ և $t < s$: Ստանանք հակասություն: Եթե $a \in mob(\alpha_1)$, ապա համաձայն հետևություն 13.3-ի $a \in mob(\alpha)$ և $a \in mob(\beta_{j_1})$ որևէ $j_1 \in \{1, \ldots, s\}$ նշիչի դեպքում: Առանց ընդհանրությունը խախտելու կարելի է ենթադրել, որ $j_1 = 1$, այսինքն՝ $a \in mob(\beta_1)$ (հակառակ դեպքում դրան կհասնեինք կատարելով տեղափոխություններ β_j անկախ շրջուն տեղադրությունների միջև՝ համաձայն հատկություն 13.4-ի): Ապացուցենք $\alpha_1 = \beta_1$ հավասարությունը: Համաձայն 13.2 հավասարության՝

$$\alpha(a) = \alpha_1(a),$$

$$\alpha(a) = \beta_1(a),$$

այսինքն՝ $\alpha_1(a) = \beta_1(a) \in mob(\alpha_1) \cap mob(\beta_1)$: Նորից նույն պատճառով՝

$$\alpha\left(\alpha_1(a)\right) = \alpha_1\left(\alpha_1(a)\right) = \alpha_1^2(a)$$

և

$$\alpha\left(\beta_1(a)\right) = \beta_1\left(\beta_1(a)\right) = \beta_1^2(a),$$

այսինքն՝ $\alpha_1^2(a) = \beta_1^2(a) \in mob(\alpha_1) \cap mob(\beta_1)$: Շարունակելով, համանման եղանակով կստանանք՝ $\alpha_1^i(a) = \beta_1^i(a)$ յուրաքանչյուր i բնական թվի համար: Հետևաբար՝

$$\alpha_1^i(a) = a \longleftrightarrow \beta_1^i(a) = a;$$

Այստեղից, քանի որ $\alpha_1 = \left(a, \alpha_1(a), \ldots, \alpha_1^{k-1}(a)\right)$ և $\beta_1 = \left(a, \beta_1(a), \ldots, \beta_1^{l-1}(a)\right)$, որտեղ k, l բնական թվերը α_1 և β_1 շրջուն տեղադրությունների երկարություններն են, ապա $k = l$ և $\alpha_1 = \beta_1$: Այժմ

$$\alpha_1 \cdots \alpha_t = \beta_1 \cdots \beta_s$$

հավասարության երկու կողմերը ձախից բազմապատկելով $\alpha_1^{-1} = \beta_1^{-1}$-ով կստանանք՝

$$\alpha_2 \cdots \alpha_t = \beta_2 \cdots \beta_s;$$

Համանման եղանակով, ստացված հավասարությունը հերթով կրճատելով α_2-ով, $\ldots$, α_t-ով, վերջավոր թվով քայլերից հետո կհասնենք մի հավասարության, որի ձախ մասը ε նույնական տեղադրությունն է, իսկ աջ մասում դեռևս կմնան β_j արտապատկերումներ, որոնց արտադրյալի շարժուն կետերի բազմությունը համաձայն հետևություն 13.7-ի չի լինի դատարկ, մինչդեռ $mob(\varepsilon) = \emptyset$: Ստացված հակասությունն ապացուցում է թեորեմի միակության մասը: $\square$

Օրինակ՝

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 4 & 5 & 3 & 6 & 1 \end{pmatrix} = (1,2,7) \cdot (3,4,5),$$

որը ստացվում է նաև համաձայն թեորեմի ապացուցման ընթացքի: Իրոք, եթե

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 4 & 5 & 3 & 6 & 1 \end{pmatrix},$$

ապա $mob(\alpha) = \{1,2,3,4,5,7\}$: Ընտրելով, օրինակ, $a = 1 \in mob(\alpha)$ կունենանք՝ $\alpha(1) = 2$, $\alpha^2(1) = \alpha(2) = 7$, $\alpha^3(1) = \alpha(7) = 1$: Հետևաբար՝

$$\alpha_1 = (1,2,7) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 3 & 4 & 5 & 6 & 1 \end{pmatrix},$$

և

$$\alpha_1^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 4 & 5 & 6 & 2 \end{pmatrix} = (1,7,2);$$

Ուստի՝

$$\beta_1 = \alpha_1^{-1} \cdot \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 5 & 3 & 6 & 7 \end{pmatrix} = (3,4,5);$$

Այսպիսով՝

$$\alpha = \alpha_1 \cdot \beta_1 = (1,2,7) \cdot (3,4,5) :$$

Վարժություններ և խնդիրներ

1. Հետևյալ հավասարությունից գտնել 6-րդ աստիճանի X տեղադրությունը՝

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 6 & 5 \end{pmatrix} \cdot X \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 5 & 2 & 6 \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 4 & 6 & 1 \end{pmatrix}:$$

2. Գտնել α^{101}-ը, եթե

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 1 & 7 & 6 & 2 & 9 & 8 \end{pmatrix}:$$

3. Գտնել α^{100}-ը, եթե

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 3 & 5 & 2 & 4 & 7 & 8 & 6 & 9 \end{pmatrix}:$$

4. Գտնել α^{144}-ը, եթե

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 4 & 6 & 9 & 7 & 2 & 1 & 8 \end{pmatrix}:$$

5. Որոշել $(1, 3, 2)$ և $(2, 3, 1)$ տեղափոխությունների արտադրյալը:

6. Որոշել

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{pmatrix}$$

տեղադրության նշանը:

7. Որոշել n-րդ աստիճանի բոլոր տեղադրությունների նշանների արտադրյալը:

Գ լ ու խ 14

ՄԱՏՐԻՑՆԵՐ ԵՎ ՈՐՈՇԻՉՆԵՐ

14.1. Մատրիցի գաղափարը: Գործողություններ մատրիցների հետ

$n \times m$ հատ a_{ij} իրական թվերի

$$A = (a_{11}, \ldots, a_{1m}, \ldots, a_{n1}, \ldots, a_{nm})$$

հաջորդականությունը՝ ներկայացված n հատ տողերով և m հատ սյունակներով ու գրված

$$A = \begin{pmatrix} a_{11}, \ldots, a_{1m} \\ \cdots \quad \cdots \quad \cdots \\ a_{n1}, \ldots, a_{nm} \end{pmatrix}$$

աղյուսակի տեսքով, կոչվում է $n \times m$-չափանի մատրից, իսկ $a_{ij} \in \mathbb{R}$ մեծությունները ($i = 1, \ldots, n$; $j = 1, \ldots, m$) կոչվում են A **մատրիցի տարրեր**, որոնք երբեմն գրվում են առանց (անջատող) ստորակետների: Ընդ որում, a_{ij}-ն երբեմն նշանակվում է $a_{i,j}$-ով և կարդացվում է «ա-ի-ժի» (օրինակ, a_{11}-ը կարդացվում է «ա-մեկ-մեկ», բայց ոչ թե «ա-տասնմեկ»): a_{ij} տարրի առաջին i նշիչը կոչվում է **տողի նշիչ** և ցույց է տալիս այն տողի համարը, որում գտնվում է տվյալ տարրը, իսկ երկրորդ j նշիչը՝ **սյունակի նշիչ** և ցույց է տալիս այն սյունակի համարը, որում գտնվում է մատրիցի տարրը: Եթե $n = 1$, ապա $n \times m$-չափանի A մատրիցը դառնում է **տող** կամ **վեկտոր**, ավելի ճիշտ m-տող կամ m-վեկտոր՝ $A = (a_{11}, \ldots, a_{1m})$: $A_i = (a_{i1}, \ldots, a_{im})$ տողը կոչվում է $n \times m$-չափանի A մատրիցի i-րդ տող, իսկ $i = 1, 2, \ldots$ դեպքում՝ առաջին տող, երկրորդ տող, ...: Եթե $m = 1$, ապա $n \times m$-չափանի A մատրիցը կոչվում է **սյունակ**, կամ n-սյունակ՝

$$A = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix},$$

իսկ n-ը կոչվում է սյունակի բարձրություն (երբեմն սյունակը, ինչպես և տողը, նշվում է առանց փակագծերի): Հետևյալ

$$A_i' = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}$$

սյունակը կոչվում է վերոհիշյալ $n \times m$-չափանի A մատրիցի i-րդ սյունակ, իսկ $i = 1, 2, \ldots$ դեպքում՝ առաջին սյունակ, երկրորդ սյունակ, $\ldots$: Ընդունված է նաև $n \times m$-չափանի A մատրիցի համառոտ նշանակման հետևյալ տարբերակները՝ $A = (a_{ij})_{n \times m}$, $A = (a_{ij})$, ըստ տողերի՝ $A = \begin{pmatrix} A_1 \\ \vdots \\ A_n \end{pmatrix}$ կամ ըստ սյունակների՝ $A = (A_1', \ldots, A_m')$:

Երկու $n \times m$-չափանի $A = (a_{ij})$ և $B = (b_{ij})$ մատրիցների միևնույն նշիչներով a_{ij} և b_{ij} տարրերը կոչվում են **համապատասխան տարրեր**: Երկու մատրիցներ կոչվում են **միևնույն չափանի**, եթե նրանք ունեն միևնույն քանակի տողեր և միևնույն քանակի սյունակներ:

Կարգավորված n-յակների հավասարության պայմանից բխում է մատրիցների հավասարության հետևյալ պայմանը:

Լեմմ 14.1: *Որպեսզի երկու միևնույն չափանի մատրիցներ լինեն հավասար անհրաժեշտ է և բավարար, որ նրանց համապատասխան տարրերը լինեն հավասար:* $\square$

A և B մատրիցների հավասարությունը նշանակվում է $A = B$ ձևով, հակառակ դեպքում գրվում է՝ $A \neq B$:

$n \times m$-չափանի մատրիցները կոչվում են նաև **ուղղանկյուն մատրիցներ**: $n \times m$-չափանի $A = (a_{ij})$ մատրիցը կոչվում է **n-րդ կարգի** կամ **քառակուսային**, եթե $n = m$; n-րդ կարգի $A = (a_{ij})$ մատրիցի $a_{11}, \ldots, a_{nn}$ տարրերի հաջորդականությունը կոչվում (կազմում) է նրա **գլխավոր անկյունագիծ**:

n-րդ կարգի մատրիցը կոչվում է **անկյունագծային**, եթե նրա գլխավոր անկյունագծից դուրս գտնվող բոլոր տարրերը հավասար են զրոյի: Անկյունագծային մատրիցը կոչվում է **սկալյար**, եթե նրա գլխավոր անկյունագծի վրա դասավորված բոլոր տարրերը հավասար են: Եվ վերջապես, n-րդ կարգի մատրիցը կոչվում է **վերին** (ներքին)

եռանկյունաձև, եթե նրա գլխավոր անկյունագծից ներքև (վերև) գտնվող բոլոր տարրերը հավասար են զրոյի, այսինքն՝ $a_{ij} = 0$, եթե $i > j$ (համապատասխանաբար, $a_{ij} = 0$, եթե $i < j$)։ Ակնհայտ է, որ յուրաքանչյուր անկյունագծային մատրից վերին և ներքին (ստորին) եռանկյունաձև է։

Ելնելով իրական թվերի նկատմամբ կատարվող գործողություններից, սահմանվում են գործողություններ նաև իրական թվերով մատրիցների հետ։ Սկսենք գումարման գործողությունից, որը սահմանվում է երկու միևնույն չափանի մատրիցների համար (միջև)։

$n \times m$-չափանի $A = (a_{ij})$ և $B = (b_{ij})$ **մատրիցների գումար** է կոչվում այն $n \times m$-չափանի $C = (c_{ij})$ մատրիցը, որի յուրաքանչյուր տարր հավասար է A և B մատրիցների համապատասխան տարրերի գումարին՝

$$c_{ij} = a_{ij} + b_{ij}\,;$$

Այս դեպքում գրվում է՝ $C = A + B$։ Այսպիսով՝

$$\begin{pmatrix} a_{11}, \ldots, a_{1m} \\ \cdots \quad \cdots \quad \cdots \\ a_{n1}, \ldots, a_{nm} \end{pmatrix} + \begin{pmatrix} b_{11}, \ldots, b_{1m} \\ \cdots \quad \cdots \quad \cdots \\ b_{n1}, \ldots, b_{nm} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11}, \ldots, a_{1m} + b_{1m} \\ \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ a_{n1} + b_{n1}, \ldots, a_{nm} + b_{nm} \end{pmatrix} :$$

Այստեղից, մասնավորապես, ստանում ենք երկու m-տողերի, կամ երկու n-սյունակների գումարման կանոնը՝

$$(a_{11}, \ldots, a_{1m}) + (b_{11}, \ldots, b_{1m}) = (a_{11} + b_{11}, \ldots, a_{1m} + b_{1m})\,,$$

$$\begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} + \begin{pmatrix} b_{11} \\ \vdots \\ b_{n1} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} \\ \vdots \\ a_{n1} + b_{n1} \end{pmatrix} :$$

Թվարկենք մատրիցների գումարման պարզագույն հատկությունները, որոնց ապացույցները ակնհայտ են և հեշտությամբ ստացվում են իրական թվերի գումարման համապատասխան հատկություններից։

1. Մատրիցների գումարը տեղափոխական է, այսինքն՝ $n \times m$-չափանի ցանկացած A և B մատրիցների համար՝

$$A + B = B + A\,;$$

2. Մատրիցների գումարը զուգորդական է, այսինքն՝ $n \times m$-չափանի ցանկացած A, B և C մատրիցների համար՝

$$A + (B + C) = (A + B) + C\,;$$

3. Գոյություն ունի այնպիսի $n \times m$-չափանի X մատրից, որ ցանկացած $n \times m$-չափանի A մատրիցի համար՝

$$A + X = X + A = A\,;$$

Այդ $n \times m$-չափանի X մատրիցը որոշվում է միարժեքորեն՝

$$X = \begin{pmatrix} 0, \ldots, 0 \\ \cdots\ \cdots \\ 0, \ldots, 0 \end{pmatrix}$$

և այն կոչվում է $n \times m$-չափանի **զրոյական մատրից** ու սովորաբար նշանակվում է $O_{n\times m}$-ով, կամ պարզապես O-ով: Յուրաքանչյուր $B \neq O$ մատրից կոչվում է **ոչ զրոյական**:

4. Յուրաքանչյուր $n \times m$-չափանի A մատրիցի համար գոյություն ունի $n \times m$-չափանի այնպիսի A' մատրից, որ

$$A + A' = A' + A = O\,;$$

Ըստ որում, A' մատրիցը որոշվում է միարժեքորեն և կոչվում է տրված A մատրիցի **հակադիր մատրից** ու նշանակվում է $-A$-ով՝

$$-A = \begin{pmatrix} -a_{11}, \ldots, -a_{1m} \\ \cdots \quad \cdots \quad \cdots \\ -a_{n1}, \ldots, -a_{nm} \end{pmatrix},$$

եթե

$$A = \begin{pmatrix} a_{11}, \ldots, a_{1m} \\ \cdots \quad \cdots \quad \cdots \\ a_{n1}, \ldots, a_{nm} \end{pmatrix}:$$

Ակնհայտ է, որ $-(A + B) = (-A) + (-B)$:

Հետևյալ արդյունքը բխում է թեորեմ 1.3-ից:

Հատկություն 14.1: *Միևնույն $n \times m$-չափանի մատրիցների $A_1, \ldots, A_s$ հաջորդականությունից փակագծերի տարբեր դասավորությամբ ստացվող բոլոր գումարները միմյանց հավասար են և այդ պատճառով էլ դրանցից յուրաքանչյուրը կարելի է գրել առանց փակագծերի՝ $A_1 + \cdots + A_s$, որտեղ $s \geqslant 3$:* □

Սահմանենք **թվի** (ձախից) **բազմապատկումը մատրիցով**: Եթե c-ն իրական թիվ է, իսկ

$$A = \begin{pmatrix} a_{11}, \ldots, a_{1m} \\ \cdots \quad \cdots \quad \cdots \\ a_{n1}, \ldots, a_{nm} \end{pmatrix},$$

ապա

$$c \cdot A = \begin{pmatrix} ca_{11}, \ldots, ca_{1m} \\ \cdots \quad \cdots \quad \cdots \\ ca_{n1}, \ldots, ca_{nm} \end{pmatrix} :$$

$c \cdot A$-ն հաճախ նշվում է առանց բազմապատկման նշանի՝ cA, որի հետևանքով խնայվում են բազմաթիվ փակագծեր: Օրինակ, $c_1A + c_2B$-ն նշանակում է՝ $(c_1 \cdot A) + (c_2 \cdot B)$:

Ցանկացած $n \times m$-չափանի A և B մատրիցների և կամայական c_1, c_2 իրական թվերի համար տեղի ունեն հետևյալ հավասարությունները, որոնք անմիջապես ստացվում են սահմանումներից՝

$$(c_1 + c_2)A = c_1A + c_2A,$$

$$c_1(A + B) = c_1A + c_1B,$$

$$(c_1c_2)A = c_1(c_2A),$$

$$1 \cdot A = A :$$

$$(-1) \cdot A = -A,$$

$$(-c_1)A = -(c_1A) :$$

Վերհանգման եղանակով առաջին երկու հավասարությունները տարածվում են նաև ցանկացած վերջավոր թվով գումարելիների դեպքի վրա՝

$$(c_1 + \cdots + c_k)A = c_1A + \cdots + c_kA,$$

$$c_1(A_1 + \cdots + A_k) = c_1A_1 + \cdots + c_1A_k \ :$$

Դիցուք $A, A_1, \ldots, A_s$ մատրիցները միևնույն $n \times m$-չափանի մատրիցներ են: Կասենք, որ A մատրիցը **գծայնորեն** (գծորեն) **արտահայտվում է** $A_1, \ldots, A_s$ մատրիցների միջոցով, եթե գոյություն ունեն այնպիսի $c_1, \ldots, c_s$ իրական թվեր, որ

$$A = c_1A_1 + \cdots + c_sA_s \ :$$

$s = 1$ դեպքում A մատրիցը կոչվում է **համեմատական** A_1 մատրիցին: $n \times m$-չափանի A և B մատրիցները կոչվում են **համեմատական**, եթե կամ A-ն է համեմատական B-ին կամ B-ն է համեմատական A-ին:

$n \times m$-չափանի $B_1, \ldots, B_k$ մատրիցների հաջորդականությունը կոչվում է **գծայնորեն** (գծորեն) **կախյալ**, եթե գոյություն ունեն այնպիսի $\alpha_1, \ldots, \alpha_k$ իրական թվեր, որոնցից գոնե մեկը զրո չէ և

$$\alpha_1 B_1 + \cdots + \alpha_k B_k = 0 \ :$$

Հակառակ դեպքում, $n \times m$-չափանի $B_1, \ldots, B_k$ մատրիցների հաջորդականությունը կոչվում է **գծայնորեն** (գծորեն) **անկախ**, այսինքն՝ երբ

$$\alpha_1 B_1 + \cdots + \alpha_k B_k = 0 \longrightarrow \alpha_1 = \cdots = \alpha_k = 0 \ :$$

Լեմմ 14.2: *Որպեսզի $n \times m$-չափանի $B_1, \ldots, B_k$ մատրիցների հաջորդականությունը ($k > 1$) լինի գծայնորեն կախյալ անհրաժեշտ է և բավարար, որ այդ մատրիցներից գոնե մեկը գծայնորեն արտահայտվի մյուս մատրիցների միջոցով:* □

Անցնենք՝ իրական թվերով մատրիցների բազմապատկման (արտադրյալ) գործողությանը:

Իրական թվերով երկու $A = (a_{ij})$ և $B = (b_{ij})$ մատրիցների արտադրյալը սահմանվում է այն դեպքում, երբ A մատրիցը $n \times m$-չափանի է, իսկ B մատրիցը $m \times k$-չափանի, այսինքն A մատրիցի սյունակների թիվը հավասար է B մատրիցի տողերի թվին: Այդ դեպքում, A և B **մատրիցների** $A \cdot B$ **արտադրյալ** ասելով հասկացվում է այն $C = (c_{ij})$ մատրիցը, որը $n \times k$-չափանի է, իսկ դրա յուրաքանչյուր c_{ij} տարր որոշվում է հետևյալ բանաձևով՝

$$c_{ij} = a_{i1} b_{1j} + a_{i2} b_{2j} + \cdots + a_{im} b_{mj} = \sum_{\alpha=1}^{m} a_{i\alpha} b_{\alpha j} \ :$$

Եթե որոշված են $A \cdot B$ և $B \cdot A$ արտադրյալները, ապա ըստ սահմանման՝ A-ի սյունակների թիվը հավասար կլինի B-ի տողերի թվին, իսկ B-ի սյունակների թիվը՝ A-ի տողերի թվին: Հետևաբար՝ $A \cdot B$ և $B \cdot A$ արտադրյալները կլինեն քառակուսային մատրիցներ, սակայն տարբեր չափերի, եթե A-ն և B-ն քառակուսային չեն:

Միևնույն կարգի երկու A և B քառակուսային մատրիցներ կոչվում են **տեղափոխական** (տեղափոխելի), եթե

$$A \cdot B = B \cdot A ;$$

Օրինակ, կամայական n-րդ կարգի A մատրիցի համար՝

$$A \cdot E = E \cdot A = A,$$

որտեղ E-ն n-րդ կարգի միավոր մատրիցն է՝

$$E = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \cdots & & \cdots & & \cdots \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

այսինքն՝ գլխավոր անկյունագծի բոլոր տարրերը հավասար են մեկի, իսկ մնացած բոլոր տարրերը՝ զրոյի: Եթե n-րդ կարգի միավոր մատրիցը նշանակենք E_n-ով, ապա կամայական $n \times m$-չափանի A մատրիցի համար կունենանք՝ $A \cdot E_m = E_n \cdot A = A$:

Ցանկացած $n \geqslant 2$ բնական թվի համար դժվար չէ կառուցել n-րդ կարգի երկու այնպիսի A և B մատրիցների օրինակներ, որ $A \cdot B \neq B \cdot A$: Օրինակ,

$$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & \cdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & \cdots & \\ 1 & 0 & \cdots & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & \cdots & \\ 1 & 0 & \cdots & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \cdots & & \cdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix} :$$

Հետևյալ հատկությունները հեշտությամբ ստացվում են մատրիցների արտադրյալի և գումարի սահմանումներից՝

$$(cA)B = A(cB) = c(A \cdot B),$$

$$(A_1 + A_2)B = A_1 B + A_2 B,$$

$$A(B_1 + B_2) = AB_1 + AB_2,$$

որտեղ A, A_1, A_2 մատրիցները $n \times m$-չափանի, B, B_1, B_2 մատրիցները $m \times k$-չափանի ցանկացած մատրիցներ են, իսկ c-ն կամայական իրական թիվ է: Վերհանգման եղանակով վերջին երկու հավասարությունները տարածվում են նաև ցանկացած վերջավոր թվով գումարելիների դեպքի վրա՝

$$(A_1 + \cdots + A_t)B = A_1 B + \cdots + A_t B,$$

$$A(B_1 + \cdots + B_t) = AB_1 + \cdots + AB_t \ :$$

Այժմ ապացուցենք մատրիցների արտադրյալի զուգորդականության հետևյալ կարևոր հատկությունը:

Թեորեմ 14.1*: Ցանկացած A, B, C մատրիցների համար՝*

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C, \quad (\textit{զուգորդական օրենք})$$

որտեղ A-ն $n \times m$-չափանի, B-ն $m \times k$-չափանի, իսկ C-ն $k \times s$-չափանի մատրիցներ են: Ավելի ճիշտ, ցանկացած A, B և C մատրիցների համար, եթե նշված հավասարության կողմերից որևէ մեկը որոշված է (այսինքն գոյություն ունի), ապա մյուս կողմը ևս կլինի որոշված և նրանք կլինեն հավասար:

Ապացուցում: Դիցուք $A = (a_{ij})_{n\times m}$, $B = (b_{ij})_{m\times k}$, $C = (c_{ij})_{k\times s}$, $A \cdot B = (d_{ij})_{n\times k}$, $(A \cdot B) \cdot C = (u_{ij})_{n\times s}$, $B \cdot C = (v_{ij})_{m\times s}$, $A \cdot (B \cdot C) = (w_{ij})_{n\times s}$: Պահանջվում է ապացուցել $u_{ij} = w_{ij}$ հավասարությունը՝ բոլոր $i = 1, \ldots, n$ և $j = 1, \ldots, s$ արժեքների դեպքում: Իրոք,

$$u_{ij} = \sum_{l=1}^{k} d_{il} c_{lj} = \sum_{l=1}^{k} \left(\sum_{t=1}^{m} a_{it} b_{tl} \right) c_{lj} = \sum_{l,t} a_{it} b_{tl} c_{lj},$$

$$w_{ij} = \sum_{t=1}^{m} a_{it} v_{tj} = \sum_{t=1}^{m} a_{it} \left(\sum_{l=1}^{k} b_{tl} c_{lj} \right) = \sum_{l,t} a_{it} b_{tl} c_{lj} \ : \qquad \square$$

Ապացուցված զուգորդական օրենքից, վերհանգման եղանակով, բխում է նաև մատրիցների արտադրյալի (բազմապատկման) ընդհանրացված զուգորդականության հետևյալ հատկությունը:

Հատկություն 14.2*: Եթե A_1 մատրիցը $m_1 \times m_2$-չափանի է, A_2 մատրիցը $m_2 \times m_3$-չափանի է, ..., A_n մատրիցը $m_n \times m_{n+1}$-չափանի է, ապա $A_1, A_2, \ldots, A_n$ հաջորդականությունից փակագծերի տարբեր դասավորությամբ ստացվող բոլոր արտադրյալները միմյանց հավասար են: Հետևաբար, այդ արտադրյալներից յուրաքանչյուրը կարելի է գրել առանց փակագծերի՝ $A_1 \cdot A_2 \cdots A_n$, որտեղ $n \geqslant 3$:* $\square$

Մասնավորապես, սահմանվում է n-րդ կարգի ցանկացած A մատրիցի բնական ցուցիչով աստիճանը՝

$$A^0 = E_n \,,$$

$$A^k = \underbrace{A \cdot A \cdots A}_{k}, \quad k > 0 \ :$$

Ակնհայտ է, որ

$$A^{k_1} \cdot A^{k_2} = A^{k_1+k_2}\,,$$

$$\left(A^{k_1}\right)^{k_2} = A^{k_1 \cdot k_2} \ \ :$$

Անցնենք շրջված մատրիցի գաղափարին:

Եթե $n \times m$-չափանի A մատրիցի տողերը դարձնենք համապատասխան համարների սյունակներ (այսինքն՝ առաջին տողը դարձնենք առաջին սյունակ, երկրորդ տողը՝ երկրորդ սյունակ, $\ldots$), ապա ստացված $m \times n$-չափանի մատրիցը կոչվում է A-ի **շրջված մատրից** և նշանակվում է A^T-ով: Այսպիսով, $m \times n$-չափանի $S = (s_{ij})$ մատրիցը կոչվում է $n \times m$-չափանի $A = (a_{ij})$ մատրիցի **շրջված մատրից**, եթե $s_{ij} = a_{ji}$, որտեղ $i = 1, \ldots, m$ և $j = 1, \ldots, n$:

Հետևյալ հավասարություններն ակնհայտ են՝

$$\left(A^T\right)^T = A,$$

$$(A + B)^T = A^T + B^T,$$

$$(\alpha A)^T = \alpha A^T$$

ցանկացած $n \times m$-չափանի A, B մատրիցների և ցանկացած α իրական թվի համար:

Ապացուցենք հետևյալ հատկությունը.

Հատկություն 14.3: *Ցանկացած A և B մատրիցների համար՝*

$$(A \cdot B)^T = B^T \cdot A^T,$$

որտեղ A-ն $n \times m$-չափանի է, իսկ B-ն $m \times k$-չափանի: Ավելի ճիշտ, եթե նշված հավասարության կողմերից որևէ մեկը որոշված է, ապա մյուս կողմը ևս կլինի որոշված և նրանք կլինեն հավասար:

Ապացուցում: Դժվար չէ նկատել, որ եթե հավասարության կողմերից որևէ մեկը որոշված է և A մատրիցը $n \times m$-չափանի է, ապա B-ն կլինի $m \times k$-չափանի: Հետևաբար, եթե հավասարության մի կողմը որոշված է, ապա մյուս կողմը ևս կլինի որոշված: Ապացուցենք հավասարությունը:

Դիցուք՝

$$A = (a_{ij})\,, \quad B = (b_{ij})\,,$$

$$A^T = C = (c_{ij})\,, \quad B^T = D = (d_{ij})\,,$$
$$AB = F = (f_{ij})\,, \quad B^T \cdot A^T = G = (g_{ij})\ ;$$

Այդ դեպքում՝

$$g_{ji} = \sum_{t=1}^{m} d_{jt}c_{ti} = \sum_{t=1}^{m} b_{tj}a_{it} = \sum_{t=1}^{m} a_{it}b_{tj} = f_{ij},$$

որտեղ $i = 1, \ldots, n$ և $j = 1, \ldots, k$: Այսպիսով՝

$$G = F^T,$$

այսինքն՝

$$B^T \cdot A^T = (A \cdot B)^T\ : \qquad \square$$

n-րդ կարգի A մատրիցը կոչվում է **սիմետրիկ** (կամ շրջուն), եթե այն համընկնում է իր շրջված մատրիցի հետ՝

$$A^T = A\,,$$

և **շեղսիմետրիկ** (կամ շեղշրջուն), եթե

$$A^T = -A\ :$$

n-րդ կարգի A մատրիցը կոչվում է **օրթոգոնալ**, եթե

$$A \cdot A^T = A^T \cdot A = E\ :$$

n-րդ կարգի բոլոր օրթոգոնալ մատրիցների բազմությունը նշանակվում է $\mathcal{O}_n(\mathbb{R})$-ով: Ակնհայտ է, որ

ա) $E_n \in \mathcal{O}_n(\mathbb{R})$,

բ) $A \in \mathcal{O}_n(\mathbb{R}) \longrightarrow A^T \in \mathcal{O}_n(\mathbb{R})$,

գ) $A, B \in \mathcal{O}_n(\mathbb{R}) \longrightarrow A \cdot B \in \mathcal{O}_n(\mathbb{R})$:

14.2. Հակադարձելի մատրիցներ

n-րդ կարգի A մատրիցը կոչվում է.

ա) **հակադարձելի աջից**, եթե գոյություն ունի այնպիսի n-րդ կարգի A' մատրից, որ $A \cdot A' = E_n$;

բ) **հակադարձելի ձախից**, եթե գոյություն ունի այնպիսի n-րդ կարգի A'' մատրից, որ $A'' \cdot A = E_n$;

գ) **հակադարձելի**, եթե գոյություն ունի այնպիսի n-րդ կարգի B մատրից, որ

$$A \cdot B = B \cdot A = E_n \ :$$

Ըստ որում, վերջին հավասարությունով n-րդ կարգի B մատրիցը որոշվում է միարժեքորեն և այն կոչվում է A-ի **հակադարձ** (մատրից) ու նշանակվում է՝ $B = A^{-1}$; Դեռ ավելին, եթե n-րդ կարգի A մատրիցը հակադարձելի է աջից ու ձախից, ապա այն կլինի հակադարձելի: Իրոք, եթե $A \cdot A' = E_n$ և $A'' \cdot A = E_n$, ապա

$$A'' = A'' \cdot E_n = A''(A \cdot A') = (A'' \cdot A) \cdot A' = E_n \cdot A' = A' :$$

Մասնավորապես, եթե $A \cdot B = B \cdot A = E$ և $A \cdot B^* = B^* \cdot A = E$, ապա $B = B^*$:

n-րդ կարգի բոլոր հակադարձելի մատրիցների բազմությունը ընդունված է նշանակել $GL_n(\mathbb{R})$-ով:

Օրինակ, ցանկացած n-րդ կարգի օրթոգոնալ A մատրից հակադարձելի է, ըստ որում՝

$$A^{-1} = A^T \ :$$

Մինչդեռ, եթե n-րդ կարգի A մատրիցի որևէ տող (սյունակ) զրոյական է, ապա A-ն հակադարձելի չէ աջից (ձախից), որովհետև զրոյական տողի դեպքում,

$$A \cdot A' = E_n$$

հավասարության ձախ մասում կունենանք զրոյական տող ունեցող $A \cdot A'$ մատրիցը, իսկ զրոյական սյունակի դեպքում,

$$A'' \cdot A = E_n$$

հավասարության ձախ մասում կունենանք զրոյական սյունակ ունեցող $A'' \cdot A$ մատրիցը: Երկու դեպքում էլ հանգում ենք հակասության:

Հատկություն 14.4: *ա) Եթե n-րդ կարգի A մատրիցը հակադարձելի է, ապա դրա հակադարձ A^{-1} մատրիցը ևս կլինի հակադարձելի, ընդ որում՝*

$$\left(A^{-1}\right)^{-1} = A;$$

բ) Եթե n-րդ կարգի A և B մատրիցները հակադարձելի են, ապա դրանց $A \cdot B$ արտադրյալը ևս կլինի հակադարձելի, ընդ որում՝

$$(A \cdot B)^{-1} = B^{-1} \cdot A^{-1} \,;$$

գ) Եթե n-րդ կարգի $A_1, A_2, \dots, A_m$ մատրիցները հակադարձելի են, ապա դրանց $A_1 \cdot A_2 \cdots A_m$ արտադրյալը ևս կլինի հակադարձելի, ընդ որում՝

$$(A_1 \cdot A_2 \cdots A_m)^{-1} = A_m^{-1} \cdot A_{m-1}^{-1} \cdots A_1^{-1} \;:$$

Ապացուցում: ա) և բ) պնդումները բխում են հակադարձելիության և հակադարձի սահմանումներից (ու հակադարձի միակությունից): գ) պնդումն ապացուցվում է վերհանգման եղանակով: □

Դիտարկենք հակադարձելի մատրիցների հետևյալ երեք կարևոր դասերը (որոնք կոչվում են նաև **տարրական մատրիցներ**):

1) Կամայական α իրական թվի և ցանկացած $i \neq j$ նշիչների համար սահմանենք n-րդ կարգի հետևյալ մատրիցը՝

$$T_{ij}(\alpha) = \begin{array}{cc} & \begin{array}{cccccc} & & & j & & \end{array} \\ \begin{array}{c} \\ \\ \\ i \\ \\ \\ \end{array} & \left(\begin{array}{cccccc} 1 & & & & & \\ & 1 & & & & \\ & & \ddots & & & \\ & & & \alpha & & \\ & & & & \ddots & \\ & & & & & 1 \end{array}\right) \end{array},$$

այսինքն՝ այս մատրիցի գլխավոր անկյունագծի բոլոր տարրերը հավասար են մեկի, i-րդ տողի և j-րդ սյունակի հատման տեղում կանգնած է α թիվը, իսկ նրա մյուս բոլոր տարրերը հավասար են զրոյի: Այսպիսով, $T_{ij}(\alpha)$ մատրիցի t_{pq} տարրերը որոշվում են հետևյալ կերպ՝

$$t_{pq} = \begin{cases} 1, & \text{եթե } p = q, \\ \alpha, & \text{եթե } p = i, q = j, \\ 0, & \text{մնացած բոլոր դեպքերում :} \end{cases}$$

2) Ցանկացած $\alpha \neq 0$ իրական թվի և կամայական i նշիչի համար սահմանենք n-րդ կարգի հետևյալ մատրիցը՝

$$L_i(\alpha) = \begin{array}{cc} & \begin{array}{cccccc} & & & i & & & \end{array} \\ \begin{array}{c} \\ \\ \\ i \\ \\ \\ \\ \end{array} & \left(\begin{array}{ccccccc} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \alpha & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{array}\right) \end{array},$$

այսինքն՝ $L_i(\alpha)$ մատրիցի ℓ_{pq} տարրերը որոշվում են հետևյալ կերպ՝

$$\ell_{pq} = \begin{cases} \alpha, & \text{եթե } p = q = i, \\ 1, & \text{եթե } p = q \neq i, \\ 0, & \text{մնացած բոլոր դեպքերում :} \end{cases}$$

3)Ցանկացած $i \neq j$ նշիչների համար սահմանենք n-րդ կարգի հետևյալ մատրիցը՝

$$S_{ij} = \begin{array}{c} \\ \\ \\ i \\ \\ j \\ \\ \end{array} \begin{array}{c} \begin{array}{ccccc} & i & & j & \end{array} \\ \begin{pmatrix} \begin{smallmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{smallmatrix} & \vdots & & \vdots & \\ \cdots & 0 & \cdots & 1 & \cdots \\ & \vdots & \begin{smallmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{smallmatrix} & \vdots & \\ \cdots & 1 & \cdots & 0 & \cdots \\ & \vdots & & \vdots & \begin{smallmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{smallmatrix} \end{pmatrix} \end{array},$$

որի s_{pq} տարրերը որոշվում են հետևյալ կերպ՝

$$s_{pq} = \begin{cases} 1, & \text{եթե } p = q \neq i, j, \\ 1, & \text{եթե } p = i, q = j, \text{ կամ } p = j, q = i, \\ 0, & \text{մնացած բոլոր դեպքերում :} \end{cases}$$

Լեմմ 14.3: *$n \times m$-չափանի A մատրիցի ձախից (աջից) բազմապատկումը n-րդ (m-րդ) կարգի $T_{ij}(\alpha)$ մատրիցով նշանակում է A-ի i-րդ տողին (j-րդ սյունակին) ավելացնել նրա j-րդ տողը (i-րդ սյունակը) նախապես այն բազմապատկելով α-ով: $T_{ij}(\alpha)$ մատրիցը հակադարձելի է, ընդ որում՝*

$$(T_{ij}(\alpha))^{-1} = T_{ij}(-\alpha)$$

Ապացուցում: Եթե $B = T_{ij}(\alpha) \cdot A$, ապա

$$b_{pq} = t_{p1}a_{1q} + t_{p2}a_{2q} + \cdots + t_{pn}a_{nq} = \begin{cases} t_{ii}a_{iq} + t_{ij}a_{jq} = a_{iq} + \alpha a_{jq}, \\ \qquad \text{եթե } p = i, \\ t_{pp}a_{pq} = a_{pq}, \\ \qquad \text{եթե } p \neq i; \end{cases}$$

Նույն եղանակով ստանում ենք աջից բազմապատկման կանոնը: Ապացուցենք երկրորդ պնդումը՝

$$T_{ij}(-\alpha) \cdot T_{ij}(\alpha) = T_{ij}(\alpha) \cdot T_{ij}(-\alpha) = E_n \,;$$

Իրոք, $T_{ij}(-\alpha)$ մատրիցի ձախից բազմապատկումը $T_{ij}(\alpha)$-ով նշանակում է $T_{ij}(-\alpha)$-ի i-րդ $\left(0,\ldots,0,\underset{i}{1},0,\ldots,0,\overset{j}{-\alpha},0,\ldots,0\right)$ տողին ավելացնել նրա j-րդ տողը՝ նախապես այն բազմապատկելով α-ով՝

$$\alpha\cdot\left(0,\ldots,0,\underset{j}{1},0,\ldots,0\right)=\left(0,\ldots,0,\underset{j}{\alpha},0,\ldots,0\right);$$

Հետևաբար, $T_{ij}(\alpha)\cdot T_{ij}(-\alpha)$ արտադրյալի i-րդ տողը կլինի նույնը ինչ որ E_n-ի i-րդ տողը, իսկ մնացած տողերը համընկնում են $T_{ij}(-\alpha)$-ի համապատասխան տողերի հետ: Այսպիսով՝

$$T_{ij}(\alpha)\cdot T_{ij}(-\alpha)=E_n;$$

Համանման եղանակով ապացուցվում է նաև

$$T_{ij}(-\alpha)\cdot T_{ij}(\alpha)=E_n$$

հավասարությունը: □

Լեմմ 14.4*: $n\times m$-չափանի A մատրիցի ձախից (աջից) բազմապատկումը n-րդ (m-րդ) կարգի $L_i(\alpha)$ մատրիցով նշանակում է A-ի i-րդ տողը (սյունակը) բազմապատկել α-ով: $L_i(\alpha)$ մատրիցը հակադարձելի է, ընդ որում՝ $(L_i(\alpha))^{-1}=L_i\left(\alpha^{-1}\right)$:*

Ապացուցում: Եթե $C=L_i(\alpha)\cdot A$, ապա

$$c_{pq}=\ell_{p1}a_{1q}+\ell_{p2}a_{2q}+\cdots+\ell_{pn}a_{nq}=\begin{cases}\alpha a_{iq}, & \text{եթե } p=i,\\ a_{pq}, & \text{եթե } p\neq i\ :\end{cases}$$

Նույն եղանակով ստանում ենք աջից բազմապատկման կանոնը: Հեշտությամբ ստուգվում է նաև

$$L_i\left(\alpha^{-1}\right)\cdot L_i(\alpha)=L_i(\alpha)\cdot L_i\left(\alpha^{-1}\right)=E_n$$

հավասարությունը: □

Լեմմ 14.5*: $n\times m$-չափանի A մատրիցի ձախից (աջից) բազմապատկումը n-րդ (m-րդ) կարգի S_{ij} մատրիցով նշանակում է A-ի i-րդ և j-րդ տողերի (սյունակների) տեղափոխություն: S_{ij} մատրիցը հակադարձելի է, ընդ որում՝*

$$S_{ij}^{-1}=S_{ij}\ ;$$

Ապացուցում: Եթե $D = S_{ij} \cdot A$, ապա

$$d_{pq} = s_{p1}a_{1q} + s_{p2}a_{2q} + \cdots + s_{pn}a_{nq} = \begin{cases} s_{ij}a_{jq} = a_{jq}, & \text{եթե } p = i, \\ s_{ji}a_{iq} = a_{iq}, & \text{եթե } p = j, \\ s_{pp}a_{pq} = a_{pq}, & \text{եթե } p \neq i, j \ : \end{cases}$$

Նույն եղանակով ստանում ենք աջից բազմապատկման կանոնը: Հաշվի առնելով բազմապատկման ստացված կանոններից որևէ մեկը, երկրորդ պնդումը դառնում է ակնհայտ՝

$$S_{ij} \cdot S_{ij} = E_n : \qquad \square$$

Քանի որ $T_{ij}(\alpha)$, $L_i(\alpha)$ և S_{ij} տեսքի n-րդ կարգի մատրիցները հակադարձելի են, ապա դրանց վերջավոր թվով արտադրյալները, համաձայն հատկութուն 14.4-ի, նույնպես կլինեն հակադարձելի n-րդ կարգի մատրիցներ: Շուտով կհամոզվենք, որ ճիշտ է նաև հակառակը, այսինքն՝ *յուրաքանչյուր հակադարձելի n-րդ կարգի A մատրից հանդիսանում > նշված տեսքի վերջավոր թվով մատրիցների արտադրյալ:*

I) Եթե $n \times m$-չափանի մատրիցի որևէ տողին գումարվում է նրա մեկ այլ տող, վերջինս բազմապատկելով որևէ թվով, ապա այս ձևափոխությունը կոչվում է (մատրիցի) տողերի **առաջին տիպի (տեսակի) տարրական ձևափոխություն**:

II) Եթե $n \times m$-չափանի մատրիցի որևէ տող բազմապատկվում է որևէ ոչ զրոյական թվով, ապա այս ձևափոխությունը կոչվում է (մատրիցի) տողերի **երկրորդ տիպի (տեսակի) տարրական ձևափոխություն**:

III) $n \times m$-չափանի մատրիցի երկու տողերի տեղափոխությունը կոչվում է (մատրիցի) տողերի **երրորդ տիպի (տեսակի) տարրական ձևափոխություն**:

Մատրիցի սյունակների առաջին, երկրորդ և երրորդ տիպի (տեսակի) տարրական ձևափոխությունները սահմանվում են համանման եղանակով:

Լեմմ 14.6*: Մատրիցի տողերի երրորդ տիպի տարրական ձևափոխությունը ստացվում է մատրիցի տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններից:*

Ապացուցում: Իրոք, դիցուք A մատրիցի մեջ պահանջվում է կատարել նրա i-րդ և j-րդ տողերի տեղափոխություն և դիցուք α_i-ն նրա i-րդ տողն է, իսկ α_j-ն` $j$-րդ տողն է: $i$-րդ տողին գումարենք $j$-րդը` վերջինս բազմապատկելով (-1)-ով, կստանանք` $\alpha_i - \alpha_j$: Այժմ $j$-րդ տողին գումարենք ստացված $i$-րդը, կունենանք` $\alpha_j + (\alpha_i - \alpha_j) = \alpha_i$: Որից հետո նոր i-րդին գումարենք նոր j-րդը, վերջինս բազմապատկելով (-1)-ով, կունենանք` $(\alpha_i - \alpha_j) - \alpha_i = -\alpha_j$: Եվ վերջապես, ստացված i-րդ տողը բազմապատկելով (-1)-ով, կունենանք պահանջվող արդյունքը: □

Հաշվի առնելով լեմմաներ 14.3, 14.4 և 14.5-ը` կատարված քայլերին համապատասխան կունենանք հետևյալ հավասարությունը`

$$S_{ij}A = L_i(-1) \cdot T_{ij}(-1) \cdot T_{ji}(1) \cdot T_{ij}(-1) \cdot A \ :$$

Մասնավորապես, $A = E$ դեպքում, կստանանք`

$$S_{ij} = L_i(-1) \cdot T_{ij}(-1) \cdot T_{ji}(1) \cdot T_{ij}(-1)$$

հավասարությունը:

Թեորեմ 14.2: *Յուրաքանչյուր n-րդ կարգի A մատրից տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է կամ զրոյական տողով մատրիցի կամ այնպիսի մատրիցի, որի գլխավոր անկյունագծի տարրերը հավասար են 1-ի, իսկ դրանից ներքև` զրոների ($n \geqslant 2$):*

Ապացուցում (վերհանգման եղանակ): Եթե $n = 2$, ապա պնդումը ճիշտ է: Իրոք, եթե

$$A = \begin{pmatrix} a_{11}, & a_{12} \\ a_{21}, & a_{22} \end{pmatrix}$$

և A-ի առաջին սյունակը զրոյական չէ, ապա կարելի է ենթադրել, որ $a_{11} \neq 0$, հակառակ դեպքում կկատարեինք տեղափոխություն առաջին և երկրորդ տողերի միջև (լեմմ 14.6): Առաջին տողը բազմապատկելով a_{11}^{-1}-ով ստանում ենք հետևյալ մատրիցը`

$$\begin{pmatrix} 1, & b_{12} \\ a_{21}, & a_{22} \end{pmatrix},$$

որից հետո երկրորդ տողին գումարելով առաջինը` վերջինս նախապես բազմապատկելով $-a_{21}$-ով, կստանանք հետևյալ մատրիցը`

$$\begin{pmatrix} 1, & b_{12} \\ 0, & b_{22} \end{pmatrix};$$

Այժմ, եթե $b_{22} = 0$, ապա պնդումն ապացուցված է, իսկ եթե $b_{22} \neq 0$, ապա երկրորդ տողը բազմապատկելով b_{22}^{-1}-ով կստանանք պահանջվող տեսքի մատրից՝

$$\begin{pmatrix} 1, & b_{12} \\ 0, & 1 \end{pmatrix};$$

Իսկ եթե երկրորդ կարգի A մատրիցի առաջին սյունակը զրոյական է՝

$$A = \begin{pmatrix} 0, & a_{12} \\ 0, & a_{22} \end{pmatrix},$$

ապա $a_{12} = 0$ դեպքում A-ի առաջին տողը կլինի զրոյական: Հակառակ դեպքում ($a_{12} \neq 0$), երկրորդ տողին գումարելով առաջինը, նախապես վերջինս բազմապատկելով $-a_{22} \cdot a_{12}^{-1}$-ով, նորից կստանանք պահանջվող տեսքի մատրից՝

$$\begin{pmatrix} 0, & a_{12} \\ 0, & 0 \end{pmatrix};$$

Կատարելով վերիանգման (վերիանգային) ենթադրություն, դիտարկենք n-րդ կարգի այնպիսի

$$A = \begin{pmatrix} a_{11}, & \cdots, & a_{1n} \\ \vdots & & \\ a_{n1}, & \cdots, & a_{nn} \end{pmatrix}$$

մատրից, որի առաջին սյունակը զրոյական չէ: Կարելի է ենթադրել, որ $a_{11} \neq 0$ (հակառակ դեպքում կկատարեինք տեղափոխություն մատրիցի երկու տողերի միջև): Այնուհետև, A-ի առաջին տողը բազմապատկելով a_{11}^{-1}-ով կստանանք

$$\begin{pmatrix} 1, & b_{12}, & \cdots, & b_{1n} \\ a_{21}, & a_{22}, & \cdots, & a_{2n} \\ \cdots & & \cdots & \\ a_{n1}, & a_{n2}, & \cdots, & a_{nn} \end{pmatrix}$$

մատրիցը, որի առաջին սյունակի բոլոր տարրերը, սկսած երկրորդից, առաջին տիպի տարրական ձևափոխություններով դարձվում են զրոներ՝

$$\begin{pmatrix} 1, & b_{12}, & \cdots, & b_{1n} \\ 0, & b_{22}, & \cdots, & b_{2n} \\ \cdots & & \cdots & \\ 0, & b_{n2}, & \cdots, & b_{nn} \end{pmatrix};$$

Որից հետո կիրառում ենք վերհանգման ենթադրությունը՝ $(n-1)$-րդ կարգի

$$\begin{pmatrix} b_{22}, & \cdots, & b_{2n} \\ \cdots & \cdots & \\ b_{n2}, & \cdots, & b_{nn} \end{pmatrix}$$

մատրիցի նկատմամբ:

Մնում է քննարկել այն դեպքը, երբ սկզբնական A մատրիցի առաջին սյունակը զրոյական է՝

$$A = \begin{pmatrix} 0, & a_{12}, & \cdots, & a_{1n} \\ \vdots & & & \\ 0, & a_{n2}, & \cdots, & a_{nn} \end{pmatrix},$$

որտեղ $(n-1)$-րդ կարգի

$$B = \begin{pmatrix} a_{12}, & \cdots, & a_{1n} \\ \vdots & & \\ a_{n-1,2}, & \cdots, & a_{n-1,n} \end{pmatrix}$$

մատրիցը, ըստ վերհանգման ենթադրության տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է զրոյական տողով մատրիցի, կամ այնպիսի մատրիցի, որի գլխավոր անկյունագծի տարրերը հավասար են մեկի, իսկ նրանից ներքև՝ զրոների: Առաջին դեպքում պնդումն ապացուցված է, իսկ երկրորդ դեպքում $a_{n2}, \ldots, a_{nn}$ տարրերը դարձվում են զրոներ՝ տողերի առաջին տիպի տարրական ձևափոխությունների օգնությամբ: □

Հետևություն 14.1: *Յուրաքանչյուր n-րդ կարգի A մատրից տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է կամ զրոյական տողով մատրիցի, կամ E_n միավոր մատրիցին:*

Ապացույց: Ակնհայտ է, որ

$$\begin{pmatrix} 1, & a_{12}, & \cdots, & a_{1n-1}, & a_{1n} \\ 0, & 1, & \cdots, & a_{2n-1}, & a_{2n} \\ \cdots & \cdots & & & \\ 0, & 0, & \cdots, & 0, & 1 \end{pmatrix}$$

տեսքի յուրաքանչյուր n-րդ կարգի մատրից տողերի առաջին տիպի տարրական ձևափոխությունների օգնությամբ բերվում է E_n միավոր մատրիցին: Մնում է օգտվել թեորեմ 14.2-ից: □

***Հետևություն 14.2**: Յուրաքանչյուր $n \times m$-չափանի A մատրից, $n > m$ դեպքում, տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է զրոյական տողով մատրիցի:*

Ապացույց: Ըստ պայմանի`

$$A = \begin{pmatrix} a_{11}, & \cdots, & a_{1m} \\ \vdots & & \\ a_{m1}, & \cdots, & a_{mn} \\ \vdots & & \\ a_{n1}, & \cdots, & a_{nn} \end{pmatrix},$$

որտեղ m-րդ կարգի

$$B = \begin{pmatrix} a_{11}, & \cdots, & a_{1m} \\ \vdots & & \\ a_{m1}, & \cdots, & a_{mm} \end{pmatrix}$$

քառակուսային մատրիցը, ըստ նախորդ հետևության, տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է կամ զրոյական տողով մատրիցի կամ E_m միավոր մատրիցին: Երկրորդ դեպքում A մատրիցի այն տողերը որոնք գտնվում են B-ից դուրս (օրինակ վերջինը) կարելի է դարձնել զրոյական` օգտվելով տողերի առաջին տիպի տարրական ձևափոխություններից: □

***Հետևություն 14.3**: Յուրաքանչյուր n-րդ կարգի մատրից տողերի (սյունակների) առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է վերին եռանկյունաձև տեսքի:* □

Թեորեմ 14.3: *Եթե n-րդ կարգի A մատրիցը տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է զրոյական տողով (սյունակով) մատրիցի, ապա A-ն հակադարձելի չէ աջից (ձախից):*

Ապացույց: Դիցուք A-ն տրված մատրիցն է և դիցուք A-ից տողերի առաջին և երկրորդ տիպի տարրական ձևափոխությունների միջոցով ստացել ենք զրոյական տողով (սյունակով) B մատրիցը: Համաձայն լեմմաներ 14.3-ի և 14.4-ի, կարող ենք գրել, որ

$$B = S \cdot A,$$

որտեղ S-ը լինելով $T_{ij}(\alpha)$ և $L_i(\alpha)$ տեսքի վերջավոր թվով հակադարձելի մատրիցների արտադրյալ, նույնպես կլինի հակադարձելի: Այժմ ենթադրելով A-ի հակադարձելիությունը աջից, ստանում ենք հակասություն: Իրոք, եթե

$$A \cdot A' = E_n\,,$$

ապա $B\left(A'S^{-1}\right)$ մատրիցը մի կողմից կունենա զրոյական տող, իսկ մյուս կողմից հավասար է միավոր մատրիցին՝

$$B\left(A'S^{-1}\right) = (SA)\left(A' \cdot S^{-1}\right) = E_n\,;$$

Իսկ եթե B-ն զրոյական սյունակով մատրից է և A-ն հակադարձելի է ձախից, այսինքն $A'' \cdot A = E_n$, ապա $\left(A''S^{-1}\right)B$ մատրիցը մի կողմից կլինի զրոյական սյունակով, իսկ մյուս կողմից հավասար է միավոր մատրիցին՝

$$\left(A''S^{-1}\right)B = \left(A'' \cdot S^{-1}\right)(S \cdot A) = E_n\,;$$

Հակասություն: □

Թեորեմ 14.4: *Եթե n-րդ կարգի A մատրիցը տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է E_n միավոր մատրիցին, ապա այն հակադարձելի է: Ընդ որում, A^{-1}-ը կլինի հավասար կատարվող տարրական ձևափոխություններին համապատասխանող $T_{ij}(\alpha)$ և $L_i(\alpha)$ տեսքի (վերջավոր թվով) մատրիցների արտադրյալին:*

Ապացույց: Եթե տրված A մատրիցը տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է E_n միավոր մատրիցին, ապա $S \cdot A = E_n$, որտեղ S-ը հակադարձելի մատրից է, որովհետև $S = S_m \cdot S_{m-1} \cdots S_2 \cdot S_1$, իսկ S_k-ն $T_{ij}(\alpha)$, $L_i(\alpha)$ տեսքի հակադարձելի մատրիցներից մեկն է: Որտեղից՝

$$S^{-1}(S \cdot A) = S^{-1} \cdot E_n \,,$$

$$A = S^{-1}$$

և, հետևաբար, A-ն հակադարձելի է, ընդ որում՝

$$A^{-1} = S \ :$$ □

Հետևություն 14.4: *Եթե երկու n-րդ կարգի A և B մատրիցների համար*

$$A \cdot B = E_n, \ \ \textit{կամ} \ \ B \cdot A = E_n \,,$$

ապա A-ն (հետևաբար և B-ն) հակադարձելի է, այսինքն՝ եթե n-րդ կարգի մատրիցը հակադարձելի է աջից կամ ձախից, ապա այն հակադարձելի է:

Ապացույցում: 1) Դիցուք $A \cdot B = E_n$; Նախորդ թեորեմի համաձայն, բավական է ապացուցել, որ A մատրիցը տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվում է E_n միավոր մատրիցին: Ենթադրելով հակառակը, ստանում ենք հակասություն: Իրոք, այդ դեպքում, համաձայն հետևություն 14.1-ի, A-ն կբերվի զրոյական տողով մի C մատրիցի, իսկ համաձայն թեորեմ 14.3-ի այն չի լինի հակադարձելի աջից:

2) $B \cdot A = E_n$ դեպքում B-ն կլինի հակադարձելի աջից և հետևաբար B-ն կլինի հակադարձելի ըստ 1)-ի: Ուստի՝ $A = B^{-1}$ և A-ն կլինի հակադարձելի: □

Հետևություն 14.5: *Որպեսզի n-րդ կարգի A մատրիցը լինի հակադարձելի անհրաժեշտ է և բավարար, որ այն տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով բերվի E_n միավոր մատրիցին:* □

Հետևություն 14.6: *Որպեսզի n-րդ կարգի A մատրիցը լինի հակադարձելի անհրաժեշտ է և բավարար, որ այն լինի հավասար $T_{ij}(\alpha)$ և $L_i(\alpha)$ տեսքի (վերջավոր թվով) մատրիցների արտադրյալի:* □

Գործնականում տրված n-րդ կարգի A մատրիցի հակադարձելիությունը (և ապա նրա հակադարձը) որոշելու համար, տողերի առաջին և երկրորդ տիպի տարրական ձևափոխությունների օգնությամբ A մատրիցը բերվում է E_n միավոր մատրիցին կամ զրոյական տողով մատրիցի: Ընդ որում, եթե

$$E_n = S_m \cdot S_{m-1} \cdots S_2 \cdot S_1 \cdot A\,,$$

որտեղ S_k-ն $T_{ij}(\alpha)$ կամ $L_i(\alpha)$ տեսքի մատրիցներից մեկն է, ապա A-ն հակադարձելի է և

$$A^{-1} = S_m \cdot S_{m-1} \cdots S_2 \cdot S_1 = S_m \cdot S_{m-1} \cdots S_2 \cdot S_1 \cdot E_n\,,$$

այսինքն A մատրիցի A^{-1} հակադարձը կարելի է ստանալ նաև E_n միավոր մատրիցից՝ կատարելով տողերի նույն առաջին և երկրորդ տիպի տարրական ձևափոխություններն այն նույն հերթականությամբ, որոնք կիրառվել են A-ի նկատմամբ E_n-ը ստանալու համար:

Օրինակ: Գտնենք

$$A = \begin{pmatrix} 2 & 4 \\ 3 & 1 \end{pmatrix}$$

մատրիցի հակադարձ մատրիցը: Կատարենք տողերի հետևյալ տարրական ձևափոխությունները.

$$\left(\begin{array}{cc|cc} 2 & 4 & 1 & 0 \\ 3 & 1 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{cc|cc} 1 & 2 & \frac{1}{2} & 0 \\ 3 & 1 & 0 & 1 \end{array}\right) \longrightarrow \left(\begin{array}{cc|cc} 1 & 2 & \frac{1}{2} & 0 \\ 0 & -5 & -\frac{3}{2} & 1 \end{array}\right) \longrightarrow$$
$$\left(\begin{array}{cc|cc} 1 & 2 & \frac{1}{2} & 0 \\ 0 & 1 & \frac{3}{10} & -\frac{1}{5} \end{array}\right) \longrightarrow \left(\begin{array}{cc|cc} 1 & 0 & -\frac{1}{10} & \frac{2}{5} \\ 0 & 1 & \frac{3}{10} & -\frac{1}{5} \end{array}\right) :$$ Այսպիսով՝

$$A^{-1} = \begin{pmatrix} -\dfrac{1}{10} & \dfrac{2}{5} \\ \dfrac{3}{10} & -\dfrac{1}{5} \end{pmatrix} :$$

Մատրիցի հակադարձելիության և հակադարձի որոշման նկարագրված եղանակը կոչվում է **Գաուսի եղանակ**:

Այժմ անցնենք n-րդ կարգի հակադարձելի մատրիցի ամբողջ աստիճանի սահմանմանը, այսինքն՝ բացասական ցուցիչով աստիճանի սահմանմանը, որովհետև մատրիցի բնական ցուցիչով աստիճանն արդեն սահմանվել է 14.1 վերնագրում: Դիցուք A-ն n-րդ կարգի հակադարձելի մատրից է, իսկ k-ն կամայական բնական թիվ է: Սահմանենք՝

$$A^{-k} = \underbrace{A^{-1} \cdots A^{-1}}_{k},$$

որտեղ A^{-1}-ը A-ի միարժեքորեն որոշվող հակադարձն է:

Ոչ զրոյական (այսինքն հակադարձելի) իրական թվերի ամբողջ աստիճանների պարզագույն հատկությունները հեշտությամբ տարածվում են նաև հակադարձելի մատրիցների ամբողջ աստիճանների վրա:

Հատկություն 14.5: *n-րդ կարգի ցանկացած հակադարձելի A մատրիցի և կամայական m ամբողջ թվի համար տեղի ունի հետևյալ հավասարությունը՝*

$$(A^m)^{-1} = A^{-m} = \left(A^{-1}\right)^m \;: \qquad \square$$

Հատկություն 14.6: *n-րդ կարգի ցանկացած հակադարձելի A մատրիցի և կամայական m_1, m_2 ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$A^{m_1} \cdot A^{m_2} = A^{m_1+m_2} \;: \qquad \square$$

Հատկություն 14.7: *n-րդ կարգի ցանկացած հակադարձելի A մատրիցի և կամայական $m_1, m_2, \ldots, m_l$ ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$A^{m_1} \cdot A^{m_2} \cdots A^{m_l} = A^{m_1+m_2+\cdots+m_l},$$

որտեղ $l \geqslant 2$: $\square$

Հատկություն 14.8: *n-րդ կարգի ցանկացած հակադարձելի A մատրիցի և կամայական m_1, m_2 ամբողջ թվերի համար տեղի ունի հետևյալ հավասարությունը՝*

$$(A^{m_1})^{m_2} = A^{m_1 \cdot m_2} \;: \qquad \square$$

14.3. Աջից կամ ձախից հակադարձելի ուղղանկյուն մատրիցներ

$n \times m$-չափանի A մատրիցը կոչվում է **հակադարձելի աջից**, եթե գոյություն ունի $m \times n$-չափանի այնպիսի A' մատրից, որ

$$A \cdot A' = E_n \, ,$$

որտեղ E_n-ը n-րդ կարգի միավոր մատրիցն է: Այդ դեպքում A'-ը կոչվում է A-ի աջ հակադարձ, որը, սակայն, ընդհանուր դեպքում միարժեքորեն չի որոշվում:

$n \times m$-չափանի A մատրիցը կոչվում է **հակադարձելի ձախից**, եթե գոյություն ունի $m \times n$-չափանի այնպիսի A'' մատրից, որ

$$A'' \cdot A = E_m \, ;$$

Այս դեպքում A''-ը կոչվում է A-ի ձախ հակադարձ, որը նույնպես ընդհանուր դեպքում միարժեքորեն չի որոշվում:

Օրինակ,

$$A = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix}$$

մատրիցը հակադարձելի է աջից, բայց հակադարձելի չէ ձախից: Իսկ նրա շրջված

$$A^T = \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix} ,$$

մատրիցը կլինի հակադարձելի ձախից, բայց չի լինի հակադարձելի աջից: Այստեղ A-ի աջ հակադարձն է՝

$$A' = \begin{pmatrix} \frac{1}{2}, & 0 \\ 0, & \frac{1}{3} \\ c_1, & c_2 \end{pmatrix}$$

մատրիցը, իսկ A^T-ի ձախ հակադարձն է՝

$$\left(A^T\right)'' = (A')^T = \begin{pmatrix} \frac{1}{2}, & 0, & c_1 \\ 0, & \frac{1}{3}, & c_2 \end{pmatrix}$$

մատրիցը, որովհետև՝

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2}, & 0 \\ 0, & \frac{1}{3} \\ c_1, & c_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} \frac{1}{2}, & 0, & c_1 \\ 0, & \frac{1}{3}, & c_2 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}:$$

Շնորհիվ c_1 և c_2 տարրերի կամայական ընտրության, այս օրինակներում աջ և ձախ հակադարձները միարժեքորեն չեն որոշվում:

Հատկություն 14.9: *1) Երկու A և B աջից հակադարձելի մատրիցների $A \cdot B$ արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է աջից, ընդ որում՝*

$$B' \cdot A' = (A \cdot B)',$$

այսինքն՝ $B' \cdot A'$ արտադրյալը կլինի $A \cdot B$ արտադրյալի աջ հակադարձներից մեկը;

2) Երկու A և B ձախից հակադարձելի մատրիցների $A \cdot B$ արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է ձախից, ընդ որում՝

$$B'' \cdot A'' = (A \cdot B)'',$$

այսինքն՝ $B'' \cdot A''$ արտադրյալը կլինի $A \cdot B$ մատրիցի ձախ հակադարձներից մեկը;

3) Վերջավոր թվով $A_1, A_2, \ldots, A_n$ աջից հակադարձելի մատրիցների $A_1 \cdot A_2 \cdots A_n$ արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է աջից, ընդ որում՝

$$A'_n \cdot A'_{n-1} \cdots A'_1 = (A_1 \cdot A_2 \cdots A_n)',$$

այսինքն՝ $A'_n \cdot A'_{n-1} \cdots A'_1$ արտադրյալը կլինի $A_1 \cdot A_2 \cdots A_n$ արտադրյալի աջ հակադարձներից մեկը;

4) Վերջավոր թվով $A_1, A_2, \ldots, A_n$ ձախից հակադարձելի մատրիցների $A_1 \cdot A_2 \cdots A_n$ արտադրյալը (եթե այն գոյություն ունի) նորից հակադարձելի է ձախից, ընդ որում՝

$$A''_n \cdot A''_{n-1} \cdots A''_1 = (A_1 \cdot A_2 \cdots A_n)'',$$

այսինքն՝ $A''_n \cdot A''_{n-1} \cdots A''_1$ արտադրյալը կլինի $A_1 \cdot A_2 \cdots A_n$ արտադրյալի աջ հակադարձներից մեկը:

Ապացուցում: 1) Դիցուք $n \times m$-չափանի A և $m \times k$-չափանի B մատրիցները հակադարձելի են աջից, այսինքն՝ գոյություն ունեն այնպիսի $m \times n$-չափանի A' և $k \times m$-չափանի B' մատրիցներ, որ

$$A \cdot A' = E_n, \quad B \cdot B' = E_m \ :$$

Հետևաբար՝

$$(A \cdot B) \cdot (B' \cdot A') = A((BB')A') = A(E_m A') = AA' = E_n \,;$$

2) Համանման եղանակով ապացուցվում է նաև, որ երկու ձախից հակադարձելի մատրիցների արտադրյալը հակադարձելի է ձախից:

3) և 4) պնդումներն ապացուցվում են վերհանգման եղանակով: □

Հատկություն 14.10: *Եթե $n \times m$-չափանի $A = (a_{ij})$ մատրիցը հակադարձելի է աջից (ձախից), ապա յուրաքանչյուր B n-սյունակի համար $A \cdot X = B$ հավասարումն ունի առնվազն (ամենաշատը) մեկ լուծում:*

Ապացուցում: Եթե A մատրիցը հակադարձելի է աջից, ապա $A \cdot A' = E_n$ որևէ $m \times n$-չափանի A' մատրիցի համար: Ընտրելով $X = A' \cdot B$, կունենանք՝

$$A \cdot X = A(A' \cdot B) = (A \cdot A')B = E_n \cdot B = B \,,$$

այսինքն՝ $A \cdot X = B$ հավասարումն ունի առնվազն մեկ լուծում: Իսկ, եթե A մատրիցը հակադարձելի է ձախից, այսինքն՝ $A'' \cdot A = E_m$ որևէ $m \times n$-չափանի A'' մատրիցի համար և $A \cdot X = B$ հավասարումն ունի որևէ X լուծում, ապա

$$A''(A \cdot X) = A'' \cdot B \,,$$

$$(A''A) \cdot X = A'' \cdot B \,,$$

$$E_m \cdot X = A'' \cdot B \,,$$

$$X = A'' \cdot B \,;$$

Այսպիսով, $A \cdot X = B$ հավասարման յուրաքանչյուր X լուծում հավասար է $A'' \cdot B$-ին: Ուստի, $A \cdot X = B$ հավասարումը (եթե A-ն հակադարձելի է ձախից) կարող է ունենալ ամենաշատը մեկ լուծում: □

Բերենք ձախից հակադարձելի A մատրիցի օրինակ, որի դեպքում $A \cdot X = B$ հավասարումը (համակարգը) չունի լուծում: Հենց այդպիսին է, օրինակ, վերոհիշյալ

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \\ 0 & 0 \end{pmatrix}$$

մատրիցը: Իրոք,

$$\begin{cases} 2x_1 + 0x_2 = 1 \\ 0x_1 + 3x_2 = 2 \\ 0x_1 + 0x_2 = 3 \end{cases}$$

համակարգը չունի լուծում:

Դիտողություն: Հատկություն 14.10-ը մնում է ուժի մեջ, եթե X անհայտ մատրիցը և B-ն կամայական $m \times k$ և $n \times k$-չափանի մատրիցներ են:

Հատկություն 14.11: *Որպեսզի $n \times m$-չափանի A մատրիցը լինի հակադարձելի աջից անհրաժեշտ է և բավարար, որ նրա շրջված A^T մատրիցը լինի հակադարձելի ձախից:*

Ապացուցում: Եթե $A \cdot B = E_n$, ապա համաձայն հատկություն 14.4-ի կունենանք՝

$$(A \cdot B)^T = (E_n)^T \ ,$$

$$B^T \cdot A^T = E_n \ ;$$

Եվ հակառակը, եթե $C \cdot A^T = E_n$,, ապա

$$\left(C \cdot A^T\right)^T = (E_n)^T \ ,$$

$$\left(A^T\right)^T \cdot C^T = E_n \ ,$$

$$A \cdot C^T = E_n \ : \qquad \square$$

$n \times m$-չափանի A մատրիցը կոչվում է **հակադարձելի**, եթե գոյություն ունի այնպիսի $m \times n$-չափանի B մատրից, որ

$$A \cdot B = E_n$$

և

$$B \cdot A = E_m \ :$$

Այս դեպքում $m\times n$-չափանի B մատրիցը որոշվում է միարժեքորեն և կոչվում է A-ի հակադարձ (մատրից) ու նշանակվում է՝ $B = A^{-1}$: Դեռ ավելին, եթե $n\times m$-չափանի A մատրիցը հակադարձելի է աջից և հակադարձելի է ձախից, ապա նրա աջ և ձախ հակադարձները կլինեն հավասար և կորոշվեն միարժեքորեն (հետևաբար, A-ն կլինի հակադարձելի): Իրոք, եթե $A\cdot A' = E_n$ և $A''\cdot A = E_m$, ապա, ինչպես և վերևում,

$$A'' = A''\cdot E_n = A''\cdot(A\cdot A') = (A''\cdot A)\cdot A' = E_m\cdot A' = A' \ :$$

Մասնավորապես, եթե

$$A\cdot B = E_n, \quad B\cdot A = E_m$$

և

$$A\cdot B' = E_n, \quad B'\cdot A = E_m \ ,$$

ապա առաջին և չորրորդ հավասարություններից կբխի $B = B'$ հավասարությունը:

Սակայն պարզվում է, որ բացի քառակուսային մատրիցներից ուրիշ հակադարձելի ուղղանկյուն մատրիցներ գոյություն չունեն:

Թեորեմ 14.5: *Եթե $n\times m$-չափանի A մատրիցը հակադարձելի է աջից, ապա $n\leqslant m$:*

Ապացուցում: Դիցուք $n\times m$-չափանի A մատրիցը հակադարձելի է աջից, այսինքն $A\cdot A' = E_n$, և դիցուք $n > m$: Այս դեպքում, համաձայն հետևություն 14.2-ի, տողերի առաջին և երկրորդ տիպի տարրական ձևափոխություններով A մատրիցը բերվում է զրոյական տողով $n\times m$-չափանի C մատրիցի: Ուստի, $C = S\cdot A$, որտեղ S-ը n-րդ կարգի հակադարձելի մատրից է, և մենք հանգում ենք հակասության՝

$$CA'S^{-1} = SAA'S^{-1} = S\cdot E_n\cdot S^{-1} = E_n \ ,$$

որովհետև հավասարության ձախ մասը զրոյական տողով մատրից է, իսկ աջ մասը՝ ոչ: □

***Հետևություն 14.7**: Եթե $n\times m$-չափանի A մատրիցը հակադարձելի է ձախից, ապա $m\leqslant n$:*

Ապացույց: Եթե $n\times m$-չափանի A մատրիցը հակադարձելի է ձախից, ապա գոյություն կունենա $m\times n$-չափանի այնպիսի A'' մատրից, որ $A''\cdot A = E_m$: Հետևաբար, A'' մատրիցը կլինի հակադարձելի աջից և համաձայն նախորդ թեորեմի՝ $m\leqslant n$: ☐

Հետևություն 14.8: *Եթե $n\times m$-չափանի A մատրիցը հակադարձելի է, ապա $n=m$, այսինքն՝ A-ն քառակուսային մատրից է:* ☐

14.4. Մատրիցի որոշիչը

Վերհիշենք $sgn : S_n \to \{\pm 1\}$ արտապատկերման սահմանումը՝

$$sgn(\sigma) = \begin{cases} 1, & \text{եթե } \sigma\in\mathbb{A}_n, \\ -1, & \text{եթե } \sigma\in S_n\setminus\mathbb{A}_n, \end{cases}$$

այսինքն՝ զույգ (կենտ) σ տեղադրության համար՝ $sgn(\sigma) = 1$ (համապատասխանաբար՝ $sgn(\sigma) = -1$): Ինչպես հայտնի է՝ $sgn(\sigma) = sgn\left(\sigma^{-1}\right)$ և $sgn(\alpha\cdot\beta) = sgn(\alpha)\cdot sgn(\beta)$:

Կամայական n-րդ կարգի

$$A = \begin{pmatrix} a_{11},\ldots,a_{1n} \\ \ldots\ \ldots\ \ldots \\ a_{n1},\ldots,a_{nn} \end{pmatrix}$$

մատրիցի որոշիչը նշանակվում է $|A|$-ով կամ $det(A)$-ով և սահմանվում է հետևյալ կերպ՝

$$|A| = \sum_{\sigma\in S_n} sgn(\sigma)\cdot a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdots a_{n,\sigma(n)},$$

որտեղ σ-ն փոփոխվում է n-րդ աստիճանի բոլոր տեղադրությունների S_n բազմության վրա (determinant – անգլ.):

Ակնհայտ է, որ եթե σ-ն տեղադրություն է, ապա $a_{1,\sigma(1)}\cdot a_{2,\sigma(2)}\cdots a_{n,\sigma(n)}$ արտադրյալի արտադրիչները վերցվում են մատրիցի ամեն սյունակից (ինչպես և ամեն տողից) մեկական: Եվ հակառակը, եթե n-րդ կարգի մատրիցի n հատ տարրերի $a_{1,i_1}\cdot a_{2,i_2}\cdots a_{n,i_n}$ արտադրյալի արտադրիչներն ընտրված են մեկական՝ մատրիցի բոլոր սյունակներից, ապա $\sigma = \begin{pmatrix} 1, & 2, & \dots, & n \\ i_1, & i_2, & \dots, & i_n \end{pmatrix}$ արտապատկերումը կլինի տեղադրություն:

Օրինակ, $n = 1$ դեպքում՝ $A = (a_{11})$, $S_1 = \{\varepsilon\}$, որտեղ $\varepsilon(1) = 1$, $sgn(\varepsilon) = 1$ և, հետևաբար, $det(A) = a_{11}$:

$n = 2$ դեպքում՝

$$A = \begin{pmatrix} a_{11}, a_{12} \\ a_{21}, a_{22} \end{pmatrix},$$

$S_2 = \{\varepsilon, \alpha\}$, որտեղ $\alpha = (1,2)$, $sgn(\alpha) = -1$ և, հետևաբար,

$$det(A) = sgn(\varepsilon) \cdot a_{1,\varepsilon(1)} \cdot a_{2,\varepsilon(2)} + sgn(\alpha) \cdot a_{1,\alpha(1)} \cdot a_{2,\alpha(2)} = a_{11}a_{22} - a_{12} \cdot a_{21} :$$

$n = 3$ դեպքում՝

$$A = \begin{pmatrix} a_{11}, a_{12}, a_{13} \\ a_{21}, a_{22}, a_{23} \\ a_{31}, a_{32}, a_{33} \end{pmatrix},$$

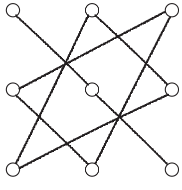
իսկ $S_3 = \{\varepsilon, \alpha, \beta, \gamma, \delta, \tau\}$, որտեղ

$$\begin{aligned} \alpha &= (1,2), & sgn(\alpha) &= -1, \\ \beta &= (1,3), & sgn(\beta) &= -1, \\ \gamma &= (2,3), & sgn(\gamma) &= -1, \\ \delta &= (1,2,3), & sgn(\delta) &= 1, \\ \tau &= (1,3,2), & sgn(\tau) &= 1, \end{aligned}$$

և, հետևաբար,

$$det(A) = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32},$$

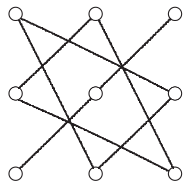
որտեղ դրական նշանով անդամները կազմվում են ըստ հետևյալ օրենքի՝



$(+)$

,

իսկ բացասական նշանով անդամները՝ ըստ հետևյալ օրենքի՝



$(-)$

:

Այժմ հաշվենք վերին եռանկյունաձև

$$A = \begin{pmatrix} a_{11}, & a_{12}, & \ldots, & a_{1n} \\ 0, & a_{22}, & \ldots, & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ 0, & 0, & \ldots, & a_{nn} \end{pmatrix}$$

մատրիցի որոշիչը: Պարզվում է, այս դեպքում տեղի ունի հետևյալ հավասարությունը՝

$$det(A) = a_{11} \cdot a_{22} \cdots a_{nn} :$$

Նախապես ապացուցենք հետևյալ պնդումը:

Լեմմ 14.7: *Եթե* $\sigma \in S_n$ *և* $\sigma \neq \varepsilon$*, ապա գոյություն ունի այնպիսի* i *բնական թիվ (*$2 \leqslant i \leqslant n$*), որ* $\sigma(i) < i$*:*

Ապացուցում: Եթե $\sigma(n) \neq n$, ապա $i = n$: Դիցուք $\sigma(n) = n$: Եթե $\sigma(n-1) \neq n-1$, ապա $i = n-1$: Իսկ եթե $\sigma(n-1) = n-1$, ապա անցնում ենք $\sigma(n-2)$-ի դիտարկմանը և այսպես շարունակ: □

Օգտվելով ապացուցված լեմմից, ստանում ենք վերին եռանկյունաձև մատրիցի որոշիչը.

$$det(A) = a_{11} \cdot a_{22} \cdots a_{nn} + \sum_{\sigma \in S_n,\, \sigma \neq \varepsilon} sgn(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} =$$
$$= a_{11} \cdot a_{22} \cdots a_{nn},$$

որովհետև

$$\sum_{\sigma \in S_n,\, \sigma \neq \varepsilon} sgn(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} = 0 :$$

Որոշիչի հաշվման նույն բանաձևը ստացվում է նաև ներքին եռանկյունաձև մատրիցի համար: Այս դեպքում պետք է արդեն հենվել հետևյալ արդյունքի վրա:

Լեմմ 14.8: *Եթե $\sigma \in S_n$ և $\sigma \neq \varepsilon$, ապա գոյություն ունի այնպիսի j բնական թիվ ($1 \leqslant j \leqslant n-1$), որ $\sigma(j) > j$:* □

Որոշիչի սահմանումից անմիջապես բխում են նրա հետևյալ հատկությունները.

Հատկություն 14.12: *Եթե n-րդ կարգի մատրիցի որևէ տողի բոլոր տարրերը հավասար են զրոյի, ապա նրա որոշիչը ևս հավասար է զրոյի:* □

Հատկություն 14.13: *Եթե n-րդ կարգի մատրիցի որևէ տող բազմապատկվում է որևէ իրական թվով, ապա նրա որոշիչը ևս կբազմապատկվի այդ նույն թվով: Այլ կերպ ասած՝*

$$det\begin{pmatrix}\xi_1\\ \vdots\\ \alpha\,\xi_i\\ \vdots\\ \xi_n\end{pmatrix} = \alpha\cdot det\begin{pmatrix}\xi_1\\ \vdots\\ \xi_i\\ \vdots\\ \xi_n\end{pmatrix},$$

որտեղ $\xi_1,\ldots,\xi_i,\ldots,\xi_n$-ը դիտարկվող մատրիցի տողերն են: □

Հատկություն 14.14: *Եթե n-րդ կարգի մատրիցի որևէ տող հավասար է երկու կամ վերջավոր թվով կամայական տողերի գումարի, ապա այդպիսի մատրիցի որոշիչը կարելի է հաշվել հետևյալ կերպ՝*

$$det\begin{pmatrix}\vdots\\ \eta_i+\cdots+\mu_i\\ \vdots\end{pmatrix} = det\begin{pmatrix}\vdots\\ \eta_i\\ \vdots\end{pmatrix} + \cdots + det\begin{pmatrix}\vdots\\ \mu_i\\ \vdots\end{pmatrix}:$$ □

Վերջին երկու հատկություններն ի նկատի ունենալով ասում են, որ մատրիցի որոշիչը գծային արտապատկերում (ֆունկցիա) է՝ ըստ իր յուրաքանչյուր տողի:

Յուրաքանչյուր $\tau \in S_n$ տեղադրության և n-րդ կարգի

$$A = \begin{pmatrix}\xi_1\\ \vdots\\ \xi_n\end{pmatrix}$$

մատրիցի համապատասխան սահմանենք (կառուցենք) $\tau(A)$ մատրիցը հետևյալ կերպ՝

$$\tau(A) = \begin{pmatrix} \xi_{\tau(1)} \\ \vdots \\ \xi_{\tau(n)} \end{pmatrix} :$$

Թեորեմ 14.6: *Կամայական n-րդ կարգի A մատրիցի և յուրաքանչյուր $\tau \in S_n$ տեղադրության համար՝*

$$|\tau(A)| = sgn(\tau) \cdot |A| \ :$$

Ապացուցում: Հաշվենք $\tau(A)$ մատրիցի որոշիչը՝

$$|\tau(A)| = det \begin{pmatrix} \xi_{\tau(1)} \\ \vdots \\ \xi_{\tau(n)} \end{pmatrix} = \sum_{\sigma \in S_n} sgn(\sigma) \cdot a_{\tau(1),\sigma(1)} \cdot a_{\tau(2),\sigma(2)} \cdots a_{\tau(n),\sigma(n)};$$

Եթե $\tau(m) = i$, ապա $m = \tau^{-1}(i)$ և $\sigma(m) = \sigma\left(\tau^{-1}(i)\right) = \left(\tau^{-1} \cdot \sigma\right) i$: Մյուս կողմից, $\sigma = \tau\left(\tau^{-1}\sigma\right)$ և $sgn\sigma = sgn(\tau) \cdot sgn\left(\tau^{-1} \cdot \sigma\right)$: Հետևաբար,

$$|\tau(A)| = \sum_{\sigma \in S_n} sgn(\tau) \cdot sgn\left(\tau^{-1}\sigma\right) \cdot a_{1,(\tau^{-1}\sigma)1} \cdot a_{2,(\tau^{-1}\sigma)2} \cdots a_{n,(\tau^{-1}\sigma)n} =$$

$$= sgn(\tau) \cdot \sum_{\gamma \in S_n} sgn(\gamma) \cdot a_{1,\gamma(1)} \cdot a_{2,\gamma(2)} \cdots a_{n,\gamma(n)} = sgn(\tau) \cdot |A|,$$

որովհետև երբ σ-ն փոփոխվում է S_n բազմության վրա, $\gamma = \tau^{-1} \cdot \sigma$ տեղադրությունը հավասարվում է S_n-ի կամայական α տարրին ($\gamma = \alpha \in S_n$, եթե $\sigma = \tau \cdot \alpha$): □

Հատկություն 14.15: *Երկու հավասար տողեր ունեցող n-րդ կարգի մատրիցի որոշիչը հավասար է զրոյի ($n > 1$):*

Ապացուցում: Դիցուք հավասար են n-րդ կարգի $A = (a_{ij})$ մատրիցի i-րդ և j-րդ տողերը, այսինքն՝ $a_{i,k} = a_{j,k}$: Այդ դեպքում, $|A|$ որոշիչի յուրաքանչյուր

$$sgn(\sigma) a_{1,\sigma(1)} \cdots a_{i,\sigma(i)} \cdots a_{j,\sigma(j)} \cdots a_{n,\sigma(n)}$$

անդամին, որտեղ $\sigma \in \mathbb{A}_n$, գումարելով

$$sgn(\sigma')a_{1,\sigma'(1)} \cdots a_{i,\sigma'(i)} \cdots a_{j,\sigma'(j)} \cdots a_{n,\sigma'(n)}$$

անդամը, որտեղ $\sigma' = (i,j) \cdot \sigma \in S_n \setminus \mathbb{A}_n$, կստանանք զրո, որովհետև

$$\begin{aligned}
&sgn(\sigma') = -sgn(\sigma),\\
&a_{1,\sigma'(1)} = a_{1,\sigma(1)},\\
&\quad \cdots \cdots \cdots\\
&a_{i-1,\sigma'(i-1)} = a_{i-1,\sigma(i-1)},\\
&a_{i,\sigma'(i)} = a_{i,\sigma(j)} = a_{j,\sigma(j)},\\
&a_{i+1,\sigma'(i+1)} = a_{i+1,\sigma(i+1)},\\
&\quad \cdots \cdots \cdots\\
&a_{j-1,\sigma'(j-1)} = a_{j-1,\sigma(j-1)},\\
&a_{j,\sigma'(j)} = a_{j,\sigma(i)} = a_{i,\sigma(i)},\\
&a_{j+1,\sigma'(j+1)} = a_{j+1,\sigma(j+1)},\\
&\quad \cdots \cdots \cdots\\
&a_{n,\sigma'(n)} = a_{n,\sigma(n)}:
\end{aligned}$$

Այսպիսով, $|A|$ որոշիչի բոլոր $n!$ գումարելիները կարելի է խմբավորել ըստ այնպիսի զույգերի, որոնց գումարը զրո է: Հետևաբար, $|A| = 0$: □

Հատկություն 14.16: *Եթե n-րդ կարգի մատրիցի մեջ կատարենք երկու տողերի տեղափոխություն, ապա դրանից կփոխվի նրա որոշիչի միայն նշանը ($n > 1$):*

Ապացուցում: Եթե

$$A = \begin{pmatrix} \vdots \\ \xi_i \\ \vdots \\ \xi_j \\ \vdots \end{pmatrix}, \quad B = \begin{pmatrix} \vdots \\ \xi_j \\ \vdots \\ \xi_i \\ \vdots \end{pmatrix},$$

ապա $B = \tau(A)$, որտեղ $\tau = (i,j)$: Հետևաբար, համաձայն թեորեմ 14.6-ի,

$$|B| = |\tau(A)| = sgn(\tau) \cdot |A| = -|A| :$$ □

Հատկություն 14.17*: Եթե n-րդ կարգի մատրիցը օժտված է երկու համեմատական տողերով, ապա դրա որոշիչը հավասար է զրոյի* $(n > 1)$: □

Հատկություն 14.18*: Եթե n-րդ կարգի մատրիցի որևէ տող գծայնորեն արտահայտվում է դրա մի քանի ուրիշ տողերի միջոցով, ապա այդ մատրիցի որոշիչը հավասար է զրոյի* $(n > 1)$: □

Հատկություն 14.19*: n-րդ կարգի մատրիցի որոշիչը չի փոխվի, եթե դրա որևէ տողին ավելացնենք մատրիցի մեկ ուրիշ տող՝ նախապես այն բազմապատկելով որևէ թվով* $(n > 1)$: □

Թեորեմ 14.7*: n-րդ կարգի երկու մատրիցների արտադրյալի որոշիչը հավասար է արտադրիչ մատրիցների որոշիչների արտադրյալին, այսինքն՝*

$$|A \cdot B| = |A| \cdot |B| :$$

Ապացուցում: ենթադրենք $A = (a_{ij})$ և $B = (b_{ij})$ մատրիցները n-րդ կարգի են և $C = A \cdot B = (c_{ij})$: B մատրիցի տողերը նշանակենք $\eta_1, \ldots, \eta_n$-ով, որտեղ

$$\eta_i = (b_{i1}, \ldots, b_{in}) ,$$

և գրենք՝

$$B = \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} :$$

C մատրիցի տողերը նշանակենք $\xi_1, \ldots, \xi_n$-ով: Ուստի,

$$C = \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} ,$$

որտեղ $\xi_1 = (c_{i1}, \ldots, c_{in})$: Քանի, որ՝

$$c_{11} = a_{11}b_{11} + a_{12}b_{21} + \cdots + a_{1n}b_{n1} ,$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$c_{1n} = a_{11}b_{1n} + a_{12}b_{2n} + \cdots + a_{1n}b_{nn},$$

ապա $\xi_1 = a_{11}\eta_1 + \cdots + a_{1n}\eta_n$: Նույն եղանակով ստացվում են նաև հետևյալ հավասարությունները՝

$$\xi_2 = a_{21}\eta_1 + \cdots + a_{2n}\eta_n \ ,$$

$$\dots \quad \dots \quad \dots$$

$$\xi_n = a_{n1}\eta_1 + \cdots + a_{nn}\eta_n \ :$$

Այժմ որոշենք C արտադրյալ մատրիցի որոշիչը.

$$|C| = |A \cdot B| = det\begin{pmatrix} \xi_1 \\ \vdots \\ \xi_n \end{pmatrix} = det\begin{pmatrix} a_{11}\eta_1 + \cdots + a_{1n}\eta_n \\ \dots \quad \dots \quad \dots \\ a_{n1}\eta_1 + \cdots + a_{nn}\eta_n \end{pmatrix} =$$

$$= det\begin{pmatrix} a_{11}\eta_1 \\ a_{21}\eta_1 + \cdots + a_{2n}\eta_n \\ \dots \quad \dots \quad \dots \\ a_{n1}\eta_1 + \cdots + a_{nn}\eta_n \end{pmatrix} + \cdots + det\begin{pmatrix} a_{1n}\eta_n \\ a_{21}\eta_1 + \cdots + a_{2n}\eta_n \\ \dots \quad \dots \quad \dots \\ a_{n1}\eta_1 + \cdots + a_{nn}\eta_n \end{pmatrix} ;$$

Նույն եղանակով, առաջացած որոշիչներից յուրաքանչյուրը վեր ենք ածում ըստ երկրորդ տողերի գումարելիների, որից հետո ստացված որոշիչներից յուրաքանչյուրը՝ ըստ երրորդ տողերի գումարելիների և այսպես շարունակ ... :

Ի վերջո ստանում ենք հետևյալ արդյունքը՝

$$|A \cdot B| = \sum_{j_1,\dots,j_n} a_{1,j_1} \cdots a_{n,j_n} \cdot det\begin{pmatrix} \eta_{j_1} \\ \vdots \\ \eta_{j_n} \end{pmatrix} ,$$

որտեղ $j_1, \dots, j_n$ տարրերը միմյանցից անկախ ստանում են $1, \dots, n$ արժեքները: Եթե $j_1, \dots, j_n$ արժեքների մեջ լինեն կրկնվողներ, ապա համապատասխան

$$det\begin{pmatrix} \eta_{j_1} \\ \vdots \\ \eta_{j_n} \end{pmatrix}$$

որոշիչը կլինի հավասար զրոյի: Այդ պատճառով, $\sum\limits_{j_1,\dots,j_n}$ գումարը կարելի է հաշվել միայն ըստ այնպիսի $(j_1, \dots, j_n)$

հաջորդականությունների, որոնց մեջ չկան կրկնություններ: Հետևաբար,

$$\sigma = \begin{pmatrix} 1, & 2, & \dots, & n \\ j_1, & j_2, & \dots, & j_n \end{pmatrix}$$

արտապատկերումը կլինի n-րդ աստիճանի ցանկացած տեղադրություն և, համաձայն թեորեմ 14.6-ի, կունենանք՝

$$|A \cdot B| = \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \cdot det \begin{pmatrix} \eta_{\sigma(1)} \\ \vdots \\ \eta_{\sigma(n)} \end{pmatrix} =$$

$$= \sum_{\sigma \in S_n} a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} \cdot sgn(\sigma) det \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} =$$

$$= det \begin{pmatrix} \eta_1 \\ \vdots \\ \eta_n \end{pmatrix} \sum_{\sigma \in S_n} sgn(\sigma) \cdot a_{1,\sigma(1)} \cdots a_{n,\sigma(n)} = |A| \cdot |B| \ : \qquad \square$$

Հատկություն 14.20: *Վերջավոր թվով n-րդ կարգի մատրիցների արտադրյալի որոշիչը հավասար է արտադրիչ մատրիցների որոշիչների արտադրյալին, այսինքն՝*

$$|A_1 \cdot A_2 \cdots A_m| = |A_1| \cdot |A_2| \cdots |A_m|, \quad m \geqslant 2 \ :$$

Ապացուցում: Վերինանգման եղանակով: $\square$

Թեորեմ 14.8: *Շրջման ժամանակ n-րդ կարգի մատրիցի որոշիչը չի փոխվում, այսինքն՝*

$$|A^T| = |A| \ :$$

Ապացուցում: Ենթադրենք $A = (a_{ij})$ և $A^T = (a^*_{ij})$, որտեղ $a^*_{ij} = a_{ji}$: Հաշվենք A^T շրջված մատրիցի որոշիչը.

$$|A^T| = \sum_{\sigma \in S_n} sgn(\sigma) \cdot a^*_{1,\sigma(1)} \cdots a^*_{n,\sigma(n)} = \sum_{\sigma \in S_n} sgn(\sigma) \cdot a_{\sigma(1),1} \cdots a_{\sigma(n),n} \ :$$

Եթե $\sigma(m) = i$, ապա $m = \sigma^{-1}(i)$ և հաշվի առնելով $sgn(\sigma) = sgn(\sigma^{-1})$ հավասարությունը, կստանանք՝

$$|A^T| = \sum_{\sigma \in S_n} sgn(\sigma^{-1}) \cdot a_{1,\sigma^{-1}(1)} \cdots a_{n,\sigma^{-1}(n)} =$$

$$= \sum_{\gamma \in S_n} sgn(\gamma) \cdot a_{1,\gamma(1)} \cdots a_{n,\gamma(n)} = |A|\,,$$

որովհետև $\gamma = \sigma^{-1}$ տեղադրությունը կարող է հավասարվել S_n բազմության կամայական տարրին: □

Ապացուցված թեորեմը հնարավորություն է տալիս մատրիցի տողերի վերաբերյալ ձևակերպված բոլոր հատկությունները վերաձևակերպել նաև սյունակների համար:

Հատկություն 14.21: *Եթե n-րդ կարգի մատրիցի որևէ սյունակի բոլոր տարրերը հավասար են զրոյի, ապա դրա որոշիչը հավասար է զրոյի:* □

Հատկություն 14.22: *Եթե n-րդ կարգի մատրիցի որևէ սյունակ բազմապատկվում է որևէ իրական թվով, ապա դրա որոշիչը ևս կբազմապատկվի այդ նույն թվով:* □

Հատկություն 14.23: $det\,(\eta_1, \ldots, \xi_i + \cdots + \mu_i, \ldots, \eta_n) =$
$= det\,(\eta_1, \ldots, \xi_i, \ldots, \eta_n) + \cdots + det\,(\eta_1, \ldots, \mu_i, \ldots, \eta_n)$: □

Հատկություն 14.24: *Եթե n-րդ կարգի մատրիցը օժտված է հավասար սյունակներով, ապա դրա որոշիչը հավասար է զրոյի* $(n > 1)$: □

Հատկություն 14.25: *Եթե n-րդ կարգի մատրիցը օժտված է համեմատական սյունակներով, ապա դրա որոշիչը հավասար է զրոյի* $(n > 1)$: □

Հատկություն 14.26: *Եթե n-րդ կարգի մատրիցի որևէ սյունակ գծայնորեն (գծորեն) արտահայտվում է նրա մի քանի ուրիշ սյունակների միջոցով, ապա դրա որոշիչը հավասար է զրոյի* $(n > 1)$: □

Հատկություն 14.27: *n-րդ կարգի մատրիցի որոշիչը չի փոխվի, եթե դրա որևէ սյունակին ավելացնենք մատրիցի մեկ ուրիշ սյունակ՝ նախապես այն բազմապատկելով որևէ թվով* $(n > 1)$: □

Հատկություն 14.28: *Եթե n-րդ կարգի մատրիցի մեջ կատարենք դրա երկու սյունակների տեղափոխություն, ապա դրանից կփոխվի նրա որոշիչի միայն նշանը* $(n > 1)$: □

14.5. Որոշիչի վերլուծությունը ըստ մատրիցի տողի (սյան) տարրերի

$n \times m$-չափանի $A = (a_{ij})$ մատրիցի **ենթամատրից** ասելով հասկացվում է այն մատրիցը, որի տարրերը գտնվում են A մատրիցի մի քանի տողերի և մի քանի սյունակների հատման տեղերում: Եթե վերցված տողերի համարները նշանակենք $i_1 < i_2 < \cdots < i_k$, իսկ վերցված սյունակների համարները նշանակենք $j_1 < j_2 < \cdots < j_l$, ապա համապատասխան ենթամատրիցը կլինի՝

$$\begin{pmatrix} a_{i_1 j_1}, & a_{i_1 j_2}, & \dots, & a_{i_1 j_l} \\ a_{i_2 j_1}, & a_{i_2 j_2}, & \dots, & a_{i_2 j_l} \\ \dots & \dots & \dots & \dots \\ a_{i_k j_1}, & a_{i_k j_2}, & \dots, & a_{i_k j_l} \end{pmatrix} :$$

Մասնավորապես, A մատրիցի յուրաքանչյուր տարր, յուրաքանչյուր տող և յուրաքանչյուր սյունակ կլինի իր ենթամատրիցը:

Դիցուք $A = (a_{ij})$ մատրիցը n-րդ կարգի է: M_{ij}-ով նշանակենք A-ի այն $(n-1)$-րդ կարգի ենթամատրիցը, որը ստացվում է A-ից հեռացնելով նրա i-րդ տողը և j-րդ սյունակը, այսինքն՝ այն տողը և սյունակը, որում գտնվում է a_{ij} տարրը: $|M_{ij}|$ որոշիչը կոչվում է A մատրիցի $(n-1)$ -րդ կարգի **մինոր**, կամ a_{ij} **տարրի մինոր** A մատրիցում, իսկ

$$A_{ij} = (-1)^{i+j} |M_{ij}|$$

մեծությունը կոչվում է a_{ij} տարրի **հանրահաշվական լրացուցիչ** A մատրիցում:

Լեմմ 14.9: *Եթե n-րդ կարգի $A = (a_{ij})$ մատրիցի առաջին տողում (սյունակում) a_{11}-ից բացի բոլոր տարրերը հավասար են զրոյի, ապա $|A| = a_{11} \cdot A_{11}$:*

Ապացուցում: Ապացուցումը կատարենք ըստ տողի: Դիցուք՝

$$A = \begin{pmatrix} a_{11}, & 0, & \dots, & 0 \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1}, & a_{n2}, & \dots, & a_{nn} \end{pmatrix} :$$

Եթե $\sigma \in S_n$ և $\sigma(1) \neq 1$, ապա $a_{1,\sigma(1)} = 0$: Յուրաքանչյուր $\sigma = \begin{pmatrix} 1, & 2, & \dots, & n \\ 1, & i_2, & \dots, & i_n \end{pmatrix} \in S_n$ տեղադրությանը համապատասխանեցնենք $\gamma = \begin{pmatrix} 1, & \ldots, & n-1 \\ i_2 - 1, & \ldots, & i_n - 1 \end{pmatrix} \in S_{n-1}$ տեղադրությունը: Ըստ որում, յուրաքանչյուր $\gamma \in S_{n-1}$ տեղադրություն ստացվում է այդ ձևով: Իրոք, եթե

$$\gamma = \begin{pmatrix} 1, & 2, & \ldots, & n-1 \\ j_1, & j_2, & \ldots, & j_{n-1} \end{pmatrix} \in S_{n-1} \,,$$

ապա այն կստացվե հետևյալ

$$\sigma = \begin{pmatrix} 1, & 2, & \ldots, & n \\ 1, & j_1 + 1, & \ldots, & j_{n-1} + 1 \end{pmatrix} \in S_n$$

տեղադրությունից: Ակնհայտ է, որ $sgn(\sigma) = sgn(\gamma)$, որովհետև σ և γ տեղադրությունների կարգի խախտումների քանակները հավասար են: Դիցուք՝

$$M_{11} = \begin{pmatrix} a_{22}, & \ldots, & a_{2n} \\ \ldots & \ldots & \ldots \\ a_{n2}, & \ldots, & a_{nn} \end{pmatrix} = \begin{pmatrix} c_{11}, & \ldots, & c_{1,n-1} \\ \ldots & \ldots & \ldots \\ c_{n-1,1}, & \ldots, & c_{n-1,n-1} \end{pmatrix} \,,$$

այսինքն՝

$$\begin{aligned} a_{2,\sigma(2)} &= c_{1,\gamma(1)}, \\ &\vdots \\ a_{n,\sigma(n)} &= c_{n-1,\gamma(n-1)} : \end{aligned}$$

Հետևաբար՝

$$|A| = \sum_{\sigma \in S_n} sgn(\sigma) \cdot a_{1,\sigma(1)} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} =$$

$$= \sum_{\sigma \in S_n, \sigma(1) \neq 1} sgn(\sigma) \cdot a_{11} \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} =$$

$$= a_{11} \cdot \sum_{\sigma \in S_n, \sigma(1) \neq 1} sgn(\sigma) \cdot a_{2,\sigma(2)} \cdots a_{n,\sigma(n)} =$$

$$= a_{11} \cdot \sum_{\gamma \in S_{n-1}} sgn(\gamma) \cdot c_{1,\gamma(1)} \cdots c_{n-1,\gamma(n-1)} = a_{11} \cdot |M_{11}| = a_{11} \cdot A_{11} \; : \quad \square$$

Լեմմ 14.10: *Եթե n-րդ կարգի $A = (a_{ij})$ մատրիցի i-րդ տողում (j-րդ սյունակում) a_{ij}-ից բացի բոլոր տարրերը հավասար են զրոյի, ապա $|A| = a_{ij} \cdot A_{ij}$:*

Ապացուցում: Հանգեցվում է նախորդ լեմմին: Ապացուցումը կատարենք ըստ տողի: Դիցուք՝

$$A = \begin{pmatrix} a_{11}, & \dots, & a_{1n} \\ \dots & \dots & \dots \\ 0, & \dots,\ a_{ij},\ \dots, & 0 \\ \dots & \dots & \dots \\ a_{n1}, & \dots, & a_{nn} \end{pmatrix} :$$

Տեղափոխենք i-րդ տողը $(i-1)$-րդ տողի հետ, այնուհետև $(i-2)$-րդ տողի հետ, ..., առաջին տողի հետ: Արդյունքում A մատրիցի i-րդ տողը կդառնա ստացվող A' մատրիցի առաջին տող, որի համար պահանջվեց $i-1$ հատ տեղափոխություններ A մատրիցի տողերի միջև: Քանի որ տողերի յուրաքանչյուր տեղափոխության ընթացքում փոխվում է մատրիցի որոշիչի միայն նշանը, ապա

$$|A'| = (-1)^{i-1}|A| :$$

Այնուհետև, ստացված A' մատրիցի մեջ j-րդ սյունակը հերթով տեղափոխելով իր նախորդ $j-1$ հատ սյունակների հետ, կստանանք հետևյալ մատրիցը՝

$$A'' = \begin{pmatrix} a_{ij}, & 0, & \dots, & 0 \\ a_{1j}, & a_{11}, & \dots, & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{nj}, & a_{n1} & \dots, & a_{nn} \end{pmatrix} :$$

Մի կողմից՝

$$|A''| = (-1)^{j-1}|A'| = (-1)^{j-1}(-1)^{i-1}|A| = (-1)^{i+j-2}|A| = (-1)^{i+j}|A| ,$$

իսկ մյուս կողմից, համաձայն նախորդ լեմմի,

$$|A''| = a_{ij}|M''_{11}| ,$$

որտեղ $|M''_{11}|$-ը a_{ij} տարրի մինորն է A'' մատրիցում, որը կլինի հավասար a_{ij} տարրի $|M_{ij}|$ մինորին սկզբնական A մատրիցում: Այսպիսով՝

$$a_{ij}|M_{ij}| = (-1)^{i+j}|A|$$

և, հետևաբար,

$$(-1)^{i+j} a_{ij} |M_{ij}| = (-1)^{2(i+j)} |A| \,,$$

$$|A| = (-1)^{i+j} a_{ij} |M_{ij}| = a_{ij} A_{ij} \ :$$

□

Թեորեմ 14.9: *n-րդ կարգի $A = (a_{ij})$ մատրիցի որոշիչը հավասար է նրա կամայական տողի (սյան) տարրերի և նրանց հանրահաշվական լրացուցիչների արտադրյալների գումարին՝*

$$|A| = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}$$

$$(|A| = a_{1i}A_{1i} + a_{2i}A_{2i} + \cdots + a_{ni}A_{ni}) \ ,$$

որտեղ $i = 1, 2, \ldots, n$:

Ապացուցում: Ապացուցումը կատարենք ըստ i-րդ տողի: Ներկայացնելով մատրիցի i-րդ տողը հետևյալ գումարի տեսքով՝

$$(a_{i1}, a_{i2}, \ldots, a_{in}) = (a_{i1}, 0, \ldots, 0) + (0, a_{i2}, \ldots, 0) + \cdots + (0, \ldots, 0, a_{in}) \,,$$

կունենանք՝

$$|A| = |A_1| + |A_2| + \cdots + |A_n| \,,$$

որտեղ $A_1, A_2, \ldots, A_n$ մատրիցները ստացվում են A-ից փոխարինելով նրա i-րդ տողը համապատասխանաբար $(a_{i1}, 0, \ldots, 0)$, $(0, a_{i2}, \ldots, 0)$, $\ldots$, $(0, \ldots, 0, a_{in})$ տողերով: Մնում է օգտվել նախորդ լեմմից: □

Հատկություն 14.29 (տարրերի և հանրահաշվական լրացուցիչների օրթոգոնալության մասին) : *n-րդ կարգի $A = (a_{ij})$ մատրիցի որևէ տողի (սյան) տարրերի և մեկ այլ տողի (սյան) համապատասխան տարրերի հանրահաշվական լրացուցիչների արտադրյալների գումարը հավասար է զրոյի՝*

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = 0, \quad \textit{եթե} \ i \neq j$$

$$(a_{1i}A_{1j} + a_{2i}A_{2j} + \cdots + a_{ni}A_{nj} = 0, \quad \textit{եթե} \ i \neq j) \ :$$

Ապացուցում: Նախ նկատենք, որ եթե երկու n-րդ կարգի մատրիցներ տարբերվում են միայն մեկ տողի (սյան) տարրերով, ապա այդ տողի (սյան) տարրերի հանրահաշվական լրացուցիչները երկու մատրիցներում էլ կլինեն նույնը, որովհետև դրանց սահմանման (հաշվման) մեջ այդ տողի (սյան) տարրերը չեն մասնակցում (ջնջվում են): Տրված A մատրիցի j-րդ տողը (սյունակը) փոխարինելով i-րդ տողով (սյունակով), որտեղ $i \neq j$, կստանանք մի A' մատրից, որը կունենա երկու հավասար տողեր (սյունակներ): Հետևաբար, $|A'| = 0$: Մյուս կողմից, $|A'|$-ը վերլուծելով ըստ A'-ի j-րդ տողի (սյան) տարրերի, կստանանք՝

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \cdots + a_{in}A_{jn} = 0$$

$$(a_{1i}A_{1j} + a_{2i}A_{2j} + \cdots + a_{ni}A_{nj} = 0) \ : \qquad \square$$

Թեորեմ 14.10 (մատրիցի հակադարձելիության հայտանիշը): *Եթե n-րդ կարգի մատրիցը հակադարձելի է աջից (ձախից), ապա նրա որոշիչը հավասար չէ զրոյի: Եվ հակառակը, եթե n-րդ կարգի մատրիցի որոշիչը հավասար չէ զրոյի, ապա այն հակադարձելի է: Այլ կերպ, n-րդ կարգի A մատրիցը կլինի հակադարձելի այն և միայն այն դեպքում, երբ $det(A) \neq 0$:*

Ապացուցում: Եթե n-րդ կարգի A մատրիցի համար գոյություն ունի այնպիսի n-րդ կարգի A' մատրից, որ $A \cdot A' = E_n$, ապա $det(A \cdot A') = det(E_n)$ և համաձայն թեորեմ 14.7-ի՝ $det(A) \cdot det(A') = 1$: Հետևաբար, $det(A) \neq 0$: Նույնը կստացվեր, եթե A մատրիցը լիներ հակադարձելի ձախից:

Եվ հակառակը, եթե $d = det(A) \neq 0$, ապա նշանակելով՝

$$A' = \begin{pmatrix} \frac{A_{11}}{d}, & \frac{A_{21}}{d}, & \ldots, & \frac{A_{n1}}{d} \\ \frac{A_{12}}{d}, & \frac{A_{22}}{d}, & \ldots, & \frac{A_{n2}}{d} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{A_{1n}}{d}, & \frac{A_{2n}}{d}, & \ldots, & \frac{A_{nn}}{d} \end{pmatrix}$$

և օգտվելով թեորեմ 14.9-ից ու հատկություն 14.29-ից, կստանանք՝

$$A \cdot A' = A' \cdot A = E_n \ : \qquad \square$$

Հետևություն 14.9 (հակադարձ մատրիցի հաշվման բանաձևը): *Եթե n-րդ կարգի A մատրիցը հակադարձելի է, ապա $det(A^{-1}) = (det\,A)^{-1}$ և*

A^{-1} հակադարձը որոշվում է հետևյալ բանաձևով՝

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{d}, & \frac{A_{21}}{d}, & \ldots, & \frac{A_{n1}}{d} \\ \frac{A_{12}}{d}, & \frac{A_{22}}{d}, & \ldots, & \frac{A_{n2}}{d} \\ \ldots & \ldots & \ldots & \ldots \\ \frac{A_{1n}}{d}, & \frac{A_{2n}}{d}, & \ldots, & \frac{A_{nn}}{d} \end{pmatrix}, \tag{14.1}$$

որտեղ $d = det(A) \neq 0$: Մասնավորապես,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix},$$

եթե $ad - bc \neq 0$: □

A մատրիցը կոչվում է ամբողջարժեք, եթե նրա տարրերը ամբողջ թվեր են:

Հետևություն 14.10: *n-րդ կարգի ամբողջարժեք A հակադարձելի մատրիցի A^{-1} հակադարձը կլինի ամբողջարժեք այն և միայն այն դեպքում, երբ $det(A) = \pm 1$:* □

Հաճախ n-րդ կարգի մատրիցը կոչվում է **վերասերված**, եթե նրա որոշիչը հավասար է զրոյի, և **չվերասերված**՝ հակառակ դեպքում:

14.6. Իրական գործակիցներով գծային հավասարումների համակարգեր: Կրամերի և Գաուսի եղանակները

Մեկ անհայտով $ax = b$ գծային հավասարումները, ինչպես նաև երկու անհայտով և իրական գործակիցներով

$$\begin{cases} ax + by = l, \\ cx + dy = f \end{cases}$$

գծային հավասարումների համակարգերը լուծվում են դպրոցական դասընթացում: Այստեղ, դպրոցական դասընթացից հայտնի արդյունքներն ու մեթոդները տարածվում են կամայական վերջավոր թվով անհայտներ պարունակող գծային հավասարումների համակարգերի վրա:

Դիտարկենք n անհայտներով m հատ գծային հավասարումների հետևյալ համակարգը՝

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1, \\ \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m, \end{cases} \tag{14.2}$$

որտեղ $x_1, \ldots, x_n$ անհայտների a_{ij} **գործակիցները** ($i = 1, \ldots, m$; $j = 1, \ldots, n$) և $b_1, \ldots, b_m$ **ազատ անդամները** իրական թվեր են, իսկ $+$ և $\cdot$ գործողությունները իրական թվերի սովորական գումարը և արտադրյալն են:

Իրական թվերի $(\alpha_1, \ldots, \alpha_n)$ կարգավորված n-յակը կոչվում է

$$a_{i1}x_1 + \cdots + a_{in}x_n = b_i$$

գծային **հավասարման լուծում**, եթե այդ հավասարման մեջ տեղադրելով $x_1 = \alpha_1$, ..., $x_n = \alpha_n$ (և կատարելով ձախ մասի գործողությունները) ստանում ենք ճիշտ հավասարություն: Ակնհայտ է, որ նշված հավասարումը չի ունենա լուծում այն և միայն այն դեպքում, երբ $a_{i1} = \cdots = a_{in} = 0$, իսկ $b_i \neq 0$: $b_i = 0$ դեպքում նշված գծային հավասարումը կոչվում է **համասեռ**:

Իրական թվերի $(\alpha_1, \ldots, \alpha_n)$ կարգավորված n-յակը կոչվում է (14.2) **համակարգի լուծում**, եթե այն լուծում է այդ համակարգի յուրաքանչյուր հավասարման համար:

Լուծել համակարգը նշանակում է գտնել (որոշել, նկարագրել) այդ համակարգի բոլոր լուծումները: Համակարգը կոչվում է **լուծելի** կամ **համատեղելի** (համատեղ), եթե այն ունի որևէ լուծում: Հակառակ դեպքում համակարգը կոչվում է **անհամատեղելի**:

Ի նկատի ունենալով մատրիցների գումարման, բազմապատկման և թիվը (ձախից) մատրիցով բազմապատկելու գործողությունները, ինչպես նաև մատրիցների հավասարության գաղափարը, գծային հավասարումների (14.2) համակարգը կարելի է գրել հետևյալ մատրիցային տեսքով.

$$x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}, \tag{14.3}$$

կամ

$$\begin{pmatrix} a_{11}, & \dots, & a_{1n} \\ \dots & \dots & \dots \\ a_{m1}, & \dots, & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} : \tag{14.4}$$

Նշանակելով՝

$$A = \begin{pmatrix} a_{11}, & \dots, & a_{1n} \\ \dots & \dots & \dots \\ a_{m1}, & \dots, & a_{mn} \end{pmatrix},$$

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad \text{և} \quad B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

(14.2) համակարգը կընդունի հետևյալ համառոտ մատրիցային տեսքը.

$$A \cdot X = B, \tag{14.5}$$

որտեղ անհայտների գործակիցներից կազմված $m \times n$-չափանի A մատրիցը կոչվում է (14.2) **համակարգի հիմնական մատրից**, իսկ

$$\tilde{A} = \begin{pmatrix} a_{11}, & \dots, & a_{1n}, & b_1 \\ \dots & \dots & \dots & \dots \\ a_{m1}, & \dots, & a_{mn}, & b_m \end{pmatrix}$$

մատրիցը՝ դրա **ընդլայնված մատրից**:

Իրական թվերի $(\alpha_1, \dots, \alpha_n)$ կարգավորված n-յակը կոչվում է (14.3) հավասարման լուծում, եթե

$$\alpha_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + \alpha_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},$$

իսկ $\beta = \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix}$ սյունակը կոչվում է (14.4) կամ (14.5) հավասարման լուծում, եթե $A \cdot \beta = B$:

Լեմմ 14.11: *1) Որպեսզի* $(\alpha_1, \ldots, \alpha_n)$*-ը լինի (14.2) համակարգի լուծում անհրաժեշտ է և բավարար, որ* $(\alpha_1, \ldots, \alpha_n)$*-ը լինի լուծում (14.3) հավասարման համար;*

2) Որպեսզի $(\alpha_1, \ldots, \alpha_n)$*-ը լինի (14.2) համակարգի լուծում անհրաժեշտ է և բավարար, որ* $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ *սյունակը լինի լուծում (14.5) հավասարման համար:* □

Եթե $b_1 = \cdots = b_m = 0$, այսինքն՝ $B = 0$, ապա (14.2) համակարգը կոչվում է **համասեռ**, ավելի ճիշտ n անհայտով m գծային հավասարումների համասեռ համակարգ; Հակառակ դեպքում, գծային հավասարումների համակարգը կոչվում է **ոչ համասեռ**: Գծային հավասարումների

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = 0, \\ \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = 0, \end{cases} \tag{14.2'}$$

համասեռ համակարգը նույնպես հաճախ գրվում է մատրիցային տեսքով՝

$$x_1 \begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix} + \cdots + x_n \begin{pmatrix} a_{1n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{14.3'}$$

$$\begin{pmatrix} a_{11}, & \ldots, & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1}, & \ldots, & a_{mn} \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{14.4'}$$

կամ՝

$$A \cdot X = 0 , \tag{14.5'}$$

և դրանցից յուրաքանչյուրը կոչվում է գծային հավասարումների (14.2) համակարգին համապատասխան (համապատասխանող) համասեռ համակարգ:

Գծային հավասարումների (14.2’) համասեռ համակարգը միշտ օժտված է $(0, \ldots, 0)$ զրոյական լուծումով:

Հատկություն 14.30: *Գծային հավասարումների (14.2') համասեռ համակարգի լուծումների $\mathfrak{N}_n$ բազմությունը փակ է n-տողերի գումարման և թվով բազմապատկման գործողությունների նկատմամբ, այսինքն՝*

$$X, Y \in \mathfrak{N}_n \longrightarrow X + Y \in \mathfrak{N}_n \ ,$$

$$X \in \mathfrak{N}_n \longrightarrow \alpha X \in \mathfrak{N}_n$$

ցանկացած α իրական թվի համար:

Ապացուցում: Կատարվում է անմիջական ստուգման եղանակով: □

Հատկություն 14.31: *Եթե իրական գործակիցներով գծային հավասարումների համասեռ համակարգն օժտված է որևէ ոչ զրոյական լուծումով, ապա նրա բոլոր լուծումների թիվն անվերջ է: Այսինքն՝ իրական գործակիցներով գծային հավասարումների համասեռ համակարգը կամ ունի միայն մեկ (զրոյական) լուծում, կամ նրա լուծումների թիվն անվերջ է:*

Ապացուցում: Եթե $X = (x_1, \ldots, x_n) \neq 0$, ապա որևէ $x_i \neq 0$ և, հետևաբար, եթե $\alpha \neq \beta$, ապա $\alpha x_i \neq \beta x_i$, ուստի՝ $\alpha X \neq \beta X$, որտեղ $\alpha, \beta \in \mathbb{R}$: Մնում է օգտվել նախորդ հատկությունից: □

Իրական թվերի $(\eta_1, \ldots, \eta_n) = \eta$ կարգավորված n-յակի և կարգավորված n-յակների որևէ $\mathfrak{N}$ ենթաբազմության $\eta + \mathfrak{N}$ գումար ասելով հասկացվում է $\eta + \mu$ տեսքի բոլոր կարգավորված n-յակների բազմությունը, որտեղ μ-ն փոփոխվում է $\mathfrak{N}$-ում՝

$$\eta + \mathfrak{N} = \{\eta + \mu \mid \mu \in \mathfrak{N}\} \ ;$$

Թեորեմ 14.11: *Եթե η-ն գծային հավասարումների (14.2) համակարգի որևէ լուծում է, $\mathfrak{M}_n$-ը նրա բոլոր լուծումների բազմությունն է, իսկ $\mathfrak{N}_n$-ը համապատասխան համասեռ համակարգի բոլոր լուծումների բազմությունը, ապա*

$$\mathfrak{M}_n = \eta + \mathfrak{N}_n \ : \tag{14.6}$$

Ապացուցում: Պահանջվում է ապացուցել հետևյալ երկու ներդրումները՝

$$\mathfrak{M}_n \subseteq \eta + \mathfrak{N}_n \ ,$$

$$\eta + \mathfrak{N}_n \subseteq \mathfrak{M}_n \ ;$$

Ցանկացած $\sigma \in \mathfrak{M}_n$ լուծման համար $\sigma - \eta$ տարբերությունը, ակնհայտորեն, կլինի լուծում (14.2)-ին համապատասխանող (14.2') համասեռ համակարգի համար՝ $\sigma - \eta \in \mathfrak{N}_n$; Նշանակելով՝ $\mu = \sigma - \eta \in \mathfrak{N}_n$, կստանանք՝ $\sigma = \eta + \mu \in \eta + \mathfrak{N}_n$: Այսպիսով՝ $\mathfrak{M}_n \subseteq \eta + \mathfrak{N}_n$; Հակառակ ներդրումն ակնհայտ է: Օրինակ, մատրիցային տեսքով՝ $A(\eta + \mu) = A\eta + A\mu = B + 0 = B$, այսինքն՝ $\eta + \mu \in \mathfrak{M}_n$, որտեղ $\mu \in \mathfrak{N}_n$: □

Հետևություն 14.11: *Իրական գործակիցներով գծային հավասարումների (14.2) համակարգը կամ չունի լուծում, կամ ունի միայն մեկ լուծում, կամ ունի անվերջ թվով լուծումներ:*

Ապացուցում: Բխում է (14.6) բանաձևից և հատկություն 14.31-ից: □

Գծային հավասարումների համատեղելի համակարգը կոչվում է **որոշյալ**, եթե այն ունի միակ լուծում; Հակառակ դեպքում, գծային հավասարումների համատեղելի համակարգը կոչվում է **անորոշ**:

Թեորեմ 14.12 (Կրամեր): *Եթե n-րդ կարգի $A = (a_{ij})$ մատրիցը հակադարձելի է, ապա ցանկացած $b_1, \ldots, b_n$ իրական թվերի համար գծային հավասարումների*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1, \\ \ldots \quad \ldots \quad \ldots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{cases} \tag{14.7}$$

համակարգը կլինի որոշյալ: Ըստ որում, այդ համակարգի միակ $(x_1, \ldots, x_n)$ լուծումը որոշվում է հետևյալ բանաձևերով՝

$$x_i = \frac{det(A_i)}{det(A)}\,, \qquad i = 1, 2, \ldots, n\,, \tag{14.8}$$

որտեղ A_i մատրիցը ստացվում է A-ից՝ նրա i-րդ սյունակը փոխարինելով ազատ անդամների $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ սյունակով:

Այս բանաձևերը կոչվում են Կրամերի բանաձևեր:

Ապացուցում: Դիտարկվող (14.7) համակարգի որոշյալ լինելու փաստը հետևում է հատկություն 14.10-ից: Ըստ որում, եթե (14.7) համակարգը գրենք $A \cdot X = B$ մատրիցային տեսքով, ապա կունենանք՝ $X = A^{-1} \cdot B$: Մնում է օգտվել A^{-1} հակադարձ մատրիցի հաշվման (14.1) բանաձևից և թեորեմ 14.9-ից: □

Հետևություն 14.12: Եթե n անհայտներով n գծային հավասարումների համակարգը չունի լուծում, ապա այդ համակարգի հիմնական մատրիցի որոշիչը հավասար է զրոյի: □

Հետևություն 14.13: Եթե n անհայտներով n գծային հավասարումների համակարգն ունի մեկից ավելի լուծումներ, ապա այդ համակարգի հիմնական մատրիցի որոշիչը հավասար է զրոյի: □

Հետևություն 14.14: Եթե n անհայտներով n գծային հավասարումների համասեռ համակարգն ունի ոչ զրոյական լուծում, ապա այդ համակարգի հիմնական մատրիցի որոշիչը հավասար է զրոյի: □

Գծային հավասարումների համակարգի լուծման Կրամերի եղանակը հիմնականում ունի տեսական, քան գործնական նշանակություն, քանի որ բարձր կարգի մատրիցների որոշիչների հաշվումը կապված է հսկայական թվով թվաբանական գործողությունների հետ: Գծային հավասարումների համակարգերի լուծման լավագույն եղանակներից մեկը, այսպես կոչված, **Գաուսի եղանակն է**:

Միևնույն $x_1, x_2, \ldots, x_n$ անհայտներից կախված երկու (a) և (b) գծային հավասարումների համակարգեր կոչվում են **համարժեք** և գրվում է $(a) \sim (b)$, եթե դրանք համատեղելի են և ունեն լուծումների նույն բազմությունները, կամ երկու համակարգերն էլ անհամատեղելի են: Ակնհայտ է, որ

ա) $(a) \sim (a)$,

բ) $(a) \sim (b) \longrightarrow (b) \sim (a)$,

գ) $(a) \sim (b)$, $(b) \sim (c) \longrightarrow (a) \sim (c)$:

Կասենք, որ գծային հավասարումների (14.2) համակարգի նկատմամբ կատարվում է.

I) առաջին տիպի (տեսակի) տարրական ձևափոխություն, եթե համակարգի բոլոր հավասարումները, բացի որևէ i-րդ հավասարումից, թողնվում են նույնը, իսկ i-րդ հավասարումը փոխարինվում է հետևյալ հավասարումով՝

$$(a_{i1} + \lambda a_{k1})\, x_1 + \cdots + (a_{in} + \lambda a_{kn})\, x_n = b_i + \lambda b_k,$$

որտեղ $\lambda \in \mathbb{R}$, $k \neq i$, $1 \leqslant k \leqslant m$: Այլ կերպ, համակարգի որևէ i-րդ հավասարմանը գումարվում է նրա մեկ այլ հավասարում, վերջինս նախապես բազմապատկելով որևէ λ թվով;

II) երկրորդ տիպի (տեսակի) տարրական ձևափոխություն, եթե համակարգի բոլոր հավասարումները, բացի որևէ i-րդ հավասարումից, թողնվում են նույնը, իսկ i-րդ հավասարումը փոխարինվում է հետևյալ հավասարումով՝

$$\lambda a_{i1}x_1 + \cdots + \lambda a_{in}x_n = \lambda b_i,$$

որտեղ $\lambda \in \mathbb{R}$, $\lambda \neq 0$: Այլ կերպ, համակարգի որևէ i-րդ հավասարում բազմապատկվում է որևէ ոչ զրոյական λ թվով;

III) երրորդ տիպի (տեսակի) տարրական ձևափոխություն, եթե համակարգի որևէ երկու i-րդ և k-րդ հավասարումների տեղերը փոխվում են, իսկ մնացած հավասարումները թողնվում են իրենց տեղերում ($i \neq k$):

Ապացուցենք գծային հավասարումների համակարգերի համարժեքության հետևյալ բավարար պայմանը:

Թեորեմ 14.13: *Եթե գծային հավասարումների (14.2) համակարգի նկատմամբ կատարվի առաջին, երկրորդ կամ երրորդ տիպի (տեսակի) տարրական ձևափոխություն, ապա ստացվող համակարգը կլինի համարժեք (14.2) սկզբնական համակարգին:*

Ապացուցում: III. Երրորդ տիպի (տեսակի) տարրական ձևափոխության դեպքում պնդումն ակնհայտ է:

II. Երկրորդ տիպի (տեսակի) տարրական ձևափոխության դեպքում պնդումը ճիշտ է, որովհետև

$$a_{i1}\alpha_1 + \cdots + a_{in}\alpha_n = b_i \longleftrightarrow \lambda a_{i1}\alpha_1 + \cdots + \lambda a_{in}\alpha_n = \lambda b_i, \quad \lambda \neq 0 :$$

I. Առաջին տիպի (տեսակի) տարրական ձևափոխության դեպքում ևս պնդումը ճիշտ է, որովհետև

$$\left\{\begin{array}{l} a_{i1}\alpha_1 + \cdots + a_{in}\alpha_n = b_i, \\ \\ a_{k1}\alpha_1 + \cdots + a_{kn}\alpha_n = b_k \end{array}\right. \leftrightarrow \left\{\begin{array}{l} (a_{i1} + \lambda a_{k1})\,\alpha_1 + \cdots + (a_{in} + \lambda a_{kn})\,\alpha_n = \\ \qquad\qquad\qquad\qquad = b_i + \lambda b_k, \\ a_{k1}\alpha_1 + \cdots + a_{kn}\alpha_n = b_k : \end{array}\right.$$

□

Գծային հավասարումների համակարգերի լուծման **Գաուսի** եղանակի (ալգորիթմի) ժամանակ, տրված գծային հավասարումների համակարգը, տարրական ձևափոխությունների միջոցով, բերվում է իրեն համարժեք մեկ այլ գծային հավասարումների համակարգի, որի բոլոր լուծումները գտնվում են հեշտությամբ: Նկարագրենք գծային հավասարումների համակարգի լուծման Գաուսի եղանակը (14.2) ընդհանուր համակարգի համար:

Սկզբից նկատենք, որ a_{i1} գործակիցներից որևէ մեկը կարելի է ենթադրել տարբեր զրոյից, հակառակ դեպքում իմաստ չէր ունենա համակարգի մեջ նշելու x_1 անհայտը: Կարելի է ենթադրել, որ $a_{11} \neq 0$ (հակառակ դեպքում առաջին հավասարումը կտեղափոխենք այնպիսի j-րդ հավասարման հետ, որի համար $a_{j1} \neq 0$): Այժմ արտաքսենք x_1 անհայտը (14.2) համակարգի բոլոր հավասարումներից՝սկսած երկրորդից: Դրա համար, i-րդ հավասարումից $(i = 2, \ldots, m)$ հանենք առաջինը նախապես այն բազմապատկելով $\lambda_i = a_{i1} \cdot a_{11}^{-1}$ գործակցով: Այս ձևով առաջանում է գծային հավասարումների նոր համակարգ, որտեղ x_1 անհայտը մասնակցում է միայն նրա առաջին հավասարման մեջ: Սակայն հնարավոր է, որ կատարվող ձևափոխության հետևանքով անհետանան նաև ուրիշ անհայտներ: Դիցուք, x_k-ն այն ամենափոքր նշիչով անհայտն է, որը մտնում է առաջացած համակարգի որևէ հավասարման մեջ՝ սկսած երկրորդից: Այդ դեպքում, ստացված համակարգը կունենա հետևյալ տեսքը՝

$$\left\{\begin{array}{llll} a_{11}x_1+ & \cdots & \cdots & +a_{1n}x_n = b_1, \\ & a'_{2k}x_k+ & \cdots & +a'_{2n}x_n = b'_2, \\ & \cdots & \cdots & \cdots \\ & a'_{mk}x_k+ & \cdots & +a'_{mn}x_n = b'_m : \end{array}\right. \qquad (14.\text{ա})$$

Ըստ որում, համաձայն թեորեմ 14.13-ի, (14.ա) համակարգը կլինի համարժեք (14.2) համակարգին:

Այժմ ենթադրելով, որ $a'_{2k} \neq 0$, սևեռում ենք (14.ա) համակարգի նաև երկրորդ հավասարումը և մնացած հավասարումների նկատմամբ կատարում համանման ձևափոխություն՝ x_k անհայտը, սկսած երրորդ հավասարումից, արտաքսելու համար: Այսպիսով, հանգում ենք գծային հավասարումների հետևյալ համակարգին՝

$$\left\{\begin{array}{lllll} a_{11}x_1+ & \cdots & \cdots & \cdots & +a_{1n}x_n = b_1, \\ & a'_{2k}x_k+ & \cdots & \cdots & +a'_{2n}x_n = b'_2, \\ & & a'_{3\ell}x_\ell+ & \cdots & +a'_{3n}x_n = b''_3, \\ & & \cdots & \cdots & \cdots \\ & & a'_{m\ell}x_\ell+ & \cdots & +a'_{mn}x_n = b''_m, \end{array}\right. \qquad (14.\text{բ})$$

որտեղ $\ell > k > 1$, $a_{11} \neq 0$, $a'_{2k} \neq 0$:

Այս համակարգը լինելով համարժեք նախորդ (14.ա) համակարգին, կլինի համարժեք նաև սկզբնական (14.2) համակարգին: Կրկնելով անհայտների արտաքսման նկարագրված քայլերը, ի վերջո հանգում ենք հետևյալ տեսքի համակարգի՝

$$\begin{cases} a_{11}x_1 + \cdots \cdots \cdots \cdots + a_{1n}x_n = b_1, \\ a'_{2k}x_k + \cdots \cdots \cdots + a'_{2n}x_n = b'_2, \\ a'_{3\ell}x_\ell + \cdots \cdots + a'_{3n}x_n = b''_3, \\ \cdots \cdots \cdots \\ \tilde{a}_{rs}x_s + \cdots + \tilde{a}_{rn}x_n = \tilde{b}_r, \\ 0 = \bar{b}_{r+1}, \\ \cdots\cdots \\ 0 = \bar{b}_m, \end{cases} \tag{14.գ}$$

որտեղ $a_{11} \neq 0$, $a'_{2k} \neq 0$, $a''_{3\ell} \neq 0$, …, $\bar{a}_{rs} \neq 0$, $1 < k < \ell < \cdots < s$:

Այս համակարգը կոչվում է **սեղանաձև** կամ **աստիճանաձև** տեսքի (համակարգ), իսկ $r = n$ դեպքում՝ **եռանկյունաձև տեսքի**:

Հնարավոր է, որ (14.գ) համակարգում՝ $r = m$, այսինքն՝ $0 = \bar{b}_t$ տեսքի հավասարում ընդհանրապես չլինի: Մյուս կողմից, եթե (14.գ) համակարգում լինի $0 = \bar{b}_t$ տեսքի հավասարում՝ ոչ զրոյական $\bar{b}_t$ ազատ անդամով, ապա ակնհայտ է, որ (14.գ) համակարգը (նրա հետ մեկտեղ նաև սկզբնական (14.2) համակարգը) կլինի ոչ համատեղելի: Իսկ, եթե (14.գ) համակարգում այդպիսի հավասարում չկա, ապա այն կլինի համատեղելի: Իրոք, դիցուք $t > r$ դեպքում $\bar{b}_t$ ազատ անդամները զրոյական են (կամ $0 = \bar{b}_t$ տեսքի հավասարում ընդհանրապես չկա): Այն անհայտները, որոնցով սկսվում են (14.գ) համակարգի առաջին r հավասարումները, այսինքն՝ $x_1, x_k, x_\ell, \ldots, x_s$-ը կոչվում են **գլխավոր** կամ **առաջատար** անհայտներ, իսկ մնացած բոլոր անհայտները (եթե այդպիսիք գոյություն ունեն)՝ **ազատ** անհայտներ: Ազատ անհայտներին տանք կամայական իրական արժեքներ և այդ արժեքները տեղադրենք (14.գ) համակարգի բոլոր հավասարումների մեջ: Մասնավորապես, r-րդ հավասարումը այդ դեպքում կընդունի հետևյալ տեսքը՝ $ax_s = b$, որտեղ $a = \tilde{a}_{rs} \neq 0$ և, հետևաբար, այն օժտված կլինի միարժեքորեն որոշվող լուծումով: Որից հետո, ի նկատի ունենալով x_s անհայտի ստացված արժեքը, $r-1$-րդ հավասարումից կարելի է որոշել մյուս գլխավոր անհայտի միարժեքորեն որոշվող արժեքը և այսպես շարունակ ... : Աստիճանաբար բարձրանալով (14.գ) համակարգի բոլոր հավասարումներով, ստանում ենք բոլոր գլխավոր անհայտների միարժեքորեն որոշվող արժեքները:

Այսպիսով, հանգում ենք հետևյալ արդյունքին:

Թեորեմ 14.14 (Գաուսի ալգորիթմը): *Որպեսզի գծային հավասարումների (14.2) համակարգը լինի համատեղելի անհրաժեշտ է և բավարար, որ տարրական ձևափոխությունների օգնությամբ (14.գ) սեղանաձև տեսքի բերելուց հետո նրանում չլինի ոչ զրոյական ազատ անդամով այնպիսի հավասարում, որի բոլոր անհայտների գործակիցները զրոներ են: Ընդսմին, եթե այդ պայմանը տեղի ունի, ապա (14.գ) սեղանաձև տեսքի մեջ ազատ անհայտներին (եթե դրանք գոյություն ունեն) տրված կամայական արժեքների դեպքում գլխավոր անհայտների արժեքները համակարգի հավասարումներից որոշվում են միարժեքորեն: Մասնավորապես, (14.2) համատեղելի համակարգը կլինի որոշյալ այն և միայն այն դեպքում, երբ դրանից ստացվող (14.գ) սեղանաձև տեսքի մեջ չկան ազատ անհայտներ, այսինքն՝ $r = n$ (երբ (14.գ) համակարգը եռանկյունաձև տեսքի է):* □

***Հետևություն 14.15**: 1) Եթե գծային հավասարումների (14.2) համատեղելի համակարգի անհայտների թիվը գերազանցում է հավասարումների թվին, ապա դրա լուծումների թիվն անվերջ է:*

2) Եթե գծային հավասարումների համասեռ համակարգի անհայտների թիվը գերազանցում է հավասարումների թվին, ապա դրա լուծումների թիվն անվերջ է:

Ապացուցում: Բոլոր դեպքերում, (14.գ) համակարգի մեջ՝ $r \leqslant m$: Այդ պատճառով, $m < n$ պայմանից հետևում է $r < n$ անհավասարությունը: Հետևաբար, (14.գ) սեղանաձև տեսքի մեջ գոյություն կունենա ազատ անհայտ, որի տարբեր արժեքներին կհամապատասխանեն տարբեր լուծումներ: □

Հետևյալ արդյունքը հանդիսանում է Կրամերի թեորեմի (թեորեմ 14.12) հակադարձումը:

Թեորեմ 14.15: *Եթե n անհայտներով n գծային հավասարումների համատեղելի համակարգը որոշյալ է, ապա այդ համակարգի հիմնական մատրիցը կլինի հակադարձելի (և, հետևաբար, կունենա ոչ զրոյական որոշիչ):*

Ապացուցում: Այս պայմանի դեպքում, համաձայն նախորդ թեորեմի, տրված համակարգը տարրական ձևափոխությունների օգնությամբ կբերվի եռանկյունաձև տեսքի և, հետևաբար, նաև

$$\begin{cases} x_1 \qquad\qquad\qquad = b_1^*, \\ \qquad x_2 \qquad\qquad = b_2^*, \\ \qquad\quad \dots \\ \qquad\qquad\qquad x_n = b_n^* \end{cases} \tag{14.դ}$$

տեսքի: Մնում է նկատել, որ գծային հավասարումների համակարգի նկատմամբ կատարվող տարրական ձևափոխություններին համապատասխանում են նրա հիմնական մատրիցի նկատմամբ կատարվող տարրական ձևափոխություններ և օգտվել թեորեմ 14.4-ից:

Երկրորդ ապացուցում: Քանի որ գծային հավասարումների համակարգի տարրական ձևափոխությունների ժամանակ, դիտարկվող համակարգի հիմնական մատրիցի որոշիչը կարող է փոխվել միայն ոչ զրոյական $\alpha \in \mathbb{R}$ արտադրիչով, իսկ (14.դ) համակարգի հիմնական մատրիցի որոշիչը հավասար է մեկի, ապա սկզբնական համակարգի հիմնական մատրիցի որոշիչը կլինի ոչ զրոյական: Մնում է օգտվել n-րդ կարգի մատրիցի հակադարձելիության հայտանիշից (թեորեմ 14.10): □

Դիտողություն: Քանի որ գծային հավասարումների համակարգի տարրական ձևափոխությունների դեպքում, նրա լուծումների բազմությունը չի փոխվում, ապա Կրամերի (14.8) բանաձևերը կարելի է նաև ապացուցել՝ ստուգելով դրանց միայն (14.դ) տեսքի համակարգի համար.

$$x_i = \frac{det(A_i)}{det(A)} = \frac{b_i^*}{1} = b_i^* \ :$$

14.7. Օղակի և դաշտի հասկացությունները: Դաշտի բնութագրիչը: Օղակների և դաշտերի իզոմորֆիզմը

Ոչ դատարկ Q բազմության վրա որոշված գործողության գաղափարը սահմանվել է 1.4 վերնագրում:

Ոչ դատարկ Q բազմությունն իր մեջ որոշված երկու գործողությունների հետ մեկտեղ (որոնցից մեկը կոչվում է «գումար» և նշանակվում է $+$ նշանով, իսկ մյուսը՝ «արտադրյալ» և նշանակվում է $\cdot$ նշանով) կոչվում է **օղակ** և նշանակվում է $Q(+,\cdot)$-ով, եթե տեղի ունեն հետևյալ պայմանները (որոնք կոչվում են օղակային աքսիոմներ).

1. Գումարման զուգորդականությունը՝
$$(x+y)+z = x+(y+z)$$
ցանկացած $x, y, z \in Q$ տարրերի համար;

2. Գումարման տեղափոխականությունը՝
$$x+y = y+x$$
ցանկացած $x, y \in Q$ տարրերի համար;

3. Գոյություն ունի այնպիսի $0 \in Q$ տարր, որ
$$x+0 = x$$
ցանկացած $x \in Q$ տարրի համար;

4. Յուրաքանչյուր $a \in Q$ տարրի համար գոյություն ունի այնպիսի $-a \in Q$ տարր, որ
$$a+(-a) = 0;$$

5. Ձախ և աջ բաշխական օրենքները՝
$$x(y+z) = xy+xz,$$
$$(y+z)x = yx+zx$$
ցանկացած $x, y, z \in Q$ տարրերի համար:

0 տարրը կոչվում է **օղակի զրո** կամ **զրոյական տարր**, իսկ $-a$ տարրը կոչվում է a-ի հակադիր տարր:

Օղակի սահմանումից բխում են նրա հետևյալ հատկությունները:

1) $a+x = a+y \to (-a)+(a+x) = (-a)+(a+y) \to ((-a)+a)+x = ((-a)+a)+y \to 0+x = 0+y \to x+0 = y+0 \to x = y$:

Հետևաբար, օղակի զրոն և տարրի հակադիրը որոշվում են միարժեքորեն, որպես $a+x = a$ և $a+x = 0$ հավասարումների լուծումներ: Այնուհետև, $a \cdot 0 = 0$, որովհետև $a \cdot 0 + 0 = a \cdot 0 = a(0+0) = a \cdot 0 + a \cdot 0$ և $0 \cdot a = 0$, որովհետև $0 \cdot a + 0 = 0 \cdot a = (0+0)a = 0 \cdot a + 0 \cdot a$: Սակայն օղակի զրոյի միակությունը կարելի է նկատել նաև անմիջականորեն՝
$$0_2 = 0_2 + 0_1 = 0_1 + 0_2 = 0_1 \ :$$

2) $Q(+,\cdot)$ օղակի ցանկացած $a, b \in Q$ տարրերի համար՝

$$x = (-a) + b \to a + x = a + ((-a) + b) = (a + (-a)) + b = 0 + b = b,$$

այսինքն՝ $a + x = b$ հավասարումն ունի $x = (-a) + b$ լուծումը և, նախորդ հատկության համաձայն, այդ լուծումը կլինի միակը:

3) $-(-a) = a$, $a(-b) = (-a)b = -(ab)$ և $(-a)(-b) = ab$, որովհետև $0 = a \cdot 0 = a(b + (-b)) = ab + a(-b)$, $0 = 0 \cdot b = (a + (-a))b = ab + (-a)b$, $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$:

4) Վերհանգման եղանակով ապացուցվում են հետևյալ հավասարությունները՝

$$x(y_1 + \cdots + y_n) = xy_1 + \cdots + xy_n,$$

$$(x_1 + \cdots + x_m)y = x_1y + \cdots + x_my,$$

որից հետո ստացվում է նաև հետևյալ հավասարությունը՝

$$(x_1 + \cdots + x_m)(y_1 + \cdots + y_n) = x_1y_1 + \cdots + x_1y_n + \cdots + x_my_1 + \cdots + x_my_n :$$

5) Գումարման զուգորդականության շնորհիվ, կարելի է սահմանել օղակի ցանկացած a տարրի **ամբողջ պատիկի** գաղափարը՝

$$na = \underbrace{a + \cdots + a}_{n}, \quad n > 0\ ,$$

$$0a = 0,$$

$$(-n)a == \underbrace{(-a) + \cdots + (-a)}_{n}, \ \ n > 0 \ :$$

Տեղի ունեն հետևյալ հավասարությունները՝

$$(m_1 + m_2)a = m_1a + m_2a,$$

$$(m_1 \cdot m_2)a = m_1(m_2a)$$

ցանկացած $m_1, m_2 \in \mathbb{Z}$ ամբողջ թվերի համար:

Օրինակներ: 1) $\mathbb{Z}(+,\cdot)$-ը օղակ է, որը կոչվում է **ամբողջ թվերի օղակ**;

2) Բոլոր զույգ թվերի բազմությունն օղակ է՝ ամբողջ թվերի գումարման և բազմապատկման նկատմամբ, որը կոչվում է **զույգ թվերի օղակ**;

3) $\mathbb{Z}_n(+,\cdot)$-ը օղակ է, որը կոչվում է n-**րդ աստիճանի մնացքների օղակ**;

4) Բոլոր n-րդ կարգի մատրիցների բազմությունն օղակ է՝ մատրիցների գումարման և բազմապատկման նկատմամբ, որը կոչվում է n-**րդ կարգի մատրիցների օղակ**;

5) $\mathcal{O}_p(+,\cdot)$-ը օղակ է, որտեղ $\mathcal{O}_p$-ն բոլոր ամբողջ p-ադիկ թվերի բազմությունն է և կոչվում է **ամբողջ** p-**ադիկ թվերի օղակ**;

6) -1-ով օժտված յուրաքանչյուր Q թվակերպ բազմություն օղակ է:

$Q(+,\cdot)$ օղակը կոչվում է.

ա) **զուգորդական**, եթե

$$(x\cdot y)\cdot z = x\cdot(y\cdot z)$$

ցանկացած $x,y,z\in Q$ տարրերի համար;

բ) **տեղափոխական**, եթե

$$x\cdot y = y\cdot x$$

ցանկացած $x,y\in Q$ տարրերի համար;

գ) **միավորով (օժտված)** օղակ, եթե գոյություն ունի այնպիսի $e\in Q$ տարր, որ

$$x\cdot e = e\cdot x = x$$

ցանկացած $x\in Q$ տարրի համար; e-ն (ինչպես և զրոն) որոշվում է միարժեքորեն և կոչվում է օղակի միավոր: Միավորով օղակում գումարման տեղափոխականության $x+y=y+x$ պայմանը բխում է օղակի մյուս աքսիոմներից, որովհետև

$$x+x+y+y=(e+e)(x+y)=x+y+x+y\ :$$

դ) **դաշտ**, եթե այն զուգորդական է, տեղափոխական, $e\neq 0$ միավորով օժտված և որի յուրաքանչյուր ոչ զրոյական $a\in Q$ տարր հակադարձելի է, այսինքն՝ գոյությունն ունի այնպիսի $a'\in Q$ տարր, որ

$$a\cdot a' = a'\cdot a = e\,;$$

Այս միարժեքորեն որոշվող $a'\in Q$ տարրը սովորաբար նշանակվում է a^{-1}-ով:

ե) **առանց զրոյի բաժանարարների**, եթե

$$a \cdot b = 0 \to a = 0 \text{ կամ } b = 0\,;$$

Հակառակ դեպքում օղակը կոչվում է օժտված զրոյի բաժանարարներով:

զ) **ամբողջության** կամ **ամբողջականության տիրույթ**, եթե այն առանց զրոյի բաժանարարների է, զուգորդական է, տեղափոխական և $e \neq 0$ միավորով օժտված:

Հատկություն 14.32: *Յուրաքանչյուր դաշտ առանց զրոյի բաժանարարների օղակ է, այսինքն՝ դաշտը ամբողջության տիրույթ է:*

Ապացուցում: Իրոք, եթե $a \cdot b = 0$ և $a \neq 0$, $b \neq 0$, ապա գոյություն կունենա a^{-1}-ը և

$$a^{-1}(a \cdot b) = a^{-1} \cdot 0 \to (a^{-1} \cdot a) \cdot b = 0 \to e \cdot b = 0 \to b = 0,$$

որը հակասում է b տարրի ընտրությանը: □

Դաշտի սահմանման հետ կապված, e միավորով օժտված $Q(+,\cdot)$ օղակի $a \in Q$ տարրը անվանենք հակադարձելի, եթե գոյություն ունի այնպիսի $a' \in Q$ տարր, որ

$$a \cdot a' = a' \cdot a = e\;:$$

Ինչպես և վերևում՝ ապացուցվում է, որ միավորով օժտված զուգորդական օղակում a' տարրը որոշվում է միարժեքորեն և կոչվում է a-ի հակադարձ ու նշանակվում է a^{-1}-ով, որովհետև եթե a-ն հակադարձելի է, ապա

$$a \cdot x = a \cdot y \longrightarrow x = y\;:$$

Այդպիսի օղակում, երկու a և b հակադարձելի տարրերի $a \cdot b$ արտադրյալը նորից կլինի հակադարձելի, ընդ որում՝

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}\;:$$

Եթե օղակը նաև տեղափոխական է, ապա

$$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}\;:$$

e միավորով օժտված զուգորդական օղակում (հետևաբար և դաշտում) կարելի է սահմանել նրա հակադարձելի a տարրի ամբողջ աստիճանի գաղափարը՝ հետևյալ կերպ.

$$a^n = \underbrace{a \cdot a \cdots a}_{n}, \quad n > 0,$$

$$a^0 = e,$$

$$a^{-n} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n}, \quad n > 0 :$$

Տեղի ունեն հետևյալ հավասարությունները.

$$a^{m_1} \cdot a^{m_2} = a^{m_1+m_2},$$

$$(a^{m_1})^{m_2} = a^{m_1 m_2}$$

ցանկացած $m_1, m_2 \in \mathbb{Z}$ ամբողջ թվերի համար: Եթե օղակը նաև տեղափոխական է, ապա

$$(a \cdot b)^m = a^m \cdot b^m :$$

$Q(+,\cdot)$ օղակը կամ դաշտը կոչվում է **վերջավոր**, եթե Q բազմությունը վերջավոր է: Հակառակ դեպքում, օղակը կամ դաշտը կոչվում է **անվերջ**: Q բազմության կարգը (հզորությունը) կոչվում է $Q(+,\cdot)$ օղակի կամ դաշտի կարգ (հզորություն):

$Q(+,\cdot)$ օղակի ոչ զրոյական $a \in Q$ տարրը կոչվում է **զրոյի բաժանարար**, եթե գոյություն ունի այնպիսի ոչ զրոյական $b \in Q$ տարր, որ $a \cdot b = 0$ կամ $b \cdot a = 0$:

Թեորեմ 14.16*: Վերջավոր, զուգորդական, տեղափոխական և միավորով օժտված օղակի $a \neq 0$ տարրը կլինի զրոյի բաժանարար այն և միայն այն դեպքում, երբ a-ն հակադարձելի չէ :*

Ապացուցում: Անհրաժեշտություն: Ապացուցենք, որ եթե $a \neq 0$ տարրը զրոյի բաժանարար է, ապա այն հակադարձելի չէ: Ենթադրելով հակառակը, ստանանք հակասություն: Դիցուք $a \cdot b = 0$, որտեղ $b \neq 0$, և դիցուք a-ն հակադարձելի է, այսինքն՝ գոյություն ունի այնպիսի $a' \in Q$ տարր, որ $a \cdot a' = a' \cdot a = e$, որտեղ e-ն օղակի միավորն է: Այդ դեպքում՝

$$0 = a' \cdot 0 = a' \cdot (a \cdot b) = (a' \cdot a) \cdot b = e \cdot b = b :$$

Բավարարություն: Դիցուք $Q = \{a_1, a_2, \ldots, a_n\}$, $a \in Q$, $a \neq 0$ և a-ն հակադարձելի չէ: Կազմենք $a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_n$ արտադրյալները: Եթե ստացված արտադրյալները լինեն զույգ առ զույգ միմյանցից տարբեր, ապա $\{a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_n\} = \{a_1, a_2, \ldots, a_n\}$ և, հետևաբար, $a \cdot a_i = e$, այսինքն՝ a-ն կլինի հակադարձելի, որը հակասում է տրված պայմանին: Ուստի, գոյություն ունեն այնպիսի $a_i \neq a_j$ տարրեր, որ $a \cdot a_i = a \cdot a_j$, որտեղից էլ՝ $a\left(a_i + (-a_j)\right) = 0$, այսինքն՝ $a \cdot b = 0$, որտեղ $b = a_i + (-a_j) \neq 0$, $b \in Q$: □

Թեորեմ 14.17: *1) Վերջավոր ամբողջության տիրույթը դաշտ է: 2) Եթե q-ն վերջավոր F դաշտի կարգն է, ապա $\alpha^{q-1} = 1$ ցանկացած ոչ զրոյական $\alpha \in F$ տարրի համար, որտեղ 1-ը F դաշտի միավորն է, իսկ $\alpha^q = \alpha$ ցանկացած $\alpha \in F$ տարրի համար:*

Ապացուցում: 1) Նախորդ թեորեմից բխում է, որ վերջավոր ամբողջության տիրույթի ցանկացած ոչ զրոյական տարր հակադարձելի է և, հետևաբար, այն կլինի դաշտ: 2) Դիցուք F դաշտի կարգը՝ $|F| = q$, $\alpha \in F$, $\alpha \neq 0$ և դիցուք $F \setminus \{0\} = \{c_1, c_2, \ldots, c_{q-1}\}$: Քանի որ $c_i\alpha \neq c_j\alpha$, եթե $i \neq j$, ապա $F \setminus \{0\} = \{\alpha c_1, \alpha c_2, \ldots, \alpha c_{q-1}\}$: Հետևաբար, $c_1 c_2 \cdots c_{q-1} = \alpha c_1 \alpha c_2 \cdots \alpha c_{q-1}$ և $\alpha^{q-1} = 1$, որտեղ 1-ը F դաշտի միավորն է: Այսպիսով, F դաշտի ցանկացած ոչ զրոյական α տարրի համար՝ $\alpha^{q-1} = 1$: Հետևաբար, $\alpha^q = \alpha$ արդեն F դաշտի ցանկացած α տարրի համար: □

Օրինակ, $\mathbb{Q}(+,\cdot)$-ը, $\mathbb{R}(+,\cdot)$-ը, $\mathbb{R}_p(+,\cdot)$-ը անվերջ դաշտեր են, որտեղ p-ն պարզ թիվ է, իսկ $\mathbb{R}_p$-ն բոլոր p-ադիկ թվերի բազմությունն է: Երկրորդ կարգի մատրիցների

$$\mathbb{C}_{\mathbb{R}} = \left\{ \begin{pmatrix} a, & b \\ -b, & a \end{pmatrix} \middle| \; a, b \in \mathbb{R} \right\}$$

բազմությունը ևս անվերջ դաշտի օրինակ է (մատրիցների գումարման և բազմապատկման գործողությունների նկատմամբ): $\mathbb{Z}_2(+,\cdot)$-ը, $\mathbb{Z}_3(+,\cdot)$-ը վերջավոր դաշտեր են, իսկ $\mathbb{Z}_4(+,\cdot)$-ը՝ ոչ, որովհետև այն օժտված է զրոյի բաժանարարով՝ $[2] \cdot [2] = [0]$:

Թեորեմ 14.18: *1) Որպեսզի $\mathbb{Z}_n(+,\cdot)$ մնացքների օղակի $[a] \in \mathbb{Z}_n$ տարրը լինի հակադարձելի անհրաժեշտ է և բավարար, որ $(a, n) = 1$, այսինքն՝ $\mathbb{Z}_n$ մնացքների օղակի հակադարձելի տարրերի քանակը հավասար է*

$\varphi(n)$-ի, որտեղ φ-ն էյլերի ֆունկցիան է: 2) Մնացքների $\mathbb{Z}_n(+,\cdot)$ օղակը կլինի դաշտ այն և միայն այն դեպքում, երբ n-ը պարզ թիվ է:

Ապացուցում: 1) Եթե $(a,n) = 1$, ապա $ax + ny = 1$, որտեղ $x, y \in \mathbb{Z}$. Հետևաբար, $[ax + ny] = [1]$,

$$[ax] + [ny] = [1]\,,$$

$$[a][x] = [1]\ :$$

Եվ հակառակը, եթե $[a][x] = [1]$, ապա $[ax] = [1]$ և $ax - 1 = nt$, որտեղ $t \in \mathbb{Z}$: Հետևաբար, $ax + n(-t) = 1$ և $(a,n) = 1$(տես նաև հետևություն 3.5-ը):

2) Եթե n-ը բաղադրյալ է և $n = n_1 \cdot n_2$, որտեղ $1 < n_1, n_2 < n$, ապա $[n_1] \neq [0]$, $[n_2] \neq [0]$, բայց

$$[n_1] \cdot [n_2] = [n_1 \cdot n_2] = [n] = [0],$$

այսինքն՝ $\mathbb{Z}_n(+,\cdot)$ օղակը օժտված է զրոյի բաժանարարներով և, հետևաբար, դաշտ չէ: Եվ հակառակը, եթե $n = p$ թիվը պարզ է, ապա զուգորդական, տեղափոխական և $e = [1]$ միավորով օժտված $\mathbb{Z}_p(+,\cdot)$ օղակը դաշտ է, որովհետև նրա յուրաքանչյուր ոչ զրոյական տարր հակադարձելի է՝ համաձայն 1)-ի: □

Այսպիսով, ստանում ենք անվերջ թվով վերջավոր դաշտերի օրինակներ՝

$$\mathbb{Z}_2 = \mathbb{Z}_2(+,\cdot),\ \ \mathbb{Z}_3 = \mathbb{Z}_3(+,\cdot),\ \ \mathbb{Z}_5 = \mathbb{Z}_5(+,\cdot), \ldots$$

Սակայն սրանցով վերջավոր դաշտերը չեն սպառվում: Կարելի է ապացուցել, որ ցանկացած p պարզ թվի և ցանկացած $n \in \mathbb{N}$ (ոչ զրոյական) բնական թվի համար գոյություն ունի p^n կարգի վերջավոր դաշտ (թեորեմ 16.30): Եվ հակառակը, վերջավոր դաշտի կարգը հավասար է p^n-ի, որտեղ p-ն պարզ, իսկ n-ը բնական թվեր են (թեորեմ 17.11):

Երկու $Q(+,\cdot)$ և $Q'(+,\cdot)$ օղակներ կամ դաշտեր կոչվում են **նույնաձև** կամ **իզոմորֆ** և գրվում է $Q \simeq Q'$ կամ $Q \cong Q'$, եթե գոյություն ունի այնպիսի $\varphi : Q \to Q'$ փոխմիարժեք (բիեկտիվ) արտապատկերում, որ

$$\varphi(x + y) = \varphi(x) + \varphi(y)$$

և

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

ցանկացած $x, y \in Q$ տարրերի համար: Այդ դեպքում, $\varphi : Q \to Q'$ փոխմիարժեք (բիեկտիվ) արտապատկերումը կոչվում է **նույնաձևություն** կամ **իզոմորֆիզմ**:

$Q(+, \cdot)$ օղակը կամ դաշտը իր մեջ արտապատկերող $\varphi : Q \to Q$ իզոմորֆիզմը կոչվում է $Q(+, \cdot)$-ի **ավտոմորֆիզմ** կամ **ինքնաձևություն**:

Կարելի է ապացուցել (E.H. Moore), որ *միևնույն կարգի ցանկացած երկու վերջավոր դաշտեր իզոմորֆ են:*

Վերջավոր դաշտերը կոչվում են նաև **Գալուայի դաշտեր**, ի պատիվ ֆրանսիացի հանրաճանաչ գիտնական է. Գալուայի, որի արդյունքները հիմք են հանդիսացել ժամանակակից հանրահաշվական գիտության զարգացնամ համար:

Հեշտությամբ ստուգվում է, որ նույնաձևության «$\simeq$» հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝

ա) $Q \simeq Q$,

բ) $Q \simeq Q' \to Q' \simeq Q$,

գ) $Q \simeq Q', Q' \simeq Q'' \to Q \simeq Q''$:

Եթե $\varphi : Q \to Q'$ փոխմիարժեք արտապատկերումը իզոմորֆիզմ է, ապա Q'-ը կոչվում է Q-ի իզոմորֆ պատկեր: Հեշտությամբ ստուգվում են նաև հետևյալ հատկությունները.

Եթե $Q(+, \cdot)$-ը զուգորդական (տեղափոխական, միավորով օժտված) օղակ է, ապա նրա յուրաքանչյուր իզոմորֆ պատկեր ևս զուգորդական (տեղափոխական, միավորով օժտված) օղակ է:

Եթե $Q(+, \cdot)$-ը ամբողջության տիրույթ է, ապա նրա յուրաքանչյուր իզոմորֆ պատկեր ևս ամբողջության տիրույթ է:

Եթե $Q(+, \cdot)$-ը դաշտ է, ապա նրա յուրաքանչյուր իզոմորֆ պատկեր ևս դաշտ է:

Իզոմորֆ օղակներն (դաշտերն) օժտված են նույն «հանրահաշվական հատկություններով», այդ պատճառով իզոմորֆ օղակները (դաշտերը) կոչվում են նաև **հանրահաշվորեն հավասար** օղակներ (դաշտեր):

Օղակի մեջ սահմանվում է նաև **հանում** գործողություն, իսկ դաշտի մեջ նաև **քանորդի** (կոտորակի) գաղափար՝ հետևյալ կերպ.

$$a - b = a + (-b),$$
$$\frac{a}{b} = a \cdot b^{-1}, \qquad \text{եթե } b \neq 0 :$$

Հեշտությամբ ստուգվում են հանման և քանորդի հետևյալ (դպրոցական) հատկությունները.

$$a(b-c) = ab - ac,$$
$$(b-c)a = ba - ca,$$
$$\frac{a}{b} = \frac{c}{d} \longleftrightarrow ad = bc, \quad \text{որտեղ } b \neq 0,\ d \neq 0,$$
$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \text{եթե } b \neq 0,\ d \neq 0,$$
$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}, \qquad \text{եթե } b \neq 0,$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}, \qquad \text{եթե } b \neq 0,\ d \neq 0,$$
$$\frac{a}{b} = \frac{a \cdot c}{b \cdot c}, \qquad \text{եթե } b \neq 0,\ c \neq 0,$$
$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}, \qquad \text{եթե } a \neq 0,\ \ b \neq 0,$$
$$\frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a \cdot d}{b \cdot c}, \qquad \text{եթե } b \neq 0,\ \ d \neq 0,\ \ c \neq 0 :$$

Կասենք, որ e միավորով $Q(+,\cdot)$ դաշտն ունի **զրո բնութագրիչ** կամ նրա բնութագրիչը հավասար է զրոյի և կգրենք $char(Q) = 0$, եթե ցանկացած $n \geqslant 1$ բնական թվի համար

$$\underbrace{e + \cdots + e}_{n} \neq 0 \ :$$

$Q(+,\cdot)$ դաշտը կոչվում է $n > 0$ բնութագրիչ ունեցող և գրվում է $char(Q) = n > 0$, եթե n-ը այն ամենափոքր բնական թիվն է, որի դեպքում

$$\underbrace{e + \cdots + e}_{n} = 0 \ :$$

Հատկություն 14.33: *Դաշտի ոչ զրոյական բնութագրիչը հավասար է պարզ թվի:*

Ապացուցում: Իրոք, քանի որ դաշտում՝ $e \neq 0$, ապա $char(Q) = n \geqslant 2$ և եթե $n = n_1 \cdot n_2$, որտեղ $1 < n_1, n_2 < n$, ապա

$$(\underbrace{e + \cdots + e}_{n_1})(\underbrace{e + \cdots + e}_{n_2}) = \underbrace{e + \cdots + e}_{n} = 0 \ :$$

Հետևաբար, կամ առաջին արտադրիչն է զրո, կամ՝ երկրորդ, որովհետև դաշտը առանց զրոյի բաժանարարների օղակ է: Հակասություն: $\square$

Օրինակ, $\mathbb{Z}_p(+,\cdot)$ դաշտի բնութագրիչը հավասար է p պարզ թվին, իսկ $\mathbb{Q}(+,\cdot)$ և $\mathbb{R}(+,\cdot)$ թվային դաշտերից յուրաքանչյուրն ունի զրո բնութագրիչ: Դժվար չէ նկատել, որ երկրորդ կարգի մատրիցների վերոհիշյալ $\mathbb{C}_{\mathbb{R}}$ դաշտի բնութագրիչը ևս հավասար է զրոյի:

$Q(+,\cdot)$ օղակի ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը կոչվում է Q օղակի **ենթաօղակ** և գրվում է $Q' \leqslant Q$, եթե տեղի ունեն հետևյալ երկու պայմանները՝

$$x, y \in Q' \longrightarrow x - y \in Q'$$

և

$$x, y \in Q' \longrightarrow x \cdot y \in Q' \ :$$

Առաջին պայմանից, $x = y$ դեպքում ստանում ենք $0 \in Q'$, իսկ $x = 0$ դեպքում՝ $-y \in Q'$, եթե $y \in Q'$: Հետևաբար,

$$x, y \in Q' \longrightarrow x,\ -y \in Q' \longrightarrow x - (-y) \in Q' \longrightarrow x + y \in Q' \ :$$

Այսպիսով, սկզբնական Q բազմության մեջ որոշված $+$ և $\cdot$ գործողություններին կարելի է դիտել նաև որպես գործողություններ, որոշված $Q' \subseteq Q$ ենթաբազմության մեջ: Այնուհետև, օղակային աքսիոմները ինքնըստինքյան (մեխանիկորեն) տեղի կունենան $Q' \subseteq Q$ ենթաբազմության համար, այսինքն՝ $Q'(+,\cdot)$-ը ևս կլինի օղակ: Ակնհայտ է, որ միևնույն օղակի ցանկացած թվով ենթաօղակների հատումը նորից ենթաօղակ է:

Դիցուք $Q(+,\cdot)$-ը օղակ է, իսկ $Q' \leqslant Q$: Q' ենթաօղակը կոչվում է $Q(+,\cdot)$ օղակի **ենթադաշտ**, եթե $Q'(+,\cdot)$ օղակը դաշտ է, այսինքն՝ $Q'(+,\cdot)$-ը $e \neq 0$ միավորով օժտված, զուգորդական ու տեղափոխական օղակ է, որի յուրաքանչյուր ոչ զրոյական $x \in Q'$ տարր հակադարձելի է, այսինքն՝ գոյություն ունի այնպիսի $x' \in Q'$ տարր, որ

$$x \cdot x' = x' \cdot x = e \ :$$

Եթե $Q' \leqslant Q$, ապա $Q(+,\cdot)$ օղակը (մասնավորապես դաշտը) կոչվում է $Q'(+,\cdot)$ **օղակի** (մասնավորապես դաշտի) **ընդլայնում**: *Օրինակ,* $\mathbb{R}(+,\cdot)$ իրական թվերի դաշտը հանդիսանում է $\mathbb{Q}(+,\cdot)$ ռացիոնալ թվերի դաշտի ընդլայնումը: Դաշտի միավորը կպատկանի իր յուրաքանչյուր ենթադաշտին և, հետևաբար, կլինի միավոր նաև իր յուրաքանչյուր ենթադաշտի համար: Մինչդեռ օղակի միավորը (եթե այն գոյություն ունի) կարող է չպատկանել իր ենթադաշտին և, այդ պատճառով, միևնույն օղակի երկու ենթադաշտեր կարող են ունենալ տարբեր միավորներ ու այդպիսի ենթադաշտերի հատումը (լինելով ենթաօղակ) չի լինի ենթադաշտ:

Ակնհայտ է, որ միևնույն դաշտի ցանկացած քանակի ենթադաշտերի հատումը նորից ենթադաշտ է, իսկ տրված դաշտի բոլոր ենթադաշտերի հատումը կոչվում է այդ դաշտի **պարզ ենթադաշտ** (տես նաև լեմմ 18.1-ը):

Դժվար չէ ապացուցել, որ եթե դաշտն ունի զրո բնութագրիչ, ապա նրա պարզ ենթադաշտն իզոմորֆ է ռացիոնալ թվերի $\mathbb{Q}(+,\cdot)$ դաշտին, իսկ եթե դաշտի բնութագրիչը հավասար է $p > 0$ պարզ թվին, ապա նրա պարզ ենթադաշտը կլինի իզոմորֆ $\mathbb{Z}_p(+,\cdot)$ դաշտին: Մասնավորապես, $\mathbb{Q}(+,\cdot)$ և $\mathbb{Z}_p(+,\cdot)$ դաշտերը չունեն իրենցից տարբեր ենթադաշտեր:

14.8. Օղակների և դաշտերի վրա որոշված մատրիցներ, որոշիչներ և գծային հավասարումների համակարգեր

Մատրիցների, որոշիչների և գծային հավասարումների համակարգերի վերաբերյալ մինչ այժմ ստացված հիմնական արդյունքները տարածվում են օղակների և դաշտերի վրա որոշված մատրիցների , որոշիչների և գծային հավասարումների համակարգերի վրա:

Դիցուք $Q(+,\cdot)$-ը կամայական օղակ է, որը համառոտ կնշանակենք նաև Q-ով: $n \times m$ հատ $a_{ij} \in Q$ տարրերի

$$A = (a_{11}, \ldots, a_{1m}, \ldots, a_{n1}, \ldots, a_{nm})$$

հաջորդականությունը՝ ներկայացված n հատ տողերով ու m հատ սյունակներով և գրված

$$A = \begin{pmatrix} a_{11}, & \dots, & a_{1m} \\ \dots & \dots & \dots \\ a_{n1}, & \dots, & a_{nm} \end{pmatrix}$$

աղյուսակի տեսքով, կոչվում է $n \times m$-չափանի մատրից (կամ համառոտ մատրից) որոշված Q օղակի վրա, իսկ $a_{ij} \in Q$ տարրերը կոչվում են A **մատրիցի տարրեր**, որոնք երբեմն գրվում են առանց (անջատող) ստորակետների: Նշված A մատրիցը նշանակվում (գրվում) է նաև $A = (a_{ij})_{n\times m}$ կամ համառոտ $A = (a_{ij})$ տեսքով:

Երկու $n \times m$-չափանի $A = (a_{ij})$ և $B = (b_{ij})$ մատրիցների միևնույն նշիչներով a_{ij} և b_{ij} տարրերը կոչվում են **համապատասխան տարրեր**: Կարգավորված n-յակների հավասարության պայմանից բխում է մատրիցների հավասարության հետևյալ պայմանը. որպեսզի երկու $n \times m$-չափանի մատրիցներ լինեն հավասար անհրաժեշտ է և բավարար, որ նրանց համապատասխան տարրերը լինեն հավասար: A և B մատրիցների հավասարությունը նշանակվում է $A = B$ ձևով, հակառակ դեպքում գրվում է՝ $A \neq B$:

Q օղակի վրա որոշված բոլոր $n \times m$-չափանի մատրիցների բազմությունը նշանակվում է $Q^{n\times m}$-ով: $n = m$ դեպքում $n \times m$-չափանի մատրիցը կոչվում է n-**րդ կարգի** կամ **քառակուսային**, իսկ ընդհանուր դեպքում $n \times m$-չափանի մատրիցները կոչվում են **ուղղանկյուն մատրիցներ**:

Մինչ այժմ մենք ուսումնասիրել ենք մատրիցներ որոշված $Q = \mathbb{R}$ իրական թվերի դաշտի վրա: $Q = \mathbb{R}$ դեպքում մատրիցների նկատմամբ սահմանված գործողությունները նույնությամբ տարածվում են կամայական Q օղակի վրա որոշված մատրիցների վրա:

$C = (c_{ij})_{n\times m}$ մատրիցը կոչվում է $A = (a_{ij})_{n\times m}$ և $B = (b_{ij})_{n\times m}$ **մատրիցների գումար** և գրվում է $C = A + B$, եթե $c_{ij} = a_{ij} + b_{ij}$ բոլոր $i = 1, \dots, n$ և $j = 1, \dots, m$ արժեքների դեպքում:

$B = (B_{ij})_{n\times m}$ մատրիցը կոչվում է $r \in Q$ տարրի և $A = (a_{ij})_{n\times m}$ **մատրիցի (ձախ) արտադրյալ** և գրվում է $B = rA$, եթե $b_{ij} = r \cdot a_{ij}$ բոլոր $i = 1, \dots, n$ և $j = 1, \dots, m$ արժեքների դեպքում:

$C = (c_{ij})_{n\times m}$ մատրիցը կոչվում է $A = (a_{ij})_{n\times k}$ և $B = (b_{ij})_{k\times m}$

մատրիցների արտադրյալ և նշանակվում է $C = A \cdot B$, եթե

$$c_{ij} = \sum_{s=1}^{k} a_{is} b_{sj}$$

բոլոր $i = 1, \ldots, n$ և $j = 1, \ldots, m$ արժեքների դեպքում:

$B = (b_{ij})_{m \times n}$ մատրիցը կոչվում է $A = (a_{ij})_{n \times m}$ **մատրիցի շրջված մատրից** և նշանակվում է $B = A^T$, եթե $b_{ij} = a_{ji}$ բոլոր $i = 1, \ldots, m$ և $j = 1, \ldots, n$ արժեքների դեպքում:

Հետևյալ արդյունքները բխում են սահմանումներից:

Հատկություն 14.34: *Q օղակի ցանկացած $r_1, r_2 \in Q$ տարրերի և ցանկացած $A, B, C \in Q^{n \times m}$ մատրիցների համար տեղի ունեն հետևյալ հավասարությունները՝*

$$(r_1 r_2)A = r_1(r_2 A)\,,$$

$$(r_1 + r_2)A = r_1 A + r_2 A\,,$$

$$(A + B)^T = A^T + B^T\,,$$

$$(rA)^T = rA^T\,,$$

$$(A + B) + C = A + (B + C)\,,$$

$$A + B = B + A\,,$$

$$A + 0 = 0 + A = A\,,$$

որտեղ $0 \in Q^{n \times m}$ մատրիցի բոլոր տարրերը հավասար են Q օղակի զրոյին,

$$A + (-A) = (-A) + A = 0\,,$$

որտեղ $-A = (-a_{ij})_{n \times m}$, եթե $A = (a_{ij})_{n \times m}$: □

$0 \in Q^{n \times m}$ մատրիցը կոչվում է **զրոյական մատրից**, իսկ յուրաքանչյուր $A \neq 0$ մատրից կոչվում է **ոչ զրոյական** (մատրից):

Հատկություն 14.35: *1) Եթե Q օղակը զուգորդական է, ապա ցանկացած $A \in Q^{n \times m}$, $B \in Q^{m \times k}$ և $C \in Q^{k \times s}$ մատրիցների համար՝*

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)\,;$$

2) Եթե Q օղակը տեղափոխական է, ապա ցանկացած $A \in Q^{n\times m}$ և $B \in Q^{m\times k}$ մատրիցների համար՝

$$(A \cdot B)^T = B^T \cdot A^T\,;$$

3) Ցանկացած $A \in Q^{n\times m}$ և $B, C \in Q^{m\times k}$ մատրիցների համար՝

$$A(B + C) = AB + AC\,;$$

4) Ցանկացած $A, B \in Q^{n\times m}$ և $C \in Q^{m\times k}$ մատրիցների համար՝

$$(A + B)C = AC + BC\ : \qquad \square$$

Թեորեմ 14.19*: 1) Կամայական Q օղակի համար մատրիցների $Q^{n\times n}$ բազմությունը օղակ է՝ մատրիցների գումարման և բազմապատկման նկատմամբ, որը կոչվում է Q օղակի վրա որոշված n-***րդ կարգի մատրիցների օղակ***; 2) $Q^{n\times n}$ օղակը կլինի զուգորդական այն և միայն այն դեպքում, երբ Q-ն զուգորդական օղակ է; 3) $Q^{n\times n}$ օղակը կլինի միավորով օժտված այն և միայն այն դեպքում, երբ Q օղակը օժտված է միավորով: Այդ դեպքում $Q^{n\times n}$ օղակի միավորը կլինի n-րդ կարգի միավոր միատրիցը, այսինքն՝*

$$E_n = \begin{pmatrix} 1, 0, \ldots, 0 \\ 0, 1, \ldots, 0 \\ \ldots\ldots\ldots \\ 0, 0, \ldots, 1 \end{pmatrix} \in Q^{n\times n}$$

մատրիցը, որտեղ 1-ը Q-ի միավորն է; 4) $n > 1$ դեպքում $Q^{n\times n}$ օղակը ունի զրոյի բաժանարար, եթե $|Q| > 1$: Հետևաբար, $n > 1$ դեպքում $Q^{n\times n}$ օղակը դաշտ չէ ցանկացած Q-ի համար: $\square$

Դիցուք Q-ն միավորով օժտված օղակ է: $A \in Q^{n\times n}$ մատրիցը կոչվում է **հակադարձելի**, եթե այն հակադարձելի է որպես $Q^{n\times n}$ միավորով օժտված օղակի տարր, այսինքն՝ գոյություն ունի այնպիսի $A' \in Q^{n\times n}$ մատրից, որ

$$A \cdot A' = A' \cdot A = E_n\,,$$

որտեղ E_n-ը n-րդ կարգի միավոր մատրիցն է: Ակնհայտ է, որ զուգորդական և միավորով օժտված $Q^{n\times n}$ օղակի դեպքում A' մատրիցը որոշվում է միարժեքորեն, այն նշանակվում է A^{-1}-ով ու կոչվում է A-ի **հակադարձ մատրից**:

Դիցուք Q-ն զուգորդական, տեղափոխական և 1 միավորով օժտված օղակ է: Սահմանենք $A = (a_{ij})_{n\times n} \in Q^{n\times n}$ **մատրիցի որոշիչը** որպես Q օղակի հետևյալ տարր՝

$$|A| = \sum_{\sigma\in S_n} sgn(\sigma)a_{1,\sigma(1)}a_{2,\sigma(2)}\cdots a_{n,\sigma(n)} \in Q\,,$$

որտեղ σ-ն փոփոխվում է n-րդ աստիճանի բոլոր տեղադրությունների S_n բազմության վրա: $|A|$ նշանակման փոխարեն գրվում է նաև $det(A)$ կամ $det\,A$:

$Q = \mathbb{R}$ դեպքում որոշիչների վերաբերյալ ապացուցված արդյունքներն իրենց ապացուցումներով և անհրաժեշտ հասկացությունների սահմանումներով հիմնականում տարածվում են այս ընդհանուր դեպքի վրա՝ ներառյալ մատրիցի տարրերի հանրահաշվական լրացուցիչների հետ կապված հատկությունները (դաշտի դեպքում որոշիչների մեզ հայտնի բոլոր հիմնական արդյունքները մնում են ուժի մեջ): Մասնավորապես, տեղի ունի հետևյալ հայտանիշը:

Թեորեմ 14.20*: Դիցուք Q-ն զուգորդական, տեղափոխական և միավորով օժտված օղակ է: Որպեսզի $A \in Q^{n\times n}$ մատրիցը լինի հակադարձելի անհրաժեշտ է և բավարար, որ նրա $|A|$ որոշիչը լինի հավասար Q օղակի որևէ հակադարձելի տարրի: Մասնավորապես, Q դաշտի դեպքում՝ $A \in Q^{n\times n}$ մատրիցը կլինի հակադարձելի այն և միայն այն դեպքում, երբ $|A|$ որոշիչը լինի հավասար Q դաշտի որևէ ոչ զրոյական տարրի:* □

$Q = \mathbb{R}$ դեպքում ստացված հակադարձ մատրիցի հաշման բանաձևը մնում է ուժի մեջ նաև այս ընդհանուր դեպքում, այսինքն՝

$$A^{-1} = |A|^{-1}\begin{pmatrix} A_{11}, & A_{21}, & \ldots, & A_{n1}\\ A_{12}, & A_{22}, & \ldots, & A_{n2}\\ \ldots & \ldots & \ldots & \ldots\\ A_{1n}, & A_{2n}, & \ldots, & A_{nn}\end{pmatrix},$$

որտեղ A_{ij}-ն $A = (a_{ij})_{n\times n} \in Q^{n\times n}$ մատրիցի $a_{ij} \in Q$ տարրի հանրահաշվական լրացուցիչն է: Այստեղ,

$$A^{\vee} = \begin{pmatrix} A_{11}, & A_{21}, & \dots, & A_{n1} \\ A_{12}, & A_{22}, & \dots, & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n}, & A_{2n}, & \dots, & A_{nn} \end{pmatrix} \in Q^{n\times n}$$

մատրիցը կոչվում է A-ի **կցորդ մատրից**, որի համար`

$$A \cdot A^{\vee} = A^{\vee} \cdot A = \begin{pmatrix} |A|, & 0, & \dots, & 0 \\ 0, & |A|, & \dots, & 0 \\ \dots & \dots & \dots & \dots \\ 0, & 0, & \dots, & |A| \end{pmatrix} :$$

n անհայտներով m հատ գծային հավասարումների հետևյալ համակարգը`

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \,, \\ \dots \; \dots \; \dots \; \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases} \tag{14.9}$$

կոչվում է **որոշված Q օղակի վրա**, եթե անհայտների a_{ij} գործակիցները ($i = 1,\dots,m$; $j = 1,\dots,n$) և $b_1,\dots,b_m$ ազատ անդամները պատկանում են Q օղակին: Q օղակի տարրերի $\gamma = (\alpha_1,\dots,\alpha_n)$ հաջորդականությունը կոչվում է

$$a_{i1}x_1 + \dots + a_{in}x_n = b_i$$

գծային **հավասարման լուծում**, եթե այդ հավասարման մեջ տեղադրելով $x_1 = \alpha_1,\dots,x_n = \alpha_n$ և Q-ում կատարելով հավասարության ձախ մասի գործողությունները, ստանում ենք ճիշտ հավասարություն Q օղակում: $\gamma = (\alpha_1,\dots,\alpha_n) \in Q^{1\times n}$ տարրը կոչվում է (14.9) **համակարգի լուծում**, եթե այն լուծում է այդ համակարգի յուրաքանչյուր գծային հավասարման համար:

Լուծել գծային հավասարումների (14.9) համակարգը նշանակում է գտնել (որոշել, նկարագրել) այդ համակարգի բոլոր լուծումները: Համակարգը կոչվում է **լուծելի** կամ **համատեղելի**, եթե այն ունի որևէ լուծում: Հակառակ դեպքում համակարգը կոչվում է **անհամատեղելի**:

Q օղակի վրա որոշված գծային հավասարումների (14.9) համակարգը կոչվում է **համասեռ**, եթե $b_1 = \dots = b_m = 0$, որտեղ

0-ն Q օղակի զրոն է: Գծային հավասարումների համասեռ համակարգը միշտ օժտված է $\gamma = (0,\ldots,0)$ **զրոյական** լուծումով: $\gamma \neq (0,\ldots,0)$ լուծումը կոչվում է **ոչ զրոյական**:

Գծային հավասարումների (14.9) համատեղելի համակարգը կոչվում է **որոշյալ**, եթե այն ունի միակ լուծում: Հակառակ դեպքում, գծային հավասարումների համատեղելի համակարգը կոչվում է **անորոշ**:

Թեորեմ 14.21 (Կրամեր): *Դիցուք Q-ն զուգորդական, տեղափոխական և միավորով օժտված օղակ է: Եթե n-րդ կարգի $A = (a_{ij})_{n\times n} \in Q^{n\times n}$ մատրիցը հակադարձելի է, ապա ցանկացած $b_1,\ldots,b_n \in Q$ տարրերի համար գծային հավասարումների*

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1\,, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ a_{n1}x_1 + \cdots + a_{nn}x_n = b_n \end{cases}$$

համակարգը կլինի որոշյալ: Ըստ որում, այդ համակարգի միակ $(\alpha_1,\ldots,\alpha_n) \in Q^{1\times n}$ լուծումը որոշվում է հետևյալ բանաձևով՝

$$\alpha_i = |A|^{-1}\cdot|A_i| \qquad i = 1,\ldots,n\,,$$

որտեղ $A_i \in Q^{n\times n}$ մատրիցը ստացվում է A-ից նրա i-րդ սյունակը փոխարինելով ազատ անդամների $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ սյունակով: □

Գծային հավասարումների համակարգերի համար ($Q = \mathbb{R}$ դեպքում) հայտնի Գաուսի ալգորիթմը կիրառելի է նաև ցանկացած դաշտի վրա որոշված գծային հավասարումների համակարգերի համար:

Վարժություններ և խնդիրներ

1. Հետևյալ հավասարումից որոշել երկրորդ կարգի X մատրիցը՝

a) $\begin{pmatrix} 2 & 5 \\ 2 & 3 \end{pmatrix} \cdot X = \begin{pmatrix} 4 & -6 \\ 2 & 1 \end{pmatrix}$;

b) $\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \cdot X \cdot \begin{pmatrix} -3 & 1 \\ 5 & -3 \end{pmatrix} = \begin{pmatrix} -2 & 3 \\ 3 & -1 \end{pmatrix}$:

2. Հետևյալ համակարգից որոշել երկրորդ կարգի X և Y մատրիցները՝

$$\begin{cases} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} X + \begin{pmatrix} 3 & 1 \\ 2 & 2 \end{pmatrix} Y = \begin{pmatrix} 2 & 8 \\ 1 & 5 \end{pmatrix}, \\ \begin{pmatrix} 3 & -1 \\ -1 & 1 \end{pmatrix} X + \begin{pmatrix} 2 & 1 \\ -1 & 1 \end{pmatrix} Y = \begin{pmatrix} 4 & 9 \\ -1 & -4 \end{pmatrix} : \end{cases}$$

3. Ապացուցել, որ զուգորդական, միավորով օժտված և առանց զրոյի բաժանարարների օղակում տեղի ունի հետևյալ հատկությունը՝

$$ab = e \longrightarrow ba = e \ :$$

4. Ապացուցել, որ իրական ֆունկցիաների

$$\mathbb{R}^{\mathbb{R}} = \{f \mid f : \mathbb{R} \to \mathbb{R}\}$$

բազմությունը զուգորդական, տեղափոխական, միավորով օժտված և զրոյի բաժանարարներով օղակ է՝ հետևյալ գործողությունների նկատմամբ.

$$(f + g)x = f(x) + g(x)\,,$$

$$(f \cdot g)x = f(x) \cdot g(x) \ :$$

5. Ապացուցել, որ $\mathbb{Z}_2$ դաշտում տեղի ունի հետևյալ բանաձևը՝

$$(a + b)^2 = a^2 + b^2, \qquad a, b \in \mathbb{Z}_2\,,$$

որը ճիշտ է նաև 2 բնութագրիչով ցանկացած դաշտում:

6. Ապացուցել, որ $\mathbb{Z}_3$ դաշտում՝

$$(a + b)^2 \neq a^2 + b^2\,,$$

$$(a + b)^3 = a^3 + b^3 \ :$$

7. Ապացուցել, որ չորս տարրանի $\{0, e, a, b\}$ բազմությունը հետևյալ $+$ և $\cdot$ գործողությունների նկատմամբ դաշտ է՝

$$\begin{array}{c|cccc} + & 0 & e & a & b \\ \hline 0 & 0 & e & a & b \\ e & e & 0 & b & a \\ a & a & b & 0 & e \\ b & b & a & e & 0 \end{array}, \qquad \begin{array}{c|cccc} \cdot & 0 & e & a & b \\ \hline 0 & 0 & 0 & 0 & 0 \\ e & 0 & e & a & b \\ a & 0 & a & b & e \\ b & 0 & b & e & a \end{array}:$$

8. Ապացուցել, որ 2-րդ կարգի մատրիցների

$$\mathbb{F}_4 = \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \middle| \; a, b \in \mathbb{Z}_2 \right\}$$

բազմությունը 4 տարրանի դաշտ է՝ մատրիցների գումարման և մատրիցների բազմապատկման նկատմամբ: Ապացուցել նաև որ այս F_4 դաշտը իզոմորֆ է նախորդ վարժության չորս տարրանի դաշտին:

9. Ապացուցել, որ 2-րդ կարգի մատրիցների

$$\mathbb{F}_9 = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \; a, b \in \mathbb{Z}_3 \right\}$$

բազմությունը 9 տարրանի դաշտ է՝ մատրիցների գումարման և մատրիցների բազմապատկման նկատմամբ:

10. Ապացուցել, որ օղակը տեղափոխական է, եթե $x^2 = x$ նրա ցանկացած x տարրի համար:

11. Որոշել $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_8$, $\mathbb{Z}_9$, $\mathbb{Z}_{10}$, $\mathbb{Z}_{12}$ օղակների

   ա) հակադարձելի տարրերը;

   բ) ոչ հակադարձելի տարրերը;

   գ) զրոյի բաժանարարները:

12. Հաշվել $\mathbb{Z}_2$-ում, $\mathbb{Z}_3$-ում, $\mathbb{Z}_5$-ում, $\mathbb{Z}_7$-ում, $\mathbb{Z}_{13}$-ում և $\mathbb{Z}_{19}$-ում՝

$$81 + \frac{19}{23} - 33,$$

որտեղ $a = [a] \in \mathbb{Z}_n$, $n = 2, 3, 5, 7, 13, 19$:

13. Լուծել հետևյալ համակարգը $\mathbb{Z}_3$-ում, $\mathbb{Z}_5$-ում և $\mathbb{Z}_7$-ում՝

$$\begin{cases} x + 2z = 1\,, \\ y + 2z = 2\,, \\ 2x + z = -1\ : \end{cases}$$

14. Վերհանգման եղանակով ապացուցել հետևյալ հավասարությունը՝

$$det \begin{pmatrix} 1, & 1, & \dots, & 1 \\ a_1, & a_2, & \dots, & a_n \\ a_1^2, & a_2^2, & \dots, & a_n^2 \\ \dots & \dots & \dots & \dots \\ a_1^{n-1}, & a_2^{n-1}, & \dots, & a_n^{n-1} \end{pmatrix} = \prod_{1 \leqslant i < j \leqslant n} (a_i - a_j)\ :$$

Այս որոշիչը կոչվում է Վանդերմոնդի որոշիչ (A. Vandermonde, 1735–1796):

15. Քանի լուծում կարող է ունենալ $\mathbb{Z}_2$ կամ $\mathbb{Z}_3$ դաշտի վրա որոշված n անհայտներով $n-1$ հատ գծային հավասարումների համակարգը:

16. Ապացուցել, որ Q օղակի վրա որոշված n-րդ կարգի մատրիցների $Q_{n\times n}$ օղակը կլինի տեղափոխական այն և միայն այն դեպքում, երբ կամ 1) $n = 1$ և Q-ն տեղափոխական օղակ է, կամ 2) $n > 1$ և Q-ն զրոյական արտադրյալով օղակ է, այսինքն՝ $x \cdot y = 0$ ցանկացած $x, y \in Q$ տարրերի համար:

17. Ապացուցել, որ եթե $Q_1(+,\cdot)$-ը և $Q_2(+,\cdot)$-ը օղակներ են, ապա $Q_1 \times Q_2$ դեկարտյան արտադրյալը կլինի օղակ՝ հետևյալ գործողությունների նկատմամբ.

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot y_1, x_2 \cdot y_2)\ :$$

Ըստ որում, $Q_1^0 = \{(x_1, 0) \mid x_1 \in Q_1\}$ և $Q_2^0 = \{(0, x_2) \mid x_2 \in Q_2\}$ բազմությունները կլինեն $Q_1 \times Q_2$ օղակի ենթաօղակներ: Եթե Q_1 և Q_2 օղակները օժտված են $e_1 \in Q_1$ և $e_2 \in Q_2$ միավորներով, ապա (e_1, e_2), $(e_1, 0)$ և $(0, e_2)$ զույգեր կլինեն համապատասխանաբար $Q_1 \times Q_2$, Q_1^0 և Q_2^0 օղակների միավորները:

18. Ապացուցել, որ m-տարրանի վերջավոր օղակի ցանկացած a տարրի համար տեղի ունի հետևյալ հավասարությունը՝ $\underbrace{a+a+\cdots+a}_{m}=0$:

19. $\mathbb{Z}_4$ օղակում՝
$$det\begin{pmatrix} [2]\,, & [2] \\ [2]\,, & [0] \end{pmatrix} = [0]\,,$$
սակայն ապացուցել, որ դետարկվող մատրիցի տողերը համեմատական չեն:
$\mathbb{Z}_{13}$ դաշտում՝
$$det\begin{pmatrix} [6]\,, & [9] \\ [1]\,, & [8] \end{pmatrix} = [0]\ :$$
Կլինե՞ն արդյոք համեմատական այս մատրիցի տողերը:

Գ լ ու խ 15

ԿՈՄՊԼԵՔՍ ԹՎԵՐ

15.1. Սահմանումը և գործողություններ կոմպլեքս թվերի հետ

Հայտնի է, որ իրական գործակիցներով ցանկացած քառակուսի հավասարման լուծման համար իրական թվերը բավարար չեն: Օրինակ, $x^2 + 1 = 0$ քառակուսի հավասարումը չունի իրական լուծում: Այժմ խնդիր է դրվում, գտնել իրական թվերի $\mathbb{R}(+,\cdot)$ դաշտի այնպիսի ընդլայնում, որը նույնպես լինի դաշտ և պարունակի նշված քառակուսի հավասարման որևէ լուծում (ու այս հատկություններով լինի «փոքրագույնը», այսինքն՝ չունենա նշված հատկություններով օժտված ուրիշ ենթադաշտ):

Իրական թվերի (a, b) կարգավորված զույգերը կոչվում են **կոմպլեքս թվեր**, որոնց գումարը և արտադրյալը (բազմապատկումը) սահմանվում են հետևյալ կերպ.

$$(a, b) + (c, d) = (a + c, b + d)\,,$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc)\ :$$

a իրական թիվը կոչվում է (a, b) կոմպլեքս թվի **իրական մաս**, իսկ b-ն՝ **կեղծ մաս**: Բոլոր կոմպլեքս թվերի բազմությունը ընդունված է նշանակել $\mathbb{C}$-ով՝

$$\mathbb{C} = \{(a, b) \mid\ a, b \in \mathbb{R}\}\ :$$

Այժմ կապացուցենք, որ իրական թվերի գումարման և բազմապատկման սովորական հատկությունները տարածվում են նաև կոմպլեքս թվերի գումարման և բազմապատկման գործողությունների վրա: Ավելի ճիշտ, կոմպլեքս թվերի $\mathbb{C}$ բազմությունը դաշտ է՝ կոմպլեքս թվերի գումարման և բազմապատկման գործողությունների նկատմամբ:

Հատկություն 15.1: *Ցանկացած $\alpha, \beta \in \mathbb{C}$ կոմպլեքս թվերի համար՝ $\alpha + \beta = \beta + \alpha$ (գումարման տեղափոխական հատկություն):*

Ապացուցում: Եթե $\alpha = (a, b)$ և $\beta = (c, d)$, ապա $\alpha + \beta = (a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b) = \beta + \alpha$: $\square$

Հատկություն 15.2: *Ցանկացած* $\alpha, \beta, \gamma \in \mathbb{C}$ *կոմպլեքս թվերի համար*՝ $(\alpha+\beta)+\gamma = \alpha+(\beta+\gamma)$ *(գումարման զուգորդական հատկություն):*

Ապացուցում: Եթե $\alpha = (a, b)$, $\beta = (c, d)$ և $\gamma = (s, t)$, ապա

$$(\alpha+\beta)+\gamma = ((a, b)+(c, d))+(s, t) = ((a+c)+s, (b+d)+t) = (a+(c+s),$$

$$b+(d+t)) = (a, b)+((c, d)+(s, t)) = \alpha+(\beta+\gamma) : \qquad \square$$

Հետևաբար, միարժեքորեն որոշվում է

$$n\alpha = \underbrace{\alpha+\cdots+\alpha}_{n}$$

գումարը՝ ցանկացած α կոմպլեքս թվի համար, $n > 0$: Այսինքն՝ սահմանված է կոմպլեքս թվի բնական պատիկի կամ n-պատիկի գաղափարը, երբ $n > 0$:

Հատկություն 15.3: *Ցանկացած* $\alpha = (a, b) \in \mathbb{C}$ *կոմպլեքս թվի համար*՝ $(a, b) + (0, 0) = (a, b)$*: Այս հատկությամբ* $(0, 0)$ *զույգը որոշվում է միարժեքորեն և նշանակվում է*՝ $(0, 0) = 0$ *ու կոչվում է* **զրո** *կոմպլեքս թիվ:* $\square$

Սահմանվում է կոմպլեքս թվի զրո պատիկը՝ $0\alpha = 0$ ցանկացած α կոմպլեքս թվի համար:

Հատկություն 15.4: *Ցանկացած* $\alpha = (a, b) \in \mathbb{C}$ *կոմպլեքս թվի համար*՝ $(a, b) + (-a, -b) = (0, 0)$*: Այս հատկությամբ* $(-a, -b)$ *զույգը որոշվում է միարժեքորեն և նշանակվում է*՝ $(-a, -b) = -\alpha$ *ու կոչվում է* α*-ի* **հակադիր** *կոմպլեքս թիվ:* $\square$

Հետևաբար, միարժեքորեն որոշվում է

$$(-n)\alpha = \underbrace{(-\alpha)+\cdots+(-\alpha)}_{n}$$

գումարը՝ ցանկացած α կոմպլեքս թվի համար, $n > 0$: Արդյունքում ստանում ենք կոմպլեքս թվի ամբողջ պատիկի գաղափարը: Ըստ որում, տեղի ունեն $m_1\alpha + m_2\alpha = (m_1 + m_2)\alpha$ և $m_1(m_2\alpha) = (m_1 \cdot m_2)\alpha$ հավասարությունները՝ ցանկացած α կոմպլեքս թվի և ցանկացած $m_1, m_2 \in \mathbb{Z}$ ամբողջ թվերի համար:

Հատկություն 15.5: *Ցանկացած* $\alpha, \beta \in \mathbb{C}$ *կոմպլեքս թվերի համար՝* $\alpha \cdot \beta = \beta \cdot \alpha$ *(բազմապատկման տեղափոխական հատկություն):*

Ապացուցում: Եթե $\alpha = (a, b)$ և $\beta = (c, d)$, ապա

$$\alpha \cdot \beta = (a, b) \cdot (c, d) = (ac - bd, ad + bc) =$$
$$= (ca - db, cb + da) = (c, d) \cdot (a, b) = \beta \cdot \alpha \ : \qquad \square$$

Հատկություն 15.6: *Ցանկացած* $\alpha, \beta, \gamma \in \mathbb{C}$ *կոմպլեքս թվերի համար՝* $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$ *(բազմապատկման զուգորդական հատկություն):*

Ապացուցում: Եթե $\alpha = (a, b)$, $\beta = (c, d)$, $\gamma = (s, t)$, ապա

$$(\alpha \cdot \beta) \cdot \gamma = (ac - bd, ad + bc) \cdot (s, t) = ((ac - bd)s - (ad + bc)t, (ac - bd)t + (ad + bc)s) =$$
$$= (acs - bds - adt - bct, act - bdt + ads + bcs),$$
$$\alpha \cdot (\beta \cdot \gamma) = (a, b)(cs - dt, ct + ds) = (a(cs - dt) - b(ct + ds), a(ct + ds) + b(cs - dt)) =$$
$$= (acs - adt - bct - bds, act + ads + bcs - bdt) \ : \qquad \square$$

Հետևաբար, միարժեքորեն որոշվում է

$$\alpha^n = \underbrace{\alpha \cdot \dots \cdot \alpha}_{n}$$

արտադրյալը՝ ցանկացած α կոմպլեքս թվի համար, $n > 0$: Այսինքն՝ սահմանված է կոմպլեքս թվի բնական ցուցիչով աստիճանը:

Հատկություն 15.7: *Ցանկացած* $\alpha, \beta, \gamma \in \mathbb{C}$ *կոմպլեքս թվերի համար՝*

$$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma\,, \quad \text{(ձախ բաշխականություն)}$$
$$(\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha \ : \quad \text{(աջ բաշխականություն)}$$

Ապացուցում: Շնորհիվ բազմապատկման տեղափոխական հատկության՝ բավական է ապացուցել նշված հավասարություններից միայն մեկը (օրինակ, առաջինը): Եթե $\alpha = (a, b)$, $\beta = (c, d)$ և $\gamma = (s, t)$, ապա

$$\alpha(\beta + \gamma) = (a, b) \cdot (c + s, d + t) = (a(c + s) - b(d + t), a(d + t) + b(c + s)) =$$
$$= (ac + as - bd - bt, ad + at + bc + bs),$$
$$\alpha\beta + \alpha\gamma = (ac - bd, ad + bc) + (as - bt, at + bs) =$$
$$= (ac - bd + as - bt, ad + bc + at + bs) \ : \qquad \square$$

Հատկություն 15.8: *Ցանկացած* $\alpha = (a, b) \in \mathbb{C}$ *կոմպլեքս թվի համար՝* $(a, b) \cdot (1, 0) = (a, b)$*: Այս հատկությամբ* $(1, 0)$ *զույգը որոշվում է միարժեքորեն և նշանակվում է՝* $(1, 0) = 1$ *ու կոչվում է* **մեկ** *կոմպլեքս թիվ:* $\square$

Սահմանվում է նաև $\alpha^0 = 1$ ցանկացած α կոմպլեքս թվի համար:

Այսպիսով, բոլոր կոմպլեքս թվերի $\mathbb{C}$ բազմությունը, կոմպլեքս թվերի գումարման և բազմապատկման նկատմամբ, կազմում է զուգորդական, տեղափոխական և միավորով օժտված օղակ՝ $\mathbb{C}(+, \cdot)$:

Մնում է ապացուցել, որ այս օղակի յուրաքանչյուր ոչ զրոյական տարր հակադարձելի է, այսինքն՝ պահանջվում է լուծել $(a, b) \cdot (x, y) = (1, 0)$ հավասարումը, որտեղ $a^2 + b^2 \neq 0$: Այստեղից հեշտությամբ ստացվում են $x = \dfrac{a}{a^2 + b^2}$ և $y = -\dfrac{b}{a^2 + b^2}$ արժեքները, որպես

$$\begin{cases} ax - by = 1, \\ bx + ay = 0 \end{cases}$$

համակարգի միակ (x, y) լուծում (հետևում է նաև Կրամերի կանոնից):

Հատկություն 15.9: *Ցանկացած* $\alpha = (a, b) \neq (0, 0)$ *կոմպլեքս թվի համար՝* $(a, b) \cdot \left(\dfrac{a}{a^2 + b^2}, \dfrac{-b}{a^2 + b^2}\right) = (1, 0)$ *: Այս հատկությամբ*

$$\alpha' = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2}\right)$$

կոմպլեքս թիվը որոշվում է միարժեքորեն և կոչվում է α*-ի հակադարձ ու նշանակվում է* α^{-1}*-ով:* $\square$

Հետևաբար, միարժեքորեն որոշվում է

$$\alpha^{-n} = \underbrace{\alpha^{-1} \cdot \alpha^{-1} \cdots \alpha^{-1}}_{n}$$

արտադրյալը՝ ցանկացած ոչ զրոյական α կոմպլեքս թվի համար, $n > 0$: Արդյունքում սահմանված է ոչ զրոյական կոմպլեքս թվի ամբողջ աստիճանի գաղափարը: Ըստ որում, ստացվում են հետևյալ հավասարությունները՝

$$\alpha^{m_1} \cdot \alpha^{m_2} = \alpha^{m_1 + m_2}, \quad (\alpha^{m_1})^{m_2} = \alpha^{m_1 m_2}$$

ցանկացած ոչ զրոյական α կոմպլեքս թվի և ցանկացած $m_1, m_2 \in \mathbb{Z}$ ամբողջ թվերի համար:

Այսպիսով, հանգում ենք հետևյալ արդյունքին:

Թեորեմ 15.1: *Բոլոր կոմպլեքս թվերի* $\mathbb{C}$ *բազմությունը զրո բնութագրիչով դաշտ է՝ կոմպլեքս թվերի գումարման և բազմապատկման նկատմամբ:* □

Հետևաբար, կարելի է խոսել նաև երկու կոմպլեքս թվերի տարբերության և քանորդի (կոտորակի) մասին, որովհետև այս երկու հասկացություններից առաջինը ներմուծվել է կամայական օղակի, իսկ երկրորդը՝ կամայական դաշտի դեպքում.

$$\alpha - \beta = \alpha + (-\beta),$$

$$\frac{\alpha}{\beta} = \alpha \cdot \beta^{-1}, \quad \text{որտեղ } \beta \neq 0 :$$

Հատկություն 15.10: *Կոմպլեքս թվերի* $\mathbb{C}(+,\cdot)$ *դաշտն իզոմորֆ է երկրորդ կարգի մատրիցների* $\mathbb{C}_{\mathbb{R}}(+,\cdot)$ *դաշտին:*

Ապացուցում: Որոնելի $\varphi : \mathbb{C} \to \mathbb{C}_{\mathbb{R}}$ իզոմորֆիզմը որոշվում է հետևյալ կերպ՝

$$\varphi : (a,b) \longrightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix} :$$

Այս φ արտապատկերումը փոխմիարժեք (բիեկտիվ) է և բավարարում է հետևյալ պայմաններին.

$$\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$$

և

$$\varphi(\alpha \cdot \beta) = \varphi(\alpha) \cdot \varphi(\beta)$$

ցանկացած $\alpha, \beta \in \mathbb{C}$ կոմպլեքս թվերի համար: □

Երկրորդ կարգի $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ մատրիցը կոչվում է $\alpha = (a,b)$ կոմպլեքս թվի **մատրիցային տեսք**: Կարելի է ասել, որ կոմպլեքս թվի մատրիցային տեսքը գտնվում է «համաձայնության» մեջ կոմպլեքս թվերի գումարման և բազմապատկման (հետևաբար և աստիճան բարձրացնելու) գործողությունների հետ: Օրինակ, $(1,-1)^8 = (16,0)$, որովհետև

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}^8 = \begin{pmatrix} 16 & 0 \\ 0 & 16 \end{pmatrix}:$$

Հետևյալ արդյունքը կոչվում է Մուավրի (A. De Moivre, 1667-1754) բանաձև՝ գրված մատրիցային տեսքով:

Հատկություն 15.11 (Մուավրի բանաձևը, 1707թ.) : *Ցանկացած* $m \in \mathbb{Z}$ *ամբողջ թվի համար՝*

$$\begin{pmatrix} cos\,\alpha & sin\,\alpha \\ -sin\,\alpha & cos\,\alpha \end{pmatrix}^m = \begin{pmatrix} cos(m\alpha) & sin(m\alpha) \\ -sin(m\alpha) & cos(m\alpha) \end{pmatrix}:$$

Ապացուցում: $m \geqslant 0$ դեպքում պնդումն ապացուցվում է վերհանգման եղանակով: $m < 0$ դեպքում՝ $m = -|m| = (-1)\cdot|m|$ և օգտվելով (14.1) բանաձևից կունենանք.

$$\begin{pmatrix} cos\,\alpha & sin\,\alpha \\ -sin\,\alpha & cos\,\alpha \end{pmatrix}^m = \left(\begin{pmatrix} cos\,\alpha & sin\,\alpha \\ -sin\,\alpha & cos\,\alpha \end{pmatrix}^{-1}\right)^{|m|} =$$

$$= \begin{pmatrix} cos(\alpha) & -sin(\alpha) \\ sin(\alpha) & cos(\alpha) \end{pmatrix}^{|m|} = \begin{pmatrix} cos(-\alpha) & sin(-\alpha) \\ -sin(-\alpha) & cos(-\alpha) \end{pmatrix}^{|m|} =$$

$$= \begin{pmatrix} cos(-|m|\alpha) & sin(-|m|\alpha) \\ -sin(-|m|\alpha) & cos(-|m|\alpha) \end{pmatrix} = \begin{pmatrix} cos(m\alpha) & sin(m\alpha) \\ -sin(m\alpha) & cos(m\alpha) \end{pmatrix}: \quad \square$$

15.2. Կոմպլեքս թվի սովորական տեսքը, մոդուլը, համալուծը, նորմը, արգումենտը և եռանկյունաչափական տեսքը: Կոմպլեքս թվից n-րդ աստիճանի արմատ հանելը

Սովորաբար $(a,0)$ տեսքի կոմպլեքս թիվը **նույնականացվում** է a իրական թվի հետ, այսինքն՝ ընդունվում է, որ $(a,0) = a$: Ըստ որում, այս նույնականացումը համաձայնեցված է իրական թվերի նկատմամբ կատարվող գործողությունների հետ, որովհետև՝

$$(a,0) + (b,0) = (a+b,0),$$

$$(a,0)\cdot(b,0) = (a\cdot b,0),$$

$$(a,0)-(b,0)=(a-b,0),$$

$$\frac{(a,0)}{(b,0)}=\left(\frac{a}{b},0\right),\;\; b\neq 0\,,$$

այսինքն՝ $(a,0)$ տեսքի բոլոր կոմպլեքս թվերի բազմությունը կազմում է կոմպլեքս թվերի $\mathbb{C}(+,\cdot)$ դաշտի ենթադաշտ (որն իզոմորֆ է իրական թվերի $\mathbb{R}(+,\cdot)$ դաշտին):

Հետևաբար, կոմպլեքս թվերի $\mathbb{C}(+,\cdot)$ դաշտը կպարունակի իրական թվերի $\mathbb{R}(+,\cdot)$ դաշտը՝ որպես ենթադաշտ: Նշանակելով նաև $i=(0,1)$, կունենանք՝

$$(a,b)=(a,0)+(0,b)=(a,0)+(b,0)(0,1)=a+bi\;,$$

որտեղ

$$i^2=i\cdot i=(0,1)(0,1)=(0-1,0+0)=(-1,0)=-1,$$

այսինքն՝ i կոմպլեքս թիվը հանդիսանում է իրական գործակիցներով $x^2+1=0$ քառակուսի հավասարման լուծում (արմատ): Այսպիսով, հանգում ենք $\alpha=(a,b)$ կոմպլեքս թվի **սովորական** կամ **հանրահաշվական տեսքին** (գրելաձևին)՝ $\alpha=a+bi=a+ib$, որտեղ i կոմպլեքս թիվը կոչվում է նաև **կեղծ միավոր**, իսկ a և b իրական թվերի համար ընդունված են հետևյալ նշանակումները՝ $a=Re(\alpha)$, $b=Im(\alpha)$: $\alpha=bi$ տեսքի կոմպլեքս թվերը կոչվում են նաև **կեղծ թվեր**:

Ակնհայտ է, որ եթե որևէ $K\leqslant\mathbb{C}$ ենթադաշտ պարունակում է $\mathbb{R}$-ը և i-ն, ապա այն կպարունակի նաև բոլոր կոմպլեքս թվերը և, հետևաբար, $K=\mathbb{C}$: Այս հատկությամբ կոմպլեքս թվերի $\mathbb{C}$ դաշտը, դաշտերի մեջ, որոշվում է միարժեքորեն՝ իզոմորֆիզմի ճշտությամբ, այսինքն՝ տեղի ունի հետևյալ արդյունքը:

Թեորեմ 15.2: *Դիցուք $P(+,\cdot)$ դաշտը պարունակում է $\mathbb{R}$-ը որպես ենթադաշտ և $j^2+1=0$ պայմանին բավարարող որևէ $j\in P$ տարր: Եթե $P(+,\cdot)$ դաշտը չունի նշված երկու պայմաններին բավարարող իրենից տարբեր որևէ ենթադաշտ, ապա $P\simeq\mathbb{C}$, այսինքն՝ $P(+,\cdot)$ դաշտն իզոմորֆ է կոմպլեքս թվերի $\mathbb{C}(+,\cdot)$ դաշտին:*

Ապացուցում: Եթե

$$P'=\{a+bj\,|a,b\in\mathbb{R}\},$$

ապա $P(+,\cdot)$ դաշտի հատկություններից և $j^2 = -1$ պայմանից, կունենանք՝

$$a_1 + b_1 j = a_2 + b_2 j \longleftrightarrow a_1 = a_2,\ b_1 = b_2,$$

$$(a_1 + b_1 j) + (a_2 + b_2 j) = (a_1 + a_2) + (b_1 + b_2)j,$$

$$(a_1 + b_1 j) \cdot (a_2 + b_2 j) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)j,$$

$$-(a + bj) = (-a) + (-b)j,$$

$$(a + bj)^{-1} = \frac{a}{a^2 + b^2} + \left(-\frac{b}{a^2 + b^2}\right) j, \text{ եթե } a^2 + b^2 \neq 0 :$$

Նշված հավասարություններից ապացուցման կարիք ունի միայն առաջինը՝ $a_1 + b_1 j = a_2 + b_2 j \to a_1 - a_2 = (b_2 - b_1)j \to (a_1 - a_2)^2 = -(b_2 - b_1)^2 \to a_1 - a_2 = 0,\, b_2 - b_1 = 0 \to a_1 = a_2, b_1 = b_2$:

Ուստի, P'-ը կլինի $P(+,\cdot)$ դաշտի ենթադաշտ, որը պարունակում է $\mathbb{R}$-ը և j-ն: Հետևաբար, ըստ թեորեմի պայմանի, $P' = P$: Սահմանելով՝

$$f(a + bj) = a + bi$$

արտապատկերումը, կստանանք որոնելի $f : P \to \mathbb{C}$ իզոմորֆիզմը, այսինքն՝ f-ը փոխմիարժեք (բիեկտիվ) է և տեղի ունեն

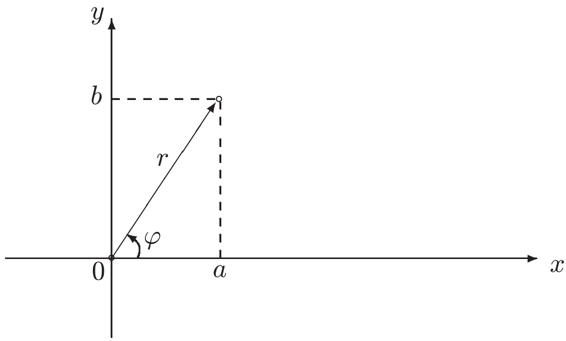
$$f(u + v) = f(u) + f(v),$$

$$f(u \cdot v) = f(u) \cdot f(v)$$

հավասարությունները՝ ցանկացած $u, v \in P$ տարրերի համար: □

Եթե հարթության վրա ընտրենք ուղղանկյուն (դեկարտյան) կոորդինատական համակարգ, ապա $\alpha = a + ib$ կոմպլեքս թիվը հարթության վրա (մեջ) կպատկերվի որպես կետ, որի ուղղանկյուն (դեկարտյան) կոորդինատներն են a-ն և b-ն: Այսպիսով, ստացվում է փոխմիարժեք (բիեկտիվ) համապատասխանություն՝ բոլոր կոմպլեքս թվերի և կոորդինատական հարթության բոլոր կետերի միջև: Այդ դեպքում, իրական թվերը կպատկերվեն աբսցիսների առանցքի կետերով, իսկ կեղծ թվերը՝ օրդինատների առանցքի կետերով: Զրոյին կհամապատասխանի կոորդինատների սկզբնակետը:

Օգտակար է նաև $\alpha = a + ib$ կոմպլեքս թիվը կոորդինատային հարթության վրա պատկերել որպես $\vec{\alpha}$ վեկտոր, որը միացնում է կոորդինատների սկզբնակետը (a, b) դեկարտյան կոորդինատներով կետի հետ՝



Այդ դեպքում՝ $\overrightarrow{\alpha+\beta} = \vec{\alpha} + \vec{\beta}$, այսինքն՝ կոմպլեքս թվերի գումարը «համաձայնեցված է» համապատասխան վեկտորների գումարի հետ: $\vec{\alpha}$ վեկտորի երկարությունը կոչվում է $\alpha = a + ib$ կոմպլեքս թվի **մոդուլ** (կամ բացարձակ արժեք) և նշանակվում է $|\alpha|$-ով՝

$$|\alpha| = \sqrt{a^2 + b^2} \geqslant 0$$

և $|\alpha| = 0 \leftrightarrow \alpha = 0$: Իրական թվի կոմպլեքս իմաստով մոդուլը համընկնում է այդ թվի իրական իմաստով մոդուլի հետ, որովհետև՝

$$|a| = |a + 0i| = \sqrt{a^2 + 0^2} = \sqrt{a^2} :$$

Ակնհայտ է նաև $|\alpha| = |-\alpha|$ հավասարությունը՝ ցանկացած α կոմպլեքս թվի դեպքում:

Լեմմ 15.1 (Եռանկյան անհավասարություններ): *Կամայական α, β կոմպլեքս թվերի համար՝*

1) $|\alpha + \beta| \leqslant |\alpha| + |\beta|$,
2) $|\alpha - \beta| \leqslant |\alpha| + |\beta|$,
3) $|\alpha + \beta| \geqslant |\alpha| - |\beta|$,
4) $|\alpha - \beta| \geqslant |\alpha| - |\beta|$,
5) $|\alpha + \beta| \geqslant ||\alpha| - |\beta||$,
6) $|\alpha - \beta| \geqslant ||\alpha| - |\beta||$*:*

Ապացուցում: 1) Դիցուք $\alpha = a + bi$, իսկ $\beta = c + di$: Քանի որ

$$(ac + bd)^2 = (a^2 + b^2)(c^2 + d^2) - (ad - bc)^2 \leqslant (a^2 + b^2)(c^2 + d^2),$$

ապա
$$ac+bd \leqslant \sqrt{a^2+b^2}\cdot\sqrt{c^2+d^2} = |\alpha|\cdot|\beta| :$$
Հետևաբար,
$$(a+c)^2+(b+d)^2 \leqslant (a^2+b^2)+(c^2+d^2)+2|\alpha|\cdot|\beta| = (|\alpha|+|\beta|)^2\,,$$
այսինքն՝
$$|\alpha+\beta|^2 \leqslant (|\alpha|+|\beta|)^2$$
և
$$|\alpha+\beta| \leqslant |\alpha|+|\beta| \;:$$
Ընդ որում, հավասարությունը տեղի կունենա այն և միայն այն դեպքում, երբ $ad-bc=0$, այսինքն՝ երբ $\alpha=\lambda\cdot\beta$ կամ $\beta=\lambda\cdot\alpha$ որևէ λ իրական թվի համար:

2) $|\alpha-\beta| = |\alpha+(-\beta)| \leqslant |\alpha|+|-\beta| = |\alpha|+|\beta|$:

3) Օգտվելով 2)-ից կունենանք՝
$$|\alpha| = |(\alpha+\beta)-\beta| \leqslant |\alpha+\beta|+|\beta|\,,$$
որտեղից $|\alpha+\beta| \geqslant |\alpha|-|\beta|$:

4) $|\alpha-\beta| = |\alpha+(-\beta)| \geqslant |\alpha|-|-\beta| = |\alpha|-|\beta|$:

5) $|\alpha+\beta| \geqslant |\alpha|-|\beta|$ և $|\alpha+\beta| = |\beta+\alpha| \geqslant |\beta|-|\alpha|$: Հետևաբար՝ $|\alpha+\beta| \geqslant ||\alpha|-|\beta||$:

6) $|\alpha-\beta| = |\alpha+(-\beta)| \geqslant ||\alpha|-|-\beta|| = ||\alpha|-|\beta||$: □

$\bar{\alpha}=a-bi$ կոմպլեքս թիվը կոչվում է $\alpha=a+bi$ կոմպլեքս թվի **համալուծ**:

Լեմմ 15.2: *Կամայական α, β կոմպլեքս թվերի համար՝*

$\overline{\alpha+\beta}=\bar{\alpha}+\bar{\beta}$,

$\overline{\alpha\cdot\beta}=\bar{\alpha}\cdot\bar{\beta}$,

$\bar{\bar{\alpha}}=\alpha$,

$\bar{\alpha}=\alpha \longleftrightarrow \alpha$*-ն իրական թիվ է*,

$|\alpha|=1 \longleftrightarrow \exists\alpha^{-1}$ *և* $\alpha^{-1}=\bar{\alpha}$,

$|\bar{\alpha}|=|\alpha|$,

$\alpha\cdot\bar{\alpha}=|\alpha|^2$,

$\alpha+\bar{\alpha}=2a$, *եթե* $Re(\alpha)=a$*:*

Ապացուցում: Անմիջական ստուգման եղանակով: □

Հետևություն 15.1: *$z \to \bar{z}$ արտապատկերումը կոմպլեքս թվերի դաշտի ավտոմորֆիզմ է:* □

Եթե $\alpha \neq 0$, ապա $\vec{\alpha}$ վեկտորի կազմած անկյունը աբսցիսների առանցքի դրական ուղղության հետ կոչվում է α-ի **արգումենտ** և նշանակվում է $arg(\alpha)$-ով: Զրոյի արգումենտը չի սահմանվում: Ոչ զրոյական կոմպլեքս թվի արգումենտը միարժեքորեն չի որոշվում, այն որոշվում է $2\pi k$ գումարելու ճշտությամբ, որտեղ $k \in \mathbb{Z}$:

Եթե $\alpha \neq 0$, $\alpha = a + ib$, $|\alpha| = r$ և $arg(\alpha) = \varphi$, ապա

$$a = r\cos\varphi \quad \text{և} \quad b = r\sin\varphi,$$

որտեղից՝

$$\alpha = r(\cos\varphi + i\sin\varphi) :$$

Այս տեսքը կոչվում է ոչ զրոյական α կոմպլեքս թվի **եռանկյունաչափական տեսք**, իսկ (r, φ) զույգը՝ նրա **բևեռային կոորդինատներ**:

Օրինակ, $i = 1\left(\cos\dfrac{\pi}{2} + i\sin\dfrac{\pi}{2}\right)$, $arg\,(\bar{\alpha}) = -arg(\alpha)$:

Այսպիսով՝

$$r_1\left(\cos\varphi_1 + i\sin\varphi_1\right) = r_2\left(\cos\varphi_2 + i\sin\varphi_2\right) \longleftrightarrow r_1 = r_2 \ \text{ և } \ \varphi_1 = \varphi_2 + 2\pi k,\ k \in \mathbb{Z},$$

որտեղ $r_1, r_2 \neq 0$:

Դիցուք $n \in \mathbb{N}$, $\alpha \in \mathbb{C}$: Բոլոր այն z կոմպլեքս թվերի բազմությունը, որոնց համար $z^n = \alpha$, կոչվում է **n-րդ աստիճանի արմատ** α կոմպլեքս թվից և նշանակվում է $\sqrt[n]{\alpha}$-ով: $\sqrt[n]{\alpha}$ բազմությանը պատկանող յուրաքանչյուր կոմպլեքս թիվ ևս կոչվում է n-րդ աստիճանի արմատ α-ից: Եթե $\alpha = 0$, ապա $\sqrt[n]{\alpha} = \{0\}$ ցանկացած $n \geqslant 1$ բնական թվի դեպքում: $n = 2$ դեպքում՝ $\sqrt[n]{\alpha}$-ի փոխարեն գրվում է $\sqrt{\alpha}$:

Հետևյալ արդյունքից բխում է, որ կոմպլեքս թվի եռանկյունաչափական տեսքը գտնվում է «լիովին համաձայնության» մեջ կոմպլեքս թվերի բազմապատկման, քանորդի, աստիճան բարձրացնելու և արմատ հանելու գործողությունների հետ:

Թեորեմ 15.3 (Մուավր): *Ոչ զրոյական կոմպլեքս թվերի համար տեղի ունեն հետևյալ հավասարությունները.*

1) $r_1(\cos\varphi_1 + i\sin\varphi_1) \cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = r_1 r_2\left(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2)\right)$;

2) $(r(\cos\varphi + i\sin\varphi))^{-1} = \dfrac{1}{r}\,(\cos(-\varphi) + i\sin(-\varphi))$*;*

3) $\dfrac{r_1(\cos\varphi_1 + i\sin\varphi_1)}{r_2(\cos\varphi_2 + i\sin\varphi_2)} = \dfrac{r_1}{r_2}\,(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2))$*;*

4) $r_1(\cos\varphi_1 + i\sin\varphi_1)\cdots r_n(\cos\varphi_n + i\sin\varphi_n) =$
$= r_1\cdots r_n\,(\cos(\varphi_1 + \cdots + \varphi_n) + i\sin(\varphi_1 + \cdots + \varphi_n))$*;*

5) $(r(\cos\varphi + i\sin\varphi))^n = r^n\,(\cos(n\varphi) + i\sin(n\varphi))$, ***որտեղ*** $n \in \mathbb{N}$*;*

6) $(r(\cos\varphi + i\sin\varphi))^m = r^m\,(\cos(m\varphi) + i\sin(m\varphi))$, ***որտեղ*** $m \in \mathbb{Z}$*;*
(Մուավրի բանաձևը)

7) $\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \left\{ \sqrt[n]{r}\left(\cos\dfrac{\varphi + 2\pi k}{n} + i\sin\dfrac{\varphi + 2\pi k}{n}\right) \,\middle|\, k \in \mathbb{Z}\right\}$*:*

Ապացուցում: 1)-ը և 2)-ը ստացվում են անմիջական ստուգման եղանակով: 3)-ը բխում է նախորդ երկու հատկություններից և $\dfrac{\alpha}{\beta} = \alpha\cdot\beta^{-1}$ սահմանումից: 4)-ը ստացվում է վերհանգման եղանակով: 5)-ը բխում է 4)-ից, երբ դիտարկվող կոմպլեքս թվերը համընկնում են: 6)-ը բխում է 5)-ից, 2)-ից և ոչ զրոյական կոմպլեքս թվի ամբողջ աստիճանի հասկացությունից՝

$$\alpha^n = \underbrace{\alpha\cdots\alpha}_{n}, \quad n > 0,$$

$$\alpha^0 = 1,$$

$$\alpha^{-n} = \underbrace{\alpha^{-1}\cdots\alpha^{-1}}_{n}, \quad n > 0:$$

Ապացուցենք 7)-ը: Դիցուք $\alpha \neq 0$, $\alpha = r(\cos\varphi + i\sin\varphi)$ և $z^n = \alpha$, որտեղ $z \in \mathbb{C}$: Հետևաբար, $z \neq 0$ և դիցուք $z = r'(\cos\varphi' + i\sin\varphi')$: Ուստի, 5)-ի համաձայն՝

$$(r')^n\,(\cos(n\varphi') + i\sin(n\varphi')) = r(\cos\varphi + i\sin\varphi)$$

և $(r')^n = r$, $n\varphi' = \varphi + 2\pi k$, $k \in \mathbb{Z}$: Այսպիսով, $r' = \sqrt[n]{r}$, $\varphi' = \dfrac{\varphi + 2\pi k}{n}$ և

$$\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \left\{ \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n}\right) \,\middle|\, k \in \mathbb{Z}\right\},$$

որտեղ $\sqrt[n]{r}$-ը r դրական թվից n-րդ աստիճանի թվաբանական (այսինքն՝ իրական և դրական) արմատն է, որը միշտ գոյություն ունի: □

Եթե նշանակենք՝

$$z_k = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right),$$

ապա կունենանք՝

$$z_k = z_{k'} \longleftrightarrow k \equiv k'(mod\, n) \longleftrightarrow [k] = [k'] :$$

Այստեղից հետևում է, որ $\alpha \neq 0$ դեպքում՝ $z^n = \alpha$ հավասարումն օժտված է միմյանցից տարբեր n հատ z_k լուծումներով, որոնք ստացվում են, օրինակ, $k = 0, 1, \ldots, n-1$ արժեքների դեպքում: Հանգում ենք հետևյալ արդյունքին.

Հետևություն 15.2: *Յուրաքանչյուր ոչ զրոյական $\alpha = r(\cos\varphi + i\sin\varphi)$ կոմպլեքս թվի համար՝*

$$\sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \left\{ \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right)\right| \\ k = 0, 1, \ldots, n-1\} :$$

Մասնավորապես՝

$$\sqrt[n]{1} = \left\{\cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}\right| \left. k = 0, 1, \ldots, n-1\right\} :$$

Եթե $n \geqslant 3$, ապա կոորդինատային հարթության վրա այս արմատներին համապատասխանող կետերը գտնվում են $(0,0)$ կենտրոնով և միավոր շառավղով շրջանագծին ներգծված այն կանոնավոր n-անկյուն բազմանկյան գագաթներում, որի մի գագաթը $(1,0)$ կետն է: □

Օրինակներ: 1) $\sqrt{1} = \{\pm 1\}$, $\sqrt[3]{1} = \left\{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right\}$, $\sqrt[4]{1} = \{\pm 1, \pm i\}$:

2) $\cos(2x) + i\sin(2x) = (\cos x + i\sin x)^2 =$
$= \cos^2 x + 2i\sin x\cos x + i^2\sin^2 x = \cos^2 x - \sin^2 x + i(2\sin x\cos x)$,

որտեղից՝

$$\cos(2x) = \cos^2 x - \sin^2 x,$$

$$\sin(2x) = 2\sin x\cos x :$$

3) $\cos(3x) + i\sin(3x) = (\cos x + i\sin x)^3 =$
$= \cos^3 x + 3i\cos^2 x\sin x + 3i^2\sin^2 x\cos x + i^3\sin^3 x =$
$= \cos^3 x - 3\cos x\sin^2 x + i(3\cos^2 x\sin x - \sin^3 x),$
որտեղից՝

$$\cos(3x) = \cos^3 x - 3\cos x\sin^2 x = 4\cos^3 x - 3\cos x,$$

$$\sin(3x) = 3\cos^2 x\sin x - \sin^3 x = 3\sin x - 4\sin^3 x :$$

4) Դիցուք $e = \lim\limits_{n\to\infty}\left(1+\dfrac{1}{n}\right)^n$: Ցանկացած $x \in \mathbb{R}$ իրական թվի համար e^{ix} աստիճանը սահմանվում է ըստ Լ. Էյլերի՝

$$e^{ix} = \cos x + i\sin x : \quad (\text{էյլերի բանաձևը})$$

Հետևաբար, ցանկացած ոչ զրոյական α կոմպլեքս թվի համար՝

$$\alpha = |\alpha| \cdot e^{i\cdot arg(\alpha)} :$$

5) $e^{\pi i} = \cos\pi + i\sin\pi = -1$, $e^{2\pi i} = \cos 2\pi + i\sin 2\pi = 1$:

$\alpha \in \mathbb{C}$ **կոմպլեքս թվի նորմը** նշանակվում է $Nr(\alpha)$-ով և սահմանվում է հետևյալ կերպ՝ $Nr(\alpha) = |\alpha|^2 = \alpha\cdot\bar{\alpha} \geqslant 0$: Դժվար չէ նկատել, որ

$$Nr(\alpha\cdot\beta) = Nr(\alpha)\cdot Nr(\beta) :$$

15.3. Մեկից n-րդ աստիճանի արմատներ և նախնական արմատներ

Եթե $X, Y \subseteq \mathbb{C}$, ապա սահմանվում է՝ $X\cdot Y = \{x\cdot y \mid x \in X, y \in Y\}$: Նշանակվում է նաև՝ $\alpha\cdot Y = \{\alpha\}\cdot Y$, եթե $\alpha \in \mathbb{C}$: Ակնհայտ է, որ $1\cdot X = X$, $X\cdot Y = Y\cdot X$ և $(X\cdot Y)\cdot Z = X\cdot(Y\cdot Z)$:

Ըստ n-րդ աստիճանի արմատի սահմանման, $\sqrt[n]{1}$-ը $x^n = 1$ հավասարման բոլոր կոմպլեքս լուծումների բազմությունն է, այսինքն՝ $x^n = 1$ հավասարման յուրաքանչյուր կոմպլեքս լուծում կոչվում է **մեկից n-րդ աստիճանի արմատ**:

Նշանակելով՝

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \qquad k = 0, 1, \ldots, n-1,$$

կստանանք՝

$$\sqrt[n]{1} = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\},$$

որտեղ $\varepsilon_0 = 1$, $\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, իսկ $(\varepsilon_1)^k = \varepsilon_k$, $k = 0, 1, \ldots, n-1$ (համաձայն Մուավրի բանաձևի), այսինքն՝

$$\sqrt[n]{1} = \left\{1, \varepsilon_1, \varepsilon_1^2, \ldots, \varepsilon_1^{n-1}\right\}:$$

Հատկություն 15.12: *Եթե $\alpha_0^n = \alpha$, որտեղ $\alpha \neq 0$, ապա*

$$\sqrt[n]{\alpha} = \alpha_0 \cdot \sqrt[n]{1}:$$

Ապացույց: Ակնհայտ է, որ $\alpha_0 \neq 0$: Ապացուցենք $\sqrt[n]{\alpha} \subseteq \alpha_0 \cdot \sqrt[n]{1}$ ներդրումը: Եթե $\beta \in \sqrt[n]{\alpha}$, ապա $\beta^n = \alpha$ և $\left(\alpha_0^{-1} \cdot \beta\right)^n = (\alpha_0^n)^{-1} \cdot \beta^n = \alpha^{-1} \cdot \alpha = 1$, այսինքն՝ $\varepsilon = \alpha_0^{-1} \cdot \beta \in \sqrt[n]{1}$ և $\beta = \alpha_0 \cdot \varepsilon$, որտեղ $\varepsilon \in \sqrt[n]{1}$: Եվ հակառակը, եթե $\beta \in \alpha_0 \cdot \sqrt[n]{1}$, ապա $\beta = \alpha_0 \cdot \varepsilon$, որտեղ $\varepsilon \in \sqrt[n]{1}$, և $\beta^n = (\alpha_0 \cdot \varepsilon)^n = \alpha_0^n \cdot \varepsilon^n = \alpha \cdot 1 = \alpha$, այսինքն՝ $\beta \in \sqrt[n]{\alpha}$: □

Հատկություն 15.13: *1) Եթե $\varepsilon_i, \varepsilon_j \in \sqrt[n]{1}$, ապա $\varepsilon_i \cdot \varepsilon_j \in \sqrt[n]{1}$;*

1′) Եթե $\varepsilon_i, \varepsilon_j \in \bigcup_{n=1}^{\infty} \sqrt[n]{1}$, ապա $\varepsilon_i \cdot \varepsilon_j \in \bigcup_{n=1}^{\infty} \sqrt[n]{1}$;

2) Եթե $\varepsilon \in \sqrt[n]{1}$, ապա $\varepsilon^{-1} \in \sqrt[n]{1}$;

2′) Եթե $\varepsilon \in \bigcup_{n=1}^{\infty} \sqrt[n]{1}$, ապա $\varepsilon^{-1} \in \bigcup_{n=1}^{\infty} \sqrt[n]{1}$;

3) Եթե $\varepsilon \in \sqrt[n]{1}$, ապա $\varepsilon^m \in \sqrt[n]{1}$ ցանկացած $m \in \mathbb{Z}$ ամբողջ թվի համար;

3′) Եթե $\varepsilon \in \bigcup_{n=1}^{\infty} \sqrt[n]{1}$, ապա $\varepsilon^m \in \bigcup_{n=1}^{\infty} \sqrt[n]{1}$ ցանկացած $m \in \mathbb{Z}$ ամբողջ թվի համար:

Ապացույց: 1) Եթե $\varepsilon_i^n = 1$ և $\varepsilon_j^n = 1$, ապա $(\varepsilon_i \cdot \varepsilon_j)^n = \varepsilon_i^n \cdot \varepsilon_j^n = 1 \cdot 1 = 1$:

1′) Եթե $\varepsilon_i^n = 1$ և $\varepsilon_j^m = 1$, ապա $(\varepsilon_i \cdot \varepsilon_j)^{nm} = \varepsilon_i^{nm} \cdot \varepsilon_j^{nm} = (\varepsilon_i^n)^m \cdot \left(\varepsilon_j^m\right)^n = 1 \cdot 1 = 1$:

2) Եթե $\varepsilon^n = 1$, ապա $(\varepsilon \cdot \varepsilon^{-1})^n = 1^n$, $\varepsilon^n \cdot (\varepsilon^{-1})^n = 1$ և $(\varepsilon^{-1})^n = 1$:

3) Եթե $\varepsilon^n = 1$, ապա $(\varepsilon^m)^n = \varepsilon^{m \cdot n} = (\varepsilon^n)^m = 1$:

Մնացած 2′) և 3′) պնդումներն ակնհայտ են: □

$\varepsilon \in \mathbb{C}$ կոմպլեքս թվի **կարգ** է կոչվում այն ամենափոքր ամբողջ և դրական q թիվը, որի համար՝ $\varepsilon^q = 1$: ε կոմպլեքս թվի կարգը կնշանակենք $o(\varepsilon)$-ով: Օրինակ, $o(1) = 1$, $o(-1) = 2$, $o\left(\frac{-1+i\sqrt{3}}{2}\right) = 3$, $o(i) = 4, \ldots$: Որպեսզի $\varepsilon \in \mathbb{C}$ կոմպլեքս թիվն ունենա կարգ անհրաժեշտ է և բավարար, որ $\varepsilon \in \bigcup\limits_{n=1}^{\infty} \sqrt[n]{1}$:

Դիցուք $n \geqslant 1$: Մեկից n-րդ աստիճանի արմատը կոչվում է **նախնական**, եթե նրա կարգը հավասար է n-ի, այսինքն՝ այն չի հանդիսանում մեկից m-րդ աստիճանի արմատ որևէ $m < n$ և $m > 0$ բնական թվի համար: Այլ կերպ, $\varepsilon \in \mathbb{C}$ կոմպլեքս թիվը կոչվում է մեկից n-րդ աստիճանի նախնական արմատ, եթե $\varepsilon^n = 1$ և $\varepsilon^m \neq 1$ ցանկացած $m < n$ և $m > 0$ բնական թվի համար:

Օրինակ,

$$\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

կոմպլեքս թիվը կլինի մեկից n-րդ աստիճանի նախնական արմատ, որովհետև $o(\varepsilon_1) = n$, այսինքն՝ $\varepsilon_1^n = 1$ և $\varepsilon_1^m \neq 1$, եթե $0 < m < n$, քանի որ $0 < \frac{2\pi m}{n} < 2\pi$: $n = 1, 2$ դեպքում, սա միակ նախնական արմատն է: Սակայն $n > 2$ դեպքում գոյություն ունեն նաև այլ նախնական արմատներ (բխում է հետևություն 15.3-ից):

Եթե ε-ը մեկից n-րդ աստիճանի կամայական նախնական արմատ է, ապա

$$\varepsilon^0 = 1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$$

կոմպլեքս թվերը կլինեն զույգ առ զույգ միմյանցից տարբեր և, հետևաբար,

$$\sqrt[n]{1} = \left\{\varepsilon^0 = 1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}\right\}:$$

Եվ հակառակը, այս հավասարության դեպքում ε-ը կլինի մեկից n-րդ աստիճանի նախնական արմատ:

Հատկություն 15.14: *Եթե $o(\varepsilon) = n$ և $\varepsilon^m = 1$, ապա m-ը բաժանվում է n-ի վրա:*

Ապացուցում: Դիցուք $m = nq + r$, որտեղ $0 \leqslant r < n$: Եթե $r \neq 0$, ապա $0 < r < n$, $r = m - nq$ և

$$\varepsilon^r = \varepsilon^{m-nq} = \varepsilon^m \cdot (\varepsilon^n)^{-q} = 1,$$

որը հակասում է $o(\varepsilon) = n$ պայմանին: Հետևաբար, $r = 0$ և $m = nq$: □

Հատկություն 15.15: *Եթե* $o(\varepsilon) = n$, *ապա*

$$o(\varepsilon^k) = \frac{n}{(n,k)}, \qquad k \in \mathbb{Z} :$$

Ապացուցում: Ստուգենք կոմպլեքս թվի կարգի սահմանման պայմանները.

ա) $(\varepsilon^k)^{\frac{n}{(n,k)}} = (\varepsilon^n)^{\frac{k}{(n,k)}} = 1$;

բ) Եթե $(\varepsilon^k)^m = 1$, $m > 0$, $m \in \mathbb{Z}$, ապա $m \geqslant \dfrac{n}{n,k}$: Իրոք, $\varepsilon^{km} = 1$ և համաձայն նախորդ հատկության՝ $km = nq$, $q \in \mathbb{Z}$: Եթե $d = (n,k)$, ապա $\left(\dfrac{n}{d}, \dfrac{k}{d}\right) = 1$ և $\dfrac{k}{d}m = \dfrac{n}{d}q$ հավասարությունից, համաձայն հատկություն 3.4-ի, կունենանք $m \Big/ \frac{n}{d}$ պայմանը, որտեղից էլ բխում է $m \geqslant \dfrac{n}{d} = \dfrac{n}{(n,k)}$ անհավասարությունը: □

Հետևություն 15.3: *Եթե* $o(\varepsilon) = n$, *ապա*

$$o(\varepsilon^k) = n \longleftrightarrow (k,n) = 1 :$$

Մասնավորապես, $o(\varepsilon_1^k) = n \leftrightarrow (k,n) = 1$, *և մեկից* n*-րդ աստիճանի բոլոր նախնական արմատների քանակը հավասար է* $\varphi(n)$*-ի, որտեղ* φ*-ն էյլերի ֆունկցիան է:* □

Հետևություն 15.4: *Ընդհանուր դեպքում՝*

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = \varepsilon_1^k$$

կոմպլեքս թիվը կլինի մեկից $\dfrac{n}{d}$*-րդ աստիճանի նախնական արմատ, որտեղ* $d = (k,n)$*:* □

Թեորեմ 15.4: *Եթե* $o(\varepsilon) = m$, $o(\delta) = n$ *և* $(m,n) = 1$, *ապա*

$$o(\varepsilon \cdot \delta) = o(\varepsilon) \cdot o(\delta) :$$

Ապացուցում: Նախ ակնհայտ է, որ

$$(\varepsilon \cdot \delta)^{m \cdot n} = \varepsilon^{m \cdot n} \cdot \delta^{m \cdot n} = (\varepsilon^m)^n \cdot (\delta^n)^m = 1 \cdot 1 = 1 :$$

Այնուհետև, եթե $\gamma = \varepsilon^i$ և $\gamma = \delta^j$, ապա $\gamma = 1$, որովհետև

$$\gamma^m = (\varepsilon^m)^i = 1,$$

$$\gamma^n = (\delta^n)^j = 1$$

և, համաձայն հատկություն 15.14-ի, m և n փոխադարձաբար պարզ թվերը կբաժանվեն $o(\gamma) = k$ բնական թվի վրա: Հետևաբար, $k = 1$ և $\gamma^k = \gamma^1 = 1$, այսինքն՝ $\gamma = 1$:

Դիցուք այժմ՝ $(\varepsilon \cdot \delta)^t = 1$, որտեղ t-ն ամբողջ և դրական թիվ է: Պահանջվում է ապացուցել, որ $t \geqslant m \cdot n$: Իրոք, նախ կունենանք՝ $\varepsilon^t \cdot \delta^t = 1$ և $\varepsilon^t = \delta^{-t}$ հավասարությունները: Նշանակելով՝ $\varepsilon^t = \delta^{-t} = \gamma$ կստանանք, ինչպես և վերևում, $\gamma = 1$: Ուստի, $\varepsilon^t = 1$ և $\delta^t = 1$: Որտեղից, հատկություն 15.14-ի համաձայն, t-ն կբաժանվի m և n փոխադարձաբար պարզ թվերից յուրաքանչյուրի վրա, հետևաբար և դրանց $m \cdot n$ արտադրյալի վրա: Այսպիսով, $t \geqslant m \cdot n$: □

Մեկից n-րդ աստիճանի բոլոր նախնական արմատների բազմությունը կնշանակենք $\left(\sqrt[n]{1}\right)^*$-ով: Այսպիսով, $\left(\sqrt[n]{1}\right)^*$ բազմության կարգը հավասար է $\varphi(n)$-ի, որտեղ φ-ն էյլերի ֆունկցիան է, և

$$\varepsilon \in \left(\sqrt[n]{1}\right)^* \longleftrightarrow o(\varepsilon) = n :$$

Թեորեմ 15.5*: Եթե* $(m, n) = 1$*, ապա*

1) $\sqrt[m]{1} \cap \sqrt[n]{1} = \{1\}$*,*

2) $\sqrt[m]{1} \cdot \sqrt[n]{1} = \sqrt[m \cdot n]{1}$*,*

3) $\left(\sqrt[m]{1}\right)^* \cdot \left(\sqrt[n]{1}\right)^* = \left(\sqrt[m \cdot n]{1}\right)^*$*:*

Մասնավորապես, 3)-ի համաձայն, նորից հանգում ենք էյլերի φ *ֆունկցիայի արտադրյալային հատկությանը՝*

$$\varphi(m) \cdot \varphi(n) = \varphi(m \cdot n),$$

եթե $(m, n) = 1$*:*

Ապացուցում: 1) Եթե $\alpha \in \sqrt[m]{1} \cap \sqrt[n]{1}$, ապա $\alpha^m = 1$, $\alpha^n = 1$ և, համաձայն հատկություն 15.14-ի, m և n փոխադարձաբար պարզ թվերը կբաժանվեն $o(\alpha)$ բնական թվի վրա: Հետևաբար, $o(\alpha) = 1$ և $\alpha = 1$:

2) Ակնհայտ է, որ հավասարության ձախ մասն ընկած է աջ մասի մեջ, որովհետև, եթե $\varepsilon^m = 1$ և $\delta^n = 1$, ապա $(\varepsilon \cdot \delta)^{m \cdot n} = \varepsilon^{m \cdot n} \cdot \delta^{m \cdot n} = 1$:

Դիցուք $\sigma^{m\cdot n} = 1$ և $mx + ny = 1$, $x, y \in \mathbb{Z}$: Այդ դեպքում՝ $\gamma_1 = \sigma^m \in \sqrt[n]{1}$, $\gamma_2 = \sigma^n \in \sqrt[m]{1}$ և

$$\sigma = \sigma^1 = \sigma^{mx+ny} = \sigma^{mx} \cdot \sigma^{ny} = (\sigma^m)^x \cdot (\sigma^n)^y = \gamma_1^x \cdot \gamma_2^y \in \sqrt[n]{1} \cdot \sqrt[m]{1}:$$

3) Եթե $\varepsilon \in \left(\sqrt[m]{1}\right)^*$, $\delta \in \left(\sqrt[n]{1}\right)^*$, ապա $o(\varepsilon) = m$, $o(\delta) = n$ և, համաձայն թեորեմ 15.4-ի, $o(\varepsilon\cdot\delta) = o(\varepsilon)\cdot o(\delta) = m\cdot n$, այսինքն՝ $\varepsilon\cdot\delta \in \left(\sqrt[m\cdot n]{1}\right)^*$: Այժմ ապացուցենք հակառակ ներդրումը՝

$$\left(\sqrt[m\cdot n]{1}\right)^* \subseteq \left(\sqrt[m]{1}\right)^* \cdot \left(\sqrt[n]{1}\right)^*:$$

Համաձայն 2)-ի, յուրաքանչյուր $z \in \left(\sqrt[m\cdot n]{1}\right)^*$ կոմպլեքս թիվ կարելի է ներկայացնել $z = x\cdot y$ արտադրյալի տեսքով, որտեղ $x \in \sqrt[m]{1}$ և $y \in \sqrt[n]{1}$: Մնում է ապացուցել, որ $o(x) = m$ և $o(y) = n$: Ենթադրելով հակառակը, ստանում ենք հակասություն: Իրոք, $o(x) = k \leqslant m$ և $o(y) = s \leqslant n$ ու

$$z^{ks} = (x\cdot y)^{ks} = x^{ks}\cdot y^{ks} = (x^k)^s \cdot (y^s)^k = 1\cdot 1 = 1$$

և, եթե $k \leqslant m$ և $s \leqslant n$ բնական թվերից գոնե մեկի համար տեղի ունենար խիստ անհավասարություն, ապա $z^{ks} = 1$ հավասարությունը կհակասեր $o(z) = m\cdot n$ պայմանին: 1) հավասարութունից բխում է նաև, որ $\psi : (\varepsilon, \delta) \to \varepsilon\cdot\delta$ համապատասխանությունը փոխմիարժեք (բիեկտիվ) արտապատկերում է՝

$$\left(\sqrt[m]{1}\right)^* \times \left(\sqrt[n]{1}\right)^* \longrightarrow \left(\sqrt[m]{1}\right)^* \cdot \left(\sqrt[n]{1}\right)^*,$$

այսինքն՝

$$\left|\left(\sqrt[m]{1}\right)^* \times \left(\sqrt[n]{1}\right)^*\right| = \left|\left(\sqrt[m]{1}\right)^* \cdot \left(\sqrt[n]{1}\right)^*\right| = \left|\left(\sqrt[m\cdot n]{1}\right)^*\right|$$

և

$$\varphi(m)\cdot\varphi(n) = \varphi(m\cdot n): \qquad \square$$

15.4. Գաուսյան և ամբողջ գաուսյան թվեր: Մնացորդով բաժանման ալգորիթմը

$\alpha = a + ib$ կոմպլեքս թիվը կոչվում է.

ա) **գաուսյան թիվ**, եթե a-ն և b-ն ռացիոնալ թվեր են, այսինքն՝ $a, b \in \mathbb{Q}$;

բ) **ամբողջ գաուսյան թիվ**, եթե a-ն և b-ն ամբողջ թվեր են, այսինքն՝ $a, b \in \mathbb{Z}$:

Բոլոր գաուսյան թվերի բազմությունը նշանակվում է $\mathbb{Q}[i]$-ով, իսկ բոլոր ամբողջ գաուսյան թվերի բազմությունը՝ $\mathbb{Z}[i]$-ով:

$\mathbb{Q}[i]$ բազմությունը կազմում է դաշտ՝ կոմպլեքս թվերի գումարման և բազմապատկման նկատմամբ, իսկ $\mathbb{Z}[i]$ բազմությունը ամբողջության տիրույթ է, այսինքն՝ զուգորդական, տեղափոխական, միավորով օժտված և առանց զրոյի բաժանարարների օղակ է, որի հակադարձելի տարրերն են ± 1 և $\pm i$ ամբողջ գաուսյան թվերը: Իրոք, նախ ակնհայտ է, որ նշված թվերից յուրաքանչյուրը հակադարձելի է $\mathbb{Z}[i]$ օղակում, իսկ եթե $\alpha \cdot \beta = 1$, որտեղ $\alpha, \beta \in \mathbb{Z}[i]$ և $\alpha = x + iy$, ապա

$$Nr(\alpha) \cdot Nr(\beta) = Nr(\alpha \cdot \beta) = Nr(1) = 1;$$

Հետևաբար, $Nr(\alpha) = 1$ և հանգում ենք $x^2 + y^2 = 1$ հավասարմանը, որի ամբողջարժեք լուծումներն են՝ $(1, 0)$, $(-1, 0)$, $(0, 1)$ և $(0, -1)$ զույգերը: Այսպիսով, $\alpha = \pm 1, \pm i$:

Ամբողջ գաուսյան թվերի օղակը շատ հատկություններով նման է ամբողջ թվերի օղակին, որի պատճառն ըստ էության թաքնված է ամբողջ գաուսյան թվերի մնացորդով բաժանման հետևյալ ալգորիթմի մեջ:

Թեորեմ 15.6 (ամբողջ գաուսյան թվերի մնացորդով բաժանման ալգորիթմը): *Ցանկացած α և $\beta \neq 0$ ամբողջ գաուսյան թվերի համար գոյություն ունեն այնպիսի σ և ρ ամբողջ գաուսյան թվեր, որ*

$$\alpha = \beta\sigma + \rho,$$

որտեղ $0 \leqslant Nr(\rho) < Nr(\beta)$:

Ապացուցում: Գոյություն ունեն այնպիսի x, y ռացիոնալ թվեր, որ

$$\alpha \cdot \beta^{-1} = x + iy :$$

Դիցուք u-ն և v-ն այնպիսի ամբողջ թվեր են, որ $|x - u| \leqslant \dfrac{1}{2}$ և $|y - v| \leqslant \dfrac{1}{2}$: Նշանակելով $\sigma = u + iv$ և $\rho = \alpha - \sigma\beta$, ստանում ենք այնպիսի ամբողջ գաուսյան թվեր, որ $\alpha = \beta\sigma + \rho$ և

$$0 \leqslant Nr(\rho) = Nr(\alpha - \sigma\beta) = Nr\left(\beta\left(\alpha\beta^{-1} - \sigma\right)\right) = Nr(\beta) \cdot Nr\left(\alpha\beta^{-1} - \sigma\right) =$$

$$= Nr(\beta)\cdot\left((x-u)^2+(y-u)^2\right) \leqslant Nr(\beta)\left(\frac{1}{4}+\frac{1}{4}\right) = \frac{Nr(\beta)}{2} < Nr(\beta) : \square$$

Օրինակ: Եթե $\alpha = 1+2i$, իսկ $\beta = 3+i$, ապա

$$\alpha\cdot\beta^{-1} = (1+2i)(3+i)^{-1} = \frac{1+2i}{3+i} = \frac{(1+2i)(3-i)}{(3+i)(3-i)} =$$

$$= \frac{3-i+6i-2i^2}{3^2-i^2} = \frac{5+5i}{10} = \frac{1}{2}+\frac{1}{2}i$$

և, ըստ թեորեմի ապացույցի, որպես σ կարելի է ընտրել ինչպես $\sigma_1 = 1+0i = 1$, այնպես էլ $\sigma_2 = 0+1i = i$ ամբողջ գաուսյան թվերը: Հետևաբար, ρ-ի համար էլ կստացվեն հետևյալ երկու հնարավոր արժեքները՝

$$\rho_1 = \alpha - \sigma_1\beta = 1+2i-3-i = -2+i$$

և

$$\rho_2 = \alpha - \sigma_2\beta = 1+2i-3i+1 = 2-i \ :$$

Այսպիսով, α և $\beta \neq 0$ ամբողջ գաուսյան թվերով σ և ρ ամբողջ գաուսյան թվերը միարժեքորեն չեն որոշվում:

Համանման օղակներ և դաշտեր կառուցվում են հետևյալ կերպ:

Դիցուք $d \in \mathbb{Z}$, $d \neq 0$ և $\sqrt{d} \notin \mathbb{Z}$, հետևաբար, $\sqrt{d} \notin \mathbb{Q}$ (հետևություն 3.3): Ըստ որում, d-ն կարող է լինել ինչպես դրական, այնպես էլ բացասական: Եթե $d > 0$, ապա $\sqrt{d}$ ասելով հասկացվում է թվաբանական արմատը, իսկ $d < 0$ դեպքում՝ $\sqrt{d} = i\sqrt{|d|}$:

Սահմանվում է՝

$$\mathbb{Q}\left[\sqrt{d}\right] = \left\{a+b\sqrt{d} \mid a,b\in\mathbb{Q}\right\},$$

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a+b\sqrt{d} \mid a,b\in\mathbb{Z}\right\} :$$

Նկատենք, որ $\mathbb{Q}\left[\sqrt{d}\right]$ (հետևաբար և $\mathbb{Z}\left[\sqrt{d}\right]$) բազմության յուրաքանչյուր տարր միարժեքորեն է ներկայացվում $a+b\sqrt{d}$ տեսքով՝

$$a_1+b_1\sqrt{d} = a_2+b_2\sqrt{d} \longrightarrow a_1-a_2 = (b_2-b_1)\sqrt{d} \longrightarrow$$

$$b_2-b_1 = 0, a_1-a_2 = 0 \longrightarrow b_1 = b_2, a_1 = a_2 :$$

$\mathbb{Q}\left[\sqrt{d}\right]$ բազմությունը դաշտ է՝ իրական կամ կոմպլեքս թվերի գումարման և բազմապատկման նկատմամբ, որովհետև

$$\left(a_1 + b_1\sqrt{d}\right) \pm \left(a_2 + b_2\sqrt{d}\right) = (a_1 + a_2) \pm (b_1 + b_2)\sqrt{d},$$

$$\left(a_1 + b_1\sqrt{d}\right)\left(a_2 + b_2\sqrt{d}\right) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d},$$

$$\left(a + b\sqrt{d}\right)^{-1} = \frac{a}{a^2 - db^2} + \frac{-b}{a^2 - db^2}\sqrt{d},$$

որտեղ $a + b\sqrt{d} \neq 0$; Այս դաշտը կոչվում է **քառակուսային դաշտ**՝ ծնված d ամբողջ թվով:

$\alpha = a + b\sqrt{d}$ **թվի նորմ** է կոչվում հետևյալ ռացիոնալ թիվը՝

$$Nr(\alpha) = a^2 - db^2 = \left(a + b\sqrt{d}\right)\left(a - b\sqrt{d}\right) = \alpha \cdot f(\alpha),$$

որտեղ $f(\alpha) = a - b\sqrt{d}$ և

$$f(\alpha + \beta) = f(\alpha) + f(\beta),$$

$$f(\alpha \cdot \beta) = f(\alpha) \cdot f(\beta) :$$

Հետևաբար,

$$Nr(\alpha) = 0 \longleftrightarrow \alpha = 0,$$

$$Nr(\alpha \cdot \beta) = \alpha\beta f(\alpha\beta) = \alpha\beta f(\alpha)f(\beta) = \alpha f(\alpha) \cdot \beta f(\beta) = Nr(\alpha) \cdot Nr(\beta) :$$

Մասնավորապես,

$$Nr(\alpha) \cdot Nr(\alpha^{-1}) = Nr(\alpha \cdot \alpha^{-1}) = Nr(1) = 1 :$$

$\mathbb{Z}\left[\sqrt{d}\right]$ բազմությունը օղակ է (ամբողջության տիրույթ է)՝ իրական կամ կոմպլեքս թվերի գումարման և բազմապատկման նկատմամբ: Այս օղակը կոչվում է **քառակուսային օղակ**՝ ծնված d ամբողջ թվով: Օրինակ, $d = -1, -3, -5$ դեպքերում ստանում ենք $\mathbb{Z}[i]$, $\mathbb{Z}\left[i\sqrt{3}\right]$ և $\mathbb{Z}\left[i\sqrt{5}\right]$ օղակները:

Վարժություններ և խնդիրներ

1. Ապացուցել, որ կոմպլեքս թվերի դաշտի վրա որոշված ցանկացած $A \in \mathbb{C}_{n\times m}$ մատրիցի համար գոյություն ունեն միարժեքորեն որոշվող այնպիսի $B, C \in \mathbb{R}_{n\times m}$ մատրիցներ, որ $A = B + iC$:

2. Հաշվել $\sqrt{i}$-ն:

3. Ապացուցել, որ

$$\sqrt{1}\ \cdot \sqrt[3]{1} = \sqrt[6]{1}, \qquad \sqrt[3]{1} \cdot \sqrt[4]{1} = \sqrt[12]{1}\ :$$

4. Ապացուցել, որ $\sqrt[n]{1} \subseteq \mathbb{C}$ ենթաբազմության բոլոր տարրերի գումարը հավասար է զրոյի, եթե $n > 1$:

5. Ապացուցել, որ եթե $o(\alpha) = n$, ապա $o(\overline{\alpha}) = n$:

6. Ապացուցել, որ իրական գործակիցներով քառակուսի հավասարումների լուծման բանաձևը ճիշտ է նաև կոմպլեքս գործակիցներով քառակուսի հավասարումների համար:

7. Վերհանգման եղանակով ապացուցել Նյուտոնի երկանդամային բանաձևը կոմպլեքս թվերի դեպքում՝

$$(\alpha + \beta)^n = \sum_{k=0}^{n} \binom{n}{k} \alpha^{n-k}\beta^k,$$

   որտեղ $\alpha, \beta \in \mathbb{C}$, $n \geqslant 1$:

8. Ապացուցել, որ ցանկացած $n \geqslant 1$ բնական թվի համար գոյություն ունի ամբողջ գործակիցներով այնպիսի f_n բազմանդամ, որ ցանկացած $x \in \mathbb{R}$ իրական թվի համար՝

$$\cos(n\,x) = f_n(\cos\, x)\ :$$

   Ավելի ճիշտ՝

$$\cos(n\,x) = \sum_{k=0}^{\left[\frac{n}{2}\right]} (-1)^k \binom{n}{2k} \cos^{n-2k} x \left(1 - \cos^2 x\right)^k\ :$$

9. Ապացուցել, որ միավոր շառավղով շրջանին ներգծված կանոնավոր 34-անկյան կողմը որոշվում է հետևյալ բանաձևով՝

$$a_{34} = \frac{\beta_1 - \sqrt{\beta_1^2 - 4\beta_2}}{2},$$

որտեղ

$$\beta_1 = \frac{\alpha_1 + \sqrt{\alpha_1^2 + 4}}{2}, \qquad \beta_2 = \frac{\alpha_2 + \sqrt{\alpha_2^2 + 4}}{2},$$

իսկ

$$\alpha_1 = \frac{-1 + \sqrt{17}}{2}, \qquad \alpha_2 = \frac{-1 - \sqrt{17}}{2} :$$

Այսպիսով, a_{34}-ը կարելի է կառուցել կարկինի և քանոնի օգնությամբ: Հետևաբար, կարկինի և քանոնի օգնությամբ կարելի է կառուցել նաև a_{17}-ը, այսինքն՝ միավոր շառավղով շրջանին ներգծված կանոնավոր 17-անկյան կողմը (Գաուս):

Գ լ ու խ 16

ԲԱԶՄԱՆԴԱՄՆԵՐ

16.1. Ներածություն

Մաթեմատիկայի դպրոցական դասընթացում բազմանդամը սահմանվում է որպես

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

տեսքի $f : \mathbb{R} \to \mathbb{R}$ ֆունկցիա, որտեղ $a_0, a_1, \ldots, a_n$ իրական թվերը կոչվում են f (կամ $f(x)$) **բազմանդամի գործակիցներ** կամ **հաստատուններ**, $a_i x^i$ գումարելիները կոչվում են f-ի անդամներ, իսկ a_0-ն կոչվում է **ազատ անդամ**: Եթե $a_n \neq 0$, ապա $a_n x^n$-ը կոչվում է f բազմանդամի **ավագ անդամ**, a_n-ը՝ **ավագ անդամի գործակից**, իսկ $n \geqslant 0$ բնական թիվը՝ f **բազմանդամի աստիճան** և նշանակվում է $deg(f)$-ով: Երկու բազմանդամների նույն նշիչով գործակիցները կոչվում են համապատասխան գործակիցներ:

Ուստի, երկու բազմանդամների $f = g$ հավասարությունը հասկացվում է որպես $f : \mathbb{R} \to \mathbb{R}$ և $g : \mathbb{R} \to \mathbb{R}$ ֆունկցիաների հավասարություն: Ակնհայտ է, որ բազմանդամի անդամների թիվը տրված բազմանդամով միարժեքորեն չի որոշվում, որովհետև $f(x)$ արտահայտության մեջ միշտ կարելի է ավելացնել զրոյական գործակիցներով $a_i x^i$ անդամներ: Հետևաբար, երկու f և g բազմանդամները միշտ կարելի է գրել հավասար թվով գործակիցներով:

Եթե f և g բազանդամների համապատասխան գործակիցները հավասար են, ապա, ակնհայտորեն, $f(x) = g(x)$ ցանկացած $x \in \mathbb{R}$ իրական թվի համար, այսինքն՝ $f = g$: Ճիշտ է նաև հակառակ պնդումը, որի ապացուցման համար կարելի է հենվել բազմանդամի անընդհատության հատկության վրա: Նախ ապացուցենք հետևյալ լեմմը.

Լեմմ 16.1: *Եթե յուրաքանչյուր $\alpha \neq 0$ իրական թիվ հանդիսանում է h բազմանդամի արմատ, ապա $h(0) = 0$:*

Ապացուցում: Եթե $\alpha_n \to 0$ և $\alpha_n \neq 0$, $\alpha_n \in \mathbb{R}$, ապա բազմանդամի անընդհատության համաձայն՝ $h(\alpha_n) \to h(0)$ և, հետևաբար, $h(0) = 0$, որովհետև $h(\alpha_n) = 0$, $n = 1, 2, \ldots$: $\square$

Լեմմ 16.2: *Եթե յուրաքանչյուր $\alpha \in \mathbb{R}$ իրական թիվ հանդիսանում է*

$$h(x) = c_0 + c_1 x + \cdots + c_m x^m$$

բազմանդամի արմատ, ապա $c_0 = c_1 = \cdots = c_m = 0$:

Ապացույց (վերհանգման եղանակ): Եթե $m = 0$, ապա պնդումն, ակնհայտորեն, ճիշտ է: Դիցուք այն ճիշտ է m-ից փոքր բնական թվերի դեպքում: Քանի որ $h(0) = c_0$, ապա $c_0 = 0$: Հետևաբար՝

$$h(x) = c_1 x + \cdots + c_m x^m = x\left(c_1 + c_2 x + \cdots + c_m x^{m-1}\right) = x \cdot h_1(x);$$

Եթե $\alpha \neq 0$, ապա

$$h(\alpha) = \alpha \cdot h_1(\alpha) = 0 \longrightarrow h_1(\alpha) = 0,$$

այսինքն՝ յուրաքանչյուր $\alpha \neq 0$ իրական թիվ հանդիսանում է h_1 բազմանդամի արմատ: Ուստի, համաձայն լեմմ 16.1-ի, նաև $h_1(0) = 0$ և վերհանգային ենթադրության համաձայն՝ $c_1 = c_2 = \cdots = c_m = 0$: □

Թեորեմ 16.1: *Եթե $f = g$, այսինքն՝ $f(\alpha) = g(\alpha)$ ցանկացած $\alpha \in \mathbb{R}$ իրական թվի համար, ապա f և g բազմանդամների համապատասխան գործակիցները կլինեն հավասար:*

Ապացույց: Դիտարկենք $h(x) = f(x) - g(x)$ բազմանդամը: Քանի որ $h(\alpha) = f(\alpha) - g(\alpha) = 0$ ցանկացած $\alpha \in \mathbb{R}$ իրական թվի համար, ապա, համաձայն լեմմ 16.2-ի, h բազմանդամի բոլոր գործակիցները հավասար են զրոյի: □

Այս մոտեցումը կիրառելի է նաև կոմպլեքս գործակիցներով բազմանդամների համար:

Սակայն բազմանդամի սահմանման նշված դպրոցական մոտեցումը չի կարող ընդունելի համարվել, օրինակ, վերջավոր դաշտից վերցրած գործակիցներով բազմանդամների համար: Մասնավորապես, $\mathbb{Z}_2(+, \cdot)$ դաշտի դեպքում, եթե

$$f(x) = x^2 \quad \text{և} \quad g(x) = x,$$

ապա $f(\alpha) = g(\alpha)$ ցանկացած $\alpha \in \mathbb{Z}_2$ տարրի համար: Մյուս կողմից, բնական է այս երկու բազմանդամները համարել տարբեր բազմանդամներ: Նմանատիպ բազմանդամների օրինակներ գոյություն ունեն ցանկացած վերջավոր դաշտի դեպքում: Օրինակ, $\mathbb{Z}_p(+,\cdot)$ վերջավոր դաշտում $f = x^p - x = x\left(x^{p-1} - 1\right)$ բազմանդամի արժեքը դաշտի յուրաքանչյուր կետում հավասար է զրոյի (բխում է Ֆերմայի փոքր թեորեմից):

Այսպիսով, անհրաժեշտություն է առաջանում վերանայել բազմանդամի դպրոցական սահմանումն այնպես, որ այն, մի կողմից, ընդունելի համարվի ցանկացած դաշտից վերցրած գործակիցների դեպքում, իսկ, մյուս կողմից, ստացվող արդյունքներն ընդգրկեն համապատասխան դպրոցական գիտելիքներն ու պատկերացումները: Այս նպատակներն իրագործելի են դառնում, երբ բազմանդամի հասկացությունը ներմուծվում է որպես իր գործակիցներից կազմված հաջորդականություն:

16.2. Բազմանդամի սահմանումը: Գործողություններ բազմանդամների հետ: Մնացորդով բաժանման ալգորիթմը

Դիցուք $K(+,\cdot)$-ը կամայական ամբողջության տիրույթ է, որը համառոտ կնշանակենք նաև K-ով: K-ի զրոյական տարրը կնշանակենք 0-ով, իսկ միավորը՝ e-ով կամ 1-ով: Մասնավորապես, K-ն կարող է լինել դաշտ:

$$\alpha = (a_0, a_1, a_2, \ldots, a_i, \ldots)$$

հաջորդականությունը կոչվում է **որոշված** K-ի վրա կամ համառոտ՝ K-հաջորդականություն, եթե $a_i \in K$ բոլոր $i = 0, 1, 2, \ldots$ նշիչների համար: $a_i \in K$ տարրերը կոչվում են α-ի գործակիցներ: Գրված α հաջորդականությունը կարելի է նշել նաև $\alpha = (a_i)$ համառոտ տեսքով: Քանի որ K-ի վրա որոշված յուրաքանչյուր α հաջորդականություն կարելի է դիտել նաև որպես $\alpha : \mathbb{N} \to K$ տեսքի ֆունկցիա (արտապատկերում), որտեղ $\alpha(0) = a_0$, $\alpha(1) = a_1$, $\alpha(2) = a_2$, ..., այսինքն՝ $\alpha(i) = a_i$ բոլոր $i \geqslant 0$ բնական թվերի համար, ապա երկու K-հաջորդականությունների հավասարությունը կարելի է հասկանալ որպես համապատասխան ֆունկցիաների հավասարություն: Այլ կերպ, $\alpha = (a_i)$ և $\beta = (b_i)$ երկու K-հաջորդականություններ կոչվում են **հավասար** և գրվում է $\alpha = \beta$, եթե $a_i = b_i$ բոլոր $i \geqslant 0$ նշիչների համար: Հակառակ դեպքում α և β K-հաջորդականությունները կոչվում են **ոչ հավասար** և գրվում է $\alpha \neq \beta$: Միևնույն նշիչով

a_i և b_i գործակիցները կոչվում են α և β հաջորդականությունների համապատասխան գործակիցներ:

K ամբողջության տիրույթի վրա որոշված

$$\alpha = (a_0, a_1, a_2, \ldots, a_i, \ldots)$$

հաջորդականությունը կոչվում է **բազմանդամ**՝ որոշված K-ի վրա կամ համառոտ՝ K-բազմանդամ, եթե գոյություն ունի այնպիսի $m \geqslant 0$ բնական թիվ, որ $a_i = 0$ բոլոր $i \geqslant m$ նշիչների համար, այսինքն՝

$$\alpha = (a_0, a_1, \ldots, a_{m-1}, 0, 0, \ldots) \ :$$

Այսպիսով, բազմանդամը կարող է ունենալ միայն վերջավոր թվով ոչ զրոյական գործակիցներ: $(0, 0, \ldots, 0, \ldots)$ տեսքի հաջորդականությունը կոչվում է **զրոյական բազմանդամ** և նշանակվում է 0-ով: Հակառակ դեպքում բազմանդամը կոչվում է **ոչ զրոյական**:

Եթե

$$\alpha = (a_0, a_1, a_2, \ldots, a_i, \ldots)$$

բազմանդամը ոչ զրոյական է, ապա գոյություն ունի այնպիսի $a_n \neq 0$, որ $a_i = 0$ բոլոր $i > n$ նշիչների համար: Այդ դեպքում a_n-ը կոչվում է α բազմանդամի **ավագ գործակից** կամ **ավագ անդամի գործակից**, իսկ n-ը՝ α-ի աստիճան և նշանակվում է՝ $n = deg(\alpha)$: Զրոյական բազմանդամին աստիճան չի վերագրվում: Այսպիսով, $deg(\alpha) = \max\{k \mid a_k \neq 0\}$:

Երկու K-բազմանդամների գումարը և արտադրյալը (բազմապատկումը) սահմանվում են հետևյալ կերպ: Եթե

$$\alpha = (a_0, a_1, a_2, \ldots, a_i, \ldots)$$

և

$$\beta = (b_0, b_1, b_2, \ldots, b_i, \ldots) \,,$$

ապա

$$\alpha + \beta = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots, a_i + b_i, \ldots)$$

և

$$\alpha \cdot \beta = (c_0, c_1, c_2, \ldots, c_k, \ldots) \,,$$

որտեղ

$$
\begin{aligned}
&c_0 = a_0 b_0,\\
&c_1 = a_0 b_1 + a_1 b_0,\\
&c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0,\\
&\ \ \dots\ \ \dots\ \ \dots\\
&c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0 = \sum_{i+j=k} a_i b_j\,,\\
&\ \ \dots\ \ \dots\ \ \dots
\end{aligned}
$$

այսինքն՝ $\alpha \cdot \beta = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots)$: Ակնհայտ է, որ երկու K-բազմանդամների գումարը և արտադրյալը K-բազմանդամներ են: Ավելի ճիշտ, եթե $a_i = 0$ բոլոր $i > m$ ճշիչների համար և $b_i = 0$ բոլոր $i > n$ ճշիչների համար, ապա $a_i + b_i = 0$ բոլոր $i > \max\{m, n\}$ ճշիչների համար և $c_i = 0$ բոլոր $i > m + n$ ճշիչների համար:

Լեմմ 16.3: *Եթե K-ն ամբողջության տիրույթ է, ապա ցանկացած ոչ զրոյական α և β K-բազմանդամների համար՝*

1) $deg(\alpha + \beta) \leqslant \max\{deg(\alpha), deg(\beta)\}$ (եթե ձախ մասը գոյություն ունի);

2) $deg(\alpha \cdot \beta) = deg(\alpha) + deg(\beta)$;

3) Բոլոր K-բազմանդամների բազմությունը նս ամբողջության տիրույթ է՝ K-բազմանդամների գումարման և բազմապատկման նկատմամբ, որը կոչվում է K-բազմանդամների օղակ:

Ապացուցում: 1) Իրոք, եթե α և β բազմանդամների աստիճանները հավասար են n-ի և նրանց ավագ անդամների գործակիցները կապված են $a_n = -b_n$ առնչությամբ, ապա՝ $deg(\alpha + \beta) < n = \max\{deg(\alpha), deg(\beta)\}$ կամ $\alpha + \beta = 0$: Մնացած դեպքերում տեղի ունի $deg(\alpha + \beta) = \max\{deg(\alpha), deg(\beta)\}$ հավասարությունը:

2) Եթե $deg(\alpha) = m$ և $deg(\beta) = n$, ապա $deg(\alpha \cdot \beta) = m + n$, որովհետև $c_{m+n} = a_m \cdot b_n \neq 0$, իսկ $c_i = 0$ բոլոր $i > m + n$ ճշիչների համար:

3) Անմիջական ստուգման եղանակով: $\square$

$(1, 0, 0, \dots, 0, \dots)$ բազմանդամը կլինի K-բազմանդամների օղակի միավորը, որը նույնպես նշանակվում է 1-ով: $-\alpha = (-a_0, -a_1, -a_2, \dots, -a_i, \dots)$ բազմանդամը կոչվում է $\alpha = (a_0, a_1, a_2, \dots, a_i, \dots)$ բազմանդամի **հակադիր բազմանդամ**, իսկ

$\alpha - \beta = \alpha + (-\beta)$ բազմանդամը կոչվում է α և β բազմանդամների **տարբերություն**: Ինչպես և կամայական զուգորդական օղակում, սահմանվում է՝

$$\alpha^n = \underbrace{\alpha \cdot \alpha \cdots \alpha}_{n}, \qquad \alpha^0 = 1 :$$

Որպեսզի հանգենք բազմանդամի սովորական գրելաձևին, կատարենք հետևյալ երկու նշանակումները՝

$$x = (0, 1, 0, 0, \ldots),$$

$$r = (r, 0, 0, \ \ldots \ ), \quad r \in K \ :$$

Վերջին նշանակումը համաձայնեցված է K օղակի գործողությունների հետ, այսինքն՝

$$(r_1, 0, 0, \ \ldots \ ) + (r_2, 0, 0, \ \ldots \ ) = (r_1 + r_2, 0, 0, \ \ldots \ ) \ ,$$

$$(r_1, 0, 0, \ \ldots \ ) \cdot (r_2, 0, 0, \ \ldots \ ) = (r_1 \cdot r_2, 0, 0, \ \ldots \ ) \ :$$

Լեմմ 16.4: *1) Ցանկացած* $\alpha = (a_0, a_1, a_2, \ldots)$ *K-բազմանդամի համար՝*

$$x\alpha = (0, a_0, a_1, a_2, \ldots),$$

$$r\alpha = (ra_0, ra_1, ra_2, \ldots);$$

2) Եթե $n \geqslant 1$*, ապա*

$$x^n = (\underbrace{0, \ldots, 0}_{n}, 1, 0, \ldots);$$

3) Ցանկացած $\alpha = (a_0, a_1, \ldots, a_n, 0, 0, \ldots)$ *K-բազմանդամ ներկայացվում է հետևյալ տեսքով՝*

$$\alpha = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \, ,$$

որը կոչվում է բազմանդամի **ավանդական** *(սովորական) գրելաձև և համառոտ նշանակվում է* $\alpha = \sum\limits_{i \geqslant 0} \alpha_i x^i$ *կամ ավելի ճշգրիտ՝* $\alpha = \sum\limits_{i=0}^{n} \alpha_i x^i$ *տեսքով: Մասնավորապես, եթե* $\beta = b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m$*, ապա*

$$\alpha + \beta = \sum_{i=0}^{t} (a_i + b_i) x^i, \quad t = \max\{m, n\}, \quad x^0 = 1,$$

$$\alpha\cdot\beta = a_0b_0+(a_0b_1+a_1b_0)x+\cdots+(a_{n-1}b_m+a_nb_{m-1})x^{m+n-1}+a_nb_mx^{m+n} =$$

$$= \sum_{i=0}^{m+n}\left(\sum_{k=0}^{i} a_kb_{i-k}\right)x^i \;:$$

Ապացույց: 1) և 2) պնդումները բխում են բազմանդամների արտադրյալի սահմանումից:

3) $\alpha = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) = (a_0, 0, 0, \ldots) + (0, a_1, 0, 0, \ldots)+$
$\cdots + (0, \ldots, 0, a_n, 0, \ldots) = a_0(1, 0, 0, \ldots) + a_1(0, 1, 0, 0, \ldots)+$
$\cdots + a_n(0, \ldots, 0, 1, 0, \ldots) = a_0 + a_1x + \cdots + a_nx^n$: □

3) հատկության շնորհիվ α բազմանդամը հաճախ նշանակվում է նաև $\alpha(x)$-ով, իսկ x-ը կոչվում է «փոփոխական» կամ «անհայտ»: a_0 գործակիցը կոչվում է

$$\alpha(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

բազմանդամի **ազատ անդամ**, a_ix^i արտադրյալները կոչվում են նրա **անդամներ**, իսկ a_nx^n-ը՝ **ավագ անդամ**, եթե $a_n \neq 0$: Ոչ զրոյական բազմանդամը կոչվում է **ունիտար** (unit = միավոր), եթե նրա ավագ անդամի գործակիցը հավասար է 1-ի, որտեղ 1-ը դիտարկվող $K(+,\cdot)$ օղակի միավորն է: $\alpha(x) = a_0$ տեսքի բազմանդամը կոչվում է **հաստատուն**, որը կլինի զրո աստիճանի բազմանդամ, եթե $a_0 \neq 0$: 1 (առաջին) աստիճանի բազմանդամը կոչվում է **գծային** կամ երբեմն **երկանդամ**, 2 (երկրորդ) աստիճանի բազմանդամը՝ **քառակուսային** կամ երբեմն **եռանդամ**, իսկ 3 (երրորդ) աստիճանի բազմանդամը՝ **խորանարդ** բազմանդամ: $f = a_ix^i$ տեսքի բազմանդամը կոչվում է **միանդամ**, որը $i = 0$ դեպքում հավասար է a_0-ին, որովհետև, ինչպես նշեցինք, ընդունվում է՝ $x^0 = 1$:

$K(+,\cdot)$ ամբողջության տիրույթի վրա որոշված բոլոր բազմանդամների օղակը սովորաբար նշանակվում է $K[x]$-ով: Այսպիսով $K[x]$ բազմությունը ամբողջության տիրույթ է՝ բազմանդամների գումարման և բազմապատկման նկատմամբ: $K[x]$ օղակը կոչվում է K-ից վերցրած գործակիցներով և մեկ փոփոխականից կախված բազմանդամների օղակ: Եթե $Q = K[x]$, ապա կարելի է դիտարկել $Q[y]$ բազմանդամների օղակը, որտեղ y-ը սահմանվում է Q-ի վրա այնպես ինչպես x-ը՝ K-ի վրա: $Q[y]$ օղակը նշանակվում է $K[x, y]$-ով և կոչվում է K-ից վերցրած գործակիցներով և x ու y փոփոխականներից կախված բազմանդամների օղակ: Վերհանգման եղանակով սահմանվում է n փոփոխականներից կախված բազմանդամների օղակը՝

$$K[x_1, x_2, \ldots, x_n] = (K[x_1, \ldots, x_{n-1}])[x_n] :$$

Այսպիսով, եթե K-ն ամբողջության տիրույթ է, ապա $K[x_1, x_2, \ldots, x_n]$ օղակը ևս կլինի ամբողջության տիրույթ: $K[x_1, x_2, \ldots, x_n]$ բազմության (օղակի) տարրերը կոչվում են $x_1, x_2, \ldots, x_n$ փոփոխականներից կախված բազմանդամներ:

Օրինակ,

$$f(x, y) = y^3 + ax^2 + by^2 + cxy + dx + sy + t =$$

$$= (t + dx + ax^2) + (s + cx)y + by^2 + y^3 \in Q[y],$$

որտեղ $Q = K[x]$, $a, b, c, d, s, t \in K$:

Թեորեմ 16.2 (բազմանդամների մնացորդով բաժանման վերաբերյալ): *Եթե K-ն ոչ զրոյական ամբողջության տիրույթ է, $f, g \in K[x]$, $g \neq 0$ և g-ի ավագ անդամի գործակիցը հակադարձելի է K-ում, ապա գոյություն ունեն միարժեքորեն որոշվող այնպիսի $q, r \in K[x]$ բազմանդամներ, որ*

$$f = gq + r,$$

որտեղ կամ $r = 0$ կամ $deg(r) < deg(g)$: (Այստեղ q-ն և r-ը կոչվում են f-ը g-ի վրա բաժանելուց ստացվող ոչ լրիվ քանորդ և մնացորդ:)

Ապացուցում: Նախ նկատենք q և r բազմանդամների միակությունը: Իրոք,

$$f = gq_1 + r_1 \quad \text{և} \quad f = gq_2 + r_2$$

հավասարություններից հետևում է, որ

$$g(q_1 - q_2) = r_2 - r_1$$

և, եթե $q_1 - q_2 \neq 0$, ապա ստացված հավասարության ձախ մասի աստիճանը փոքր չի լինի $deg(g)$-ից, իսկ հավասարության աջ մասի աստիճանը կամ խիստ փոքր է $deg(g)$-ից կամ՝ $r_2 - r_1 = 0$: Ստացված հակասությունից բխում է $q_1 - q_2 = 0$ հավասարությունը, այսինքն՝ $q_1 = q_2$, որտեղից էլ հետևում է $r_2 - r_1 = 0$ հավասարությունը, այսինքն՝ $r_1 = r_2$:

Անցնենք q և r բազմանդամների գոյության ապացուցին: Եթե $deg(f) < deg(g)$ կամ $f = 0$, ապա $q = 0$ և $r = f$, որովհետև

$$f = g \cdot 0 + f :$$

Իսկ եթե $f \neq 0$ և $deg(f) \geqslant deg(g)$, ապա պնդումն ապացուցենք վերհանգման եղանակով՝ ըստ $f \neq 0$ բազմանդամի $n = deg(f)$ աստիճանի: Վերհանգման հենքը $n = 0$ թիվն է, որովհետև $deg(f) = 0$ դեպքում կունենանք $deg(g) = 0$, այսինքն, եթե $f = a \neq 0$, ապա $g = b \neq 0$, որտեղ $a, b \in K$, և

$$f = g(b^{-1}a) + 0 \ :$$

Հետևաբար, այս դեպքում՝ $q = b^{-1}a$ և $r = 0$:

Ենթադրենք n-ից փոքր աստիճան ունեցող $f \neq 0$ բազմանդամների համար պնդումը ճիշտ է: Դիցուք

$$f = a_0 + a_1 x + \cdots + a_n x^n, \quad a_n \neq 0,$$

և

$$g = b_0 + b_1 x + \cdots + b_m x^m, \quad b_m \neq 0,$$

որտեղ $n \geqslant m$: Այդ դեպքում, կամ

$$f - a_n b_m^{-1} x^{n-m} g = f_1$$

բազմանդամի աստիճանը փոքր է n-ից, կամ $f_1 = 0$: Երկու դեպքում էլ գոյություն ունեն այնպիսի q_1 և r K-բազմանդամներ, որ $f_1 = gq_1 + r$, որտեղ կամ $r = 0$ կամ $deg(r) < deg(g)$: Հետևաբար,

$$f = a_n b_m^{-1} x^{n-m} g + f_1 = a_n b_m^{-1} x^{n-m} g + gq_1 + r =$$

$$= g\left(a_n b_m^{-1} x^{n-m} + q_1\right) + r = gq + r,$$

որտեղ $q = a_n b_m^{-1} x^{n-m} + q_1$: □

Ստացված թեորեմի ապացուցման ընթացքը համընկնում է դպրոցական դասընթացից հայտնի իրական գործակիցներով բազմանդամների «անկյունով» բաժանման ընթացքի հետ: Օրինակ,

$$5x^4 + 3x^3 + x^2 + 11x + 6 = (x^2 + x + 1)(5x^2 - 2x - 2) + 15x + 8\,,$$

որովհետև՝

$$
\begin{array}{r|l}
5x^4+3x^3+x^2+11x+6 & x^2+x+1 \\ \cline{2-2}
-\ 5x^4+5x^3+5x^2 & 5x^2-2x-2 \\ \cline{1-1}
-2x^3-4x^2+11x & \\
-\ -2x^3-2x^2-2x & \\ \cline{1-1}
-2x^2+13x+6 & \\
-\ -2x^2-2x-\ 2 & \\ \cline{1-1}
15x+8 &
\end{array}
$$

Հետևություն 16.1: *Եթե K-ն դաշտ է, ապա ցանկացած $f, g \in K[x]$, $g \neq 0$, բազմանդամների համար գոյություն ունեն միարժեքորեն որոշվող այնպիսի $q, r \in K[x]$ բազմանդամներ, որ*

$$f = gq + r,$$

որտեղ կամ $r = 0$ կամ $deg(r) < deg(g)$: □

Հետևություն 16.2: *1) Եթե $K \leqslant K'$, այսինքն՝ K' ամբողջության տիրույթը հանդիսանում է K ամբողջության տիրույթի ընդլայնումը, ապա $K[x] \leqslant K'[x]$: 2) Եթե $f, g \in K[x]$, $g \neq 0$, և*

$$f = gq + r, \quad \text{որտեղ} \quad q, r \in K[x], \quad r = 0 \ \text{ կամ } \ deg(r) < deg(g),$$

$$f = gq' + r', \ \text{ որտեղ } \ q', r' \in K'[x], \quad r' = 0 \ \text{ կամ } \ deg(r') < deg(g),$$

ապա $q = q'$ և $r = r'$: Մասնավորապես, եթե

$$f = gq + r, \quad \text{որտեղ} \quad q, r \in K[x], \quad r = 0 \ \text{ կամ } \ deg(r) < deg(g),$$

$$f = gq', \qquad q' \in K'[x],$$

ապա $q' \in K[x]$: □

Հետևություն 16.3: *Եթե K-ն ոչ զրոյական ամբողջության տիրույթ է, ապա ցանկացած $f \in K[x]$ բազմանդամի և ցանկացած $c \in K$ հաստատունի համար գոյություն ունեն միարժեքորեն որոշվող այնպիսի $q \in K[x]$ բազմանդամ և $r \in K$ հաստատուն, որ*

$$f = (x - c)q + r \ : \qquad □$$

Եթե $f = a_0 + a_1x + \cdots + a_nx^n$, ապա համեմատելով $f = (x-c)q + r$ հավասարության աջ և ձախ մասերի համապատասխան գործակիցները, կստանանք $q = b_0 + b_1x + \cdots + b_{n-1}x^{n-1}$ բազմանդամի գործակիցները և r հաստատունը.

$$\begin{array}{lll}
a_n = b_{n-1} & \to & b_{n-1} = a_n\,, \\
a_{n-1} = b_{n-2} - cb_{n-1} & \to & b_{n-2} = a_{n-1} + cb_{n-1}\,, \\
a_{n-2} = b_{n-3} - cb_{n-2} & \to & b_{n-3} = a_{n-2} + cb_{n-2}\,, \\
\quad\dots \quad \dots & \dots & \quad \dots \quad \dots \\
a_1 = b_0 - cb_1 & \to & b_0 = a_1 + cb_1\,, \\
a_0 = r - cb_0 & \to & r = a_0 + cb_0\ :
\end{array}$$

Գործակիցների որոշման այս եղանակը կոչվում է **Հորների բանաձևեր** կամ **Հորների սխեմա**:

Եթե K-ն ոչ զրոյական ամբողջության տիրույթ է, $c \in K$ և $f \in K[x]$, որտեղ

$$f = a_0 + a_1x + \cdots + a_nx^n,$$

ապա

$$f(c) = a_0 + a_1c + \cdots + a_nc^n \in K$$

տարրը կոչվում է f բազմանդամի արժեք $c \in K$ կետում: $c \in K$ տարրը կոչվում է $f \in K[x]$ **բազմանդամի արմատ**, եթե $f(c) = 0$: f բազմանդամի արմատը կոչվում է նաև $f = 0$ **հավասարման արմատ** կամ **լուծում**, իսկ $f = 0$ հավասարումը կոչվում է նաև n**-րդ աստիճանի հանրահաշվական հավասարում**, եթե f-ը n-րդ աստիճանի բազմանդամ է: Ակնհայտ է, որ եթե

$$f = f_1 + f_2$$

և

$$g = f_1 \cdot f_2,$$

ապա ցանկացած $c \in K$ տարրի համար՝

$$f(c) = f_1(c) + f_2(c)$$

և

$$g(c) = f_1(c) \cdot f_2(c)\ :$$

Ակնհայտ է նաև, որ եթե $f_1 = f_2$, ապա $f_1(c) = f_2(c)$ ցանկացած $c \in K$ տարրի համար: Հետաքրքրական է հակառակ հարցը, որը պարզաբանվում է թեորեմ 16.5-ում և հետևություն 16.4-ում:

Եթե $\alpha, \beta \in K[x]$ բազմանդամների համար գոյություն ունի այնպիսի $\gamma \in K[x]$ բազմանդամ, որ $\alpha = \beta \cdot \gamma$, ապա կասենք, որ α բազմանդամը **բաժանվում է** β բազմանդամի վրա: Հետևյալ արդյունքը կոչվում է Բեզուի թեորեմ և հաճախ կիրառվում է:

Թեորեմ 16.3 (Բեզու): *Որպեսզի ոչ զրոյական $\alpha \in K[x]$ բազմանդամը բաժանվի $x - c$ երկանդամի վրա անհրաժեշտ է և բավարար, որ c-ն լինի α-ի արմատ, որտեղ $c \in K$:*

Ապացուցում: Անհրաժեշտություն: Եթե $\alpha = (x - c) \cdot \gamma$, ապա $\alpha(c) = (c - c) \cdot \gamma(c) = 0$:
Բավարարություն: Եթե $\alpha(c) = 0$, ապա $\alpha = (x - c)q + r$ հավասարությունից կունենանք՝ $r = \alpha(c) = 0$, այսինքն՝ $\alpha = (x - c) \cdot q$: $\square$

Թեորեմ 16.4*: Եթե K-ն ոչ զրոյական ամբողջության տիրույթ է, ապա n-րդ աստիճանի ոչ զրոյական $f \in K[x]$ բազմանդամի միմյանցից տարբեր արմատների թիվը չի գերազանցում n-ը:*

Ապացուցում: Թեորեմն ապացուցենք վերհանգման եղանակով՝ ըստ $n = deg(f) \geqslant 0$ բնական թվի: Վերհանգման հենքը $n = 0$ թիվն է, որովհետև $f = a_0 \neq 0$ բազմանդամը չունի արմատ: Ենթադրենք թե n-ից փոքր աստիճանի բոլոր բազմանդամների համար թեորեմի պնդումը ճիշտ է: Դիցուք $deg(f) = n \geqslant 1$: Եթե f-ը չունի որևէ արմատ, ապա թեորեմի պնդումը նրա համար կլինի ճիշտ: Դիցուք f բազմանդամն ունի որևէ $c_1 \in K$ արմատ: Այդ դեպքում, համաձայն Բեզուի թեորեմի, կունենանք՝

$$f = (x - c_1)q\,,$$

որտեղ $q = b_0 + b_1x + \cdots + b_{n-1}x^{n-1} \in K[x]$: Եթե $c_2 \in K$ տարրը հանդիսանում է f բազմանդամի արմատը և $c_2 \neq c_1$, ապա

$$(c_2 - c_1)q(c_2) = f(c_2) = 0 \longrightarrow q(c_2) = 0\,,$$

այսինքն՝ c_1-ից տարբեր f-ի ցանկացած արմատ հանդիսանում է արմատ նաև q բազմանդամի համար: Սակայն ըստ վերհանգման ենթադրության q-ի միմյանցից տարբեր արմատների թիվը չի գերազանցում $n-1$-ը: Հետևաբար, f-ի միմյանցից տարբեր արմատների թիվը չի գերազանցի n-ը: □

Օրինակ, $\mathbb{Z}_8(+,\cdot)$ մնացքների օղակը ամբողջության տիրույթ չէ, որովհետև հակառակ դեպքում 2 աստիճանի $f = (-1) + x^2$ բազմանդամն այդ օղակում կունենար ամենաշատը 2 արմատ: Սակայն $\mathbb{Z}_8$ օղակում $f = (-1) + x^2$ բազմանդամն ունի միմյանցից տարբեր չորս արմատ՝ $[1]$, $[3]$, $[5]$, $[7]$ (իսկ $g = x^3$ բազմանդամը՝ $[0]$, $[2]$, $[4]$, $[6]$ արմատները):

Թեորեմ 16.5 (Բազմանդամների հավասարության հայտանիշը): *Եթե K ամբողջության տիրույթը պարունակում է անվերջ թվով տարրեր և $f_1, f_2 \in K[x]$ բազմանդամների արժեքները հավասար են ցանկացած $c \in K$ տարրի համար, ապա $f_1 = f_2$, այսինքն՝ f_1, f_2 բազմանդամների համապատասխան գործակիցները կլինեն հավասար:*

Ապացուցում: Եթե $F = f_1 - f_2$ բազմանդամը ոչ զրոյական է և $n = deg(F) \geqslant 0$, ապա միմյանցից տարբեր $c_1, c_2, \ldots, c_{n+1} \in K$ տարրերի համար կունենանք՝

$$\begin{array}{l} F(c_1) = f_1(c_1) - f_2(c_1) = 0, \\ F(c_2) = f_1(c_2) - f_2(c_2) = 0, \\ \quad \ldots \quad \ldots \\ F(c_{n+1}) = f_1(c_{n+1}) - f_2(c_{n+1}) = 0, \end{array}$$

այսինքն՝ n-րդ աստիճանի ոչ զրոյական $F \in K[x]$ բազմանդամը կունենա n-ից շատ արմատներ, որը հակասում է նախորդ թեորեմին: Հետևաբար, $F = f_1 - f_2 = 0$ և $f_1 = f_2$: □

Սակայն վերջավոր ամբողջության տիրույթների (դաշտերի) համար ապացուցված հայտանիշը ճիշտ չէ: **Օրինակ,** $\mathbb{Z}_2(+,\cdot)$ դաշտում $f_1 = x$ և $f_2 = x^2$ բազմանդամների համար $f_1(c) = f_2(c)$ ցանկացած $c \in \mathbb{Z}_2$ տարրի համար, չնայած՝ $f_1 \neq f_2$: Մինչդեռ ապացուցված թեորեմից բխում է հետևյալ պնդումը:

Հետևություն 16.4: *Եթե K-ն ոչ զրոյական ամբողջության տիրույթ է, ոչ զրոյական $f_1, f_2 \in K[x]$ բազմանդամների աստիճանները $\leqslant n$ և f_1, f_2 բազմանդամները ընդունում են հավասար արժեքներ՝ K օղակի միմյանցից տարբեր $n+1$ կետերում, ապա $f_1 = f_2$:* □

Հետևյալ արդյունքն ավելի հեշտ ապացուցվում է կոմպլեքս փոփոխականի ֆունկցիաների տեսության մեջ և համարվում է հանրահաշվի հիմնական թեորեմներից մեկը, որն ապացուցվել է Գաուսի կողմից՝ 22 տարեկան հասակում: Ներկայումս հայտնի է այս դասական թեորեմի ավելի քան 100 ապացուցումներ:

Թեորեմ 16.6 (Գաուս, 1799): *Հաստատունից տարբեր կոմպլեքս գործակիցներով ցանկացած բազմանդամ ունի գոնե մեկ կոմպլեքս արմատ (այսինքն՝ կոմպլեքս թվերի $\mathbb{C}$ դաշտին պատկանող արմատ):*
□

Օգտվելով այս և Բեզուի թեորեմներից, կոմպլեքս գործակիցներով և $deg(f) \geqslant 2$ աստիճան ունեցող ցանկացած f բազմանդամ կարելի է ներկայացնել առաջին աստիճանի բազմանդամների արտադրյալի տեսքով:

Դիտողություն: Մենք K-բազմանդամի գաղափարը սահմանեցինք այն դեպքում, երբ K-ն ամբողջության տիրույթ է, այսինքն՝ զուգորդական, տեղափոխական և միավորով օղակ է, որը չունի զրոյի բաժանարարներ: Եթե $K(+,\cdot)$-ը ոչ թե ամբողջության տիրույթ է, այլ կամայական օղակ է, ապա ճիշտ նույն եղանակով կարելի է սահմանել K-բազմանդամի գաղափարը, նրա աստիճանը, ավագ անդամի գործակիցը և K-բազմանդամների գումարն ու արտադրյալը: Այս դեպքում ստացվող K-բազմանդամների օղակը կլինի.

1. միավորով օժտված այն և միայն այն դեպքում, երբ K-ն օժտված է միավորով;
2. տեղափոխական այն և միայն այն դեպքում, երբ K-ն տեղափոխական օղակ է;
3. զուգորդական այն և միայն այն դեպքում, երբ K-ն զուգորդական օղակ է;
4. ամբողջության տիրույթ այն և միայն այն դեպքում, երբ K-ն ամբողջության տիրույթ է:

Միավորով օժտված կամայական $K(+,\cdot)$ օղակի դեպքում ևս ստացվում է K-բազմանդամի սովորական (ավանդական) գրելաձևը, եթե նշանակենք՝

$$a = (a, 0, 0, \ldots), \qquad a \in K,$$

$$x^n = (\underbrace{0, \ldots, 0}_{n}, 1, 0, \ldots), \qquad n \geqslant 1:$$

Որից հետո դժվար չէ նաև նկատել, որ

$$x^i \cdot x^j = x^{i+j},$$

$$\left(x^i \cdot x^j\right) \cdot x^k = x^{i+j+k} = x^i \cdot \left(x^j \cdot x^k\right),$$

$$x^n = \underbrace{x \cdot x \cdots x}_{n},$$

$$a \cdot x^i = x^i \cdot a,$$

որտեղ $x = x^1$, $a \in K$:

Ամբողջության տիրույթի (դաշտի) վրա որոշված բազմանդամների մնացորդով բաժանման վերոհիշյալ ալգորիթմը (թեորեմ 16.2), այս ընդհանուր դեպքում, վեր է ածվում «ձախից» և «աջից» մնացորդով բաժանման հետևյալ երկու ա) և բ) ալգորիթմներին:

Թեորեմ 16.7: *Եթե $K(+,\cdot)$-ը ոչ զրոյական, միավորով օժտված և զուգորդական օղակ է, f-ը և g-ն կամայական K-բազմանդամներ են, որտեղ $g \neq 0$ և g-ի ավագ անդամի գործակիցը հակադարձելի է K-ում, ապա*

ա) գոյություն ունեն միարժեքորեն որոշվող այնպիսի q և r K-բազմանդամներ, որ

$$f = gq + r,$$

որտեղ կամ $r = 0$ կամ $deg(r) < deg(g)$;

բ) գոյություն ունեն միարժեքորեն որոշվող այնպիսի q' և r' K-բազմանդամներ, որ

$$f = q'g + r',$$

որտեղ կամ $r' = 0$ կամ $deg(r') < deg(g)$: □

Եթե միավորով օժտված և զուգորդական K օղակը լինի տեղափոխական, ապա նշված ա) և բ) ալգորիթմները կհամընկնեն:

16.3. Բազմանդամների ամենամեծ ընդհանուր բաժանարար

Դիցուք P-ն կամայական դաշտ է՝ 1 միավորով, $P[x]$-ը P դաշտից վերցրած գործակիցներով բազմանդամների բազմությունն է, իսկ $f, g \in P[x]$: Կասենք, որ f բազմանդամը **բաժանվում է** g բազմանդամի վրա, եթե գոյություն ունի այնպիսի $h \in P[x]$ բազմանդամ, որ $f = g \cdot h$: Այս դեպքում g-ն կոչվում է f-ի **բաժանարար**, իսկ f-ը **բաժանելի** կամ g-ի **բազմապատիկ** (կամ պատիկ) և այդ փաստը գրառվում է $f/_g$ կամ $_g\backslash f$ ձևով: Հակառակ դեպքում գրվում է $f\not/_g$ կամ $_g\not\backslash f$ և կարդացվում է f-ը չի բաժանվում g-ի վրա: Եթե $g \neq 0$, ապա h-ը որոշվում է միարժեքորեն և այն կոչվում է **քանորդ** ու նշանակվում է $\dfrac{f}{g}$ ձևով: Իրոք,

$$f = g \cdot h_1 = g \cdot h_2 \longrightarrow g(h_1 - h_2) = 0 \longrightarrow h_1 - h_2 = 0 \longrightarrow h_1 = h_2 :$$

$f \in P[x]$ բազմանդամը կոչվում է **հակադարձելի**, եթե այն 1-ի բաժանարար է, այսինքն՝ գոյություն ունի այնպիսի $h \in P[x]$ բազմանդամ, որ $f \cdot h = 1$: Ակնհայտ է, որ ոչ զրոյական հաստատունը հակադարձելի է, որովհետև $c \cdot c^{-1} = 1$, որտեղ $c \in P$, $c \neq 0$:

Լեմմ 16.5: *1) Զրոն բաժանվում է ցանկացած բազմանդամի վրա;*

2) Եթե $f/_g$, ապա $f{\cdot}h/_{g\cdot h}$ ցանկացած $h \in P[x]$ բազմանդամի համար;

3) Եթե $f_1/_g$ և $f_2/_g$, ապա $f_1{\pm}f_2/_g$;

4) Եթե $f/_g$ և $f \neq 0$, ապա $g \neq 0$ և $deg(f) \geqslant deg(g)$;

5) Եթե $f/_g$ և $g/_h$, ապա $f/_h$;

6) Եթե $f/_g$ և $c \in P$, $c \neq 0$, ապա $f/_{c\cdot g}$;

7) Եթե $f \in P[x]$ բազմանդամը հակադարձելի է, ապա $f = c \neq 0$, որտեղ $c \in P$;

8) Եթե $f/_g$ և $g/_f$, ապա գոյություն ունի այնպիսի $c \in P$, $c \neq 0$ տարր, որ $f = c \cdot g$:

Ապացուցում: 7) Եթե $f \cdot h = 1$, ապա $f \neq 0$ և $h \neq 0$: Դիցուք $deg\, f \neq 0$: Հետևաբար՝

$$0 = deg(1) = deg(f \cdot h) = deg(f) + deg(h) \geqslant deg(f) > 0 :$$

Ստացված հակասությունից բխում է $deg(f) = 0$ հավասարությունը, այսինքն՝ $f = c \neq 0$, որտեղ $c \in P$:

8) Եթե $f = g \cdot h_1$ և $g = f \cdot h_2$, ապա $f = fh_2h_1$ և $f(1 - h_2h_1) = 0$: Եթե $f = 0$, ապա $g = f \cdot h_2 = 0$ և $f = c \cdot g$, որովհետև $0 = c \cdot 0$ ցանկացած $c \neq 0$ և $c \in P$ տարրի համար: Եթե $1 - h_2h_1 = 0$, ապա $h_2h_1 = 1$ և h_1-ը կլինի հակադարձելի: Համաձայն 7) հատկության՝ $h_1 = c \neq 0$: Ուստի,

$$f = g \cdot h_1 = g \cdot c :$$

Մնացած հատկությունները ակնհայտ են: □

$d \in P[x]$ բազմանդամը կոչվում է $f \in P[x]$ և $g \in P[x]$ բազմանդամների **ընդհանուր բաժանարար**, եթե d-ն f-ի և g-ի բաժանարարն է, այսինքն՝ $f/_d$ և $g/_d$: f-ի և g-ի ընդհանուր բաժանարարների մեջ ամենամեծ աստիճան ունեցող ցանկացած d ոչ զրոյական բազմանդամ կոչվում է նրանց **ամենամեծ ընդհանուր բաժանարար** կամ **ընդհանուր ամենամեծ բաժանարար** և նշանակվում է $d \rightleftharpoons (f, g)$ ձևով:

Եթե $f = 0$ և $g = 0$, ապա, ակնհայտորեն, f և g բազմանդամները չունեն ամենամեծ ընդհանուր բաժանարար, իսկ մնացած դեպքերում՝ ունեն (բխում է նախորդ լեմմի 4) հատկությունից):

Լեմմ 16.6: *9) Եթե $d_1 \in P[x]$ բազմանդամը $f \in P[x]$ և $g \in P[x]$ բազմանդամների ամենամեծ ընդհանուր բաժանարարն է և $c \in P$, $c \neq 0$, ապա $d_2 = c \cdot d_1 \in P[x]$ բազմանդամը ևս կլինի այդ բազմանդամների ամենամեծ ընդհանուր բաժանարարը:*

10) Եթե $f = gq + r$, ապա f և g բազմանդամները կունենան նույն ընդհանուր բաժանարարները, ինչ որ՝ g և r բազմանդամները: Հետևաբար, f և g բազմանդամները կունենան նույն ամենամեծ ընդհանուր բաժանարարները, ինչ որ՝ g և r բազմանդամները: □

Այսպիսով տրված f և g բազմանդամների ամենամեծ ընդհանուր բաժանարարը միարժեքորեն չի որոշվում, այսինքն՝ միակը չէ:

Թեորեմ 16.8: *$f, g \in P[x]$ բազմանդամների յուրաքանչյուր d ամենամեծ ընդհանուր բաժանարար ունի հետևյալ գծային ներկայացումը՝*

$$d = fu + gv,$$

որտեղ $u, v \in P[x]$ բազմանդամները կոչվում են f, g զույգի Բեզուի գործակիցներ:

Ապացուցում: Դիտարկենք P-բազմանդամների հետևյալ բազմությունը՝

$$\langle f, g\rangle = \{ff_1 + gg_1 \mid f_1, g_1 \in P[x]\},$$

որտեղ f_1 և g_1 բազմանդամները միմյանցից անկախ փոփոխվում են բազմանդամների $P[x]$ բազմության վրա: Մասնավորապես, $f, g \in \langle f, g\rangle$: d_0-ով նշանակենք $\langle f, g\rangle$ բազմությանը պատկանող ամենափոքր աստիճան ունեցող ոչ զրոյական բազմանդամը, որի գոյությունն ակնհայտ է: Նախ ապացուցենք, որ d_0-ն տրված f և g բազմանդամների համար ամենամեծ ընդհանուր բաժանարար է: Իրոք, d_0-ն f և g բազմանդամների ընդհանուր բաժանարարն է, այսինքն՝ $f/_{d_0}$ և $g/_{d_0}$: Օրինակ, եթե

$$f = d_0q + r,$$

որտեղ $r \neq 0$, ապա $deg(r) < deg(d_0)$ և $r = f - d_0q \in \langle f, g\rangle$, որը հակասում է d_0-ի ընտրությունը: Հետևաբար, $r = 0$ և $f = d_0q$, այսինքն՝ $f/_{d_0}$: Նույն դատողություններով ստացվում է նաև $g/_{d_0}$ առնչությունը: Այժմ ապացուցենք, որ d_0-ն ունի ամենամեծ աստիճանը՝ f-ի և g-ի բոլոր ընդհանուր բաժանարարների մեջ: Քանի որ $d_0 \in \langle f, g\rangle$, ապա գոյություն ունեն այնպիսի $f', g' \in P[x]$ բազմանդամներ, որ

$$d_0 = ff' + gg' :$$

Եթե $\delta \in P[x]$ բազմանդամը f և g բազմանդամների ցանկացած ոչ զրոյական ընդհանուր բաժանարարն է, ապա այն կլինի բաժանարար նաև $ff' + gg' = d_0$ ոչ զրոյական բազմանդամի համար: Հետևաբար $deg(d_0) \geqslant deg(\delta)$ (լեմմ 16.5, հատկություն 4)):

Դիցուք d-ն f և g բազմանդամների ցանկացած ամենամեծ ընդհանուր բաժանարար է: Այդ դեպքում $d_0 = ff' + gg'$ բազմանդամը կբաժանվի d-ի վրա, այսինքն՝ $d_0 = dq'$, որտեղ $q' \in P[x]$, և քանի որ $deg(d_0) = deg(d)$, ապա $deg(q') = 0$, այսինքն՝ $q' = c \neq 0$, որտեղ $c \in P$: Այսպիսով՝

$$ff' + gg' = d_0 = d \cdot c,$$

որտեղից՝

$$d = f\left(f'c^{-1}\right) + g\left(g'c^{-1}\right) = fu + gv,$$

որտեղ $u = f'c^{-1}$ և $v = g'c^{-1}$: □

Հետևություն 16.5: *1) $f, g \in P[x]$ բազմանդամների d ընդհանուր բաժանարարը կլինի ամենամեծ ընդհանուր բաժանարար այն և միայն այն դեպքում, երբ d-ն բաժանվում է այդ բազմանդամների ցանկացած ընդհանուր բաժանարարի վրա;*

2) Եթե d-ն և d'-ը ամենամեծ ընդհանուր բաժանարարներ են f և g բազմանդամների համար, ապա գոյություն ունի այնպիսի $c \in P$, $c \neq 0$ տարր, որ $d = c \cdot d'$;

3) $\langle f, g\rangle \subseteq P[x]$ բազմության ամենափոքր աստիճանի ոչ զրոյական բազմանդամները հանդիսանում են f և g բազմանդամների ամենամեծ ընդհանուր բաժանարարները;

4) $\langle f, g\rangle \subseteq P[x]$ բազմությունը կազմված է բոլոր այն P-բազմանդամներից, որոնք հանդիսանում են f և g բազմանդամների որևէ ամենամեծ ընդհանուր բաժանարարի բազմապատիկներ: $\square$

$f, g \in P[x]$ բազմանդամները կոչվում են **զուգորդված** և գրվում է $f \sim g$, եթե գոյություն ունի այնպիսի $c \in P$, $c \neq 0$ տարր, որ $f = c \cdot g$: Հակառակ դեպքում f, g բազմանդամները կոչվում են **չզուգորդված** կամ **ոչ զուգորդված**: Օրինակ, եթե f-ը բաժանվում է g-ի վրա, իսկ g-ն բաժանվում է f-ի վրա, ապա $f \sim g$ (բխում է լեմմ 16.5-ի 8)-րդ հատկությունից):

Սահմանված «$\sim$» հարաբերությունը կոչվում է **P-բազմանդամների զուգորդման հարաբերություն**:

Լեմմ 16.7: *P-բազմանդամների զուգորդման հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $f \sim f$ ցանկացած $f \in P[x]$ բազմանդամի համար;

բ) $f \sim g \longrightarrow g \sim f$;

գ) $f \sim g, g \sim h \longrightarrow f \sim h$:

Ապացուցում: ա) Բխում է $f = 1 \cdot f$ հավասարությունից:
բ) Եթե $f = c \cdot g$, որտեղ $c \in P$ և $c \neq 0$, ապա $g = c^{-1} \cdot f$:
գ) Եթե $f = c_1 \cdot g$ և $g = c_2 \cdot h$, որտեղ $c_1, c_2 \in P$ և $c_1 \neq 0$, $c_2 \neq 0$, ապա $f = c_1 c_2 \cdot h$, որտեղ $c_1 \cdot c_2 \in P$ և $c_1 \cdot c_2 \neq 0$: $\square$

Ելնելով P-բազմանդամների զուգորդման հարաբերությունից, կարելի է այժմ ասել, որ $f, g \in P[x]$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը P-բազմանդամների զուգորդման (հարաբերության) ճշտությամբ որոշվում է միարժեքորեն, որովհետև

Ա) $d \rightleftharpoons (f, g)$, $d' \sim d \longrightarrow d' \rightleftharpoons (f, g)$, Բ) $d \rightleftharpoons (f,g)$, $d' \rightleftharpoons (f,g) \longrightarrow d' \sim d$:

Բազմանդամների համար կրկնելով երկու ամբողջ թվերի ամենամեծ ընդհամնուր բաժանարարը գտնելու Էվկլիդեսի հայտնի ալգորիթմը, ստանում ենք $f,g \in P[x]$ ոչ զրոյական բազմանդամների ամենամեծ ընդհանուր բաժանարարը և այդ բազմանդամների Բեզուի գործակիցները գտնելու (որոշելու) ալգորիթմներ:

Էվկլիդեսի ալգորիթմը բազմանդամների համար: *Ելնելով բազմանդամների մնացորդով բաժանման ալգորիթմից, կստանանք՝*

$$\begin{array}{ll} f = q_1 g + r_1, & r_1 \neq 0, \\ g = q_2 r_1 + r_2, & r_2 \neq 0, \\ r_1 = q_3 r_2 + r_3, & r_3 \neq 0, \\ \quad \cdots \quad \cdots & \quad \cdots \\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, & r_{n-1} \neq 0, \\ r_{n-2} = q_n r_{n-1} + r_n, & r_n \neq 0, \\ r_{n-1} = q_{n+1} r_n + r_{n+1}, & r_{n+1} = 0; \end{array}$$

Հետևաբար՝ $r_n \rightleftharpoons (f,g)$*:*

Ապացույց: Քանի որ $deg(g) > deg(r_1) > deg(r_2) > deg(r_3) > \cdots$, ապա վերջավոր թվով քայլերից հետո կստացվի զրոյական մնացորդ՝ $r_{n+1} = 0$: Այդ դեպքում պնդվում է, որ $r_n \rightleftharpoons (f,g)$: Իրոք, նշված հավասարություններով ներքևից վերև շարժվելով նկատում ենք, որ r_n-ը g-ի և f-ի ընդհանուր բաժանարարն է, իսկ՝ վերևից ներքև շարժվելով նկատում ենք, որ եթե h-ը f-ի և g-ի ընդհանուր բաժանարարն է, ապա այն կլինի բաժանարար նաև ցանկացած r_i բազմանդամի համար, մասնավորապես նաև r_n-ի համար: Հետևաբար, r_n-ը f, g բազմանդամների բոլոր ընդհանուր բաժանարարների մեջ ունի ամենամեծ աստիճանը, այսինքն՝ $r_n \rightleftharpoons (f,g)$: Այնուհետև,

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} = \\ &= r_{n-2} - q_n \left(r_{n-3} - q_{n-1} r_{n-2}\right) = \\ &= \left(1 + q_{n-1}\right) r_{n-2} - q_n r_{n-3} = \\ &= \left(1 + q_{n-1}\right)\left(r_{n-4} - q_{n-2} r_{n-3}\right) - q_n r_{n-3} = \\ &= \left(1 + q_{n-1}\right) r_{n-4} - \left[\left(1 + q_{n-1}\right) q_{n-2} + q_n\right] r_{n-3} = \\ &\cdots \quad \cdots \quad \cdots \\ &= fu + gv : \end{aligned}$$

$\square$

Թեորեմ 16.9 (էվկլիդես): *Եթե P-ն դաշտ է, ապա գոյություն ունեն ալգորիթմներ, որոնցով կարելի է հաշվել ցանկացած երկու P-բազմանդամների ամենամեծ ընդհանուր բաժանարարը և դրանց Բեզուի գործակիցները:* □

Բազմանդամների էվկլիդեսի ալգորիթմը տալիս է մեկ լրացուցիչ և օգտակար արդյունք ևս, որի ձևակերպման համար նախ պայմանավորվենք հետևյալ անվանման մեջ: Եթե $d, f, g \in P[x]$ և $d \rightleftharpoons (f, g)$, ապա d բազմանդամը կոչվում է նաև f, g բազմանդամների ամենամեծ ընդհանուր բաժանարար P դաշտի նկատմամբ:

Հետևություն 16.6: *Դիցուք P-ն դաշտ է, $d, f, g \in P[x]$ և $d \rightleftharpoons (f, g)$: Եթե P' դաշտը P դաշտի ընդլայնումն է, ապա d-ն կլինի f, g բազմանդամների ամենամեծ ընդհանուր բաժանարարը նաև P' դաշտի նկատմամբ:*

Ապացուցում: Բխում է երկու բազմանդամների ամենամեծ ընդհանուր բաժանարարի որոշման էվկլիդեսի ալգորիթմից: Իրոք, գրելով f, g բազմանդամների համար էվկլիդեսի ալգորիթմի առաջին հավասարությունը $P[x]$-ում, կունենանք՝

$$f = q_1 g + r_1,$$

որտեղ $q_1, r_1 \in P[x]$, իսկ $P'[x]$-ում՝

$$f = q_1' g + r_1',$$

որտեղ $q_1', r_1' \in P'[x]$: Սակայն $f = q_1 g + r_1$ հավասարությունը տեղի ունի նաև $P'[x]$-ում, որովհետև $P \leqslant P'$, հետևաբար բազմանդամների մնացորդով բաժանման թեորեմի միակության մասի համաձայն՝ $q_1' = q_1$ և $r_1' = r$: Այսպիսով, f, g բազմանդամների համար էվկլիդեսի ալգորիթմի հավասարությունների համակարգերը գրված $P[x]$-ում և $P'[x]$-ում ստացվում են նույնը: □

Դիցուք $n \in \mathbb{N}$ և $n \geqslant 2$: $d \in P[x]$ բազմանդամը կոչվում է $f_1, f_2, \ldots, f_n \in P[x]$ բազմանդամների ընդհանուր բաժանարար, եթե d-ն $f_1, f_2, \ldots, f_n$ բազմանդամների բաժանարարն է, այսինքն՝ $f_1\big/d$, $f_2\big/d$, ... $f_n\big/d$: $f_1, f_2, \ldots, f_n$ բազմանդամների ընդհանուր բաժանարարների մեջ ամենամեծ աստիճան ունեցող d ոչ զրոյական բազմանդամը կոչվում է նրանց ամենամեծ ընդհանուր բաժանարար և նշանակվում է $d \rightleftharpoons (f_1, f_2, \ldots, f_n)$ ձևով:

Երկու բազմանդամների ամենամեծ ընդհանուր բաժանարարների վերաբերյալ ապացուցված բոլոր արդյունքները հեշտությամբ տարածվում են n բազմանդամների ամենամեծ ընդհանուր բաժանարարների վրա: Որպես օրինակ ձևակերպենք հետևյալ արդյունքը:

Թեորեմ 16.10: $f_1, f_2, \ldots, f_n \in P[x]$ *բազմանդամների յուրաքանչյուր* d *ամենամեծ ընդհանուր բաժանարարի համար գոյություն ունեն այնպիսի* $u_1, u_2, \ldots, u_n \in P[x]$ *բազմանդամներ, որ*

$$d = f_1u_1 + f_2u_2 + \cdots + f_nu_n,$$

որտեղ $u_1, u_2, \ldots, u_n$ *բազմանդամները կոչվում են* $f_1, f_2, \ldots, f_n$ *բազմանդամների Բեզուի գործակիցներ:* $\square$

Վերջավոր թվով բազմանդամների ամենամեծ ընդհանուր բաժանարարները գտնելու խնդիրը հանգում է երկու բազմանդամների դեպքին, որովհետև վերհանգման եղանակով դժվար չէ նկատել, որ $n \geqslant 3$ դեպքում՝

$$d \rightleftharpoons (f_1, f_2, \ldots, f_n) \longleftrightarrow$$

$$d \rightleftharpoons ((f_1, f_2, \ldots, f_{n-1}), f_n) \longleftrightarrow d \rightleftharpoons (\ldots((f_1, f_2), f_3)\ldots, f_n):$$

16.4. Փոխդարձաբար պարզ բազմանդամներ

Շարունակում ենք դիտարկել բազմանդամներ՝ որոշված կամայական P դաշտի վրա, որի տարրերը կոչվում են նաև հաստատուններ:

Երկու $f, g \in P[x]$ բազմանդամներ կոչվում են **փոխադարձաբար պարզ** և գրվում է $(f, g) = 1$ կամ $f \perp g$, եթե նրանց բոլոր ամենամեծ ընդհանուր բաժանարարները ոչ զրոյական հաստատուններ են: Հետևաբար, այդպիսի բազմանդամների բոլոր ընդհանուր բաժանարարները ևս կլինեն ոչ զրոյական հաստատուններ: Իհարկե, սահմանման մեջ բավական է պահանջել, որ f, g բազմանդամների որևէ ամենամեծ ընդհանուր բաժանարար լինի հավասար ոչ զրոյական հաստատունի (օրինակ 1-ի): Հակառակ դեպքում կգրենք՝ $(f, g) \neq 1$:

Հետևություն 16.6-ից բխում է, որ $f, g \in P[x]$ բազմանդամների փոխադարձաբար պարզության հատկությունը պահպանվում է P դաշտի ընդլայնման ժամանակ:

Թեորեմ 16.11 (բազմանդամների փոխադարձաբար պարզության հայտանիշը): *Որպեսզի $f, g \in P[x]$ բազմանդամները լինեն փոխադարձաբար պարզ անհրաժեշտ է և բավարար, որ գոյություն ունենան այնպիսի $f', g' \in P[x]$ բազմանդամներ, որ*

$$ff' + gg' = 1 :$$

Ապացուցում: Բավարարություն: Եթե $ff' + gg' = 1$, ապա f և g բազմանդամների ցանկացած ընդհանուր բաժանարար կլինի հակադարձելի $P[x]$ օղակում և, հետևաբար կլինի հավասար ոչ զրոյական $c \in P$ հաստատունի:

Անհրաժեշտություն: Եթե $(f, g) = 1$, ապա, համաձայն թեորեմ 16.8-ի,

$$c = fu + gv, \quad \text{որտեղ} \quad c \in P,\ c \neq 0 :$$

Հետևաբար,

$$cc^{-1} = f\left(uc^{-1}\right) + g\left(vc^{-1}\right) ,$$

այսինքն՝

$$1 = ff' + gg' ,$$

որտեղ $f' = uc^{-1} \in P[x]$, $g' = vc^{-1} \in P[x]$: □

Հետևություն 16.7 Եթե $d \rightleftharpoons (f, g)$, ապա $\dfrac{f}{d}$ և $\dfrac{g}{d}$ բազմանդամները կլինեն փոխադարձաբար պարզ: □

Թեորեմ 16.12: *Եթե բազմանդամների $f_1 f_2$ արտադրյալը բաժանվում է f_3 բազմանդամի վրա և $(f_1, f_3) = 1$, ապա f_2 բազմանդամը բաժանվում է f_3-ի վրա:*

Ապացուցում: Բազմանդամների փոխադարձաբար պարզության հայտանիշի համաձայն, գոյություն ունեն այնպիսի f_1' և f_3' բազմանդամներ, որ $f_1 f_1' + f_3 f_3' = 1$: Հավասարության երկու մասերը բազմապատկելով f_2-ով կստանանք՝

$$f_1 f_2 f_1' + f_3 f_2 f_3' = f_2,$$

որտեղ երկրորդ գումարելին ակնհայտորեն բաժանվում է f_3-ի վրա, իսկ առաջին գումարելին բաժանվում է f_3-ի վրա՝ համաձայն տրված պայմանի: Հետևաբար, դրանց f_2 գումարը ևս կբաժանվի f_3-ի վրա: □

Թեորեմ 16.13: *Եթե f բազմանդամը բաժանվում է g_1 և g_2 փոխադարձաբար պարզ բազմանդամներից յուրաքանչյուրի վրա, ապա f-ը կբաժանվի նաև դրանց $g_1 \cdot g_2$ արտադրյալի վրա:*

Ապացույց: Ըստ պայմանի՝ $f = g_1q_1$ և $f = g_2q_2$: Հետևաբար, $g_1q_1 = g_2q_2$, որտեղ $(g_1, g_2) = 1$: Համաձայն նախորդ թեորեմի՝ q_1-ը կբաժանվի g_2-ի վրա, այսինքն՝ $q_1 = g_2q_3$: Ուստի,

$$f = g_1 \cdot q_1 = g_1(g_2q_3) = (g_1g_2)q_3 :$$ □

Հատկություն 16.1: *Եթե f_1 և f_2 բազմանդամները փոխադարձաբար պարզ են g բազմանդամի հետ, ապա դրանց $f_1 \cdot f_2$ արտադրյալը ևս կլինի փոխադարձաբար պարզ g-ի հետ:*

Ապացույց: Բազմանդամների փոխադարձաբար պարզության հայտանիշի համաձայն, գոյություն ունեն այնպիսի f_1', f_2', g' և g'' բազմանդամներ, որ

$$f_1f_1' + gg' = 1,$$
$$f_2f_2' + gg'' = 1 :$$

Հետևաբար,

$$1 = 1 \cdot 1 = (f_1f_1' + gg')\,(f_2f_2' + gg'') =$$
$$= f_1f_2\,(f_1'f_2') + g\,(g'f_2f_2' + g'gg'' + f_1f_1'g'') :$$

Մնում է օգտվել բազմանդամների փոխադարձաբար պարզության հայտանիշից: □

Հատկություն 16.2: *Եթե $f_1, f_2, \ldots, f_n$ բազմանդամներից յուրաքանչյուրը փոխադարձաբար պարզ է g բազմանդամի հետ, ապա դրանց $f_1 \cdot f_2 \cdots f_n$ արտադրյալը ևս կլինի փոխադարձաբար պարզ g-ի հետ:*

Ապացույց: Վերհանգման եղանակով: □

Հատկություն 16.3: *Եթե $f_1, f_2, \ldots, f_n$ բազմանդամներից յուրաքանչյուրը փոխադարձաբար պարզ է $g_1, g_2, \ldots, g_m$ բազմանդամներից յուրաքանչյուրի հետ, ապա $f_1 \cdot f_2 \cdots f_n$ արտադրյալը կլինի փոխադարձաբար պարզ $g_1 \cdot g_2 \cdots g_m$ արտադրյալի հետ:*

Ապացույց: Ըստ նախորդ հատկության $f_1 \cdot f_2 \cdots f_n$ արտադրյալը կլինի փոխադարձաբար պարզ $g_1, g_2, \ldots, g_m$ բազմանդամներից յուրաքանչյուրի հետ: Հետևաբար, նույն պատճառով, $f_1 \cdot f_2 \cdots f_n$ արտադրյալը կլինի փոխադարձաբար պարզ նաև $g_1 \cdot g_2 \cdots g_m$ արտադրյալի հետ: □

Հետևություն 16.8 Եթե f և g բազմանդամները փոխադարձաբար պարզ են, ապա f^n և g^m բազմանդամները ևս կլինեն փոխադարձաբար պարզ՝ ցանկացած $m, n \geqslant 1$ բնական թվերի համար:

Ապացույց: Բխում է նախորդ հատկությունից, եթե $f_1 = f_2 = \cdots = f_n = f$ և $g_1 = g_2 = \cdots = g_n = g$ դեպքում: □

Հատկություն 16.4: *Եթե f բազմանդամը բաժանվում է զույգ առ զույգ փոխադարձաբար պարզ $g_1, g_2, \ldots, g_m$ բազմանդամներից յուրաքանչյուրի վրա, ապա f-ը կբաժանվի նաև դրանց $g_1 \cdot g_2 \cdots g_m$ արտադրյալի վրա:*

Ապացույց: Վերհանգման եղանակով: □

Հատկություն 16.5: *Եթե $f, g \in P[x]$ բազմանդամները փոխադարձաբար պարզ են, ապա դրանք չունեն ընդհանուր արմատ ինչպես P դաշտում, այնպես էլ P դաշտի ցանկացած P' ընդլայնման մեջ:*

Ապացույց: Հատկության մի ապացույցը բխում է Բեզուի թեորեմից: Բերենք նաև հետևյալ ապացույցը:

Դիցուք $x_0 \in P$ տարրը f և g բազմանդամների ընդհանուր արմատն է, այսինքն՝ $f(x_0) = g(x_0) = 0$: Քանի որ $(f, g) = 1$, ապա գոյություն ունեն այնպիսի $f', g' \in P[x]$ բազանդամներ, որ

$$ff' + gg' = 1 \ :$$

Հետևաբար,

$$f(x_0)f'(x_0) + g(x_0)g'(x_0) = 1\,,$$

այսինքն՝ $0 = 1$: Հակասություն:

Նույն ապացույցը կարելի է կրկնել P դաշտի ցանկացած P' ընդլայնման համար: □

Վերջավոր թվով $f_1, \ldots, f_n \in P[x]$ բազմանդամները $(n \geqslant 2)$ կոչվում են **փոխադարձաբար պարզ**, եթե $1 \rightleftharpoons (f_1, \ldots, f_n)$: Երկու փոխադարձաբար պարզ բազմանդամների վերաբերյալ ապացուցված հիմնական արդյունքները տարածվում են այս ընդհանուր դեպքի վրա:

16.5. Չբերվող (պարզ) բազմանդամներ

Չբերվող բազմանդամի գաղափարը հանդիսանում է պարզ թվի հասկացության նմանակը բազմանդամների մեջ:

Հաստատունից տարբեր $f \in P[x]$ բազմանդամը կոչվում է **չբերվող** կամ **պարզ** P դաշտում (կամ P դաշտի նկատմամբ), եթե f-ը չի բաժանվում այնպիսի ոչ զրոյական $g \in P[x]$ բազմանդամի վրա, որի համար $0 < deg(g) < deg(f)$: Հակառակ դեպքում հաստատունից տարբեր $f \in P[x]$ բազմանդամը կոչվում է **բերվող** P դաշտում (կամ P դաշտի նկատմամբ): Այսպիսով հաստատունը չի համարվում բերվող կամ չբերվող բազմանդամ:

Օրինակներ: 1) $f = 1 + x^2$ բազմանդամը բերվող է $\mathbb{Z}_2$ դաշտում (որովհետև $\mathbb{Z}_2$-ում՝ $1 + x^2 = (1 + x)^2$), սակայն չբերվող է իրական թվերի $\mathbb{R}$ դաշտում (որովհետև չունի արմատ $\mathbb{R}$-ում):
2) $f = x^2 - 2$ բազմանդամը չբերվող է ռացիոնալ թվերի $\mathbb{Q}$ դաշտում (որովհետև չունի ռացիոնալ արմատ), սակայն բերվող է իրական թվերի $\mathbb{R}$ դաշտում, որովհետև $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$:
3) 1-ից մեծ աստիճան ունեցող և կոմպլեքս գործակիցներով ցանկացած f բազմանդամ բերվող է կոմպլեքս թվերի $\mathbb{C}$ դաշտում (բխում է Գաուսի թեորեմից (թեորեմ 16.6)):

Լեմմ 16.8: *1) Եթե $deg(f) = 1$, ապա $f \in P[x]$ բազմանդամը չբերվող է P դաշտում;*
2) Եթե $f \in P[x]$ բազմանդամը չբերվող (բերվող) է P դաշտում և $\lambda \in P$, $\lambda \neq 0$, ապա $\lambda f \in P[x]$ բազմանդամը ևս կլինի չբերվող (բերվող) P դաշտում;
3) P դաշտում արմատ ունեցող և $deg(f) \geqslant 2$ աստիճանի ցանկացած $f \in P[x]$ բազմանդամ բերվող է P-ում (բխում է Բեզուի թեորեմից);
4) Հաստատունից տարբեր $f \in P[x]$ բազմանդամը կլինի բերվող այն և միայն այն դեպքում, երբ դրան կարելի է ներկայացնել երկու այնպիսի բազմանդամների արտադրյալի տեսքով, որոնց աստիճանները խիստ փոքր են $deg(f)$-ից;
5) Հաստատունից տարբեր $f \in P[x]$ բազմանդամը կլինի չբերվող այն և միայն այն դեպքում, երբ

$$f = g \cdot h \longrightarrow deg(g) = 0 \quad \text{կամ} \quad deg(h) = 0\,,$$

որտեղ $g, h \in P[x]$: □

Հատկություն 16.6: *Որպեսզի 2 կամ 3 աստիճան ունեցող $f \in P[x]$ բազմանդամը լինի չբերվող P դաշտում անհրաժեշտ է և բավարար, որ այն չունենա արմատ P դաշտում:*

Ապացույց: Նկատենք, որ 2 կամ 3 աստիճան ունեցող $f \in P[x]$ բազմանդամը կլինի բերվող այն և միայն այն դեպքում, երբ f-ը բաժանվում է առաջին աստիճանի որևէ $g \in P[x]$ բազմանդամի վրա: Հետևաբար, այդպիսի f բազմանդամը կլինի բերվող այն և միայն այն դեպքում, երբ f-ը ունի արմատ P դաշտում (որովհետև առաջին աստիճանի $g \in P[x]$ բազմանդամը միշտ ունի $c \in P$ արմատ): □

Օրինակ, x^2+x+1, x^3+x+1, x^3+x^2+1 բազմանդամները չբերվող են $P=\mathbb{Z}_2$ դաշտում, որովհետև նրանք չունեն արմատ $\mathbb{Z}_2$-ում: Սակայն

$$f = \left(x^2+x+1\right)^2 = x^4+x^2+1\,,$$

$$g = \left(x^2+x+1\right)\left(x^3+x+1\right)$$

բազմանդամները լինելով բերվող $P=\mathbb{Z}_2$ դաշտում, չունեն արմատ $\mathbb{Z}_2$ դաշտում, այսինքն՝ ապացուցված հատկությունը տեղի չունի $n \geqslant 4$ աստիճան ունեցող բազմանդամների համար: x^2+1, x^2+x-1, x^2-x-1, x^2-x+1, x^3+x^2-x+1, x^3-x^2+1, x^3+x^2+x-1, x^3-x^2-x-1 բազմանդամները չբերվող են $P=\mathbb{Z}_3$ դաշտում, որովհետև դրանք չունեն արմատ $\mathbb{Z}_3$-ում:

Օգտվելով Գաուսի թեորեմից կարելի է բնութագրել նաև բոլոր իրական գործակիցներով չբերվող բազմանդամները՝ իրական թվերի $\mathbb{R}$ դաշտում:

Թեորեմ 16.14: *Իրական թվերի $\mathbb{R}$ դաշտի նկատմամբ չբերվող բազմանդամներ են հանդիսանում իրական գործակիցներով բոլոր առաջին աստիճանի բազմանդամները, բոլոր երկրորդ աստիճանի բացասական դիսկրիմինանտով բազմանդամները և միայն դրանք:*

Ապացույց: Ակնհայտ է, որ նշված բազմանդամները չբերվող են $\mathbb{R}$-ում: Ապացուցենք, որ $\mathbb{R}$-ում ուրիշ չբերվող բազմանդամներ չկան:

Դիցուք $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{R}[x]$ բազմանդամը $n > 1$ աստիճանի չբերվող բազմանդամ է $\mathbb{R}$-ում: Այդ դեպքում f-ը չունի արմատ $\mathbb{R}$-ում (լեմմ 16.9), սակայն թեորեմ 16.6-ի համաձայն, f-ը կունենա $\alpha = a+bi \in \mathbb{C}$ կոմպլեքս արմատ, որտեղ $b \neq 0$: Հետևաբար,

α կոմպլեքս թվի $\overline{\alpha} \in \mathbb{C}$ համալուծը ևս կլինի արմատ f-ի համար, որովհետև

$$f\left(\overline{\alpha}\right) = a_0 + a_1\overline{\alpha} + \cdots + a_n\left(\overline{\alpha}\right)^n = \overline{a}_0 + \overline{a}_1\overline{\alpha} + \cdots + \overline{a}_n\overline{\left(\alpha^n\right)} =$$

$$= \overline{a}_0 + \overline{a_1\alpha} + \cdots + \overline{a_n\alpha^n} = \overline{a_0 + a_1\alpha + \cdots + a_n\alpha^n} = \overline{f\left(\alpha\right)} = \overline{0} = 0 :$$

Ըստ Բեզուի թեորեմի, f-ը կբաժանվի $x-\alpha$ և $x-\overline{\alpha}$ բազմանդամների վրա, որոնք փոխադարձաբար պարզ են: Հետևաբար, համաձայն թեորեմ 16.13-ի, f-ը $\mathbb{C}$-ում կբաժանվի նաև դրանց $\varphi = (x-\alpha)(x-\overline{\alpha}) = x^2 - (\alpha+\overline{\alpha})x + \alpha\overline{\alpha}$ արտադրյալի վրա, որտեղ $\alpha+\overline{\alpha} = 2a$, $\alpha\overline{\alpha} = a^2+b^2 \in \mathbb{R}$, այսինքն՝ $\varphi \in \mathbb{R}[x]$: Քանի որ $f = \varphi \cdot q$, որտեղ $q \in \mathbb{C}[x]$, ապա $q \in \mathbb{R}[x]$ (հետևություն 16.2):

Եթե այժմ $n > 2$, ապա f-ը կլինի բերվող $\mathbb{R}$-ում, քանի որ $deg(\varphi) = 2$: Հետևաբար, $n = 2$ և $deg(q) = 0$, այսինքն՝ $q = c \in \mathbb{R}$, $c \neq 0$, և

$$f = \varphi \cdot c = cx^2 - c\left(\alpha+\overline{\alpha}\right)x + c\alpha\overline{\alpha} = cx^2 - 2cax + ca^2 + cb^2 \ :$$

Մնում է հաշվել f-ի դիսկրիմինանտը՝ $D(f) = -4c^2b^2 < 0$: □

Հետևություն 16.9: *Կենտ աստիճան ունեցող իրական գործակիցներով ցանկացած բազմանդամ ունի գոնե մեկ իրական արմատ:*

Ապացուցում: Վերհանգման եղանակով՝ ըստ բազմանդամի $n = 2k+1$ աստիճանի: Եթե $n = 1$, ապա պնդումն ակնհայտ է: Ենթադրենք, թե n-ից փոքր կենտ աստիճան ունեցող բոլոր իրական գործակիցներով բազմանդամների համար պնդումը ճիշտ է և $deg(f) = n = 2k+1 \geqslant 3$: Ըստ նախորդ թեորեմի, f-ը կլինի բերվող և, հետևաբար, $f = f_1 \cdot f_2$, որտեղ $deg(f_1) < n$, $deg(f_2) < n$, և f_1, f_2 բազմանդամներից մեկի (դիցուք f_1-ի) աստիճանը կլինի կենտ: Ուստի, համաձայն վերհանգային ենթադրության, f_1-ը կունենա $x_0 \in \mathbb{R}$ իրական արմատ, որը կլինի արմատ նաև f-ի համար, որովհետև $f(x_0) = f_1(x_0) \cdot f_2(x_0) = 0 \cdot f_2(x_0) = 0$: □

Այս արդյունքը կարելի է բխեցնել նաև հաջորդ թեորեմից, այսինքն՝ թեորեմ 16.15-ից: Իրոք, $deg(f) \geqslant 3$ կենտ աստիճան ունեցող իրական գործակիցներով f բազմանդամը, այդ թեորեմի համաձայն, վերլուծվում է չբերվող բազմանդամների արտադրյալի՝

$$f = f_1 \cdot f_2 \cdots f_k \ ,$$

որտեղ $f_1, f_2, \ldots, f_k$ չբերվող բազմանդամները, թեորեմ 16.14-ի համաձայն, կամ առաջին կամ երկրորդ աստիճանի բազմանդամներ են: Սակայն, քանի որ f-ի աստիճանը կենտ թիվ է, ապա $f_1, f_2, \ldots, f_k$ բազմանդամների շարքում գոյություն կունենա գոնե մեկ առաջին աստիճանի բազմանդամ, որի իրական արմատն էլ հենց կլինի արմատ նաև f-ի համար, որովհետև $f(x_0) = f_1(x_0) \cdot f_2(x_0) \cdots f_k(x_0)$:

Մաթեմատիկական անալիզի դասընթացում հետևություն 16.9-ը բխեցվում է Բոլցանո–Կոշիի միջանկյալ արժեքի թեորեմից: Իրոք, եթե $f \in \mathbb{R}[x]$ բազմանդամի աստիճանը կենտ թիվ է և նրա ավագ անդամի գործակիցը դրական է, ապա

$$\lim_{x\to+\infty} f(x) = +\infty, \qquad \lim_{x\to-\infty} f(x) = -\infty :$$

Հետևաբար, գոյություն կունենան այնպիսի $a < b$ իրական թվեր, որ $f(a) < 0 < f(b)$ և, Բոլցանո–Կոշիի միջանկյալ արժեքի թեորեմի համաձայն, գոյություն կունենա այնպիսի $c \in (a,b)$ իրական թիվ, որ $f(c) = 0$ (որովհետև բազմանդամն անընդհատ ֆունկցիա է):

Ավելի բարդ է ռացիոնալ թվերի $\mathbb{Q}$ դաշտում չբերվող բազմանդամների նկարագրության խնդիրը: Կարելի է ապացուցել, որ ցանկացած $n \geqslant 1$ բնական թվի համար գոյություն ունի ռացիոնալ թվերի $\mathbb{Q}$ դաշտում չբերվող n-րդ աստիճանի բազմանդամ: Օրինակ, այդպիսին է

$$f = x^n - p$$

բազմանդամը, որտեղ p-ն պարզ թիվ է (էյզենշտեյն): Սակայն մինչ այժմ ռացիոնալ թվերի $\mathbb{Q}$ դաշտի նկատմամբ չբերվող բոլոր բազմանդամների նկարագրությունը հայտնի չէ:

Շատ ավելի բարդ է վերջավոր դաշտերում բոլոր չբերվող բազմանդամների բնութագրման խնդիրը: Այստեղ ևս կարելի է ապացուցել, որ ցանկացած $n \geqslant 1$ բնական թվի համար գոյություն ունի վերջավոր դաշտում չբերվող n-րդ աստիճանի բազմանդամ (թեորեմ 19.5): Սակայն ընդհանուր խնդրի լուծումը բաց է նաև այս կարևոր դեպքում:

Հատկություն 16.7 *Եթե $f \in P[x]$ և φ բազմանդամը չբերվող է P դաշտում, ապա կամ f-ը բաժանվում է φ-ի վրա կամ $(f, \varphi) = 1$:*

Ապացուցում: Դիցուք $d \rightleftharpoons (f, \varphi)$ և $\varphi = d \cdot q_1$, $f = d \cdot q_2$: Քանի որ φ-ն չբերվող է, ապա կամ $deg(d) = 0$ կամ $deg(q_1) = 0$: Առաջին դեպքում՝

$d = c \neq 0$, $c \in P$ և $(f, \varphi) = 1$: Երկրորդ դեպքում՝ $q_1 = c \neq 0$, $c \in P$ և $d = \varphi \cdot c^{-1}$, $f = d \cdot q_2 = \varphi\left(c^{-1} \cdot q_2\right)$, այսինքն՝ f-ը բաժանվում է φ-ի վրա:
□

Հատկություն 16.8: *Եթե $\varphi_1, \varphi_2 \in P[x]$ բազմանդամները չբերվող են P դաշտում, ապա կամ $(\varphi_1, \varphi_2) = 1$ կամ $\varphi_1 = \varphi_2 \cdot c$, որտեղ $c \in P$, $c \neq 0$ (այսինքն՝ φ_1, φ_2 բազմանդամները զուգորդված են): Մասնավորապես, եթե φ_1, φ_2 չբերվող բազմանդամները ունեն ընդհանուր արմատ P դաշտի որևէ P' ընդլայնման մեջ, ապա նրանք զուգորդված են:*

Ապացույց: Նախորդ հատկության համաձայն, եթե $(\varphi_1, \varphi_2) \neq 1$, ապա φ_1-ը կբաժանվի φ_2-ի վրա՝ $\varphi_1 = \varphi_2 \cdot q$: Այստեղից, քանի որ φ_1-ը չբերվող է, կստանանք $q = c \in P$, $c \neq 0$: Մնում է օգտվել հատկություն 16.5-ից:
□

Հատկություն 16.9: *Եթե բազմանդամների $f_1 \cdot f_2$ արտադրյալը բաժանվում է φ չբերվող բազմանդամի վրա, ապա f_1, f_2 արտադրիչներից գոնե մեկը կբաժանվի φ-ի վրա:*

Ապացույց: Կամ f_1-ը բաժանվում է φ-ի վրա կամ $(f_1, \varphi) = 1$ (հատկություն 16.7): Երկրորդ դեպքում f_2-ը կբաժանվի φ-ի վրա՝ համաձայն թեորեմ 16.12-ի: □

Հատկություն 16.10: *Եթե վերջավոր թվով բազմանդամների $f_1 \cdot f_2 \cdots f_n$ արտադրյալը բաժանվում է φ չբերվող բազմանդամի վրա, ապա $f_1, f_2, \ldots, f_n$ արտադրիչներից գոնե մեկը կբաժանվի φ-ի վրա:*

Ապացույց: Վերհանգման եղանակով: □

Հատկություն 16.11: *Եթե P' դաշտը P դաշտի ընդլայնումն է և $f \in P[x]$ բազմանդամն ու P դաշտի նկատմամբ չբերվող $\varphi \in P[x]$ բազմանդամն ունեն ընդհանուր $x_0 \in P'$ արմատ, ապա f-ը բաժանվում է φ-ի վրա:*

Ապացույց: $f, \varphi \in P'[x]$ բազմանդամները փոխադարձաբար պարզ չեն, որովհետև երկուսն էլ, ըստ Բեզուի թեորեմի, բաժանվում են $x - x_0 \in P'[x]$ բազմանդամի վրա: Հետևաբար, համաձայն հատկություն 16.7-ի, f-ը կբաժանվի φ-ի վրա: □

Լեմմ 16.9: *Հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամ բաժանվում է P դաշտի նկատմամբ չբերվող որևէ $\varphi \in P[x]$ բազմանդամի վրա:*

Ապացույց: Որպես φ կարելի է վերցնել f-ի ամենափոքր դրական աստիճան ունեցող որևէ բաժանարար, որի գոյությունն ակնհայտ է: □

Հատկություն 16.12: *Կամայական P դաշտի նկատմամբ չբերվող բազմանդամների քանակն անվերջ է:*

Ապացույց (էվկլիդես): Դիցուք որևէ P դաշտի նկատմամբ չբերվող բազմանդամների քանակը վերջավոր է և դիցուք դրանք են $\varphi_1, \varphi_2, \ldots, \varphi_n$ բազմանդամները: Դիտարկենք

$$f = \varphi_1 \cdot \varphi_2 \cdots \varphi_n + 1$$

բազմանդամը, որտեղ 1-ը P դաշտի միավորն է: Քանի որ f-ը հաստատունից տարբեր է, ապա, նախորդ լեմմի համաձայն, f-ը կբաժանվի P-ի նկատմամբ չբերվող որևէ $\varphi \in P[x]$ բազմանդամի վրա: Մնում է նկատել, որ $\varphi \neq \varphi_1, \varphi_2, \ldots, \varphi_n$: Հակասություն: □

Հետևություն 16.10: *Եթե P դաշտը վերջավոր է, ապա ցանկացած m բնական թվի համար գոյություն կունենա P-ի նկատմամբ չբերվող և $n \geqslant m$ աստիճան ունեցող բազմանդամ, այսինքն՝ այս դեպքում, չբերվող բազմանդամների աստիճանների բազմությունը սահմանափակ չէ վերևից:* □

Թեորեմ 16.15: *Հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամ կամ չբերվող է P դաշտի նկատմամբ կամ հավասար է P-ի նկատմամբ չբերվող բազմանդամների արտադրյալի: Ըստ որում, այդ վերլուծությունը միակն է արտադրիչների տեղափոխելիության և զուգորդման ճշտությամբ, այսինքն, եթե*

$$f = \varphi_1 \cdot \varphi_2 \cdots \varphi_n = \varphi'_1 \cdot \varphi'_2 \cdots \varphi'_m\,,$$

որտեղ $\varphi_1, \varphi_2, \ldots, \varphi_n, \varphi'_1, \varphi'_2, \ldots, \varphi'_m$ բազմանդամներից յուրաքանչյուրը չբերվող է P-ում, ապա $n = m$ և գոյություն ունեն զույգ առ զույգ միմյանցից տարբեր այնպիսի $i_1, i_2, \ldots, i_n \in \{1, 2, \ldots, n\}$ համարներ, որ $\varphi_1 = c_1\varphi'_{i_1}$, $\varphi_2 = c_2\varphi'_{i_2}$, …, $\varphi_n = c_n\varphi'_{i_n}$, որտեղ $c_1, c_2, \ldots, c_n \in P$:

Ապացույց: Վերլուծության գոյությունն ապացուցենք վերհանգման եղանակով՝ ըստ $k = deg(f) \geqslant 1$ բնական թվի: Եթե $k = 1$, ապա f-ը չբերվող է: Դիցուք $k \geqslant 2$ և դիցուք վերլուծության գոյությունը ճիշտ է k-ից փոքր աստիճան ունեցող բոլոր բազմանդամների համար: Եթե f-ը չբերվող է, ապա պնդումն ապացուցված է: Հակառակ դեպքում, ըստ նախորդ լեմմի, f-ը բաժանվում է որևէ φ չբերվող բազմանդամի վրա՝ $f = \varphi \cdot f_1$: Քանի որ f-ը բերվող է, ապա $f_1 \neq c \in P$ և $0 < deg(f_1) < deg(f) = k$: Հետևաբար, համաձայն վերհանգային ենթադրության, կամ f_1-ը չբերվող է կամ հավասար է չբերվող բազմանդամների արտադրյալի՝

$$f_1 = \varphi_1 \cdot \varphi_2 \cdots \varphi_\ell \ :$$

Արդունքում՝

$$f = \varphi \cdot f_1 = \varphi \cdot \varphi_1 \cdot \varphi_2 \cdots \varphi_\ell \,,$$

որտեղ բոլոր արտադրիչները չբերվող են:

Վերլուծության միակությունը նույնպես կապացուցենք վերհանգման եղանակով՝ ըստ $k = deg(f) \geqslant 1$ բնական թվի: Եթե $k = 1$, ապա պնդումն ակնհայտ է: Դիցուք $k \geqslant 2$ և k-ից փոքր աստիճան ունեցող բոլոր բազմանդամների համար պնդումը ճիշտ է: Եթե f-ը չբերվող է, ապա պնդումն ակնհայտ է: Դիցուք f-ը բերվող է և

$$f = \varphi_1 \cdot \varphi_2 \cdots \varphi_n = \varphi_1' \cdot \varphi_2' \cdots \varphi_m' \ :$$

Հետևաբար, չբերվող բազմանդամների $\varphi_1' \cdot \varphi_2' \cdots \varphi_m'$ արտադրյալը բաժանվում է φ_1 չբերվող բազմանդամի վրա: Համաձայն հատկություն 16.10-ի, $\varphi_1', \varphi_2', \ldots, \varphi_m'$ արտադրիչներից գոնե մեկը կբաժանվի φ_1-ի վրա: Դիցուք այդ արտադրիչը φ_{i_1}' բազմանդամն է՝ $\varphi_{i_1}' = \varphi_1 \cdot q$: Որտեղից՝ $q = c \in P$, $c \neq 0$, և $\varphi_1 = c^{-1} \cdot \varphi_{i_1}' = c_1 \varphi_{i_1}'$, որտեղ $c_1 = c^{-1}$: Մյուս կողմից, $f = \varphi_1 \cdot f_1$, որտեղ f_1-ը տարբեր է հաստատունից և $0 < deg(f_1) < deg(f) = k$: Այսպիսով, f_1-ի համար կունենանք երկու վերլուծություններ՝

$$f_1 = \varphi_2 \cdots \varphi_n = (c\varphi_2') \cdots \varphi_m' \,,$$

որտեղ բոլոր արտադրիչները ևս չբերվող բազմանդամներ են: Մնում է օգտվել վերհանգային ենթադրությունից: □

Եթե բազմանդամի վերլուծության մեջ միևնույն φ_1 չբերվող և ունիտար բազմանդամի հետ զուգորդված բոլոր n_1 հատ չբերվող բազմանդամների արտադրյալը գրենք $c_1 \cdot \varphi_1^{n_1}$ տեսքով, ապա, համաձայն թեորեմ 16.15-ի, հաստատունից տարբեր յուրաքանչյուր $f \in P[x]$ բազմանդամի համար կստանանք նրա հետևյալ **վերլուծությունը**՝

$$f = c \cdot \varphi_1^{n_1} \cdot \varphi_2^{n_2} \cdots \varphi_s^{n_s} \,,$$

որտեղ $\varphi_1, \varphi_2, \ldots, \varphi_s \in P[x]$ բազմանդամներն արդեն միմյանցից տարբեր, ունիտար և չզուգորդված չբերվող բազմանդամներ են P դաշտի նկատմամբ, $c \in P$, $c \neq 0$: Այս վերլուծությունը կոչվում է f բազմանդամի **կանոնական վերլուծություն** P դաշտում: Օրինակ,

$$f = \left(2x^2 + 2x + 4\right)\left(3x^2 + 3x + 6\right)(x+1)\left(x^2 + x + 2\right)(2x+2) \in \mathbb{R}[x]$$

բազմանդամի կանոնական վերլուծությունն է՝

$$f = 12\left(x^2 + x + 2\right)^3 (x+1)^2 \ :$$

16.6. Բազմանդամի բազմապատիկ արմատներ և ածանցյալ: Թեյլորի բանաձևը զրո բնութագրիչով դաշտի դեպքում

Ըստ Բեզուի թեորեմի՝ P դաշտի c տարրը կլինի արմատ $f \in P[x]$ բազմանդամի համար այն և միայն այն դեպքում, երբ f-ը բաժանվում է $x - c$ երկանդամի վրա, այսինքն՝ $f = (x-c)q$, որտեղ $q \in P[x]$: Սակայն f-ը երբեմն կարող է բաժանվել նաև $x - c$ երկանդամի ավելի բարձր աստիճանի վրա: Հանգում ենք հետևյալ հասկացությանը:

Դիցուք $k \in \mathbb{N}$ և $k \geqslant 1$: $c \in P$ տարրը կոչվում է $f \in P[x]$ բազմանդամի k**-պատիկ արմատ**, եթե f-ը բաժանվում է $(x-c)^k$-ի վրա, բայց չի բաժանվում $(x-c)^{k+1}$-ի վրա: Եթե $k > 1$, ապա c-ն կոչվում է f -ի **բազմապատիկ արմատ**; $k = 1$ դեպքում c-ն կոչվում է **պարզ արմատ**, $k = 2$ դեպքում՝ **կրկնակի (կրկնապատիկ) արմատ**, իսկ $k = 3$ դեպքում՝ **եռապատիկ արմատ**: Եթե c-ն f բազմանդամի k-պատիկ արմատն է, ապա k բնական թիվը կոչվում է c արմատի **պատիկություն**: Այս դեպքում ասում են նաև, որ f բազմանդամն ունի k հատ համընկնող կամ կրկնվող արմատներ:

Լեմմ 16.10: *1) $c \in P$ տարրը կլինի $f \in P[x]$ բազմանդամի k-պատիկ արմատ այն և միայն այն դեպքում, երբ*

$$f = (x-c)^k q\,,$$

որտեղ $q(c) \neq 0$:

2) $c \in P$ տարրը կլինի $f \in P[x]$ բազմանդամի բազմապատիկ արմատ այն և միայն այն դեպքում, երբ

$$f = (x-c)^2 q \ : \qquad \square$$

Թեորեմ 16.16: *Եթե հաստատունից տարբեր $f \in P[x]$ բազմանդամը P դաշտում ունի միմյանցից տարբեր $c_1, c_2, \ldots, c_m \in P$ արմատները, որոնց պատիկությունները համապատասխանաբար հավասար են $k_1, k_2, \ldots, k_m$-ի, ապա f-ը բաժանվում է*

$$(x - c_1)^{k_1} \cdot (x - c_2)^{k_2} \cdots (x - c_m)^{k_m}$$

արտադրյալի վրա: Մասնավորապես՝ $k_1 + k_2 + \cdots + k_m \leqslant deg(f)$, այսինքն՝ դաշտում $n > 0$ աստիճանի բազմանդամի ունեցած բոլոր արմատների թիվը, հաշված իրենց պատիկություններով, չի գերազանցում n-ը:

Ապացուցում: Եթե $c_i \neq c_j$, ապա $x - c_i$ և $x - c_j$ բազմանդամները կլինեն փոխադարձաբար պարզ: Ըստ հետևություն 16.8-ի, $(x - c_i)^{k_i}$ և $(x - c_j)^{k_j}$ բազմանդամները ևս կլինեն փոխադարձաբար պարզ: Հետևաբար, հատկություն 16.4-ի համաձայն, f-ը կբաժանվի $(x - c_1)^{k_1} \cdot (x - c_2)^{k_2} \cdots (x - c_m)^{k_m}$ արտադրյալի վրա, այսինքն՝

$$f = (x - c_1)^{k_1} \cdot (x - c_2)^{k_2} \cdots (x - c_m)^{k_m} \cdot q$$

և $deg(f) = k_1 + k_2 + \cdots + k_m + deg(q)$: □

Թեորեմ 16.16-ը կմնա ճիշտ նաև այն դեպքում, երբ P դաշտի փոխարեն վերցնենք կամայական ամբողջության տիրույթը: Սակայն, օրինակ, $\mathbb{Z}_8$ օղակի դեպքում այն ճիշտ չէ:

Թեորեմ 16.17: *Եթե $\alpha \in \mathbb{C}$ կոմպլեքս թիվը $f \in \mathbb{R}[x]$ բազմանդամի k-պատիկ արմատն է, ապա $\bar{\alpha}$ համալուծը նույնպես կլինի f-ի k-պատիկ արմատը ($k \geqslant 1$):*

Ապացուցում: Ինչպես գիտենք, եթե α-ն f-ի արմատն է, ապա նրա $\bar{\alpha}$ համալուծը ևս կլինի f-ի արմատ և f-ը կբաժանվի

$$\varphi = (x - \alpha)(x - \bar{\alpha}) = x^2 - (\alpha + \bar{\alpha})\,x + \alpha\bar{\alpha} \in \mathbb{R}[x]$$

բազմանդամի վրա (տես թեորեմ 16.14-ի ապացուցումը), այսինքն՝ $f = \varphi \cdot q$, որտեղ $q \in \mathbb{R}[x]$: Այստեղից բխում է, որ եթե α-ն f-ի բազմապատիկ արմատ է, ապա α-ն կլինի նաև արմատ q բազմանդամի համար: Հետևաբար, $\bar{\alpha}$ համալուծը ևս կլինի արմատ q-ի համար: Ուստի, $\bar{\alpha}$-ը կլինի բազմապատիկ արմատ f-ի համար: Դժվար չէ նկատել նաև α և $\bar{\alpha}$ արմատների պատիկությունների հավասարությունը: □

Եթե n-րդ աստիճանի $f = a_0 + a_1x + \cdots + a_nx^n \in P[x]$ բազմանդամը վերլուծվում է գծային արտադրիչների, ապա

$$f = a_n(x - c_1)(x - c_2)\cdots(x - c_n)\,,$$

որտեղ $c_1, c_2, \ldots, c_n \in P$: Իրոք,

$$f = (b_1 + b_1'x)(b_2 + b_2'x)\cdots(b_n + b_n'x) =$$

$$= b_1'b_2'\cdots b_n'\left(x + \frac{b_1}{b_1'}\right)\cdots\left(x + \frac{b_n}{b_n'}\right) = c(x - c_1)(x - c_2)\cdots(x - c_n),$$

որտեղ $-c_i = \dfrac{b_i}{b_i'} = b_i(b_i')^{-1}$, $c = b_1'b_2'\cdots b_n' = a_n$, իսկ $c_1, c_2, \ldots, c_n \in P$ տարրերը կլինեն f-ի արմատները:

Վերհանգման եղանակով դժվար չէ ստուգել հետևյալ հավասարությունը՝

$$(x - c_1)(x - c_2)\cdots(x - c_n) = (-1)^n c_1c_2\cdots c_n +$$

$$(-1)^{n-1}\left(c_1c_2\cdots c_{n-1} + c_1c_2\cdots c_{n-2}c_n + \cdots + c_2c_3\cdots c_n\right)x + \cdots$$

$$-\left(c_1c_2c_3 + c_1c_2c_4 + \cdots + c_{n-2}c_{n-1}c_n\right)x^{n-3} +$$

$$+\left(c_1c_2 + c_1c_3 + \cdots + c_1c_n + c_2c_3 + \cdots + c_{n-1}c_n\right)x^{n-2} -$$

$$-\left(c_1 + c_2 + \cdots + c_n\right)x^{n-1} + x^n\,;$$

Այնուհետև, համեմատելով

$$a_0 + a_1x + \cdots + a_nx^n = a_n(x - c_1)(x - c_2)\cdots(x - c_n), \quad a_n \neq 0\,,$$

հավասարության համապատասխան գործակիցները, կստանանք հետևյալ բանաձևերը՝

$$c_1 + c_2 + \cdots + c_n = -\frac{a_{n-1}}{a_n},$$

$$c_1c_2 + c_1c_3 + \cdots + c_{n-1}c_n = \frac{a_{n-2}}{a_n},$$

$$c_1c_2c_3 + c_1c_2c_4 + \cdots + c_{n-2}c_{n-1}c_n = -\frac{a_{n-3}}{a_n},$$

$$\cdots \qquad \cdots \qquad \cdots$$

$$\sum_{i_1<i_2<\cdots<i_k} c_{i_1}c_{i_2}\cdots c_{i_k} = (-1)^k\frac{a_{n-k}}{a_n},$$

$\ldots \quad \ldots \quad \ldots$
$c_1c_2\cdots c_n = (-1)^n\dfrac{a_0}{a_n}$,

որոնք կոչվում են **Վիետի բանաձևեր**:

Օրինակներ: 1) $(x-c_1)(x-c_2) = c_1c_2 - (c_1+c_2)x + x^2$;

2) $(x-c_1)(x-c_2)(x-c_3) = -c_1c_2c_3 + (c_1c_2 + c_1c_3 + c_2c_3)x - (c_1 + c_2 + c_3)x^2 + x^3$;

3) Գտնենք այն իրական գործակիցներով

$$f = a_0 + a_1x + a_2x + a_3x^3 + 2x^4$$

բազմանդամը, որի համար 2-ը լինի կրկնակի արմատ, իսկ 1-ը և 3-ը պարզ արմատներ: Վիետի բանաձևերի համաձայն՝

$2+2+1+3 = -\dfrac{a_3}{2}$,

$2\cdot 2 + 2\cdot 1 + 2\cdot 3 + 2\cdot 1 + 2\cdot 3 + 1\cdot 3 = \dfrac{a_2}{2}$,

$2\cdot 2\cdot 1 + 2\cdot 2\cdot 3 + 2\cdot 1\cdot 3 + 2\cdot 1\cdot 3 = -\dfrac{a_1}{2}$,

$2\cdot 2\cdot 1\cdot 3 = (-1)^4\dfrac{a_0}{2}$,

որտեղից՝ $a_3 = -16$, $a_2 = 46$, $a_1 = -56$, $a_0 = 24$ և $f = 24 - 56x + 46x^2 - 16x^3 + 2x^4$:

Բազմանդամն իր արմատներով և դրանց պատիկություններով միարժեքորեն չի որոշվում, որովհետև եթե բազմանդամը բազմապատկենք $c \neq 0$ հաստատունով, ապա դրանից բազմանդամի արմատները և դրանց պատիկությունները չեն փոխվի:

Այսպիսով, այն դեպքում, երբ բազմանդամի արմատների թիվը (հաշված իրենց պատիկություններով) հավասար է բազմանդամի աստիճանին, Վիետի բանաձևերը հնարավորություն են տալիս ունիտար բազմանդամի գործակիցներն արտահայտել նրա արմատների միջոցով՝ դիտարկվող P դաշտի $+$ և $\cdot$ գործողությունների և հակադիրի միջոցով: Բնականորեն ծագում է հակադարձ հարցը, կարելի է արդյո՞ք բազմանդամի արմատներն արտահայտել նրա գործակիցների միջոցով: Այս կարևոր և պատմական հարցի պատասխանը կախված է թույլատրելի գործողություններից: Հանգում ենք հետևյալ գաղափարին:

Կասենք, որ բազմանդամը **լուծելի է արմատանշաններով**, եթե նրա արմատները ստացվում են բազմանդամի գործակիցներից՝

գումարման, հանման, բազմապատկման, բաժանման գործողություններ կատարելով և արմատ հանելով:

Դպրոցական դասընթացից հայտնի քառակուսի հավասարման լուծման բանաձևերը նշանակում են, որ (իրական կամ կոմպլեքս) թվային գործակիցներով երկրորդ աստիճանի բազմանդամը լուծելի է արմատանշաններով: 16-րդ դարում նմանատիպ բանաձևեր հայտնաբերվել են ընդհանուր տեսքի 3-րդ և 4-րդ աստիճանի բազմանդամների արմատների համար (Ջ. Կարդանո, Լ. Ֆերրարի, Ս. դել Ֆերրո, Ն. Տարտալիա): Ավելի ճիշտ, այդ բազմանդամներից յուրաքանչյուրը բերվում է $x^3 + px + q$ տեսքի, որի արմատները տրվում են

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^2}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^2}{27}}}$$

բանաձևով, որը կոչվում է **Կարդանոյի բանաձև**: 1545թ. հրատարակվում է Ջերոլամո Կարդանոյի «մեծ արվեստ» գիրքը՝ նվիրված 3-րդ և 4-րդ աստիճանի բազմանդամների արմատներին, որի մասին 20-րդ դարում Ֆ. Քլայնը գրել է «այդ բարձրաստիճան արժեքավոր ստեղծագործությունը պարունակում է ժամանակակից հանրահաշվի սաղմ»: 1827թ. հռչակավոր նորվեգ մաթեմատիկոս Ն. Աբելը ապացուցում է, որ n-րդ աստիճանի ընդհանուր տեսքի բազմանդամը, $n \geqslant 5$ դեպքում, լուծելի չէ արմատանշաններով: 1831թ. տաղանդավոր ֆրանսիացի մաթեմատիկոս Էվարիստ Գալուայի կողմից ապացուցվում է հայտանիշ՝ թվային գործակիցներով բազմանդամի արմատանշաններով լուծելիության վերաբերյալ: Մասնավորապես պարզվում է, որ յուրաքանչյուր $n \geqslant 5$ բնական թվի համար գոյություն ունի արմատանշաններով չլուծվող n-րդ աստիճանի բազմանդամ: Այդպիսին է, օրինակ,

$$f = 1 - \frac{n}{1}x + \frac{n(n-1)}{1\cdot 2}\cdot\frac{1}{1\cdot 2}x^2 - \frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}\cdot\frac{1}{1\cdot 2\cdot 3}x^3 + \cdots$$
$$+(-1)^n\frac{1}{1\cdot 2\cdots n}x^n$$

բազմանդամը:

Աբելի և Գալուայի արդյունքները և գաղափարները մեծ ազդեցություն են ունեցել մաթեմատիկայի հետագա զարգացման վրա, մասնավորապես հիմք են հանդիսացել ժամանակակից հանրահաշվի և նրա կիրառությունների համար:

Բազմանդամի պարզ և բազմապատիկ արմատների անջատման ամենաարդյունավետ եղանակը կապված է բազմանդամի ածանցյալի հետ:

Դիցուք P-ն կամայական դաշտ է, որի միավորը նշանակված է 1-ով, իսկ $f \in P[x]$: Եթե

$$f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n\,,$$

ապա f **բազմանդամի ածանցյալ** ասելով հասկացվում է հետևյալ բազմանդամը՝

$$f' = 0 + a_1 + 2a_2x + \cdots + na_nx^{n-1} = a_1 + 2a_2x + \cdots + na_nx^{n-1} \in P[x]\,,$$

որտեղ $ka = (\underbrace{1 + \cdots + 1}_{k})a = \underbrace{a + \cdots + a}_{k} \in P$, այսինքն՝ k գործակիցը դաշտի $\underbrace{1 + \cdots + 1}_{k}$ տարրն է:

Օրինակ, $f = 3 + 2x + x^2 + 4x^3 \in \mathbb{Z}_3[x]$ բազմանդամի ածանցյալը հավասար է

$$f' = 2 + 2x + 12x^2 = 2 + 2x \in \mathbb{Z}_3[x]$$

բազմանդամին, որովհետև $\mathbb{Z}_3$-ում՝ $12 = [12] = [0] = 0$: Հաստատունի ածանցյալը հավասար է զրոյի, այսինքն՝ $c' = 0$, որտեղ $c \in P$: $(x+c)' = 1$, մասնավորապես՝ $x' = 1$:

Լեմմ 16.11*: Հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամի համար՝ $deg(f') = deg(f) - 1$, եթե P դաշտի բնութագրիչը հավասար է զրոյի, այսինքն՝ $char(P) = 0$:*

Ապացուցում: Եթե $deg(f) = n \geqslant 1$, ապա $f = a_0 + a_1x + \cdots + a_nx^n$, $a_n \neq 0$, և $f' = a_1 + 2a_2x + \cdots + na_nx^{n-1}$: Մնում է նկատել, որ $na_n \neq 0$: Իրոք, $a_n \neq 0$ և $n = \underbrace{1 + \cdots + 1} \neq 0$՝ ըստ $char(P) = 0$ պայմանի, իսկ դաշտը չունի զրոյի բաժանարարներ: □

Եթե $P = \mathbb{R}$, ապա բազմանդամի ածանցյալի նշված գաղափարը համընկնում է մաթեմատիկական անալիզի դասընթացում սահմանվող բազմանդամի ածանցյալի հետ որպես սահմանի՝

$$\lim_{\triangle x \to 0} \frac{f(x + \triangle x) - f(x)}{\triangle x}\,,$$

ինչը իմաստավորվում է կամայական P դաշտի դեպքում՝ առանց տոպոլոգիայի առկայության:

Բազմանդամի ածանցյալը բավարարում է հետևյալ ընդհանուր հատկություններին:

Թեորեմ 16.18*: 1)* $(f_1+f_2)'=f_1'+f_2'$,
$(f_1+\cdots+f_n)'=f_1'+\cdots+f_n'$*;*
2) $(cf)'=cf'$*;*
3) $(c_1f_1+c_2f_2)'=c_1f_1'+c_2f_2'$,
$(c_1f_1+\cdots+c_nf_n)'=c_1f_1'+\cdots+c_nf_n'$*;*
4) $(f_1f_2)'=f_1'f_2+f_1f_2'$,
$(f_1f_2\cdots f_k)'=f_1'f_2\cdots f_k+f_1f_2'f_3\cdots f_k+\cdots+f_1\cdots f_{k-1}f_k'$,
$(f^k)'=kf^{k-1}f'$, *մասնավորապես՝* $\big((x+c)^k\big)'=k(x+c)^{k-1}$*;*
5) Եթե $D:P[x]\to P[x]$ *արտապատկերումը բավարարում է հետևյալ երեք պայմաններին՝*
ա) $D(x)=1$, *որտեղ* 1*-ը* P *դաշտի միավորն է,*
բ) $D(cf)=cD(f)$, $c\in P$,
$D(f_1+f_2)=D(f_1)+D(f_2)$,
գ) $D(f_1f_2)=D(f_1)f_2+f_1D(f_2)$,
ապա $D(f)=f'$ *ցանկացած* $f\in P[x]$ *բազմանդամի համար: Այս* D *արտապատկերումը կոչվում է* $P[x]$ **բազմանդամների օղակի դիֆերենցում***:*

Ապացուցում: 1) և 2) հատկություններն անմիջապես բխում են բազմանդամի ածանցյալի սահմանումից, իսկ 3) հատկությունը բխում է 1) և 2) հատկություններից: Ապացուցենք 4)-ը:

Նախ նկատենք, որ

$$\big(ax^k\cdot bx^m\big)'=\big(abx^{k+m}\big)'=(k+m)abx^{k+m-1}=$$

$$=kax^{k-1}\cdot bx^m+ax^k\cdot mbx^{m-1}=(ax^k)'bx^m+ax^k(bx^m)'\ :$$

Այստեղից, ընդհանուր դեպքում, ստանում ենք՝

$$(f_1\cdot f_2)'=\left(\left(a_0+a_1x+\cdots+a_nx^n\right)\left(b_0+b_1x+\cdots+b_mx^m\right)\right)'=$$

$$=\left(\sum_{k=0}^{n}a_kx^k\cdot\sum_{\ell=0}^{m}b_\ell x^\ell\right)'=\sum_{k=0}^{n}\sum_{\ell=0}^{m}\left(\left(a_kx^k\right)\left(b_\ell x^\ell\right)\right)'=$$

$$= \sum_{k=0}^{n} \sum_{\ell=0}^{m} \left(\left(a_k x^k\right)' \left(b_\ell x^\ell\right) + \left(a_k x^k\right) \left(b_\ell x^\ell\right)' \right) =$$

$$= \sum_{k=0}^{n} \left(a_k x^k\right)' \sum_{\ell=0}^{m} \left(b_\ell x^\ell\right) + \sum_{k=0}^{n} \left(a_k x^k\right) \sum_{\ell=0}^{m} \left(b_\ell x^\ell\right)' = f_1' f_2 + f_1 f_2' \ :$$

4)-ի երկրորդ հավասարությունն ապացուցվում է վերհանգման եղանակով՝ ըստ k բնական թվի: Սրանից էլ ստացվում է 4)-ի երրորդ հավասարությունը, երբ $f_1 = f_2 = \cdots = f_k = f$:

Ապացուցենք 5)-ը: Նախ նկատենք, որ բ)-ի երկրորդ պայմանից վերհանգման եղանակով ստանում ենք՝

$$D(f_1 + \cdots + f_k) = D(f_1) + \cdots + D(f_k) \ :$$

Այնուհետև՝

$$D(1) = D(1 \cdot 1) = (D1) \cdot 1 + 1 \cdot (D1) = D1 + D1\,,$$

որտեղից՝ $D(1) = 0$: Որից հետո կունենանք՝ $D(c) = D(c \cdot 1) = c \cdot D(1) = c \cdot 0 = 0$, որտեղ $c \in P$: Վերհանգման եղանակով այժմ ապացուցենք $D(x^n) = nx^{n-1}$ հավասարությունը: $n = 1$ դեպքում այն ճիշտ է՝ համաձայն ա) պայմանի: Ենթադրելով հավասարությունը ճիշտ n-ից փոքր բնական թվերի դեպքում, կստանանք՝

$$D\left(x^n\right) = D\left(x^{n-1} \cdot x\right) = \left(Dx^{n-1}\right) x + x^{n-1} \left(Dx\right) = (n-1)x^{n-2} \cdot x + x^{n-1} \cdot 1 =$$

$$= (n-1)x^{n-1} + 1 \cdot x^{n-1} = \left((n-1) + 1\right) x^{n-1} = nx^{n-1} \ :$$

Այսպիսով, եթե $f = a_0 + a_1 x + \cdots + a_n x^n$, ապա

$$D(f) = D\left(a_0\right) + a_1 D(x) + a_2 D\left(x^2\right) + \cdots + a_n D\left(x^n\right) =$$

$$= 0 + a_1 + a_2 2x + \cdots + a_n n x^{n-1} = a_1 + 2a_2 x + \cdots + n a_n x^{n-1} = f' \ : \ \square$$

Ածանցյալի գաղափարը հնարավորություն է տալիս բազմանդամի բազմապատիկ արմատները գտնելու խնդիրը հանգեցնել մեկ այլ բազմանդամի արմատները գտնելու խնդրին:

Թեորեմ 16.19: *1) $f \in P[x]$ բազմանդամի $c \in P$ արմատը կլինի պարզ այն և միայն այն դեպքում, երբ $f'(c) \neq 0$;*

2) $f \in P[x]$ բազմանդամի $c \in P$ արմատը կլինի բազմապատիկ այն և միայն այն դեպքում, երբ $f'(c) = 0$;

3) $f \in P[x]$ բազմանդամի բոլոր $c \in P$ բազմապատիկ արմատների բազմությունը համընկնում է $d \rightleftharpoons (f, f')$ բազմանդամի բոլոր $c \in P$ արմատների բազմության հետ: Մասնավորապես, f-ը չի ունենա բազմապատիկ արմատ այն և միայն այն դեպքում, երբ f և f' բազմանդամները փոխադարձաբար պարզ են;

4) Եթե $char(P) = 0$, ապա $f \in P[x]$ բազմանդամի յուրաքանչյուր k-պատիկ արմատ կլինի $f' \in P[x]$ ածանցյալի $(k-1)$-պատիկ արմատ $(k \geqslant 2)$:

Ապացուցում: Եթե $k \geqslant 1$ և $c \in P$ տարրը $f \in P[x]$ բազմանդամի k-պատիկ արմատ է, ապա

$$f = (x-c)^k g, \quad \text{որտեղ } g(c) \neq 0 \ :$$

Հետևաբար,

$$f' = k(x-c)^{k-1} g + (x-c)^k g' \ :$$

Եթե այստեղ $k = 1$, այսինքն՝ c-ն f-ի պարզ արմատն է, ապա

$$f' = g + (x-c)g' \quad \text{և} \quad f'(c) = g(c) \neq 0 \ :$$

$k \geqslant 2$ դեպքում կունենանք՝

$$f'(c) = k(c-c)^{k-1} g(c) + (c-c)^k g'(c) = 0 \ :$$

Ուստի, $f'(c) \neq 0$ պայմանից կբխի՝ $k = 1$: Այսպիսով, 1) և 2) պնդումներն ապացուցված են: Ապացուցենք 3) պնդումը՝ օգտվելով 2)-ից և Բեզուի թեորեմից.

$$f(c) = f'(c) = 0 \ \longleftrightarrow \ f \big/ x-c, \quad f' \big/ x-c \ \longleftrightarrow \ d \big/ x-c \ \longleftrightarrow \ d(c) = 0\,,$$

որտեղ $d \rightleftharpoons (f, f')$:

4)-ի ապացուցման համար նկատենք, որ եթե $f = (x-c)^k g$, որտեղ $g(c) \neq 0$, ապա $f' = (x-c)^{k-1} F$, որտեղ $F = kg + (x-c)g'$ և $F(c) = kg(c) \neq 0$, որովհետև $k = \underbrace{1 + \cdots + 1} \neq 0$՝ ըստ $char(P) \neq 0$ պայմանի: $\square$

Օրինակ, որոշենք $f = x^4 - 3x^3 + 3x^2 - 3x + 2 \in \mathbb{Z}_5[x]$ բազմանդամի բազմապատիկ արմատները: Նախ էվկլիդեսի ալգորիթմով որոշում ենք f և $f' = 4x^3 - 9x^2 + 6x - 3 = 4x^3 - 4x^2 + x - 3 \in \mathbb{Z}_5[x]$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը՝ $x - 2 \rightleftharpoons (f, f')$: Հետևաբար, ապացուցված թեորեմի համաձայն, $2 = [2] \in \mathbb{Z}_5$ տարրը f-ի միակ բազմապատիկ արմատն է, այսինքն՝ f-ը կբաժանվի $(x-2)^2$ բազմանդամի վրա.

$$f = (x-2)^2(x^2 + x + 3) \ :$$

Այնուհետև, $g = x^2 + x + 3$ բազմանդամը $\mathbb{Z}_5$-ում ունի 1 և 3 արմատները, որովհետև $g(0) \neq 0$, $g(1) = 0$, $g(2) \neq 0$, $g(3) = 0$ և $g(4) \neq 0$: Հետևաբար,

$$x^2 + x + 3 = (x-1)(x-3)$$

և

$$f = (x-2)^2(x-1)(x-3) \ :$$

Միաժամանակ ստացանք f բազմանդամի կանոնական վերլուծությունը:

Ապացուցված թեորեմի վերջին 4) հատկությունն ակնհայտորեն խախտվում է $char(P) > 0$ դեպքում: Օրինակ, $P = \mathbb{Z}_p$ դաշտի դեպքում, որտեղ p-ն պարզ թիվ է, $x^p \in \mathbb{Z}_p[x]$ բազմանդամի ածանցյալը հավասար է զրոյի՝ $(x^p)' = px^{p-1} = 0$, որովհետև p գործակիցը $\mathbb{Z}_p$-ում հավասար է զրոյի:

Պայմանավորվենք հետևյալ նշանակումների մեջ: $(f')'$-ը կոչվում է $f \in P[x]$ բազմանդամի **երկրորդ (կարգի) ածանցյալ** և նշանակվում է f''-ով: $(f'')'$-ը կոչվում է $f \in P[x]$ բազմանդամի **երրորդ (կարգի) ածանցյալ** և նշանակվում է f'''-ով, և այլն: $f^{(k)}$-ով կնշանակվի $f \in P[x]$ բազմանդամի k-րդ (կարգի) ածանցյալը, որը սահմանվում է՝

$$f^{(k)} = \left(f^{(k-1)}\right)' \ :$$

Մաթեմատիկական անալիզի դասընթացում, բազմանդամի Թեյլորի բանաձևն ապացուցվում է $P = \mathbb{R}$ իրական թվերի դաշտի դեպքում: Սակայն այդ բանաձևը ճիշտ է նաև զրո բնութագրիչով ցանկացած P դաշտի դեպքում, որից կարելի է օգտվել բազմանդամի արմատների պատիկությունները որոշելու (հաշվելու) համար:

Թեորեմ 16.20 (Թեյլոր): *Հաստատունից տարբեր կամայական n-րդ աստիճանի $f \in P[x]$ բազմանդամի և կամայական $c \in P$ հաստատունի* *համար գոյություն ունեն միարժեքորեն որոշվող այնպիսի* $b_0, b_1, \dots, b_n \in P$ *տարրեր, որ*

$$f = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n\,, \tag{16.1}$$

որտեղ $b_0 = f(c)$, $b_1 = f'(c)$*: Եթե* $char(P) = 0$*, ապա* $b_k = \dfrac{f^{(k)}(c)}{k!}$*,* $k = 2, \dots, n$*, այսինքն՝*

$$f = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \cdots + \frac{f^{(n)}}{n!}(x-c)^n\,, \tag{16.2}$$

որը կոչվում է f **բազմանդամի Թեյլորի բանաձև**՝ *գրված* c *տարրի համար:*

Ապացուցում: (16.1) բանաձևն ապացուցենք վերհանգման եղանակով՝ ըստ $n = deg(f)$-ի: Եթե $n = 1$, այսինքն՝ $f = a_0 + a_1 x$, ապա $f = a_0 + a_1 c + a_1(x-c)$, որտեղ $a_0 + a_1 c = b_0$, $a_1 = b_1$: Դիցուք $deg(f) = n > 1$ և (16.1) բանաձևը ճիշտ է n-ից փոքր աստիճան ունեցող բոլոր բազմանդամների համար: Բազմանդամների մնացորդով բաժանման թեորեմի համաձայն՝

$$f = (x-c)q + f(c)\,,$$

որտեղ $deg(q) = n - 1$ և, հետևաբար, q բազմանդամի համար (16.1) վերլուծությունը ճիշտ է՝

$$q = b_0 + b_1(x-c) + \cdots + b_{n-1}(x-c)^{n-1}\ :$$

Տեղադրելով q-ի այս վերլուծությունը $f = (x-c)q + f(c)$ արտահայտության մեջ, կստանանք f-ի պահանջվող վերլուծությունը (ներկայացումը):

Ապացուցենք $b_0, b_1, \dots, b_n$ գործակիցների միակությունը: Դիցուք՝

$$f = b_0 + b_1(x-c) + \cdot + b_n(x-c)^n = b_0' + b_1'(x-c) + \cdots + b_n'(x-c)^n\ :$$

Այդ դեպքում,

$$0 = (b_0 - b_0') + (b_1 - b_1')\,x + \cdots + (b_n - b_n')\,(x-c)^n \tag{16.3}$$

և եթե որևէ $b_i - b_i' \neq 0$, ապա նշանակելով $m = \max\{i \mid b_i - b_i' \neq 0\}$, (16.3) հավասարության աջ մասում կունենանք m-րդ աստիճանի բազմանդամ, իսկ ձախ մասում զրոյական բազմանդամն է: Հակասություն: Հետևաբար, $b_i - b_i' = 0$ բոլոր $i = 0, 1, \ldots, n$ նշիչների համար, այսինքն՝ $b_0 = b_0'$, $b_1 = b_1'$, ..., $b_n = b_n'$:

(16.1) հավասարությունից կունենանք՝ $b_0 = f(c)$ և $f' = b_1 + 2b_2(x - c) + \cdots + na_n(x - c)^{n-1}$, որտեղից՝ $b_1 = f'(c)$:

Դիցուք $char(P) = 0$: (16.1) բանաձևից գտնելով f-ի k-րդ ածանցյալը, կունենանք՝

$$f^{(k)}(c) = k!b_k, \quad k = 1, 2, \ldots, n,$$

որտեղ $k! = 1 \cdot 2 \cdots k \in P$: Ըստ $char(P) = 0$ պայմանի՝ $k! \neq 0$, այսինքն՝

$$b_k = (k!)^{-1} f^{(k)}(c) = \frac{f^{(k)}(c)}{k!}$$

և (16.2) վերլուծությունն ապացուցված է: □

Եթե $c \in P$ տարրը $f \in P[x]$ բազմանդամի համար արմատ չէ, ապա դրան անվանում են f-ի 0-**պատիկ արմատ**:

Հետևություն 16.11: *$f \in P[x]$ բազմանդամի $c \in P$ արմատի պատիկությունը հավասար է (16.1) վերլուծության առաջին ոչ զրոյական գործակցի նշիչին:* □

Նկատենք, որ տրված $f \in P[x]$ բազմանդամի և $c \in P$ տարրի համար (16.1) վերլուծության գործակիցները, ինչպես նաև c-ի պատիկությունը, կարելի է գտնել բազմանդամների մնացորդով բաժանման ալգորիթմով: Իրոք,

$$f = (x - c)q + f(c), \quad \text{որտեղ } f(c) = b_0 \in P,$$

$$\begin{aligned} q &= (x - c)q_1 + q(c), \quad \text{որտեղ } q(c) = b_1 \in P, \\ q_1 &= (x - c)q_2 + q_1(c), \quad \text{որտեղ } q_1(c) = b_2 \in P, \\ &\ldots \quad \ldots \quad \ldots \end{aligned}$$

16.7. Ռացիոնալ կոտորակներ (ֆունկցիաներ)

Դիցուք P-ն կամայական դաշտ է: Բազմանդամների (f, g) զույգը, որտեղ $f, g \in P[x]$ և $g \neq 0$, կոչվում է P դաշտի նկատմամբ որոշված **ռացիոնալ կոտորակ** կամ **ռացիոնալ ֆունկցիա**: Հարմարության համար (f, g) զույգը նշանակվում է $\dfrac{f}{g}$ կոտորակի տեսքով: Երկու ռացիոնալ կոտորակների **հավասարությունը** սահմանվում է հետևյալ կերպ՝

$$\frac{f_1}{g_1} = \frac{f_2}{g_2} \longleftrightarrow f_1 g_2 = f_2 g_1 \ :$$

P դաշտի նկատմամբ որոշված բոլոր ռացիոնալ կոտորակների բազմությունը նշանակվում է $P(x)$-ով:

Լեմմ 16.12: *Ռացիոնալ կոտորակների հավասարությունը բավարարում է համարժեքության հարաբերության սահմանման երեք պայմաններին, այսինքն՝*

ա) $\dfrac{f}{g} = \dfrac{f}{g}$ *ցանկացած* $\dfrac{f}{g} \in K(x)$ *ռացիոնալ կոտորակի համար; (ռեֆլեքսիվություն)*

բ) $\dfrac{f_1}{g_1} = \dfrac{f_2}{g_2} \longrightarrow \dfrac{f_2}{g_2} = \dfrac{f_1}{g_1}$*; (համաչափություն)*

գ) $\dfrac{f_1}{g_1} = \dfrac{f_2}{g_2}, \ \dfrac{f_2}{g_2} = \dfrac{f_3}{g_3} \longrightarrow \dfrac{f_1}{g_1} = \dfrac{f_3}{g_3}$*: (փոխանցականություն)*

Ապացուցում: ա) և բ) պայմաններն ակնհայտորեն տեղի ունեն: Ապացուցենք գ)-ն: Դիցուք $f_1 g_2 = f_2 g_1$ և $f_2 g_3 = f_3 g_2$, այսինքն՝ $f_1 g_2 - f_2 g_1 = 0$ և $f_2 g_3 - f_3 g_2 = 0$: Հետևաբար,

$$g_2 (f_1 g_3 - f_3 g_1) = g_2 f_1 g_3 - g_2 f_3 g_1 = g_2 f_1 g_3 - g_2 f_3 g_1 + g_1 f_2 g_3 - g_1 f_2 g_3 =$$

$$= g_3 (f_1 g_2 - f_2 g_1) + g_1 (f_2 g_3 - f_3 g_2) = g_3 \cdot 0 + g_1 \cdot 0 = 0 ;$$

Քանի որ $P[x]$-ը ամբողջության տիրույթ է և $g_2 \neq 0$, ապա $g_2 (f_1 g_3 - f_3 g_1) = 0$ հավասարությունից բխում է՝ $f_1 g_3 - f_3 g_1 = 0$ և $f_1 g_3 = f_3 g_1$: Ուստի, $\dfrac{f_1}{g_1} = \dfrac{f_3}{g_3}$: □

Օրինակ, $\dfrac{f}{g} = \dfrac{fh}{gh}$ ցանկացած $h \in P[x]$, $h \neq 0$, բազմանդամի համար: Մասնավորապես, $\dfrac{h}{h} = \dfrac{1}{1}$ և $\dfrac{0}{h} = \dfrac{0}{1}$, որտեղ 1-ը P դաշտի միավորն է:

Սահմանենք ռացիոնալ կոտորակների **գումարը** և **արտադրյալը** հետևյալ կերպ՝

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2} \, ,$$

$$\frac{f_1}{g_1}\cdot\frac{f_2}{g_2}=\frac{f_1f_2}{g_1g_2}\ :$$

Մասնավորապես, $\dfrac{f_1}{g}+\dfrac{f_2}{g}=\dfrac{f_1g+f_2g}{gg}=\dfrac{(f_1+f_2)\,g}{gg}=\dfrac{f_1+f_2}{g}$:

Նախ պահանջվում է ապացուցել, որ ռացիոնալ կոտորակների գումարն ու արտադրյալը չի փոխվի, եթե ռացիոնալ կոտորակները փոխարինվեն իրենց հավասարներով: Իրոք, եթե $\dfrac{f_1}{g_1}=\dfrac{f_1'}{g_1'}$ և $\dfrac{f_2}{g_2}=\dfrac{f_2'}{g_2'}$, ապա ըստ գումարի և արտադրյալի սահմանման՝

$$\frac{f_1}{g_1}+\frac{f_2}{g_2}=\frac{f_1g_2+f_2g_1}{g_1g_2}\,,\qquad \frac{f_1'}{g_1'}+\frac{f_2'}{g_2'}=\frac{f_1'g_2'+f_2'g_1'}{g_1'g_2'}\,,$$

$$\frac{f_1}{g_1}\cdot\frac{f_2}{g_2}=\frac{f_1f_2}{g_1g_2}\,,\qquad\qquad \frac{f_1'}{g_1'}\cdot\frac{f_2'}{g_2'}=\frac{f_1'f_2'}{g_1'g_2'}$$

և պահանջվում է ապացուցել հետևյալ հավասարությունները՝

$$\frac{f_1g_2+f_2g_1}{g_1g_2}=\frac{f_1'g_2'+f_2'g_1'}{g_1'g_2'}\,,\qquad \frac{f_1f_2}{g_1g_2}=\frac{f_1'f_2'}{g_1'g_2'}\ :$$

Իրոք, ստուգենք գրված ռացիոնալ կոտորակների հավասարության պայմանները.

$$g_1'g_2'\,(f_1g_2+f_2g_1)-g_1g_2\,(f_1'g_2'+f_2'g_1')=$$

$$=g_1'g_2'f_1g_2+g_1'g_2'f_2g_1-g_1g_2f_1'g_2'-g_1g_2f_2'g_1'=$$

$$=g_1'g_2\,(f_1g_1'-f_1'g_1)+g_1'g_1\,(f_2g_2'-f_2'g_2)=g_1'g_2\cdot 0+g_1'g_1\cdot 0=0+0=0\,,$$

$$f_1f_2g_1'g_2'-f_1'f_2'g_1g_2=f_1f_2g_1'g_2'-f_2g_2'f_1'g_1+f_2g_2'f_1'g_1-f_1'f_2'g_1g_2=$$

$$=f_2g_2'\,(f_1g_1'-f_1'g_1)+f_1'g_1\,(f_2g_2'-f_2'g_2)=f_2g_2'\cdot 0+f_1'g_1\cdot 0=0+0=0\ :$$

Թեորեմ 16.21: *Ռացիոնալ կոտորակների $P(x)$ բազմությունը դաշտ է՝ ռացիոնալ կոտորակների գումարման և բազմապատկման նկատմամբ:*

Ապացուցում: Սահմանումից բխում է, որ ռացիոնալ կոտորակների գումարն ու արտադրյալը տեղափոխական են, զուգորդական և կապված են բաշխական օրենքով՝

$$\left(\frac{f_1}{g_1}+\frac{f_2}{g_2}\right)\frac{f_3}{g_3}=\frac{f_1}{g_1}\cdot\frac{f_3}{g_3}+\frac{f_2}{g_2}\cdot\frac{f_3}{g_3}\ :$$

$\dfrac{0}{1} \in P(x)$ տարրը կատարում է զրոյի դերը, իսկ $\dfrac{1}{1} \in P(x)$ տարրը՝ միավորի դերը, որովհետև

$$\frac{f}{g} + \frac{0}{1} = \frac{f}{g}, \qquad \frac{f}{g} \cdot \frac{1}{1} = \frac{f}{g} :$$

$\dfrac{-f}{g} \in P(x)$ տարրը հանդիսանում է $\dfrac{f}{g} \in P(x)$ տարրի հակադիրը, որովհետև

$$\frac{f}{g} + \frac{-f}{g} = \frac{fg - fg}{g \cdot g} = \frac{0}{g^2} = \frac{0}{1},$$

իսկ եթե $\dfrac{f}{g} \neq \dfrac{0}{1}$, այսինքն՝ $f \neq 0$, ապա $\dfrac{g}{f}$-ը կլինի $\dfrac{f}{g}$-ի հակադարձը, որովհետև

$$\frac{f}{g} \cdot \frac{g}{f} = \frac{f \cdot g}{f \cdot g} = \frac{1}{1} : \qquad \square$$

Քանի որ,

$$\frac{f_1}{1} = \frac{f_2}{1} \longleftrightarrow f_1 \cdot 1 = f_2 \cdot 1 \longleftrightarrow f_1 = f_2 \,,$$

$$\frac{f_1}{1} + \frac{f_2}{1} = \frac{f_1 + f_2}{1},$$

$$\frac{f_1}{1} \cdot \frac{f_2}{1} = \frac{f_1 \cdot f_2}{1},$$

ապա $\dfrac{f}{1}$ ռացիոնալ կոտորակը կարելի է նույնականացնել f բազմանդամի հետ, որի հետևանքով $P(x)$ դաշտը դառնում է $P[x]$ օղակի ընդլայնումը: Արդյունքում՝

$$\frac{f}{g} = \frac{f}{1} \cdot \left(\frac{g}{1}\right)^{-1} = \frac{\frac{f}{1}}{\frac{g}{1}},$$

այսինքն՝ $\dfrac{f}{g}$ կոտորակը ստանում է «բովանդակություն», $P(x)$ դաշտում դառնալով f և g բազմանդամների հարաբերություն:

$\dfrac{f}{g}$ ռացիոնալ կոտորակի համար, սովորաբար, f-ը կոչվում է **համարիչ**, իսկ g-ն՝ **հայտարար**: Եթե $\dfrac{f}{g} \neq \dfrac{0}{1}$, այսինքն՝ $f \neq 0$, ապա

$\frac{f}{g}$ ռացիոնալ կոտորակը կոչվում է **ոչ զրոյական**, իսկ $deg(f) - deg(g)$ տարբերությունը՝ ոչ զրոյական $\frac{f}{g}$ **ռացիոնալ կոտորակի աստիճան** և նշանակվում է $deg\left(\frac{f}{g}\right)$-ով:

Լեմմ 16.13: *Երկու հավասար ոչ զրոյական ռացիոնալ կոտորակների աստիճանները հավասար են, այսինքն՝ ոչ զրոյական ռացիոնալ կոտորակի աստիճանը կախված չէ նրա ներկայացումից:*

Ապացուցում: Եթե $\frac{f_1}{g_1} = \frac{f_2}{g_2}$, որտեղ $f_1 \neq 0$ և $f_2 \neq 0$, ապա $f_1 g_2 = f_2 g_1$ և

$$deg\left(\frac{f_1}{g_1}\right) = deg(f_1) - deg(g_1) = deg(f_1) + deg(g_2) - deg(g_2) - deg(g_1) =$$

$$= deg(f_1 g_2) - deg(g_2) - deg(g_1) = deg(f_2 g_1) - deg(g_2) - deg(g_1) =$$

$$= deg(f_2) + deg(g_1) - deg(g_2) - deg(g_1) = deg(f_2) - deg(g_2) = deg\left(\frac{f_2}{g_2}\right):$$

□

$\frac{f}{g} \in P(x)$ ռացիոնալ կոտորակը կոչվում է **անկրճատելի**, եթե f և g բազմանդամները փոխադարձաբար պարզ են: Հակառակ դեպքում $\frac{f}{g}$ ռացիոնալ կոտորակը կոչվում է **կրճատելի**:

Հատկություն 16.13: *Յուրաքանչյուր $\frac{f}{g} \in P(x)$ ռացիոնալ կոտորակ հավասար է անկրճատելի ռացիոնալ կոտորակի, որի համարիչն ու հայտարարը որոշվում են միարժեքորեն՝ միևնույն ոչ զրոյական հաստատունի ճշտությամբ:*

Ապացուցում: Եթե $d \rightleftharpoons (f, g)$, ապա $f = d \cdot f_1$, $g = d \cdot g_1$ և

$$\frac{f}{g} = \frac{d \cdot f_1}{d \cdot g_1} = \frac{f_1}{g_1},$$

որտեղ $(f_1, g_1) = 1$: Այժմ ապացուցենք այդ ներկայացման միակությունը: Դիցուք՝

$$\frac{f}{g} = \frac{f_1}{g_1} \quad \text{և} \quad \frac{f}{g} = \frac{f_2}{g_2},$$

որտեղ $(f_1, g_1) = 1$ և $(f_2, g_2) = 1$: Այդ դեպքում՝

$$\frac{f_1}{g_1} = \frac{f_2}{g_2},$$

այսինքն՝ $f_1 g_2 = f_2 g_1$: Այստեղից, համաձայն թեորեմ 16.12-ի, g_2-ը կբաժանվի g_1-ի վրա, իսկ g_1-ը կբաժանվի g_2-ի վրա: Հետևաբար, գոյություն կունենա այնպիսի $c \in P$, $c \neq 0$, հաստատուն, որ $g_1 = c \cdot g_2$ (բխում է լեմմ 16.5-ի 8)-րդ հատկությունից): Տեղադրելով այս արդյունքը $f_1 g_2 = f_2 g_1$ հավասարության մեջ, կստանանք՝ $f_1 g_2 = f_2 c g_2$, որտեղից՝ $f_1 = c f_2$, որովհետև $g_2 \neq 0$: □

$\frac{f}{g} \in P(x)$ ռացիոնալ կոտորակը կոչվում է **կանոնավոր**, եթե $f = 0$ կամ $deg(f) < deg(g)$ (այսինքն՝ $deg\left(\frac{f}{g}\right) < 0$):

Հատկություն 16.14: *Կանոնավոր ռացիոնալ կոտորակների գումարը, տարբերությունը և արտադրյալը նորից կանոնավոր ռացիոնալ կոտորակներ են:*

Ապացույցում: $\frac{f_1}{g_1} \in P(x)$ և $\frac{f_2}{g_2} \in P(x)$ կանոնավոր ռացիոնալ կոտորակների համար՝

$$\frac{f_1}{g_1} \pm \frac{f_2}{g_2} = \frac{f_1 g_2 \pm f_2 g_1}{g_1 g_2},$$

որտեղ կամ՝ $f_1 g_2 \pm f_2 g_1 = 0$ կամ՝ $deg\,(f_1 g_2 \pm f_2 g_1) < deg(g_1 g_2)$: Արտադրյալի դեպքում՝

$$\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2},$$

որտեղ եթե $f_1, f_2 \in P[x]$ բազմանդամներից գոնե մեկը զրոյական է, ապա $f_1 f_2 = 0$, հակառակ դեպքում՝

$$deg(f_1 f_2) = deg(f_1) + deg(f_2) < deg(g_1) + deg(g_2) = deg(g_1 g_2) \; : \qquad \square$$

Հետևություն 16.12: *$P(x)$ դաշտին պատկանող բոլոր կանոնավոր ռացիոնալ կոտորակների բազմությունը օղակ է՝ ռացիոնալ կոտորակների գումարման և բազմապատկման նկատմամբ:* □

Նկատենք, որ կանոնավոր ռացիոնալ թվերի գումարը, ընդհանուր դեպքում, կանոնավոր ռացիոնալ թիվ չէ (օրինակ՝ $\frac{1}{2}+\frac{1}{2}=1$):

Հատկություն 16.15: *Յուրաքանչյուր* $\frac{f}{g} \in P(x)$ *ռացիոնալ կոտորակ միարժեքորեն ներկայացվում է բազմանդամի և կանոնավոր ռացիոնալ կոտորակի գումարի տեսքով:*

Ապացուցում: Նախ ապացուցենք ներկայացման գոյությունը: Դիցուք $f, g \in P[x]$ և $g \neq 0$: f-ը մնացորդով բաժանենք g-ի վրա.

$$f = gq + r\,, \quad \text{որտեղ } r = 0 \text{ կամ } deg(r) < deg(g)\ :$$

Հետևաբար,

$$\frac{f}{g} = \frac{gq+r}{g} = q + \frac{r}{g}\,,$$

որտեղ $\frac{r}{g}$ ռացիոնալ կոտորակը կանոնավոր է: Այստեղ $q \in P[x]$ բազմանդամը կոչվում է $\frac{f}{g}$ ռացիոնալ կոտորակի **ամբողջ մաս**: Այժմ ապացուցենք ներկայացման միակությունը:

Եթե նաև

$$\frac{f}{g} = q' + \frac{r'}{g'}\,,$$

որտեղ $q' \in P[x]$, իսկ $\frac{r'}{g'}$ ռացիոնալ կոտորակը կանոնավոր է, ապա

$$q + \frac{r}{g} = q' + \frac{r'}{g'}\,,$$

$$q - q' = \frac{r'}{g'} - \frac{r}{g}\,,$$

որտեղ հավասարության աջ մասը կանոնավոր ռացիոնալ կոտորակ է (հատկություն 16.14): Եթե $\frac{r'}{g'} - \frac{r}{g} \neq \frac{0}{1}$, ապա կունենանք հետևյալ երկու ոչ զրոյական ռացիոնալ կոտորակների հավասարությունը՝

$$\frac{q-q'}{1} = \frac{r'}{g'} - \frac{r}{g}\,,$$

որտեղ ձախ մասի աստիճանը փոքր չէ 0-ից, իսկ աջ մասի աստիճանը փոքր է 0-ից, ինչը հակասում է լեմմ 16.13-ին: Ուստի, $\frac{r'}{g'} - \frac{r}{g} = 0$ և $q - q' = 0$: Հետևաբար, $\frac{r'}{g'} = \frac{r}{g}$ և $q = q'$: □

$\frac{f}{g} \in K(x)$ կանոնավոր ռացիոնալ կոտորակը կոչվում է **պարզագույն**, երբ $g = \varphi^n$, $n \geqslant 1$, որտեղ φ-ն չբերվող բազմանդամ է, իսկ $deg(f) < deg(\varphi)$, եթե $f \neq 0$:

Այժմ անցնենք ռացիոնալ կոտորակների վերաբերյալ հիմնական արդյունքին, որը օգտագործվում է նաև մաթեմատիկական անալիզի դասընթացում, ռացիոնալ ֆունկցիաների ինտեգրման ժամանակ՝ $P = \mathbb{R}$ դեպքում:

Թեորեմ 16.22: *1)* $\frac{f}{g_1 g_2} \in P(x)$ *տեսքի յուրաքանչյուր կանոնավոր ռացիոնալ կոտորակ, որտեղ* g_1 *և* g_2 *բազմանդամները փոխադարձաբար պարզ են, միարժեքորեն ներկայացվում է* g_1 *և* g_2 *հայտարարներով երկու կանոնավոր ռացիոնալ կոտորակների գումարի տեսքով՝*

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2} \ :$$

2) $\frac{f}{g_1 g_2 \cdots g_n} \in P(x)$ *տեսքի յուրաքանչյուր կանոնավոր ռացիոնալ կոտորակ, որտեղ* $g_1, g_2, \ldots, g_n$ *բազմանդամները զույգ առ զույգ փոխադարձաբար պարզ են , միարժեքորեն ներկայացվում է* $g_1, g_2, \ldots, g_n$ *հայտարարներով կանոնավոր ռացիոնալ կոտորակների գումարի տեսքով՝*

$$\frac{f}{g_1 g_2 \cdots g_n} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \cdots + \frac{f_n}{g_n} \ :$$

3) $\frac{f}{\varphi^m} \in P(x)$ *տեսքի յուրաքանչյուր կանոնավոր ռացիոնալ կոտորակ, որտեղ* φ*-ն չբերվող բազմանդամ է, միարժեքորեն ներկայացվում է* $\varphi^m, \varphi^{m-1}, \ldots, \varphi$ *հայտարարներով պարզագույն ռացիոնալ կոտորակների գումարի տեսքով՝*

$$\frac{f}{\varphi^m} = \frac{f_1}{\varphi^m} + \frac{f_2}{\varphi^{m-1}} + \cdots + \frac{f_m}{\varphi} \ :$$

4) Յուրաքանչյուր $\dfrac{f}{g} \in P(x)$ *կանոնավոր ռացիոնալ կոտորակ միարժեքորեն ներկայացվում է պարզագույն ռացիոնալ կոտորակների գումարի տեսքով: Ավելի ճշգրիտ, եթե* g*-ի կանոնական վերլուծությունն է՝* $g = \varphi_1^{m_1} \cdot \varphi_2^{m_2} \cdots \varphi_n^{m_n}$*, ապա* $\dfrac{f}{g}$ *կանոնավոր ռացիոնալ կոտորակը միարժեքորեն ներկայացվում է* $\varphi_1, \varphi_1^2, \ldots, \varphi_1^{m_1}$*,* $\varphi_2, \varphi_2^2, \ldots, \varphi_2^{m_2}$*,* $\ldots$*,* $\varphi_n, \varphi_n^2, \ldots, \varphi_n^{m_n}$ *հայտարարներով պարզագույն ռացիոնալ կոտորակների գումարի տեսքով:*

Ապացուցում: 1) Քանի որ $(g_1, g_2) = 1$, ապա գոյություն ունեն այնպիսի $g_1', g_2' \in P[x]$ բազմանդամներ, որ

$$g_1 g_1' + g_2 g_2' = 1 \ :$$

Միաժամանակ, fg_2'-ը մնացորդով բաժանելով g_1-ի վրա, կունենանք՝

$$fg_2' = g_1 q + f_1, \quad \text{որտեղ} \ \ f_1 = 0 \ \ \text{կամ} \ \ deg(f_1) < deg(g_1) \ :$$

Հետևաբար,

$$\frac{f}{g_1 g_2} = \frac{f \cdot 1}{g_1 g_2} = \frac{f\,(g_1 g_1' + g_2 g_2')}{g_1 g_2} = \frac{fg_1'}{g_2} + \frac{fg_2'}{g_1} =$$

$$= \frac{fg_1'}{g_2} + q + \frac{f_1}{g_1} = \frac{fg_1' + qg_2}{g_2} + \frac{f_1}{g_1} \ :$$

Այստեղ երկրորդ կոտորակը կանոնավոր է: Հետևաբար, այդպիսին կլինի նաև առաջին գումարելին՝ որպես երկու կանոնավոր կոտորակների տարբերություն: Այսպիսով,

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2},$$

որտեղ $\dfrac{f_1}{g_1}$ և $\dfrac{f_2}{g_2}$ ռացիոնալ կոտորակները կանոնավոր են: Ապացուցենք միակությունը: Դիցուք՝

$$\frac{f}{g_1 g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1'}{g_1'} + \frac{f_2'}{g_2'},$$

որտեղ բոլոր կոտորակները կանոնավոր են: Այստեղից հանգում ենք հետևյալ երկու կանոնավոր կոտորակների հավասարությանը՝

$$\frac{f_1 - f_1'}{g_1} = \frac{f_2' - f_2}{g_2} \, ,$$

այսինքն՝

$$(f_1 - f_1')\, g_2 = (f_2' - f_2)\, g_1 \, ,$$

որտեղ $(g_1, g_2) = 1$: Հետևաբար (թեորեմ 16.12), $f_1 - f_1'$ բազմանդամը կբաժանվի g_1-ի վրա: Մյուս կողմից, եթե $f_1 - f_1' \neq 0$, ապա $deg\,(f_1 - f_1') < deg(g_1)$ (քանի որ $\dfrac{f_1 - f_1'}{g_1}$ կոտորակը կանոնավոր է), իսկ այս դեպքում $f_1 - f_1'$ բազմանդամը չի կարող բաժանվել g_1-ի վրա: Ստացված հակասությունն ապացուցում է $f_1 - f_1' = 0$ հավասարությունը, որտեղից էլ բխում է $f_2 - f_2' = 0$ հավասարությունը: Այսպիսով, $f_1 = f_1'$ և $f_2 = f_2'$:

2) Ապացուցվում է վերհանգման եղանակով:

3) Ապացուցվում է վերհանգման եղանակով՝ ըստ $m \geqslant 1$ բնական թվի: Իրոք, $m = 1$ դեպքում պնդումն ակնհայտ է: Ենթադրենք այն ճիշտ է m-ից փոքր բոլոր բնական թվերի դեպքում: Եթե f-ը մնացորդով բաժանենք φ-ի վրա՝

$$f = \varphi q_1 + f_1, \quad \text{որտեղ} \;\; f_1 = 0 \;\; \text{կամ} \;\; deg(f_1) < deg(\varphi)\, ,$$

ապա կունենանք՝

$$\frac{f}{\varphi^m} = \frac{f_1}{\varphi^m} + \frac{q_1}{\varphi^{m-1}} \, ,$$

որտեղ $\dfrac{q_1}{\varphi^{m-1}}$ ռացիոնալ կոտորակը, որպես $\dfrac{f}{\varphi^m}$ և $\dfrac{f_1}{\varphi^m}$ կանոնավոր ռացիոնալ կոտորակների տարբերություն, ևս կլինի կանոնավոր: Ըստ որում, այս ներկայացումը միակն է, որովհետև եթե նաև

$$\frac{f}{\varphi^m} = \frac{f_1'}{\varphi^m} + \frac{q_1'}{\varphi^{m-1}} \, ,$$

որտեղ $f_1' = 0$ կամ $deg(f_1') < deg(\varphi)$, ապա

$$f = \varphi q_1' + f_1'$$

և $q_1' = q$, $f_1' = f$ (թեորեմ 16.2): Մնում է $\dfrac{q_1}{\varphi^{m-1}}$ կանոնավոր ռացիոնալ կոտորակի համար կիրառել վերհանգային ենթադրությունը:

4) Նախ ապացուցենք ներկայացման գոյությունը: Թեորեմի ձևակերպման մեջ, առանց ընդհանրությունը խախտելու, $g \in P[x]$ բազմանդամը ենթադրվում է ունիտար, այսինքն` նրա ավագ անդամի գործակիցը վերցվում է $1 \in P$: Օգտվենք $g$-ի կանոնական վերլուծությունից`

$$g = \varphi_1^{m_1} \cdot \varphi_2^{m_2} \cdots \varphi_n^{m_n}\,,$$

որտեղ $\varphi_1, \varphi_2, \ldots, \varphi_n \in P[x]$ բազմանդամները չբերվող, չզուգորդված և զույգ առ զույգ փոխադարձաբար պարզ բազմանդամներ են (հատկություն 16.8): Հետևաբար, $\varphi_1^{m_1}, \varphi_2^{m_2}, \ldots, \varphi_n^{m_n}$ բազմանդամները ևս կլինեն զույգ առ զույգ փոխադարձաբար պարզ (հետևություն 16.8): Ուստի, համաձայն 2) պնդման`

$$\frac{f}{g} = \frac{f}{\varphi_1^{m_1} \cdot \varphi_2^{m_2} \cdots \varphi_n^{m_n}} = \frac{f_1}{\varphi_1^{m_1}} + \frac{f_2}{\varphi_2^{m_2}} + \cdots + \frac{f_n}{\varphi_n^{m_n}}\,,$$

որտեղ աջ մասի բոլոր կոտորակները նույնպես կանոնավոր են: Մնում է օգտվել 3) պնդումից:
Ներկայացման միակությունը բխում է 2), 3) պնդումների միակության մասերից: □

Օրինակներ: 1) Եթե $g \in P[x]$ ունիտար բազմանդամն ունի հետևյալ կանոնական վերլուծությունը`

$$g = (x - c_1)^{m_1} \cdot (x - c_2)^{m_2} \cdots (x - c_n)^{m_n}, \qquad c_i \in P\,,$$

ապա $\dfrac{f}{g} \in P(x)$ կանոնավոր ռացիոնալ կոտորակը կունենա հետևյալ վերլուծությունը` ըստ պարզագույն ռացիոնալ կոտորակների գումարի.

$$\frac{f}{g} = \frac{c_{11}}{(x - c_1)^{m_1}} + \cdots + \frac{c_{1m_1}}{x - c_1} + \frac{c_{21}}{(x - c_2)^{m_2}} + \cdots + \frac{c_2 m_2}{x - c_2} + \cdots$$

$$\cdots + \frac{c_{n1}}{(x - c_n)^{m_n}} + \cdots + \frac{c_{nm_n}}{x - c_n}\,,$$

որտեղ $c_{im_i} \in P$: Մասնավորապես, եթե g բազմանդամը P դաշտում չունի բազմապատիկ արմատներ և

$$g = (x - c_1) \cdot (x - c_2) \cdots (x - c_n), \qquad c_i \in P\,,$$

ապա $\frac{f}{g} \in P(x)$ կանոնավոր ռացիոնալ կոտորակի համար կունենանք հետևյալ վերլուծությունը՝

$$\frac{f}{g} = \frac{a_1}{x-c_1} + \frac{a_2}{x-c_2} + \cdots + \frac{a_n}{x-c_n}\,,$$

որտեղ $a_1, a_2, \ldots, a_n \in P$, $c_i \neq c_j$, եթե $i \neq j$: Այստեղից, բազմապատկելով հավասարության երկու կողմերը g-ով, կստանանք՝

$$f(c_i) = a_i(c_i - c_1)\cdots(c_i - c_{i-1})(c_i - c_{i+1})\cdots(c_i - c_n) = a_i g'(c_i)\,,$$

որտեղ $g'(c_i) \neq 0$: Հետևաբար,

$$a_i = \frac{f(c_i)}{g'(c_i)} \quad \text{և} \quad \frac{f}{g} = \sum_{i=1}^{n} \frac{f(c_i)}{g'(c_i)(x-c_i)} \ :$$

Այս բանաձևը կոչվում է **Լագրանժի բանաձև**:

2) Ֆերմայի փոքր թեորեմից բխում է, որ $\mathbb{Z}_p$ դաշտի յուրաքանչյուր տարր $g = x^p - x \in \mathbb{Z}_p[x]$ բազմանդամի արմատ է և, հետևաբար, $\mathbb{Z}_p$ դաշտում $x^p - x$ բազմանդամը չունի բազմապատիկ արմատ (թեորեմ 16.16): Նշանակելով $[k] \in \mathbb{Z}_p$ դասը k-ով և օգտվելով Բեզուի թեորեմից ու հատկություն 16.4-ից, կունենանք՝

$$x^p - x = x(x-1)\cdots(x-(p-1)) \ :$$

Ուստի, համաձայն Լագրանժի ստացված բանաձևի,

$$\frac{1}{x^p - x} = -\sum_{k=0}^{p-1} \frac{1}{x-k}\,,$$

որովհետև $f = 1$, իսկ $g' = (x^p - x)' = px^{p-1} - 1 = -1$:

3) Թեորեմ 16.19-ի համաձայն $g = x^n - 1 \in \mathbb{C}[x]$ բազմանդամը կոմպլեքս թվերի $\mathbb{C}$ դաշտում չունի բազմապատիկ արմատ և $x^n - 1 = (x - \varepsilon_0)(x - \varepsilon_1)\cdots(x - \varepsilon_n)$, որտեղ $\{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\} = \sqrt[n]{1} \subseteq \mathbb{C}$: Հետևաբար, Լագրանժի բանաձևի օգնությամբ ստացվում է նաև $\frac{1}{x^n - 1} \in \mathbb{C}(x)$ կանոնավոր ռացիոնալ կոտորակի հետևյալ վերլուծությունը՝

$$\frac{1}{x^n - 1} = \frac{1}{n}\sum_{i=0}^{n-1} \frac{1}{\varepsilon_i^{n-1}(x-\varepsilon_i)} = \frac{1}{n}\sum_{i=0}^{n-1} \frac{\varepsilon_i}{x-\varepsilon_i} \ :$$

16.8. Մնացքների օղակ և մնացքների դաշտ՝ ըստ տրված բազմանդամի

Դիցուք P-ն կամայական դաշտ է և դիցուք տրված է $h \in P[x]$ բազմանդամը, որն այստեղ կարելի է անվանել **հենք** կամ **մոդուլ**: Երկու $f_1, f_2 \in P[x]$ բազմանդամներ կոչվում են **բաղդատելի** ըստ h բազմանդամի և նշանակվում է $f_1 \equiv f_2(mod\, h)$, եթե $f_1 - f_2 = f_1 + (-f_2)$ տարբերությունը բաժանվում է h-ի վրա: Սահմանված «$\equiv$» հարաբերությունը կոչվում է **բազմանդամների բաղդատման հարաբերություն**:

Լեմմ 16.14: *Բազմանդամների բաղդատման հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $f \equiv f(mod\, h)$ ցանկացած $f \in P[x]$ բազմանդամի համար; (ռեֆլեքսիվություն)

բ) $f_1 \equiv f_2(mod\, h) \longrightarrow f_2 \equiv f_1(mod\, h)$; (համաչափություն)

գ) $f_1 \equiv f_2(mod\, h)$, $f_2 \equiv f_3(mod\, h) \longrightarrow f_1 \equiv f_3(mod\, h)$: (փոխանցականություն) □

Լեմմ 16.15: *Որպեսզի $f_1, f_2 \in P[x]$ բազմանդամները լինեն բաղդատելի ըստ $h \neq 0$ բազմանդամի անհրաժեշտ է և բավարար, որ*

$$f_1 = hq_1 + r\,,$$

$$f_2 = hq_2 + r\,,$$

որտեղ $r = 0$ կամ $deg(r) < deg(h)$: □

Օրինակներ: 1) Եթե $h = 0$, ապա

$$f_1 \equiv f_2(mod\, h) \longleftrightarrow f_1 = f_2\,;$$

2) Եթե $h = c \in P$, $c \neq 0$, ապա

$$f_1 \equiv f_2(mod\, h) \longleftrightarrow f_1, f_2 \in P[x]\ :$$

Հատկություն 16.16: *Եթե $f_1 \equiv f_2(mod\, h)$ և $f_3 \equiv f_4(mod\, h)$, ապա*

$$f_1 \pm f_3 \equiv f_2 \pm f_4(mod\, h) \quad \text{և} \quad f_1 f_3 \equiv f_2 f_4(mod\, h)\ :$$

Ապացուցում: Առաջին բաղդատումն ակնհայտ է, իսկ երկրորդը բխում է հետևյալ հավասարությունից՝

$$f_1f_3 - f_2f_4 = f_1f_3 - f_2f_3 + f_2f_3 - f_2f_4 = (f_1 - f_2)f_3 + f_2(f_3 - f_4) \ : \quad \square$$

$f \in P[x]$ տարրի համարժեքության դասը, ըստ «$\equiv$» համարժեքության, կլինի՝

$$[f] = \{g \in P[x] \mid g \equiv f(mod\, h)\} \ :$$

$[f]$ համարժեքության դասի յուրաքանչյուր տարր կոչվում է այդ դասի **ներկայացուցիչ** կամ **մնացք**, իսկ $[f]$-ը կոչվում է նաև **մնացքների դաս**: Ըստ որում՝

$$[f] = [f'] \longleftrightarrow f \equiv f'(mod\, h) \ :$$

Մասնավորապես,

$$f' \in [f] \longrightarrow f' \equiv f(mod\, h) \longrightarrow [f'] = [f] \ :$$

Ստացվող բոլոր համարժեքության դասերի բազմությունը նշանակվում է $P[x]\big/(h)$-ով, այսինքն՝

$$P[x]\big/(h) = \{[f] \mid f \in P[x]\} \ :$$

Համարժեքության դասերի այս բազմության մեջ սահմանենք **գումարման** և **բազմապատկման** (արտադրյալի) հետևյալ երկու գործողությունները՝

$$[f_1] + [f_2] = [f_1 + f_2] \, ,$$
$$[f_1] \cdot [f_2] = [f_1 \cdot f_2] \ :$$

Նախ նկատենք, որ համարժեքության դասերի այս գումարման և բազմապատկման արդյունքները կախված չեն ներկայացուցիչների ընտրությունից: Իրոք, եթե $[f_1] = [f_1']$ և $[f_2] = [f_2']$, ապա $f_1 \equiv f_1'(mod\, h)$, $f_2 \equiv f_2'(mod\, h)$ և, հատկություն 16.16-ի համաձայն,

$$f_1 + f_2 \equiv f_1' + f_2'(mod\, h) \, ,$$

$$f_1 \cdot f_2 \equiv f_1' \cdot f_2'(mod\, h) \ ,$$

այսինքն՝

$$[f_1 + f_2] = [f_1' + f_2'] \, ,$$
$$[f_1 \cdot f_2] = [f_1' \cdot f_2'] \ :$$

Հատկություն 16.17: *$P[x]\big/(h)$ բազմությունը օղակ է՝ համարժեքության դասերի գումարման և բազմապատկման նկատմամբ: Այս օղակը զուգորդական է, տեղափոխական, միավորով օժտված և կոչվում է* P **դաշտի նկատմամբ սահմանված մնացքների օղակ՝ ըստ տրված** h **բազմանդամի:**

Ապացույց: Համարժեքության դասերի գումարը և արտադրյալը զուգորդական են, տեղափոխական և կապված են բաշխական օրենքով՝

$$[f_1]\left([f_2]+[f_3]\right)=[f_1][f_2]+[f_1][f_3] \ :$$

$[0]$ դասը կատարում է զրոյի դերը, այսինքն՝

$$[f]+[0]=[f+0]=[f] \ :$$

$[-f]$ դասը կլինի $[f]$-ի հակադիրը, որովհետև

$$[f]+[-f]=[f+(-f)]=[0] \ :$$

$[1]$ դասը կլինի օղակի միավորը, որովհետև

$$[f]\cdot[1]=[f\cdot 1]=[f] \ : \qquad \square$$

Լեմմ 16.16: *1) Եթե $g\in[f]$, ապա*

$$d \rightleftharpoons (g,h) \longleftrightarrow d \rightleftharpoons (f,h) \ :$$

2) Որպեսզի $P[x]\big/(h)$ օղակի $[f]$ տարրը լինի հակադարձելի անհրաժեշտ է և բավարար, որ f և h բազմանդամները լինեն փոխադարձաբար պարզ:

Ապացույց: Ապացուցենք 1)-ը: Եթե $g\in[f]$, ապա $g\equiv f(mod\, h)$, այսինքն՝ $g-f=hq$, $q\in P[x]$, և $g=f+hq$: Իսկ վերջին հավասարությունից բխում է, որ f, h զույգի բոլոր ընդհանուր բաժանարարների բազմությունը համընկնում է g, h զույգի բոլոր ընդհանուր բաժանարարների բազմության հետ:

Ապացուցենք 2)-ը: Եթե $[f]\in P[x]\big/(h)$ տարրը հակադարձելի է $P[x]\big/(h)$ օղակում, ապա գոյություն ունի այնպիսի $[f']\in P[x]\big/(h)$ տարր, որ $[f][f']=[1]$, այսինքն՝ $[f\cdot f']=[1]$ և $ff'\equiv 1(mod\, h)$, այսինքն` $ff' - 1 = hq$ կամ $ff' + h(-q) = 1$ և $(f, h) = 1$ (համաձայն բազմանդամների փոխադարձաբար պարզության հայտանիշի):

Հակառակ քայլերով ապացուցվում է, որ եթե $(f, h) = 1$, ապա $[f] \in P[x]\big/(h)$ տարրը հակադարձելի է $P[x]\big/(h)$ օղակում: $\square$

Թեորեմ 16.23: $P[x]\big/(h)$ *մնացքների օղակը կլինի դաշտ այն և միայն այն դեպքում, երբ h-ը չբերվող բազմանդամ է: Այս դաշտը կոչվում է P դաշտի նկատմամբ սահմանված մնացքների դաշտ` ըստ տրված h չբերվող բազմանդամի:*

Ապացուցում: Դիցուք $h \in P[x]$ բազմանդամը չբերվող է և $[f] \in P[x]\big/(h)$, որտեղ $[f] \neq [0]$, այսինքն` f-ը չի բաժանվում h-ի վրա: Հետևաբար, հատկություն 16.7-ի համաձայն, $(f, h) = 1$: Մնում է օգտվել լեմմ 16.16-ից:

Հակառակ դեպքում, h բազմանդամը կամ հաստատուն է կամ բերվող: Առաջին դեպքում կամ` $h = 0$ կամ` $h = c \in P$, $c \neq 0$: Եթե $h = c \in P$, $c \neq 0$, ապա $P[x]\big/(h)$ օղակը կլինի մեկ տարրանի և, հետևաբար, դաշտ չէ: Իսկ եթե $h = 0$, ապա $P[x]\big/(h)$ օղակը դաշտ չէ, որովհետև նրա յուրաքանչյուր $[f]$ տարր, որտեղ f-ը տարբեր է հաստատունից, հակադարձելի չէ:

Դիցուք h-ը բերվող է, այսինքն` $h = f_1 \cdot f_2$, որտեղ $0 < deg(f_1) < deg(h)$, $0 < deg(f_2) < deg(h)$: Հետևաբար, $[f_1] \neq [0]$, $[f_2] \neq [0]$ և

$$[f_1] \cdot [f_2] = [f_1 \cdot f_2] = [h] = [0]\,,$$

այսինքն` $P[x]\big/(h)$ օղակն, այս դեպքում, ունի զրոյի բաժանարարներ և, հետևաբար, դաշտ չէ: $\square$

Քանի որ $P[x]\big/(h)$ մնացքների դաշտում`

$$[c_1] = [c_2] \longleftrightarrow c_1 = c_2\,,$$

$$[c_1] + [c_2] = [c_1 + c_2]\,,$$

$$[c_1] \cdot [c_2] = [c_1 \cdot c_2]\,,$$

որտեղ $c_1, c_2 \in P$, ապա $[c] \in P[x]\big/(h)$ տարրը կարելի է նույնականացնել $c \in P$ տարրի հետ, որի հետևանքով $P[x]\big/(h)$ դաշտը դառնում է P դաշտի ընդլայնումը:

Օրինակներ: 1) Քանի որ $h = 1 + x + x^2$ բազմանդամը չբերվող է $\mathbb{Z}_2$ դաշտում, ապա $\mathbb{Z}_2[x]\big/(1 + x + x^2)$ մնացքների օղակը կլինի դաշտ: Ըստ որում,

$$\mathbb{Z}_2[x]\big/(1 + x + x^2) = \{[0], [1], [x], [x + 1]\} \ :$$

Այստեղ մենք օգտվեցինք այն փաստից, որ եթե մնացորդով բաժանման ժամանակ՝

$$f = hq + r, \quad \text{որտեղ } r = 0 \text{ կամ } deg(r) < deg(h)\,,$$

ապա $[f] = [r]$: Այսպիսով, մնում է հաշվել ստացվող $r \in \mathbb{Z}_2[x]$ մնացորդները: Դրանք են՝ 0, 1, x, $x + 1$ բազմանդամները:

2) Քանի որ $h = 1 + x + x^3$ բազմանդամը չբերվող է $\mathbb{Z}_2$ դաշտի նկատմամբ, ապա $\mathbb{Z}_2[x]\big/(1 + x + x^3)$ մնացքների օղակը ևս դաշտ է: Ըստ որում,

$$\mathbb{Z}_2[x]\big/(1 + x + x^3) = \big\{[0], [1], [x], [x + 1], [x^2], [x^2 + 1], [x^2 + x], [x^2 + x + 1]\big\} \ :$$

3) Եթե $|P| = p$, իսկ $h \in P[x]$ չբերվող բազմանդամի աստիճանը հավասար է n-ի, ապա $P[x]\big/(h)$ մնացքների դաշտի կարգը կլինի՝ p^n, որովհետև h-ի վրա բաժանելուց ստացվող բոլոր

$$r = b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}\,, \quad b_i \in P\,,$$

տեսքի մնացորդների քանակը կլինի հավասար բոլոր $(b_0, b_1, \ldots, b_{n-1})$ կարգավորված n-յակների քանակին, որտեղ $b_0, b_1, \ldots, b_{n-1}$ տարրերը փոփոխվում են P բազմության վրա:

4) Քանի որ $h = 1 + x^2$ բազմանդամը չբերվող է իրական թվերի $\mathbb{R}$ դաշտում, ապա $\mathbb{R}[x]\big/(1 + x^2)$ մնացքների օղակը դաշտ է և այն կլինի իզոմորֆ կոմպլեքս թվերի $\mathbb{C}$ դաշտին, այսինքն՝

$$\mathbb{R}[x]\big/(1 + x^2) \simeq \mathbb{C} \ :$$

Իրոք, ցանկացած $f \in \mathbb{R}[x]$ բազմանդամի համար գոյություն ունի միարժեքորեն որոշվող այնպիսի $a, b \in \mathbb{R}$ զույգ, որ

$$f = (1 + x^2)q + (ax + b)\,,$$

որտեղից $[f] = [ax + b]$ և $\lambda: \ [f] \to (a, b)$ արտապատկերումը կլինի փոխմիարժեք (բիեկտիվ) արտապատկերում՝ $\mathbb{R}[x]\Big/(1 + x^2) \to \mathbb{C}$: Ըստ որում,

$$\lambda(u + v) = \lambda(u) + \lambda(v) \quad \text{և} \quad \lambda(u \cdot v) = \lambda(u) \cdot \lambda(v)$$

ցանկացած $u, v \in \mathbb{R}[x]\Big/(1 + x^2)$ տարրերի համար:

5) Ցանկացած P դաշտի համար՝

$$P[x]\Big/(x) \simeq P\ :$$

16.9. Դաշտի պարզ ընդլայնումներ

Դիցուք F դաշտը P դաշտի ընդլայնումն է և $\alpha \in F$: F-ի բոլոր այն ենթադաշտերի հատումը, որոնք պարունակում են P-ն և α-ն, ևս կլինի F-ի ենթադաշտ և այդ ենթադաշտը նշանակվում է $P_F[\alpha]$-ով: $P_F[\alpha] \leqslant F$ ենթադաշտը կոչվում է P **դաշտի պարզ ընդլայնում** $\alpha \in F$ **տարրի միջոցով** (օգնությամբ): Ակնհայտ է, որ $P_F[\alpha]$-ն ընկած է F-ի բոլոր այն ենթադաշտերի մեջ, որոնք պարունակում են P-ն և α-ն, այսինքն՝ $P_F[\alpha]$-ն P-ն և α-ն պարունակող F-ի փոքրագույն (մինիմալ) ենթադաշտն է: Հետևաբար, եթե $P_1 \leqslant P_F[\alpha]$ ենթադաշտը պարունակում է P-ն և α-ն, ապա $P_1 = P_F[\alpha]$:

Լեմմ 16.17: *Եթե F դաշտը P դաշտի ընդլայնումն է և $\alpha \in F$, ապա*

$$P_F[\alpha] = \left\{ \frac{f(\alpha)}{g(\alpha)} \in F \,\middle|\, \ f, g \in P[x],\ g(\alpha) \neq 0 \right\}\ :$$

Ապացույց: Բավական է նկատել, որ հավասարության աջ մասը բավարարում է հետևյալ երեք պայմաններին. F-ի ենթադաշտ է, պարունակում է P-ն և α-ն, ընկած է P-ն և α-ն պարունակող F-ի ցանկացած ենթադաշտի մեջ: Մասնավորապես, հավասարության աջ մասը ընկած է $P_F[\alpha]$-ի մեջ: $\square$

$\alpha \in F$ տարրը կոչվում է **տրանսցենդենտ** $P \leqslant F$ դաշտի նկատմամբ, եթե գոյություն չունի հաստատունից տարբեր այնպիսի $f \in P[x]$ բազմանդամ, որ $f(\alpha) = 0$: Հակառակ դեպքում՝ α-ն կոչվում է **հանրահաշվական** $P \leqslant F$ դաշտի նկատմամբ:

Օրինակներ: Քանի որ ռացիոնալ թվերի $\mathbb{Q}$ բազմությունը հաշվելի է, ապա կլինի հաշվելի նաև բազմանդամների $\mathbb{Q}[x]$ բազմությունը: Մյուս կողմից, յուրաքանչյուր ոչ զրոյական $f \in \mathbb{Q}[x]$ բազմանդամ $\mathbb{R}$-ում կարող է ունենալ միայն վերջավոր թվով արմատներ: Հետևաբար, $\mathbb{R}$-ում գոյություն ունեն ամենաշատը հաշվելի թվով տարրեր, որոնք հանրահաշվական են $\mathbb{Q}$-ի նկատմամբ: Քանի որ $\mathbb{R}$-ը հաշվելի չէ, ապա $\mathbb{R}$-ում գոյություն ունեն այնպիսի տարրեր, որոնք տրանսցենդենտ են $\mathbb{Q}$-ի նկատմամբ: Այդպիսին են, օրինակ, π, e, $2^{\sqrt{2}}$ թվերը:

$P_F[\alpha]$ պարզ ընդլայնումը կոչվում է տրանսցենդենտ, եթե $\alpha \in F$ տարրը տրանսցենդենտ է $P \leqslant F$ դաշտի նկատմամբ և՝ հանրահաշվական, եթե $\alpha \in F$ տարրը հանրահաշվական է $P \leqslant F$ դաշտի նկատմամբ:

Դաշտի պարզ ընդլայնումները նկարագրվում (բնութագրվում) են հետևյալ երկու դեպքով:

Թեորեմ 16.24: *1) $P \leqslant F$ դաշտի ցանկացած $P_F[\alpha]$ տրանսցենդենտ ընդլայնում իզոմորֆ է ռացիոնալ կոտորակների $P(x)$ դաշտին, այսինքն՝*

$$P_F[\alpha] \simeq P(x)$$

ցանկացած $\alpha \in F$ տրանսցենդենտ տարրի համար:

2) $P \leqslant F$ դաշտի ցանկացած $P_F[\alpha]$ հանրահաշվական ընդլայնում իզոմորֆ է $P[x]\Big/(\varphi)$ մնացքների դաշտին, որտեղ $\varphi \in P[x]$ բազմանդամը չբերվող է P դաշտի նկատմամբ և $\varphi(\alpha) = 0$ (օրինակ, որպես φ կարելի է վերցնել այն փոքրագույն աստիճանի բազմանդամը, որի համար $\varphi(\alpha) = 0$):

Ապացույցում: 1) Եթե α-ն տրանսցենդենտ է P դաշտի նկատմամբ, ապա $g(\alpha) \neq 0$ ցանկացած ոչ զրոյական $g \in P[x]$ բազմանդամի համար: Հետևաբար, $\dfrac{f(\alpha)}{g(\alpha)}$-ն գոյություն կունենա ցանկացած $\dfrac{f}{g} \in P(x)$ ռացիոնալ կոտորակի համար: Մնում է ստուգել, որ

$$\mu : \frac{f}{g} \longrightarrow \frac{f(\alpha)}{g(\alpha)}$$

արտապատկերումը իզոմորֆիզմ է $P(x)$ և $P_F[\alpha]$ (տես նախորդ լեմմը) դաշտերի միջև, այսինքն՝ սահմանված $\mu\ :\ \ P(x)\ \to\ P_F[\alpha]$ արտապատկերումը փոխմիարժեք է և

$$\mu(u+v)=\mu(u)+\mu(v)\,,$$

$$\mu(u\cdot v)=\mu(u)\cdot\mu(v)\ :$$

Օրինակ, ստուգենք μ արտապատկերման ներդրող (ինյեկտիվ) լինելը, ելնելով α-ի տրանսցենդենտությունից.

$$\mu\left(\frac{f_1}{g_1}\right)=\mu\left(\frac{f_2}{g_2}\right)\longrightarrow\frac{f_1(\alpha)}{g_1(\alpha)}=\frac{f_2(\alpha)}{g_2(\alpha)}\longrightarrow$$

$$\longrightarrow f_1(\alpha)\cdot(g_1(\alpha))^{-1}=f_2(\alpha)\cdot(g_2(\alpha))^{-1}\longrightarrow f_1(\alpha)\cdot g_2(\alpha)=f_2(\alpha)\cdot g_1(\alpha)\longrightarrow$$

$$\longrightarrow f_1(\alpha)\,g_2(\alpha)-f_2(\alpha)\,g_1(\alpha)=0\longrightarrow(f_1g_2-f_2g_1)\alpha=0\longrightarrow$$

$$\longrightarrow f_1g_2-f_2g_1=0\longrightarrow\frac{f_1}{g_1}=\frac{f_2}{g_2}\ :$$

μ արտապատկերման վերադրող (սյուրեկտիվ) լինելն ակնհայտ է, իսկ մյուս երկու պայմանները ստուգվում են հեշտությամբ:

2) Դիցուք $\alpha\in F$ տարրը հանրահաշվական է $P\leqslant F$ դաշտի նկատմամբ և $f(\alpha)=0$, որտեղ $f\in P[x]$, $f\neq c\in P$: Քանի որ (թեորեմ 16.5), $f=\varphi_1\cdot\varphi_2\cdots\varphi_n$, որտեղ $\varphi_1\cdot\varphi_2\cdots\varphi_n\in P[x]$ բազմանդամները չբերվող են P դաշտի նկատմամբ, ապա $f(\alpha)=\varphi_1(\alpha)\cdot\varphi_2(\alpha)\cdots\varphi_n(\alpha)=0$, որտեղից $\varphi_i(\alpha)=0$ որևէ $i=1,2,\ldots,n$ արժեքի դեպքում: Այսպիսով, կարող ենք ենթադրել, որ α հանրահաշվական տարրի համար միշտ գոյություն ունի P դաշտի նկատմամբ չբերվող այնպիսի $\varphi\in P[x]$ բազմանդամ, որ $\varphi(\alpha)=0$: Ակնհայտ է, որ այդպիսի φ չբերվող բազմանդամի աստիճանը որոշվում է միարժեքորեն, որովհետև եթե $\varphi(\alpha)=\varphi'(\alpha)=0$, այսինքն՝ φ և φ' չբերվող բազմանդամներն ունեն ընդհանուր $\alpha\in F$ արմատ, ապա նրանք կլինեն զուգորդված (հատկություն 16.8):

Համաձայն թեորեմ 16.23-ի, $P[x]\big/_{(\varphi)}$ մնացքների օղակը կլինի դաշտ: Այժմ ապացուցենք հետևյալ հավասարությունը՝

$$\left\{\frac{f(\alpha)}{g(\alpha)}\in F\,\middle|\ \ f,g\in P[x],\ g(\alpha)\neq0\right\}=\{f(\alpha)\in F\,|\ \ f\in P[x]\}\ :$$

Աջ մասն ակնհայտորեն ընկած է ձախ մասի մեջ: Ապացուցենք հակառակ ներդրումը: Քանի որ $g(\alpha) \neq 0$, ապա (հատկություն 16.7) g և φ բազմանդամները կլինեն փոխադարձաբար պարզ, այսինքն՝ գոյություն կունենան այնպիսի $g', \varphi' \in P[x]$ բազմանդամներ, որ $gg' + \varphi\varphi' = 1$ և $g(\alpha)g'(\alpha) + \varphi(\alpha)\varphi'(\alpha) = 1$ կամ $g(\alpha)g'(\alpha) = 1$ և $\dfrac{f(\alpha)}{g(\alpha)} = f(\alpha)g'(\alpha)$: Ուստի, $\dfrac{f(\alpha)}{g(\alpha)}$ կոտորակը հավասար է $f \cdot g' \in P[x]$ բազմանդամի արժեքին $\alpha \in F$ կետում: Այսպիսով, համաձայն լեմմ 16.17-ի, $P_F[\alpha] = \{f(\alpha) \in F \mid f \in P[x]\}$: Այնուհետև, $f_1, f_2 \in P[x]$ բազմանդամների համար՝

$$f_1(\alpha) = f_2(\alpha) \longleftrightarrow f_1 \equiv f_2(mod\,\varphi) \ :$$

Իրոք, եթե $f_1 \equiv f_2(mod\,\varphi)$, ապա $f_1 - f_2 = \varphi q$ և

$$f_1(\alpha) - f_2(\alpha) = \varphi(\alpha)\,q(\alpha) = 0 \ :$$

Եվ հակառակը, եթե $f_1(\alpha) - f_2(\alpha) = 0$, ապա $f_1 - f_2 \in P[x]$ բազմանդամը կունենա ընդհանուր $\alpha \in F$ արմատ $\varphi \in P[x]$ չբերվող բազմանդամի հետ և, հետևաբար, $f_1 - f_2$ բազմանդամը կբաժանվի φ-ի վրա (հատկություն 16.7):

Մնում է նկատել, որ $\mu : [f] \to f(\alpha)$ արտապատկերումը կլինի իզոմորֆիզմ $P[x]\big/(\varphi)$ և $P_F[\alpha]$ դաշտերի միջև: □

16.10. Բազմանդամի վերլուծության դաշտ: Կրոնեկերի և Գալուայի թեորեմները

Եթե $f \in P[x]$ բազմանդամը չբերվող է P դաշտի նկատմամբ և $deg(f) \geqslant 2$, ապա այն չունի արմատ P-ում:

Թեորեմ 16.25: *P դաշտի նկատմամբ չբերվող ցանկացած $f \in P[x]$ բազմանդամի համար գոյություն ունի P դաշտի ընդլայնում հանդիսացող այնպիսի F դաշտ, որտեղ f-ն ունի արմատ: Որպես F կարելի է վերցնել $P[x]\big/(f)$ մնացքների դաշտը:*

Ապացուցում: Իրոք, ինչպես գիտենք, եթե $f \in P[x]$ բազմանդամը չբերվող է P դաշտում, ապա $P[x]\big/(f)$ մնացքների օղակը P դաշտի ընդլայնում հանդիսացող դաշտ է (թեորեմ 16.23), իսկ $\alpha = [x] \in$

$P[x]\big/(f)$ տարրը կլինի արմատ $f = a_0 + a_1x + \cdots + a_nx^n$ բազմանդամի համար, որովհետև

$$0 = [0] = [f] = [a_0 + a_1x + \cdots + a_nx^n] = [a_0] + [a_1x] + \cdots + [a_nx^n] =$$

$$= a_0 + a_1[x] + \cdots + a_n[x]^n = f([x]) = f(\alpha) \ :$$

Թեորեմ 16.24-ի համաձայն՝

$$F = P[x]\big/(f) = P_F[\alpha] \ : \qquad \square$$

Հետևություն 16.13 *:* Ցանկացած P դաշտի և հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամի համար գոյություն ունի P դաշտի ընդլայնում հանդիսացող այնպրսի F դաշտ, որտեղ f-ն ունի արմատ:

Ապացուցում: Դիցուք $f \in P[x]$ բազմանդամն ունի հետևյալ կանոնական վերլուծությունը P դաշտում՝

$$f = c \cdot \varphi_1^{n_1} \cdot \varphi_2^{n_2} \cdots \varphi_s^{n_s} \ :$$

Համաձայն ապացուցված թեորեմի, գոյություն ունի այնպիսի $F \geqslant P$ դաշտ և այնպիսի $c_1 \in F$ տարր, որ $\varphi_1(c_1) = 0$: Հետևաբար $f(c_1) = 0$: $\square$

Թեորեմ 16.26 (Կրոնեկեր): *Ցանկացած P դաշտի և հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամի համար գոյություն ունի P դաշտի ընդլայնում հանդիսացող այնպիսի P' դաշտ, որի նկատմամբ f-ը վերլուծվում է գծային բազմանդամների արտադրյալի, այսինքն՝*

$$f = c(x - c_1)(x - c_2) \cdots (x - c_n)\,,$$

որտեղ $c_1, c_2, \ldots, c_n \in P'$, $n = deg(f) \geqslant 1$:

Ապացուցում: Ապացուցվում է վերհանգման եղանակով՝ ըստ $n = deg(f) \geqslant 1$ բնական թվի: Եթե $n = 1$, ապա f-ը կլինի գծային և կարելի է ընտրել $P' = P$: Եթե $n = deg(f) > 1$, ապա f-ը բաժանվում է որևէ $\varphi \in P[x]$ չբերվող բազմանդամի վրա (լեմմ 16.9), այսինքն՝ $f = \varphi \cdot q$: Սակայն, համաձայն թեորեմ 16.25-ի, գոյություն ունի այնպիսի $F \geqslant P$ դաշտ, որը պարունակում է φ-ի որևէ c արմատ: Հետևաբար, Բեզուի թեորեմի համաձայն, $F[x]$-ում կունենանք՝ $\varphi = (x - c)q_1$ և $f = \varphi \cdot q = (x - c)q_1q$, որտեղ $0 < deg(q_1q) = n - 1 < n$: Մնում է q_1q բազմանդամի նկատմամբ կիրառել վերհանգային ենթադրությունը: $\square$

P դաշտի F ընդլայնումը կոչվում է հաստատունից տարբեր $f \in P[x]$ **բազմանդամի վերլուծության դաշտ**, եթե F-ի նկատմամբ f-ը վերլուծվում է գծային բազմանդամների արտադրյալի և F-ը չունի նույն հատկությամբ օժտված իրենից տարբեր որևէ ենթադաշտ:

Հետևություն 16.14*:* *Հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամ ունի վերլուծության դաշտ:*

Ապացուցում: Ըստ Կրոնեկերի թեորեմի, գոյություն ունի P դաշտի այնպիսի P' ընդլայնում, որի նկատմամբ f-ը վերլուծվում է գծային բազմանդամների արտադրյալի՝ $f = c(x - c_1) \cdots (x - c_n)$, որտեղ $c_1, \ldots, c_n \in P'$, $n = deg(f)$: Որոնելի F դաշտը կլինի հավասար P'-ի բոլոր այն ենթադաշտերի հատմանը, որոնք պարունակում են P-ն և $c_1, \ldots, c_n \in P'$ տարրերը: □

Այս տեսակետից օգտակար է հետևյալ հասկացությունը: $f \in P[x]$ բազմանդամը կոչվում է **սեպարաբել**, եթե այն չունի բազմապատիկ արմատ P դաշտի ցանկացած ընդլայնման մեջ: Հակառակ դեպքում $f \in P[x]$ բազմանդամը կոչվում է **ոչ սեպարաբել**:

Հատկություն 16.18: *$f \in P[x]$ բազմանդամը կլինի սեպարաբել այն և միայն այն դեպքում, երբ f և f' բազմանդամները փոխադարձաբար պարզ են:*

Ապացուցում: Բխում է թեորեմ 16.19-ից և հետևություն 16.6-ից: □

Հատկություն 16.19: *Զրո բնութագրիչով դաշտի նկատմամբ չբերվող բազմանդամը սեպարաբել է:* □

P դաշտը կոչվում է **հանրահաշվորեն փակ**, եթե հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամ P դաշտում ունի գոնե մեկ արմատ, այսինքն՝ հաստատունից տարբեր ցանկացած $f \in P[x]$ բազմանդամ $P[x]$-ում վերլուծվում է առաջին աստիճանի բազմանդամների արտադրյալի:

Այսպիսով, բոլոր կոմպլեքս թվերի $\mathbb{C}$ դաշտը հանրահաշվորեն փակ է (թեորեմ 16.6): Սակայն վերջավոր դաշտերը հանրահաշվորեն փակ չեն: Իրոք, եթե P դաշտը վերջավոր է և $P = \{a_0, a_1, \ldots, a_n\}$, ապա

$$f = (x - a_0)(x - a_1) \cdots (x - a_n) + 1$$

բազմանդամը չունի արմատ P-ում, որտեղ 1-ը P դաշտի միավորն է:

Առանց ապացուցման նշենք հետևյալ կարևոր արդյունքները:

Թեորեմ 16.27 (Շտեյնից): *Յուրաքանչյուր դաշտ հանդիսանում է որևէ հանրահաշվորեն փակ դաշտի ենթադաշտ, այսինքն՝ յուրաքանչյուր դաշտ կարելի է ընդլայնել մինչև հանրահաշվորեն փակ դաշտի:* □

P դաշտի P' ընդլայնումը կոչվում է P դաշտի **հանրահաշվական ընդլայնում**, եթե P' դաշտի ցանկացած տարր հանդիսանում է հաստատունից տարբեր որևէ $f \in P[x]$ բազմանդամի արմատ:

Թեորեմ 16.28 (Շտեյնից): *Յուրաքանչյուր P դաշտի համար գոյություն ունի P-ի հանրահաշվական ընդլայնում հանդիսացող այնպիսի P' դաշտ, որը նաև հանրահաշվորեն փակ է:* □

Նախքան Գալուայի թեորեմին անցնելը անհրաժեշտ է ապացուցել Նյուտոնի երկանդամի բանաձևը՝ կամայական զուգորդական և տեղափոխական օղակում (մասնավորապես կամայական դաշտում):

Ցանկացած $n \geqslant 0$ բնական թվի և ցանկացած k բնական թվի համար, որտեղ $0 \leqslant k \leqslant n$, սահմանենք՝

$$\begin{pmatrix} n \\ k \end{pmatrix} = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!}, \quad \text{որտեղ } 0! = 1 \ :$$

Այս $\binom{n}{k}$ թիվը կոչվում է **երկանդամային գործակից**:

Լեմմ 16.18: *Տեղի ունեն հետևյալ նույնությունները՝*

1) $\begin{pmatrix} n \\ k \end{pmatrix} = \begin{pmatrix} n \\ n-k \end{pmatrix}$*; (Սիմետրիկության օրենք)*

2) $\begin{pmatrix} n+1 \\ k \end{pmatrix} = \begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix}$*, (Պասկալի օրենք)*

որտեղ $1 \leqslant k \leqslant n$*:*

Ապացուցում: 1)-ի ապացուցումը նշված է $\begin{pmatrix} n \\ k \end{pmatrix}$-ի սահմանման մեջ: Ապացուցենք 2)-ը:

$$\begin{pmatrix} n \\ k \end{pmatrix} + \begin{pmatrix} n \\ k-1 \end{pmatrix} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!} =$$

$$= \frac{n!\,(n-k+1) + n!\,k}{k!\,(n-k+1)!} = \frac{n!\,(n-k+1+k)}{k!\,(n-k+1)!} =$$

$$= \frac{n!\,(n+1)}{k!\,(n-k+1)!} = \frac{(n+1)!}{k!\,(n+1-k)!} = \begin{pmatrix} n+1 \\ k \end{pmatrix} :$$ □

Թեորեմ 16.29: *1)* $\binom{n}{k}$ *երկանդամային գործակիցը բնական թիվ է՝ ցանկացած $n \geqslant 0$ և ցանկացած $0 \leqslant k \leqslant n$ բնական թվերի համար:*

2) Եթե K-ն կամայական զուգորդական և տեղափոխական օղակ է, ապա ցանկացած $x, y \in K$ տարրերի և ցանկացած $n \geqslant 1$ բնական թվի համար՝

$$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n \ :$$

Համառոտ՝

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k \ :$$

Այս բանաձևը կոչվում է **Նյուտոնի երկանդամի** *(կամ երկանդամային)* **բանաձև***:*

3) Եթե p-ն պարզ թիվ է, իսկ $1 \leqslant k \leqslant p-1$, ապա $\binom{p}{k}$ երկանդամային գործակիցը բաժանվում է p-ի վրա: Մասնավորապես, p բնութագրիչով P դաշտի ցանկացած $x, y \in P$ տարրերի համար՝

$(x+y)^p = x^p + y^p$, (Ֆրոբենիուսի օրենք)

$(x+y)^{p^n} = x^{p^n} + y^{p^n}$, (Ֆրոբենիուսի ընդհանրացված օրենք)

կամայական $n \geqslant 0$ բնական թվի համար:

Ապացուցում: 1) Ակնհայտ է, որ $\binom{n}{k}$ երկանդամային գործակիցը բնական թիվ է, եթե $n = 0$ կամ $k = 0$ (այդ երկու դեպքում էլ՝ $\binom{n}{k} = 1$): Մնացած դեպքերում 1) հատկությունն ապացուցելու համար նախ $\mathfrak{A}(n)$-ով նշանակենք հետևյալ պնդումը՝ «n-ը չգերազանցող ցանկացած $k \geqslant 1$ բնական թվի համար $\binom{n}{k}$-ն բնական թիվ է»: Այժմ, վերհանգման եղանակով ապացուցենք, որ $\mathfrak{A}(n)$ պնդումը ճիշտ է՝ ցանկացած $n \geqslant 1$ դեպքում: Իրոք, $n = 1$ դեպքում $\mathfrak{A}(n)$-ը ճիշտ է և եթե $\mathfrak{A}(n)$-ը ճիշտ է n-ից փոքր բոլոր բնական թվերի դեպքում, ապա $\mathfrak{A}(n)$-ը ևս կլինի ճիշտ, որովհետև, համաձայն Պասկալի օրենքի,

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \,,$$

որտեղ աջ մասի երկու գումարելիներն էլ բնական թվեր են:

2) Նյուտոնի երկանդամային բանաձևն ապացուցենք վերհանգման եղանակով` ըստ $n \geqslant 1$ բնական թվի: $n = 1$ դեպքում այն ակնհայտորեն ճիշտ է: Դիցուք $n > 1$ և դիցուք բանաձևը ճիշտ է $n$-ից փոքր բոլոր բնական թվերի համար: Հաշվենք $(x+y)^n$-ը` օգտվելով օղակի տեղափոխականությունից.

$$(x+y)^n = (x+y)(x+y)^{n-1} = (x+y)\left(\binom{n-1}{0}x^{n-1} + \binom{n-1}{1}x^{n-2}y + \cdots\right.$$

$$\left. + \binom{n-1}{n-1}y^{n-1}\right) = \binom{n-1}{0}x^n + \binom{n-1}{1}x^{n-1}y + \cdots$$

$$+ \binom{n-1}{n-1}xy^{n-1} + \binom{n-1}{0}x^{n-1}y + \binom{n-1}{1}x^{n-2}y^2 + \cdots$$

$$+ \binom{n-1}{n-1}y^n = \binom{n-1}{0}x^n + \left(\binom{n-1}{1} + \binom{n-1}{0}\right)x^{n-1}y +$$

$$+ \left(\binom{n-1}{2} + \binom{n-1}{1}\right)x^{n-2}y^2 + \cdots$$

$$+ \left(\binom{n-1}{n-1} + \binom{n-1}{n-2}\right)xy^{n-1} + \binom{n-1}{n-1}y^n =$$

$$= \binom{n}{0}x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{n-1}xy^{n-1} + \binom{n}{n}y^n :$$

Վերջին հավասարությունը ստացվեց համաձայն Պասկալի օրենքի:

3) Ապացուցենք, որ

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{1\cdot 2\cdots k} = \frac{p\cdot t}{s}$$

բնական թիվը, որտեղ $t = (p-1)(p-2)\cdots(p-k+1)$, $s = 1\cdot 2\cdots k$, բաժանվում է p-ի վրա: Իրոք, եթե $\dfrac{p\cdot t}{s} = m$, ապա $p\cdot t = m\cdot s$, այսինքն $m\cdot s$ արտադրյալը բաժանվում է p պարզ թվի վրա, որտեղ հատկություն 6.4-ի համաձայն, s-ը չի բաժանվում p-ի վրա, որովհետև $s = 1\cdot 2\cdots k$: Հետևաբար, հատկություն 6.3-ի համաձայն, m-ը կբաժանվի p-ի վրա:

Եթե P դաշտի բնութագրիչը հավասար է p պարզ թվին, ապա $(\ell p)a = \underbrace{a + \cdots + a}_{\ell p} = a(\underbrace{1 + \cdots + 1}_{\ell p}) = a(\underbrace{0 + \cdots + 0}_{\ell}) = a \cdot 0 = 0$, որտեղ $a \in P$, և

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^{p-k} y^k = x^p + y^p\,,$$

որովհետև, այս դեպքում, Նյուտոնի երկանդամային բանաձևի գումարելիները, բացառությամբ առաջինից և վերջինից, հավասար են զրոյի: Ֆրոբենիուսի ընդհանրացված օրենքը ապացուցվում է վերհանգման եղանակով՝ ըստ n-ի: $\square$

Թեորեմ 16.30 (Գալուա): *Ցանկացած p պարզ թվի և ցանկացած $n \geqslant 1$ բնական թվի համար գոյություն ունի վերջավոր դաշտ, որի տարրերի քանակը ճիշտ հավասար է p^n-ի:*

Ապացուցում: Նշանակենք $q = p^n$ և դիտարկենք $f = x^q - x \in \mathbb{Z}_p[x]$ բազմանդամը: Կրոնեկերի թեորեմի համաձայն, գոյություն ունի $\mathbb{Z}_p$ դաշտի ընդլայնում հանդիսացող այնպիսի F դաշտ, որի նկատմամբ f-ը վերլուծվում է գծային բազմանդամների արտադրյալի: S-ով նշանակենք f-ի բոլոր արմատների բազմությունը F դաշտում՝

$$S = \{c \in F \mid \ f(c) = 0\}\ :$$

Քանի որ $f' = qx^{q-1} - 1 = p^n x^{q-1} - 1 = 0 - 1 = -1$, ապա, համաձայն թեորեմ 16.19-ի, f-ը չունի բազմապատիկ արմատ, այսինքն՝ f-ի բոլոր արմատները պարզ են: Այսպիսով, F դաշտում f-ն ունի միմյանցից տարբեր q հատ արմատներ, այսինքն $S \subseteq F$ ենթաբազմությունը կազմված է ճիշտ $q = p^n$ տարրերից: Մնում է ապացուցել, որ S-ը F-ի ենթադաշտ է, այսինքն S-ը դաշտ է F-ի $+$ և $\cdot$ գործողությունների նկատմամբ: Իրոք, եթե $\alpha, \beta \in S$, ապա $\alpha^q - \alpha = 0$, $\beta^q - \beta = 0$ և $\alpha^q = \alpha$, $\beta^q = \beta$: Հետևաբար,

$$(\alpha \cdot \beta)^q = \alpha^q \cdot \beta^q = \alpha \cdot \beta\,,$$

և, Ֆրոբենիուսի ընդհանրացված օրենքի համաձայն,

$$(\alpha - \beta)^q = (\alpha + (-\beta))^q = \alpha^q + (-\beta)^q = \alpha^q + (-(\beta)^q) = \alpha + (-\beta) = \alpha - \beta\,,$$

այսինքն՝ $\alpha \cdot \beta \in S$ և $\alpha - \beta \in S$: Իսկ եթե $\gamma \in S$ և $\gamma \neq 0$, ապա $\gamma^q = \gamma$ հավասարությունից բխում է $\gamma^{q-1} = 1$ հավասարությունը, այսինքն՝ $\gamma \cdot$

$\gamma^{q-2} = 1$ և $\gamma^{-1} = \gamma^{q-2} \in S$, քանի որ S-ը պարունակում է իր ցանկացած երկու (հետևաբար և վերջավոր թվով) տարրերի արտադրյալը ($q = p^n \geqslant 2$): □

Հետևություն 16.15 *Եթե p-ն կամայական պարզ թիվ է, $1 \leqslant n$-ը կամայական բնական թիվ է, իսկ $q = p^n$, ապա գոյություն ունի $f = x^q - x \in \mathbb{Z}_p[x]$ բազմանդամի վերլուծության դաշտ՝ կազմված q թվով տարրերից:*

Ապացուցում: Բավական է նկատել, որ նախորդ թեորեմի ապացուցման ժամանակ կառուցված S դաշտը հանդիսանում է $\mathbb{Z}_p \subseteq F$ դաշտի ընդլայնումը, այսինքն՝ $\mathbb{Z}_p \subseteq S$: Իրոք, ըստ Ֆերմայի փոքր թեորեմի, եթե $\alpha \in \mathbb{Z}_p$ և $\alpha \neq 0$, ապա $\alpha^{p-1} = 1$, որտեղ 1-ը $\mathbb{Z}_p$-ի միավորն է: Հետևաբար, $\alpha^p = \alpha$ արդեն ցանկացած $\alpha \in \mathbb{Z}_p$ տարրի համար, որտեղից $\alpha^{p^2} = \alpha^p = \alpha$, $\alpha^{p^3} = \left(\alpha^{p^2}\right)^p = \alpha^p = \alpha$, ..., $\alpha^{p^n} = \left(\alpha^{p^{n-1}}\right)^p = \alpha^p = \alpha$, այսինքն՝ $f(\alpha) = \alpha^q - \alpha = 0$ և $\alpha \in S$ ցանկացած $\alpha \in \mathbb{Z}_p$ տարրի համար: Այսպիսով, $\mathbb{Z}_p \subseteq S$: Այս ներդրումը բխում է նաև թեորեմ 14.17-ից: □

Վարժություններ և խնդիրներ

1. Դիցուք P-ն կամայական դաշտ է: Ապացուցել, որ բազմանդամների $P[x]$ օղակը դաշտ չէ:

2. Դիցուք P-ն կամայական դաշտ է: $\alpha, \beta \in P[x]$ և $\alpha = \sum\limits_{i=0}^{n} a_i x^i$: Սահմանենք՝
$$\alpha(\beta) = \sum_{i=0}^{n} a_i \beta^i \in P[x] \ :$$
Ապացուցել ածանցման հետևյալ կանոնը՝
$$(\alpha(\beta))' = \alpha'(\beta) \cdot \beta' \ :$$

3. Ապացուցել, որ եթե $\alpha, \beta \in P[x]$ բազմանդամները փոխադարձաբար պարզ են, ապա $\alpha(\gamma), \beta(\gamma) \in P[x]$

բազմանդամները ևս կլինեն փոխադարձաբար պարզ՝ ցանկացած $\gamma \in P[x]$ բազմանդամի համար:

4. Ապացուցել, որ $\mathbb{Z}_4[x]$ բազմանդամների օղակի զրոյի բաժանարարները կազմված են բոլոր այն ոչ զրոյական բազմանդամներից, որոնց գործակիցները զույգ են:

5. Ապացուցել, որ $f \in \mathbb{Z}_4[x]$ տարրը կլինի հակադարձելի $\mathbb{Z}_4[x]$ օղակում այն և միայն այն դեպքում, երբ նրա ազատ անդամը հավասար է 1 կամ 3, իսկ մնացած գործակիցները զույգ են:

6. Ապացուցել, որ եթե $\alpha \in P[x]$ բազմանդամը բերվող է, ապա այդպիսին է նաև $\alpha(\beta) \in P[x]$ բազմանդամը՝ հաստատունից տարբեր ցանկացած $\beta \in P[x]$ բազմանդամի համար:

7. Ապացուցել, որ
$$\mathbb{Z}_3[x]\Big/(x^2+1) \simeq \mathbb{Z}_3[x]\Big/(x^2+x-1) \simeq \mathbb{Z}_3[x]\Big/(x^2-x-1) \ :$$

8. Ապացուցել, որ
$$\mathbb{Z}_3[x]\Big/(x^3-x-1) \simeq \mathbb{Z}_3[x]\Big/(x^3-x^2+x+1) \ :$$

9. Ապացուցել, որ
$$P[x]\Big/(x+1) \simeq P \ :$$

10. Ապացուցել, որ p բնութագրիչով P դաշտի ցանկացած $x_1, x_2, \ldots, x_m \in P$ տարրերի համար տեղի ունի հետևյալ հավասարությունը՝
$$(x_1+x_2+\cdots+x_m)^p = x_1^p + x_2^p + \cdots + x_m^p \ :$$

11. Ապացուցել, որ p բնութագրիչով P դաշտի ցանկացած $x_1, x_2, \ldots, x_m \in P$ տարրերի համար տեղի ունի հետևյալ հավասարությունը՝
$$(x_1+x_2+\cdots+x_m)^{p^n} = x_1^{p^n} + x_2^{p^n} + \cdots + x_m^{p^n} \,,$$
ցանկացած $n \geqslant 0$ բնական թվի համար:

12. Դիցուք p-ն պարզ թիվ է, $Q(+,\cdot)$-ը զուգորդական և տեղափոխական օղակ է, որտեղ $px = 0$ ցանկացած $x \in Q$ տարրի համար: Ապացուցել, որ ցանկացած $x, y \in Q$ տարրերի համար՝
$$(x+y)^{p^n} = x^{p^n} + y^{p^n},$$
ցանկացած $n \geqslant 0$ բնական թվի համար:

13. Ապացուցել, որ Գաուսյան թվերի դաշտը հանդիսանում է $f = 1 + x^2 \in \mathbb{Q}[x]$ բազմանդամի համար վերլուծության դաշտ:

14. Ապացուցել, որ կոմպլեքս թվերի $\mathbb{C}$ դաշտը հանդիսանում է $f = 1 + x^2 \in \mathbb{R}[x]$ բազմանդամի համար վերլուծության դաշտ:

15. Ապացուցել, որ եթե F-ը վերջավոր դաշտ է կազմված p^n թվով տարրերից, ապա $\alpha^{p^{nt}} = \alpha$ ցանկացած $\alpha \in F$ տարրի և ցանկացած $t \geqslant 1$ բնական թվի համար:

16. Վերջավոր դաշտի նկատմամբ չբերվող բազմանդամը սեպարաբել է:

17. Դիցուք p-ն պարզ թիվ է, $q = p^n$, $n \in N$, F_q-ն q տարրանի կամայական վերջավոր դաշտ է, իսկ $\Psi_q(n)$-ը F_q վերջավոր դաշտի նկատմամբ բոլոր n-րդ աստիճանի չբերվող և ունիտար բազմանդամների քանակն է: Ապացուցել հետևյալ հավասարությունը՝
$$\Psi_q(n) = \frac{1}{n} \sum_{n/d\,,\, d>0} \mu(d)\, q^{\frac{n}{d}},$$
որտեղ μ-ն Մյոբիուսի ֆունկցիան է:

Օրինակ,
$$\Psi_2(2) = \frac{1}{2}(2^2 - 2) = 1\,,$$
$$\Psi_2(3) = \frac{1}{3}(2^3 - 2) = 2\,,$$
$$\Psi_2(4) = \frac{1}{4}(2^4 - 2) = 3\,,$$
$$\Psi_2(5) = \frac{1}{5}(2^5 - 2) = 6\,,$$
$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

18. Նկարագրել բնական թվերի բոլոր այն (n, m) զույգերը, որոնց համար $x^n + x^m + 1$ բազմանդամը չբերվող է $\mathbb{Z}_2$ կամ $\mathbb{Z}_3$ դաշտում (չլուծված խնդիր):

19. Նկարագրել բնական թվերի բոլոր այն (n, m, k) եռյակները, որոնց համար $x^n + x^m + x^k + 1$ բազմանդամը չբերվող է $\mathbb{Z}_2$ կամ $\mathbb{Z}_3$ դաշտում (չլուծված խնդիր):

20. Ապացուցել, որ միևնույն $f \in P[x]$ բազմանդամի ցանկացած երկու վերլուծության դաշտեր իզոմորֆ են: Մասնավորապես, միևնույն կարգի ցանկացած երկու վերջավոր դաշտեր իզոմորֆ են:

Գ լ ու խ 17

ԳԾԱՅԻՆ (ՎԵԿՏՈՐԱԿԱՆ) ՏԱՐԱԾՈՒԹՅՈՒՆՆԵՐ

17.1. Գծային (վեկտորական) տարածության գաղափարը: Գծային կախվածություն և անկախություն: Գծային կախվածության հիմնական թեորեմը

Կդիտարկենք գծային տարածություններ որոշված P դաշտի վրա: Այստեղ P դաշտի տարրերը կոչվում են նաև **սկալյարներ** (պարզության համար կարելի է ենթադրել $P = \mathbb{R}$):

Հաճախ հանդիպում ենք ընդակների, այսինքն՝ օբյեկտների (թվերի, վեկտորների, մատրիցների, բազմանդամների, ֆունկցիաների և այլն), որոնց նկատմամբ կատարվում են գումարման և սկալյարով բազմապատկման գործողություններ:

Կասենք, որ

1) $Q \neq \emptyset$ բազմության մեջ (հետ) սահմանված է **սկալյարով** (ձախից) **բազմապատկման գործողություն**, եթե ցանկացած $\alpha \in P$ սկալյարի և ցանկացած $x \in Q$ տարրի (α, x) կարգավորված զույգին համապատասխանության մեջ է դրված միարժեքորեն որոշվող $u \in Q$ տարր, որը նշանակվում է՝ $u = \alpha x$;

2) $Q \neq \emptyset$ բազմության մեջ սահմանված է **գումարման** (գումար) **գործողություն**, եթե ցանկացած $x, y \in Q$ տարրերի (x, y) կարգավորված զույգին համապատասխանության մեջ է դրված միարժեքորեն որոշվող $v \in Q$ տարր, որը նշանակվում է՝ $v = x + y$:

$Q \neq \emptyset$ բազմությունն իր մեջ սահմանված գումարման և սկալյարով (ձախից) բազմապատկման գործողությունների հետ մեկտեղ կոչվում է **գծային տարածություն**, եթե տեղի ունեն հետևյալ ութ պայմանները (աքսիոմները).

(1) $(x + y) + z = x + (y + z)$ ցանկացած $x, y, z \in Q$ տարրերի համար (գումարման զուգորդականություն);

(2) $x + y = y + x$ ցանկացած $x, y \in Q$ տարրերի համար (գումարման տեղափոխականություն);

(3) գոյություն ունի այնպիսի $0 \in Q$ տարր, որ

$$x + 0 = 0 + x = x$$

ցանկացած $x \in Q$ տարրի համար: Ակնհայտ է, որ այս $0 \in Q$ տարրը որոշվում է միարժեքորեն, այն կոչվում է **գծային տարածության զրո** կամ **զրոյական տարր**:

Իրոք, եթե գոյություն ունեն նշված հատկությամբ օժտված երկու 0_1 և 0_2 տարրեր, ապա

$$0_1 = 0_1 + 0_2 = 0_2\,;$$

(4) յուրաքանչյուր $x \in Q$ տարրի համար գոյություն ունի այնպիսի $x' \in Q$ տարր, որ

$$x + x' = x' + x = 0\ :$$

Գումարման զուգորդականությունից բխում է, որ այս $x' \in Q$ տարրը որոշվում է միարժեքորեն, որը կոչվում է x-ի **հակադիր** և նշանակվում է՝ $x' = -x$: Հետևաբար, x'-ի հակադիրն էլ կլինի x-ը՝ $-(x') = x$, այսինքն՝ $-(-x) = x$;

(5) $\alpha(\beta x) = (\alpha\beta)x$ ցանկացած $\alpha, \beta \in P$ սկալյարների և ցանկացած $x \in Q$ տարրի համար;

(6) $\alpha(x + y) = \alpha x + \alpha y$ ցանկացած $\alpha \in P$ սկալյարի և ցանկացած $x, y \in Q$ տարրերի համար;

(7) $(\alpha+\beta)x = \alpha x+\beta x$ ցանկացած $\alpha, \beta \in P$ սկալյարների և ցանկացած $x \in Q$ տարրի համար;

(8) $1x = x$ ցանկացած $x \in Q$ տարրի համար, որտեղ 1-ը P դաշտի միավորն է:

Այս դեպքում Q-ն կոչվում է գծային տարածություն՝ տրված գումարման և սկալյարով (ձախից) բազմապատկման գործողությունների նկատմամբ; Q բազմությունը կամ $Q(+)$-ը կոչվում է նաև գծային տարածություն՝ որոշված P դաշտի վրա (նկատմամբ); Q-ի գումարման և սկալյարով (ձախից) բազմապատկման գործողությունները կոչվում են նաև գծային տարածության գործողություններ:

Օրինակներ: 1) Ուղղի վրա գտնվող բոլոր երկրաչափական վեկտորների բազմությունը գծային տարածություն է՝ վեկտորների գումարման և վեկտորը (ձախից) թվով բազմապատկելու գործողությունների նկատմամբ;

2) Հարթության վրա (մեջ) գտնվող բոլոր երկրաչափական վեկտորների բազմությունը գծային տարածություն է՝ նույն գործողությունների նկատմամբ;

3) Իրական թվերով բոլոր n-սյունակների $\mathbb{R}^n$ բազմությունը գծային տարածություն է՝ n-սյունակների գումարման և n-սյունակը (ձախից) թվով բազմապատկելու գործողությունների նկատմամբ ($n \in \mathbb{N}$ բնական թիվը սևեռված է);

4) Իրական թվերով բոլոր n-տողերի $\mathbb{R}_n$ բազմությունը գծային տարածություն է՝ n-տողերի գումարման և n-տողը (ձախից) թվով բազմապատկելու գործողությունների նկատմամբ ($n \in \mathbb{N}$ բնական թիվը սևեռված է);

5) Իրական թվերով բոլոր $n \times m$-չափանի մատրիցների $\mathbb{R}^{n\times m}$ բազմությունը գծային տարածություն է՝ մատրիցների գումարման և մատրիցը (ձախից) թվով բազմապատկելու գործողությունների նկատմամբ ($n, m \in \mathbb{N}$ բնական թվերը սևեռված են);

6) Նույն ձևով սահմանվում է P դաշտի տարրերով (այսինքն՝ P-ի վրա որոշված) բոլոր $n \times m$-չափանի մատրիցների $P^{n\times m}$ գծային տարածությունը՝ կամայական P դաշտի համար: Մասնավորապես, ստանում ենք P դաշտի վրա որոշված բոլոր n-սյունակների P^n գծային տարածությունը և P դաշտի վրա որոշված բոլոր n-տողերի P_n գծային տարածությունը՝ կամայական P դաշտի համար;

7) $P[x]$ բազմանդամների բազմությունը գծային տարածություն է՝ բազմանդամների գումարման և բազմանդամը (ձախից) սկալյարով բազմապատկելու գործողությունների նկատմամբ:

8) Մեկ տարրից կազմված Q գծային տարածությունը կոչվում է **զրոյական գծային տարածություն**: Հակառակ դեպքում, գծային տարածությունը կոչվում է **ոչ զրոյական**:

9) Եթե $F(+,\cdot)$-ը դաշտ է, ապա F-ը կլինի գծային տարածություն որոշված իր վրա, որտեղ գումարման և սկալյարով (ձախից) բազմապատկման գործողությունները համընկնում են F դաշտի $+$ և $\cdot$ գործողությունների հետ ($\alpha x = \alpha \cdot x$):

Նկատենք, որ գծային տարածության գումարման գործողության $x+y=y+x$ տեղափոխական հատկությունը բխում է գծային տարածության սահմանման մյուս աքսիոմներից: Իրոք,

$$x+x+y+y=(1+1)(x+y)=x+y+x+y\ :$$

Եթե Q-ն գծային տարածություն է որոշված P դաշտի վրա, ապա

Q բազմության տարրերը կոչվում են նաև Q գծային տարածության տարրեր, որոնք հաճախ կոչվում են **վեկտորներ**, իսկ ինքը գծային տարածությունը՝ **վեկտորական տարածություն**:

Q գծային տարածությունը կոչվում է **վերջավոր**, եթե Q բազմությունը վերջավոր է:

Գծային տարածություններում, բնական եղանակով, ներմուծվում է նաև **հանման գործողություն**՝ հետևյալ կերպ.

$$x - y = x + (-y) \ :$$

Մասնավորապես, $x - x = x + (-x) = 0$:

Լեմմ 17.1: *Եթե Q-ն գծային տարածություն է որոշված P դաշտի վրա, ապա ցանկացած $x, y \in Q$ տարրերի և $\alpha, \beta \in P$ սկալյարների համար*

ա) $0x = 0 = \alpha 0$, *(ձախից գրված 0-ն զրո սկալյարն է, այսինքն՝ P դաշտի զրոն է)*

բ) $(-1)x = -x$,

գ) $-(\alpha x) = (-\alpha)x = \alpha(-x)$, $(-\alpha)(-x) = \alpha x$,

դ) $(\alpha - \beta)x = \alpha x - \beta x$,

ե) $\alpha(x - y) = \alpha x - \alpha y$,

զ) $\alpha \neq 0, x \neq 0 \longrightarrow \alpha x \neq 0$ *կամ որ նույնն է՝*

$\alpha x = 0 \longrightarrow \alpha = 0$ *կամ* $x = 0$*:*

Ապացուցում: ա) $\alpha x = (\alpha + 0)x = \alpha x + 0x$: Ստացված հավասարության երկու կողմերին գումարելով $-(\alpha x)$, կստանանք՝ $0x = 0$: Նույն եղանակով ապացուցվում է $\alpha 0 = 0$ հավասարությունը:

բ) $0 = 0x = (1 + (-1))x = 1x + (-1)x = x + (-1)x$: Հետևաբար, $-x = (-1)x$:

գ) $0 = 0x = (\alpha + (-\alpha))x = \alpha x + (-\alpha)x$: Հետևաբար, $-(\alpha x) = (-\alpha)x$: Այնուհետև, $0 = \alpha 0 = \alpha(x + (-x)) = \alpha x + \alpha(-x)$: Հետևաբար, $-(\alpha x) = \alpha(-x)$: Եվ $(-\alpha)(-x) = -(\alpha(-x)) = -(-(\alpha x)) = \alpha x$:

դ) $(\alpha - \beta)x = (\alpha + (-\beta))x = \alpha x + (-\beta)x = \alpha x + (-(\beta x)) = \alpha x - \beta x$:

ե) $\alpha(x - y) = \alpha(x + (-y)) = \alpha x + \alpha(-y) = \alpha x + (-(\alpha y)) = \alpha x - \alpha y$:

գ) Դիցուք $\alpha x = 0$ և $\alpha \neq 0$: Հետևաբար, ըստ դաշտի սահմանման, գոյություն կունենա $\alpha^{-1} \in P$ հակադարձը և

$$\alpha^{-1}(\alpha x) = \alpha^{-1}0 = 0\,,$$

$$\left(\alpha^{-1}\alpha\right)x = 0\,,$$

$$1x = 0\,,$$

$$x = 0\ :$$

Այսպիսով, եթե $\alpha x = 0$, ապա կամ $\alpha = 0$ կամ $x = 0$: □

Քանի որ գծային տարածության գումարման գործողությունը զուգորդական է, ապա գծային տարածության վերջավոր թվով տարրերի (վեկտորների) գումարը կախված չէ փակագծերի դասավորությունից և այդ պատճառով գրվում է առանց փակագծերի (թեորեմ 1.3):

Հետևյալ հավասարությունները հեշտությամբ ստուգվում են վերհանգման եղանակով.

$$(\alpha_1\alpha_2\ldots\alpha_n)\,x = \alpha_1\left(\alpha_2\left(\ldots\alpha_{n-1}\left(\alpha_n x\right)\ldots\right)\right)\,,$$

$$\alpha\left(x_1 + \cdots + x_n\right) = \alpha x_1 + \cdots + \alpha x_n\,,$$

$$\left(\alpha_1 + \cdots + \alpha_n\right)x = \alpha_1 x + \cdots + \alpha_n x\ :$$

Գծային տարածություններում ներմուծվում են նրանց տարրերի (վեկտորների) գծային կախվածության և անկախության հասկացությունները:

Նախ կասենք, որ Q գծային տարածության $x \in Q$ տարրը (վեկտորը) գծայնորեն արտահայտվում է նրա $x_1, x_2, \ldots, x_n \in Q$ տարրերի (վեկտորների) միջոցով, եթե գոյություն ունեն այնպիսի $\alpha_1, \alpha_2, \ldots, \alpha_n \in P$ սկալյարներ, որ

$$x = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n\ :$$

Այս հավասարության աջ մասը կոչվում է $x_1, x_2, \ldots, x_n$ տարրերի գծային զուգակցություն (կոմբինացիա):

Q գծային տարածության տարրերի (վեկտորների) $y_1, y_2, \ldots, y_m$ վերջավոր հաջորդականությունը կամ համակարգը կոչվում է

գծայնորեն (գծորեն) **կախյալ** (կախված), եթե գոյություն ունեն այնպիսի $\alpha_1, \alpha_2, \ldots, \alpha_m \in P$ սկալյարներ, որոնցից գոնե մեկը զրո չէ և

$$\alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_m y_m = 0$$

(այս առնչությունը կոչվում է տրված **համակարգի գծային կախվածություն**): Հակառակ դեպքում, Q-ի տարրերի $y_1, y_2, \ldots, y_m$ վերջավոր հաջորդականությունը կոչվում է **գծայնորեն** (գծորեն) **անկախ**, այսինքն՝ երբ

$$\alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_m y_m = 0 \longrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_m = 0 \ :$$

Օրինակ, զրոյական տարր պարունակող յուրաքանչյուր վերջավոր հաջորդականություն գծայնորեն կախյալ է, իսկ յուրաքանչյուր ոչ զրոյական տարր գծայնորեն անկախ հաջորդականություն է:

Եթե $y_1, y_2, \ldots, y_m$ վերջավոր հաջորդականության (համակարգի) մի քանի տարրերի հեռացումից ստացվում է $y_{i_1}, \ldots, y_{i_n}$ հաջորդականությունը, ապա երկրորդ հաջորդականությունը կոչվում է առաջինի **ենթահաջորդականություն** (ենթահամակարգ), իսկ առաջին հաջորդականությունը կոչվում է երկրորդի վերջավոր **ընդլայնում** (ըստ որում, յուրաքանչյուր հաջորդականություն համարվում է իր ենթահաջորդականությունը և իր վերջավոր ընդլայնումը): Դժվար չէ նկատել, որ գծայնորեն կախյալ հաջորդականության յուրաքանչյուր վերջավոր ընդլայնում նս գծայնորեն կախյալ է, իսկ գծայնորեն անկախ վերջավոր հաջորդականության յուրաքանչյուր ենթահաջորդականություն նս գծայնորեն անկախ է:

Լեմմ 17.2: *1) Որպեսզի Q գծային տարածության տարրերի $y_1, y_2, \ldots, y_m$ հաջորդականությունը լինի գծայնորեն կախյալ անհրաժեշտ է և բավարար, որ y_i ($i = 1, 2, \ldots, m$) տարրերից որևէ մեկը գծայնորեն արտահայտվի մյուսների միջոցով:*

2) Եթե Q գծային տարածության տարրերի $y_1, y_2, \ldots, y_m$ հաջորդականությունը գծայնորեն անկախ է, իսկ $y_1, y_2, \ldots, y_m, y_{m+1}$ հաջորդականությունը գծայնորեն կախյալ է, ապա $y_{m+1} \in Q$ տարրը գծայնորեն կարտահայտվի $y_1, y_2, \ldots, y_m$ տարրերի միջոցով:

Ապացուցում: 1) Դիցուք

$$\alpha_1 y_1 + \alpha_2 y_2 + \cdots + \alpha_m y_m = 0 \, ,$$

որտեղ $\alpha_1, \alpha_2, \ldots, \alpha_m \in P$ սկալյարներից գոնե մեկը զրո չէ: Եթե $\alpha_i \neq 0$, ապա գոյություն ունի $\alpha_i^{-1} \in P$ հակադարձը և

$$\alpha_i^{-1}\left(\alpha_1 y_1 + \cdots + \alpha_i y_i + \cdots + \alpha_m y_m\right) = \alpha_i^{-1} 0 = 0\,,$$

$$\alpha_i^{-1}\left(\alpha_1 y_1\right) + \cdots + \alpha_i^{-1}\left(\alpha_i y_i\right) + \cdots + \alpha_i^{-1}\left(\alpha_m y_m\right) = 0\,,$$

$$\left(\alpha_i^{-1}\alpha_1\right) y_1 + \cdots + \left(\alpha_i^{-1}\alpha_i\right) y_i + \cdots + \left(\alpha_i^{-1}\alpha_m\right) y_m = 0\,,$$

$$\left(\alpha_i^{-1}\alpha_1\right) y_1 + \cdots + y_i + \cdots + \left(\alpha_i^{-1}\alpha_m\right) y_m = 0\,;$$

Հետևաբար,

$$y_i = \beta_1 y_1 + \cdots + \beta_{i-1} y_{i-1} + \beta_{i+1} y_{i+1} + \cdots + \beta_m y_m\,,$$

որտեղ $\beta_1 = -\alpha_i^{-1}\alpha_1$, …, $\beta_m = -\alpha_i^{-1}\alpha_m$: Հակառակն ակնհայտ է:

2) Դիցուք

$$\alpha_1 y_1 + \cdots + \alpha_m y_m + \alpha_{m+1} y_{m+1} = 0\,,$$

որտեղ $\alpha_1, \ldots, \alpha_m, \alpha_{m+1} \in P$ սկալյարներից գոնե մեկը զրո չէ: Եթե այստեղ $\alpha_{m+1} = 0$, ապա $y_1, y_2, \ldots, y_m$ հաջորդականությունը կլիներ գծայնորեն կախյալ, որը հակասում է տրված պայմանին: Հետևաբար, $\alpha_{m+1} \neq 0$ և գոյություն կունենա $\alpha_{m+1}^{-1} \in P$ հակադարձը, որի օգնությամբ, ինչպես և քիչ առաջ, ստանում ենք՝

$$\alpha_{m+1}^{-1}\left(\alpha_1 y_1 + \cdots + \alpha_m y_m + \alpha_{m+1} y_{m+1}\right) = \alpha_{m+1}^{-1} 0 = 0\,,$$

$$\left(\alpha_{m+1}^{-1}\alpha_1\right) y_1 + \cdots + \left(\alpha_{m+1}^{-1}\alpha_m\right) y_m + y_{m+1} = 0$$

և

$$y_{m+1} = \gamma_1 y_1 + \cdots + \gamma_m y_m\,,$$

որտեղ $\gamma_1 = -\alpha_{m+1}^{-1}\alpha_1$, …, $\gamma_m = -\alpha_{m+1}^{-1}\alpha_m$: $\square$

Հետևյալ արդյունքը կոչվում է գծային կախվածության հիմնական թեորեմ:

Թեորեմ 17.1 (հիմնական): *Եթե Q գծային տարածության $y_1, y_2, \ldots, y_m, y_{m+1}$ տարրերից յուրաքանչյուրը գծայնորեն արտահայտվում է Q-ի $x_1, x_2, \ldots, x_m$ տարրերի միջոցով, ապա $y_1, y_2, \ldots, y_m, y_{m+1}$ հաջորդականությունը գծայնորեն կախյալ է:*

Ապացույց (վերհանգման եղանակ): Եթե $m = 1$, ապա ըստ պայմանի՝

$$y_1 = \alpha_1 x_1, \quad y_2 = \alpha_2 x_1 \ :$$

Դիցուք $\alpha_1 = 0$: Այս դեպքում՝ $y_1 = 0$ և y_1, y_2 հաջորդականությունը կլինի գծայնորեն կախյալ: $\alpha_1 \neq 0$ դեպքում կունենանք հետևյալ գծային կախվածությունը՝

$$(-\alpha_2)\, y_1 + \alpha_1 y_2 = (-\alpha_2)\,(\alpha_1 x_1) + \alpha_1\,(\alpha_2 x_1) = 0 \ :$$

Ենթադրելով պնդումը ճիշտ $m-1$ բնական թվի դեպքում, ապացուցենք այն m բնական թվի համար: Ըստ պայմանի՝

$$\begin{aligned}
&y_1 = \alpha_{11}x_1 + \alpha_{12}x_2 + \cdots + \alpha_{1m}x_m\,, \\
&y_2 = \alpha_{21}x_1 + \alpha_{22}x_2 + \cdots + \alpha_{2m}x_m\,, \\
&\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
&y_{m+1} = \alpha_{m+1,1}x_1 + \alpha_{m+1,2}x_2 + \cdots + \alpha_{m+1,m}x_m \ :
\end{aligned}$$

Եթե $\alpha_{11} = \alpha_{12} = \cdots = \alpha_{1m} = 0$, ապա $y_1 = 0$ և $y_1, y_2, \ldots, y_{m+1}$ հաջորդականությունը կլինի գծայնորեն կախյալ: Այժմ ենթադրենք թե α_{1i} $(i = 1, 2, \ldots, m)$ սկալյարներից գոնե մեկը զրո չէ: Դիցուք $\alpha_{11} \neq 0$: Այդ դեպքում, օգտվելով α_{11}^{-1}-ից, սկսած երկրորդ հավասարությունից, արտաքսում ենք x_1-ը՝

$$\begin{aligned}
&z_2 = y_2 - \left(\alpha_{11}^{-1}\alpha_{21}\right) y_1 = \alpha'_{22}x_2 + \cdots + \alpha'_{2m}x_m\,, \\
&\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
&z_{m+1} = y_{m+1} - \left(\alpha_{11}^{-1}\alpha_{m+1,1}\right) y_1 = \alpha'_{m+1,2}x_2 + \cdots + \alpha'_{m+1,m}x_m \ :
\end{aligned}$$

Հետևաբար, համաձայն վերհանգման ենթադրության, $z_2, \ldots, z_{m+1}$ հաջորդականությունը կլինի գծայնորեն կախյալ, այսինքն՝ գոյություն կունենան այնպիսի $\beta_2, \ldots, \beta_{m+1}$ սկալյարներ, որոնցից գոնե մեկը զրո չէ և

$$\beta_2 z_2 + \cdots + \beta_{m+1} z_{m+1} = 0 \ :$$

Այժմ, տեղադրելով $z_2, \ldots, z_{m+1}$ տարրերի արժեքները, կստանանք՝

$$\gamma_1 y_1 + \beta_2 y_2 + \cdots + \beta_{m+1} y_{m+1} = 0\,,$$

այսինքն՝ $y_1, y_2, \ldots, y_{m+1}$ հաջորդականությունը գծայնորեն կախյալ է: □

***Հետևություն* 17.1**: *Եթե Q գծային տարածության $y_1, y_2, \ldots, y_k$ տարրերից յուրաքանչյուրը գծայնորեն արտահայտվում է Q-ի $x_1, x_2, \ldots, x_m$ տարրերի միջոցով և $k > m$, ապա $y_1, y_2, \ldots, y_k$ հաջորդականությունը գծայնորեն կախյալ է:* □

***Հետևություն* 17.2**: *Եթե Q գծային տարածության $y_1, y_2, \ldots, y_k$ տարրերից յուրաքանչյուրը գծայնորեն արտահայտվում է Q-ի $x_1, x_2, \ldots, x_m$ տարրերի միջոցով և $y_1, y_2, \ldots, y_k$ հաջորդականությունը գծայնորեն անկախ է, ապա $k \leqslant m$:* □

***Հետևություն* 17.3**: *$n+1$ հատ n-սյունակների (n-տողերի) յուրաքանչյուր հաջորդականություն գծայնորեն կախյալ է P^n-ում (P_n-ում):*

Ապացուցում: Յուրաքանչյուր n-սյունակ ունի հետևյալ ներկայացումը՝

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \alpha_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \alpha_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \alpha_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

$(= \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n)$: Մնում է օգտվել գծային կախվածության հիմնական թեորեմից: □

***Հետևություն* 17.4**: *n-ից շատ թվով n-սյունակների (n-տողերի) ցանկացած հաջորդականություն գծայնորեն կախյալ է P^n-ում (P_n-ում):* □

Որպես կիրառություն դիտարկենք գծային հավասարումների հետևյալ համասեռ համակարգը՝

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0\,, \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0\,, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0\,, \end{cases} \tag{17.1}$$

որտեղ $a_{ij} \in P$, $i = 1, \ldots, m$, $j = 1, \ldots, n$:

***Հետևություն* 17.5**: *Եթե գծային հավասարումների (17.1) համասեռ համակարգի հավասարումների թիվը քիչ է անհայտների թվից, ապա այդպիսի համակարգն օժտված է ոչ զրոյական լուծումով:*

Ապացուցում: Եթե (17.1) համակարգի մեջ $n > m$, ապա n հատ m-սյունակներից կազմված

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix}, \dots, \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{nm} \end{pmatrix}$$

հաջորդականությունը, համաձայն հետևություն 17.4--ի, կլինի գծայնորեն կախյալ, այսինքն՝ գոյություն կունենան այնպիսի $\alpha_1, \dots, \alpha_n \in P$ սկալյարներ, որոնցից գոնե մեկը զրո չէ և

$$\alpha_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + \dots + \alpha_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} :$$

Այսպիսով,

$$\begin{cases} a_{11}\alpha_1 + \dots + a_{1n}\alpha_n = 0\,, \\ a_{21}\alpha_1 + \dots + a_{2n}\alpha_n = 0\,, \\ \dots \quad \dots \quad \dots \\ a_{m1}\alpha_1 + \dots + a_{mn}\alpha_n = 0\,, \end{cases}$$

այսինքն՝ $(\alpha_1, \dots, \alpha_n)$ ոչ զրոյական հաջորդականությունը լուծում է (17.1) համասեռ համակարգի համար: □

$P = \mathbb{R}$ դեպքում Q գծային (վեկտորական) տարածությունը կոչվում է **իրական**, իսկ $P = \mathbb{C}$ դեպքում՝ **կոմպլեքս գծային** (վեկտորոկան) **տարածություն**:

17.2. Համակարգի (հաջորդականության) հենք և ռանգ

Կասենք, որ Q գծային տարածության տարրերի

$$y_1, y_2, \dots, y_k \tag{17.2}$$

հաջորդականությունը (համակարգը) գծայնորեն արտահայտվում է Q-ի տարրերի

$$x_1, x_2, \dots, x_m \tag{17.3}$$

հաջորդականության միջոցով, եթե (17.2) հաջորդականության յուրաքանչյուր տարր գծայնորեն արտահայտվում է (17.3)-ի միջոցով: (17.2) և (17.3) հաջորդականությունները կոչվում են **համարժեք** և գրվում է (17.2)$\sim$(17.3), եթե դրանցից յուրաքանչյուրը գծայնորեն արտահայտվում է մյուսի միջոցով: Ակնհայտ է, որ հաջորդականությունների համարժեքության այս գաղափարն օժտված է հետևյալ երեք հատկություններով՝

(I) $\sim$ (I), (առինքնություն)
(I) $\sim$ (II) $\longrightarrow$ (II) $\sim$ (I), (համաչափություն)
(I) $\sim$ (II), (II) $\sim$ (III) $\longrightarrow$ (I) $\sim$ (III): (փոխանցականություն)

Հատկություն 17.1: *Եթե Q գծային տարածության տարրերի (17.2) և (17.3) հաջորդականությունները գծայնորեն անկախ են և համարժեք, ապա $k = m$:*

Ապացուցում: Բխում է հետևություն 17.2-ից: □

(17.2) հաջորդականության

$$y_{i_1}, y_{i_2}, \ldots, y_{i_t} \tag{17.2$'$}$$

ենթահաջորդականությունը կոչվում է (17.2)-ի **հենք** կամ **առավելապես** (մաքսիմալ) **գծայնորեն անկախ** ենթահաջորդականություն, եթե այն գծայնորեն անկախ է և նրա միջոցով գծայնորեն արտահայտվում է (17.2)-ը:

Հատկություն 17.2: *(17.2) հաջորդականության յուրաքանչյուր գծայնորեն անկախ ենթահաջորդականություն կամ (17.2)-ի հենք է կամ դրան կարելի է ընդլայնել մինչև (17.2)-ի հենքի: Մասնավորապես, (17.2) հաջորդականության յուրաքանչյուր ոչ զրոյական տարրից կազմված ենթահաջորդականություն կամ (17.2)-ի հենք է կամ դրան կարելի է ընդլայնել մինչև (17.2)-ի հենքի:*

Ապացուցում: Եթե (17.2) հաջորդականության տրված (I) գծայնորեն անկախ ենթահաջորդականությունը (17.2)-ի հենք է, ապա պնդումն ապացուցված է: Հակառակ դեպքում, (17.2) հաջորդականության որևէ y_i տարր գծայնորեն չի արտահայտվի (I) ենթահաջորդականության միջոցով: Հետևաբար, (I) հաջորդականությանը ավելացնելով այդ y_i տարրը, կստանանք (17.2)-ի նոր գծայնորեն անկախ ենթահաջորդականություն: Եթե այս նոր (II) ենթահաջորդականությունը (17.2)-ի հենք է, ապա պնդումն ապացուցված է: Հակառակ դեպքում, նորից գոյություն կունենա (17.2) հաջորդականության այնպիսի y_j տարր, որ (II)-ին ավելացնելով այս y_j տարրը, կստանանք (17.2)-ի մեկ այլ գծայնորեն անկախ ենթահաջորդականություն: Վերջավոր թվով նմանատիպ քայլերից հետո կհանգենք (17.2)-ի հենքի: □

Հետևաբար, ամեն մի ոչ զրոյական հաջորդականություն (այսինքն՝ որևէ ոչ զրոյական տարր պարունակող հաջորդականություն) օժտված է հենքով և ոչ զրոյական հաջորդականությունը համարժեք է իր յուրաքանչյուր հենքի: Ուստի, միևնույն ոչ զրոյական հաջորդականության բոլոր հենքերը համարժեք են միմյանց և, հետևաբար, օժտված են միևնույն քանակի տարրերով (հատկություն 17.1): Այդ թիվը կոչվում է դիտարկվող ոչ զրոյական **հաջորդականության ռանգ**: Զրոյական հաջորդականության (այսինքն՝ այն հաջորդականության, որի բոլոր տարրերը հավասար են զրոյի) ռանգը ընդունվում է հավասար զրոյի:

Ակնհայտ է, որ տարրերի տեղափոխությունից հաջորդականության ռանգը չի փոխվի:

Հատկություն 17.3: *1) Եթե (17.2) հաջորդականության ռանգը հավասար է r-ի, ապա r-ից շատ թվով տարրեր պարունակող նրա յուրաքանչյուր ենթահաջորդականություն գծայնորեն կախյալ է;*

2) Եթե (17.2) հաջորդականության ռանգը հավասար է r-ի, ապա r թվով տարրեր պարունակող նրա յուրաքանչյուր գծայնորեն անկախ ենթահաջորդականություն կլինի հենք:

Ապացուցում: 1)-ը բխում է հետևություն 17.1-ից, իսկ 2)-ը բխում է 1)-ից՝ համաձայն լեմմ 17.2-ի: □

Հատկություն 17.4: *Եթե (17.2) հաջորդականությունը գծայնորեն արտահայտվում է (17.3) հաջորդականության միջոցով, ապա (17.2)-ի ռանգը չի գերազանցում (17.3)-ի ռանգին: Մասնավորապես, համարժեք հաջորդականություններն ունեն հավասար ռանգեր:*

Ապացուցում: Եթե (17.2) հաջորդականությունը զրոյական է, ապա պնդումն ակնհայտ է: Հակառակ դեպքում, (17.3)-ը ևս կլինի ոչ զրոյական և (17.2)-ը կլինի համարժեք իր $(17.2')$ հենքին, որն ըստ տրված պայմանի գծայնորեն կարտահայտվի (17.3) հաջորդականության հենքի միջոցով: Մնում է օգտվել հետևություն 17.2-ից: □

Կասենք, որ Q գծային տարածության տարրերի (17.2) հաջորդականության նկատմամբ կատարվում է.

I) առաջին տիպի (տեսակի) տարրական ձևափոխություն, եթե (17.2) հաջորդականության բոլոր տարրերը, բացի որևէ i-րդ տարրից, թողնվում են նույնը, իսկ i-րդ տարրը փոխարինվում է $y_i + \lambda y_j$ տարրով, որտեղ $\lambda \in P$, $j \neq i$, $1 \leqslant j \leqslant k$: Այլ կերպ, հաջորդականության որևէ i-րդ տարրին գումարվում է նրա մեկ այլ տարր, վերջինս նախապես (ձախից) բազմապատկելով որևէ λ սկալյարով:

II) երկրորդ տիպի (տեսակի) տարրական ձևափոխություն, եթե (17.2) հաջորդականության բոլոր տարրերը, բացի որևէ i-րդ տարրից, թողնվում են նույնը, իսկ i-րդ տարրը փոխարինվում է λy_i տարրով, որտեղ $\lambda \in P$, $\lambda \neq 0$: Այլ կերպ, հաջորդականության որևէ i-րդ տարր (ձախից) բազմապատկվում է որևէ ոչ զրոյական λ սկալյարով:

III) երրորդ տիպի (տեսակի) տարրական ձևափոխություն, եթե (17.2) հաջորդականության որևէ երկու i-րդ և j-րդ տարրերի տեղերը փոխվում են, իսկ մնացած տարրերը թողնվում են իրենց տեղերում $(i \neq j)$:

Լեմմ 17.3: *Եթե (17.2) հաջորդականության նկատմամբ կատարվի առաջին, երկրորդ կամ երրորդ տիպի (տեսակի) տարրական ձևափոխություն, ապա ստացվող հաջորդականությունը կլինի համարժեք (17.2) սկզբնական հաջորդականությանը և, հետևաբար, կունենա (17.2) հաջորդականության ռանգին հավասար ռանգ: Այլ կերպ, տարրական ձևափոխություններից հաջորդականության ռանգը չի փոխվում:* □

17.3. Մատրիցի ռանգ

Անցնենք մատրիցի ռանգին:

$n \times m$-չափանի $A = (a_{ij})$ մատրիցի տողերից կազմված

$$(a_{11}, a_{12}, \ldots, a_{1m}), (a_{21}, a_{22}, \ldots, a_{2m}), \ldots, (a_{n1}, a_{n2}, \ldots, a_{nm})$$

հաջորդականության ռանգը (P_m-ում) կոչվում է A **մատրիցի տողային** ռանգ կամ ռանգ ըստ տողերի, իսկ նրա սյունակներից (սյուներից) կազմված

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix}, \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{n2} \end{pmatrix}, \ldots, \begin{pmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{pmatrix}$$

հաջորդականության ռանգը (P^n-ում) կոչվում է A-ի **սյունակային ռանգ** կամ ռանգ ըստ սյուների (սյունակների)։ A մատրիցի տողային ռանգը կարելի է նշանակել $rank_{\text{տ}}(A)$-ով, իսկ սյունակային ռանգը՝ $rank_{\text{ս}}(A)$-ով։

Օրինակներ: 1) Զրոյական մատրիցի տողային և սյունակային ռանգերը հավասար են զրոյի;

2) n-րդ կարգի E_n միավոր մատրիցի տողային և սյունակային ռանգերը հավասար են n-ի։

3) n-րդ կարգի A հակադարձելի մատրիցի տողային և սյունակային ռանգերը հավասար են n-ի (որովհետև $det(A) \neq 0$)։

Ակնհայտ է, որ $n \times m$-չափանի $A = (a_{ij})$ մատրիցի համար՝ $rank_{\text{տ}}(A) \leqslant m$ (հետևություն 17.3) և $rank_{\text{տ}}(A) \leqslant n$, այսինքն՝ $rank_{\text{տ}}(A) \leqslant \min\{m, n\}$։ Նույնպիսի առնչություն տեղի ունի նաև A մատրիցի սյունակային ռանգի համար՝ $rank_{\text{ս}}(A) \leqslant \min\{m, n\}$։

Լեմմ 17.4: *1) $B_1, B_2, \ldots, B_k$ n-տողերի հաջորդականությունը գծայնորեն կախյալ է այն և միայն այն դեպքում, երբ $B_1^T, B_2^T, \ldots, B_k^T$ n-սյունակների հաջորդականությունը գծայնորեն կախյալ է;*

2) $B_1, B_2, \ldots, B_k$ n-տողերի հաջորդականությունը գծայնորեն անկախ է այն և միայն այն դեպքում, երբ $B_1^T, B_2^T, \ldots, B_k^T$ n-սյունակների հաջորդականությունը գծայնորեն անկախ է;

3) Յանկացած $n \times m$-չափանի A մատրիցի համար՝

$$rank_{\text{տ}}(A) = rank_{\text{ս}}(A^T)\,,$$

$$rank_{\text{ս}}(A) = rank_{\text{տ}}(A^T)\,,$$

որտեղ A^T-ն A-ի շրջված մատրիցն է:

Ապացուցում:

$$\alpha_1 B_2 + \alpha_2 B_2 + \cdots + \alpha_k B_k = (\underbrace{0, 0, \ldots, 0}_{n}) \longleftrightarrow$$

$$\alpha_1 B_1^T + \alpha_2 B_2^T + \cdots + \alpha_k B_k^T = \left.\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}\right\} n \ : \qquad \square$$

Թեորեմ 17.2: *$n \times m$-չափանի ցանկացած $A = (a_{ij})$ մատրիցի տողային և սյունակային ռանգերը հավասար են: Այդ ռանգերից յուրաքանչյուրը կոչվում է A մատրիցի ռանգ և նշանակվում է $rank(A)$-ով:*

Ապացույց: Դիցուք r-ը և k-ն ոչ զրոյական $A = (a_{ij})$ մատրիցի տողային և սյունակային ռանգերն են՝ $rank_{\text{տ}}(A) = r$, $rank_{\text{ս}}(A) = k$ (զրոյական մատրիցի համար պնդումն ակնհայտ է): Քանի որ տողերի (սյունակների) տեղափոխություններից մատրիցի տողային (սյունակային) ռանգը չի փոխվում, ապա կարող ենք ենթադրել, որ A մատրիցի սկզբի r տողերը գծայնորեն անկախ են, իսկ մնացած $n - r$ տողերը գծայնորեն արտահայտվում են սկզբի r տողերի միջոցով՝

$$A_{r+1} = \beta_{r+1,1}A_1 + \beta_{r+1,2}A_2 + \cdots + \beta_{r+1,r}A_r \, ,$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots$$

$$A_n = \beta_{n,1}A_1 + \beta_{n,2}A_2 + \cdots + \beta_{n,r}A_r \, ,$$

որտեղ $A_1, A_2, \ldots, A_n$-ը տրված $A = (a_{ij})$ մատրիցի տողերն են, այսինքն՝ կարելի է գրել՝

$$A = \begin{pmatrix} A_1 \\ \vdots \\ A_r \\ A_{r+1} \\ \vdots \\ A_n \end{pmatrix} \ :$$

Նշանակելով՝

$$B = \begin{pmatrix} A_1 \\ \vdots \\ A_r \end{pmatrix} , \quad C = \begin{pmatrix} A_{r+1} \\ \vdots \\ A_n \end{pmatrix} , \quad T = \begin{pmatrix} \beta_{r+1,1} & \ldots, & \beta_{r+1,1} \\ \ldots & \ldots & \ldots \\ \beta_{n1}, & \ldots, & \beta_{nr} \end{pmatrix} ,$$

կստանանք՝ $C = T \cdot B$, իսկ A-ի համար կունենանք հետևյալ համառոտ ներկայացումը՝

$$A = \begin{pmatrix} B \\ C \end{pmatrix} = \begin{pmatrix} B \\ TB \end{pmatrix} \; :$$

Այժմ ապացուցենք, որ A և B մատրիցներն ունեն նույն k սյունակային ռանգը: Դիցուք $A'_1, A'_2, \ldots, A'_m$ սյունակները A մատրիցի, իսկ $A''_1, A''_2, \ldots, A''_m$ սյունակները՝ B մատրիցի սյունակներն են: Դիցուք $A'_1, A'_2, \ldots, A'_k$ հաջորդականությունը A մատրիցի սյունակների հաջորդականության հենքն է: Ապացուցենք, որ այդ դեպքում $A''_1, A''_2, \ldots, A''_k$ հաջորդականությունը կլինի B մատրիցի սյունակների հաջորդականության հենքը: Բավական է ապացուցել, որ $A''_1, A''_2, \ldots, A''_k$ հաջորդականությունը գծայնորեն անկախ է: Իրոք, եթե

$$\alpha_1 A''_1 + \alpha_2 A''_2 + \cdots + \alpha_k A''_k = 0\,,$$

ապա

$$\alpha_1 A''_1 + \alpha_2 A''_2 + \cdots + \alpha_k A''_k + 0A''_{k+1} + \cdots + 0A''_m = 0 \; :$$

Հետևաբար,

$$B \cdot \alpha = 0\,,$$

որտեղ

$$\alpha = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \\ 0 \\ \vdots \\ 0 \end{pmatrix} \; :$$

Ուստի,

$$A \cdot \alpha = \begin{pmatrix} B \\ TB \end{pmatrix} \cdot \alpha = \begin{pmatrix} B \cdot \alpha \\ T(B \cdot \alpha) \end{pmatrix} = 0\,,$$

այսինքն՝

$$\alpha_1 A'_1 + \alpha_2 A'_2 + \cdots + \alpha_k A'_k + 0A'_{k+1} + \cdots + 0A'_m = 0\,,$$

$$\alpha_1 A'_1 + \alpha_2 A'_2 + \cdots + \alpha_k A'_k = 0 \; :$$

Հետևաբար, $\alpha_1 = \alpha_2 = \cdots = \alpha_k = 0$: Այժմ, հետևություն 17.3-ի համաձայն՝ $k \leqslant r$: Եթե նույն դատողությունները կիրառենք A մատրիցի շրջված A^T մատրիցի նկատմամբ (լեմմ 17.4), ապա կստանանք նաև $r \leqslant k$ անհավասարությունը: Այսպիսով, $r = k$ և թեորեմն ապացուցված է: □

***Հետևություն 17.6**: Մատրիցի ռանգը չի փոխվում նրա շրջման դեպքում, այսինքն՝ $rank(A) = rank(A^T)$:* □

$n \times m$-չափանի $A \in P^{n\times m}$ մատրիցի **տողերի տարրական ձևափոխություններ** են կոչվում նրա տողերի հաջորդականության նկատմամբ կատարվող տարրական ձևափոխությունները, այսինքն՝

I) մատրիցի մի տողին մեկ այլ տող գումարելը՝ վերջինս նախապես (ձախից) բազմապատկելով որևէ $\lambda \in P$ սկալյարով;

II) մատրիցի մի տողի (ձախից) բազմապատկումը որևէ ոչ զրոյական $\lambda \in P$ սկալյարով;

III) մատրիցի երկու տողերի տեղափոխությունը:

$P = \mathbb{R}$ դեպքում, այս ձևափոխությունները դիտարկվել են 14.2 վերնագրում և այնտեղ ապացուցված հիմնական հատկությունները մնում են ուժի մեջ նաև ընդհանուր դեպքում (այսինքն՝ կամայական P դաշտի դեպքում): Համաձայն լեմմ 17.3-ի, մատրիցի ռանգը հաշվելու համար, նրան տողերի տարրական ձևափոխությունների օգնությամբ նախապես կարելի է բերել պարզ տեսքի:

$(\alpha_{i1}, \alpha_{i2}, \ldots, \alpha_{in}) \in P_n$ հաջորդականության առաջին ոչ զրոյական տարրը (եթե այն գոյություն ունի) կոչվում է **առաջատար տարր**, իսկ $k = \min\{s \in \mathbb{N} \mid \alpha_{is} \neq 0\}$ թիվը կոչվում է առաջատար տարրի համար: $n \times m$-չափանի $A = (a_{ij}) \in P^{n\times m}$ մատրիցը կոչվում է **աստիճանաձև** (տեսքի), եթե այն բավարարում է հետևյալ երկու պայմաններին.

ա) A մատրիցի զրոյական տողերը, եթե դրանք գոյություն ունեն, գտնվում են մատրիցի վերջում, այսինքն՝ եթե որևէ տող զրոյական է, ապա նրանից ներքև գտնվող բոլոր տողերը նույնպես զրոյական են;

բ) A մատրիցի ոչ զրոյական տողերի (եթե այդպիսիք գոյություն ունեն) առաջատար տարրերի համարները կազմում են աճող հաջորդականություն:

Այսպիսով, ոչ զրոյական աստիճանաձև մատրիցը, ընդհանուր դեպքում, ունի հետևյալ տեսքը.

$$\begin{pmatrix} a_{1j_1} & \dots & \dots & \dots & \dots \\ & a_{2j_2} & \dots & \dots & \dots \\ & & \dots & \dots & \dots \\ & & & a_{mj_m} & \dots \\ 0 & & & & \end{pmatrix},$$

որտեղ $a_{1j_1}, a_{2j_2}, \dots, a_{mj_m}$ տարրերը ոչ զրոյական տողերի առաջատարներն են և հավասար չեն զրոյի, դրանցից ձախ և ներքև գտնվող բոլոր հնարավոր տարրերը հավասար են զրոյի, իսկ $j_1 < j_2 < \dots < j_m$:

Լեմմ 17.5: *Աստիճանաձև մատրիցի ոչ զրոյական տողերի հաջորդականությունը գծայնորեն անկախ է: Հետևաբար, ոչ զրոյական աստիճանաձև մատրիցի ռանգը հավասար է նրա ոչ զրոյական տողերի թվին:*

Ապացուցում: Անմիջական ստուգման եղանակով: □

Թեորեմ 17.3: *Յուրաքանչյուր $n \times m$-չափանի $A \in P$ մատրից տողերի տարրական ձևափոխությունների օգնությամբ կարելի է բերել աստիճանաձև տեսքի, որը կոչվում է A մատրիցի աստիճանաձև տեսք: Ըստ որում, A մատրիցի ռանգը հավասար է նրա աստիճանաձև տեսքում գոյություն ունեցող ոչ զրոյական տողերի թվին:*

Ապացուցում: Եթե A-ն զրոյական մատրից է, ապա այն աստիճանաձև տեսքի է: Եթե $A \neq 0$, ապա դիցուք j_1-ը նրա առաջին ոչ զրոյական սյան համարն է: Անհրաժեշտության դեպքում, տողերի տեղափոխության օգնությամբ, կարելի է հասնել նրան, որ $a_{1j_1} \neq 0$: Որից հետո, տողերի 1) տեսակի տարրական ձևափոխությունների օգնությամբ, a_{1j_1} տարրից ներքև գտնվող բոլոր տարրերը դարձվում են զրո: Ստացված մատրիցում անտեսելով առաջին տողը, ստանում ենք $(n-1) \times m$-չափանի մատրից, որի առաջին j_1 սյունակները զրոյական են: Նույն դատողությունները կրկնելով այս մատրիցի նկատմամբ, ի վերջո հանգում ենք աստիճանաձև մատրիցի:

Երկրորդ պնդումը բխում է նախորդ լեմմից և լեմմ 17.3-ից: □

Հետևություն 17.7: *$n \times m$-չափանի մատրիցի ցանկացած աստիճանաձև տեսքում ոչ զրոյական տողերի թիվը նույնն է:* □

Հատկություն 17.5: *Որպեսզի գծային հավասարումների (17.1) համասեռ համակարգն ունենա ոչ զրոյական լուծում անհրաժեշտ է և բավարար, որ անհայտների գործակիցներից կազմված*

$$A = \begin{pmatrix} a_{11}, & a_{12}, & \dots, & a_{1n} \\ a_{21}, & a_{22}, & \dots, & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1}, & a_{m2}, & \dots, & a_{mn} \end{pmatrix}$$

մատրիցի ռանգը լինի փոքր անհայտների թվից` $rank(A) < n$*:*

Ապացուցում: Որպեսզի (17.1) համասեռ համակարգն ունենա ոչ զրոյական լուծում անհրաժեշտ է և բավարար, որ անհայտների գործակիցներից կազմված A մատրիցի սյունակների համակարգը լինի գծայնորեն կախյալ: Վերջինս էլ նշանակում է, որ A մատրիցի ռանգը փոքր է դիտարկվող համասեռ համակարգի անհայտների թվից: $\square$

17.4. Արտադրյալ մատրիցի ռանգը: Ուղղանկյուն մատրիցի աջից (կամ ձախից) հակադարձելիության հայտանիշը

Թեորեմ 17.4: *Արտադրյալ մատրիցի ռանգը մեծ չէ արտադրիչ մատրիցների ռանգերից*` $rank(A \cdot B) \leqslant rank(A)$, $rank(A \cdot B) \leqslant rank(B)$, *այսինքն*`

$$rank(A \cdot B) \leqslant \min\{rank(A), rank(B)\}$$

ցանկացած $n \times m$*-չափանի* A *և ցանկացած* $m \times k$*-չափանի* B *մատրիցների համար:*

Ապացուցում: Դիցուք $A = (a_{ij})$-ն $n \times m$-չափանի, իսկ $B = (b_{ij})$-ն $m \times k$-չափանի մատրիցներ են, $C = A \cdot B$ և $C = (c_{ij})$: Հետևաբար, $n \times k$-չափանի C մատրիցի c_{ij} տարրը կլինի հավասար`

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{im}b_{mj} \,,$$

որտեղ $i = 1, \dots, n$; $j = 1, \dots, k$: Տալով $i = 1, \dots, n$ արժեքները, կունենանք`

$$\begin{pmatrix} c_{1j} \\ \vdots \\ c_{nj} \end{pmatrix} = b_{1j} \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} + b_{2j} \begin{pmatrix} a_{12} \\ \vdots \\ a_{n2} \end{pmatrix} + \dots + b_{mj} \begin{pmatrix} a_{1m} \\ \vdots \\ a_{nm} \end{pmatrix} ,$$

այսինքն՝ C մատրիցի յուրաքանչյուր սյունակ գծայնորեն արտահայտվում է A մատրիցի բոլոր սյունակների միջոցով: Հետևաբար, հատկություն 17.2-ի համաձայն, $rank(C) \leqslant rank(A)$:

Տալով c_{ij} տարրի j նշիչին $j = 1, \ldots, k$ արժեքները, կստանանք՝

$$(c_{i1}, \ldots, c_{ik}) = a_{i1}\,(b_{11}, \ldots, b_{1k}) + \cdots + a_{im}\,(b_{m1}, \ldots, b_{mk}) \ ;$$

Այսպիսով, C մատրիցի յուրաքանչյուր տող գծայնորեն արտահայտվում է B մատրիցի բոլոր տողերի միջոցով: Հետևաբար, $rank(C) \leqslant rank(B)$ (հատկություն 17.2): $\square$

Հետևություն 17.8: *Եթե $n \times m$-չափանի A մատրիցը ձախից կամ աջից բազմապատկենք հակադարձելի մատրիցով, ապա A մատրիցի ռանգը չի փոխվի: Մասնավորապես, եթե A-ն n-րդ կարգի հակադարձելի մատրից է, ապա*

$$n = rank(A) = rank\left(A^2\right) = \cdots \ ,$$

$$n = rank\left(A^{-1}\right) = rank\left(A^{-2}\right) = \cdots \ :$$

Ապացուցում: Եթե $C = A \cdot B$, որտեղ B-ն m-րդ կարգի հակադարձելի մատրից է, ապա գոյություն ունի այնպիսի m-րդ կարգի B' մատրից, որ $B \cdot B' = E_m$: Հետևաբար, $CB' = (AB)B' = A(BB') = AE_m = A$ և, համաձայն նախորդ թեորեմի,

$$rank(C) \leqslant rank(A)\,,$$

$$rank(A) \leqslant rank(C)\,,$$

այսինքն՝ $rank(C) = rank(A)$: Նույն եղանակով քննարկվում է նաև A մատրիցը ձախից B հակադարձելի մատրիցով բազմապատկելու դեպքը:

Երկրորդ պնդումն ապացուցելու համար, բավական է հաշվի առնել $A \cdot A^{-1} = E_n$ և $rank\,(E_n) = n$ հավասարությունները: $\square$

$A \in P^{n\times m}$ մատրիցը (այսինքն՝ P դաշտի վրա որոշված $n \times m$-չափանի A մատրիցը) կոչվում է

ա) հակադարձելի աջից, եթե գոյություն ունի այնպիսի $A' \in P^{m\times n}$ մատրից, որ $A \cdot A' = E_n$;

բ) հակադարձելի ձախից, եթե գոյություն ունի այնպիսի $A'' \in P^{m\times n}$ մատրից, որ $A'' \cdot A = E_m$:

Թեորեմ 17.5: *Որպեսզի $A \in P^{n\times m}$ մատրիցը լինի հակադարձելի աջից անհրաժեշտ է և բավարար, որ նրա ռանգը լինի հավասար իր տողերի թվին՝ $rank(A) = n$:*

Ապացուցում: Անհրաժեշտություն: Եթե $n \times m$-չափանի $A = (a_{ij})$ մատրիցը հակադարձելի է աջից, ապա, ըստ սահմանման, գոյություն ունի այնպիսի $m \times n$-չափանի $A' = (b_{ij})$ մատրից, որ $A \cdot A' = E_n$: Հետևաբար, n-րդ կարգի E_n միավոր մատրիցի սյունակների հաջորդականությունը՝

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}, \tag{17.4}$$

լինելով գծայնորեն անկախ, գծայնորեն արտահայտվում է A-ի սյունակների միջոցով՝

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = b_{11}\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + \cdots + b_{m1}\begin{pmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{pmatrix},$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = b_{1n}\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + \cdots + b_{mn}\begin{pmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{pmatrix}:$$

Միաժամանակ, A-ի յուրաքանչյուր սյունակ, լինելով n-սյունակ, համաձայն հետևություն 17.3-ի ապացուցման գծայնորեն կարտահայտվի (17.4) հաջորդականության միջոցով: Այսպիսով, A մատրիցի սյունակների հաջորդականությունը և (17.4) հաջորդականությունը համարժեք են և, հետևաբար, ունեն հավասար ռանգեր (հատկություն 17.4): Սակայն (17.4) հաջորդականության ռանգը հավասար է n-ի, ուստի՝ $rank(A) = n$: Այս հավասարությունը բխում է նաև նախորդ թեորեմից: Իրոք, $A \cdot A' = E_n$ հավասարությունից բխում է $n \leqslant rank(A)$ անհավասարությունը: Հետևաբար $n = rank(A)$:

Բավարարություն: Եթե $rank(A) = n$, ապա A մատրիցի սյունակներից կազմված հաջորդականությունը կունենա հենք՝ կազմված n հատ սյունակներից: Ուստի, հետևություն 17.3-ի համաձայն, յուրաքանչյուր n-սյունակ գծայնորեն կարտահայտվի այդ հենքի միջոցով: Մասնավորապես, (17.4) հաջորդականության յուրաքանչյուր տարր գծայնորեն կարտահայտվի այդ հենքի միջոցով, հետևաբար, նաև A մատրիցի բոլոր սյունակների միջոցով՝

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \lambda_{11} \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + \cdots + \lambda_{1m} \begin{pmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{pmatrix},$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots$$

$$\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \lambda_{n1} \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{n1} \end{pmatrix} + \cdots + \lambda_{nm} \begin{pmatrix} a_{1m} \\ a_{2m} \\ \vdots \\ a_{nm} \end{pmatrix}:$$

Նշանակելով՝

$$B = \begin{pmatrix} \lambda_{11}, & \dots, & \lambda_{n1} \\ \dots & \dots & \dots \\ \lambda_{1m}, & \dots, & \lambda_{nm} \end{pmatrix}$$

կստանանք՝ $A \cdot B = E_n$, այսինքն՝ A-ն հակադարձելի է աջից: □

Թեորեմ 17.6: *Որպեսզի $A \in P^{n\times m}$ մատրիցը լինի հակադարձելի ձախից անհրաժեշտ է և բավարար, որ նրա ռանգը լինի հավասար իր սյունակների թվին՝ $rank(A) = m$:*

Ապացուցում: $A \in P^{n\times m}$ մատրիցը կլինի հակադարձելի ձախից այն և միայն այն դեպքում, երբ նրա շրջված $A^T \in P^{m\times n}$ մատրիցը հակադարձելի է աջից: Մնում է օգտվել նախորդ թեորեմից: □

***Հետևություն 17.9*:** *Որպեսզի $A \in P^{n\times m}$ մատրիցը լինի հակադարձելի աջից և ձախից անհրաժեշտ է և բավարար, որ*

$$n = rank(A) = m\,,$$

այսինքն՝ որ A մատրիցը լինի հակադարձելի քառակուսային մատրից:

□

17.5. Կրոնեկեր-Կապելլիի թեորեմը

Գծային հավասարումների համակարգը կոչվում է **լուծելի** կամ **համատեղելի**, եթե այն ունի որևէ լուծում:

Անցնենք գծային հավասարումների ընդհանուր համակարգի լուծման գոյության հարցին՝

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1, \\ \quad \dots \quad \dots \quad \dots \quad \dots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m, \end{cases} \tag{17.5}$$

որտեղ $a_{ij}, b_k \in P$, $k, i = 1, \dots, m$, $j = 1, \dots, n$, իսկ

$$A = \begin{pmatrix} a_{11}, & \dots, & a_{1n} \\ \dots & \dots & \dots \\ a_{m1}, & \dots, & a_{mn} \end{pmatrix} \quad \text{և} \quad \bar{A} = \left(\begin{array}{ccc|c} a_{11}, & \dots, & a_{1n} & b_1 \\ \dots & \dots & \dots & \dots \\ a_{m1}, & \dots, & a_{mn} & b_m \end{array} \right)$$

մատրիցները, համապատասխանաբար, կոչվում են (17.5) **համակարգի հիմնական** և **ընդլայնված մատրիցներ**:

Թեորեմ 17.7 (Կրոնեկեր, Կապելլի): *Որպեսզի գծային հավասարումների (17.5) համակարգն ունենա լուծում (այսինքն՝ լինի լուծելի) անհրաժեշտ է և բավարար, որ նրա հիմնական և ընդլայնված մատրիցների ռանգերը լինեն հավասար՝* $rank(A) = rank\left(\bar{A}\right)$*:*

Ապացուցում: Եթե (17.5) համակարգն ունի լուծում, ապա նրա ազատ անդամների

$$B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$$

սյունակը գծայնորեն կարտահայտվի հիմնական A մատրիցի սյունակների միջոցով: Ուստի, $\bar{A}$ ընդլայնված մատրիցի սյունակների համակարգը կլինի համարժեք A մատրիցի սյունակների համակարգին և, հետևաբար (հատկություն 17.4), $rank\left(\bar{A}\right) = rank(A)$:

Եվ հակառակը, եթե A և $\bar{A}$ մատրիցների ռանգերը հավասար են, ապա A մատրիցի սյունակներից կազմված համակարգի յուրաքանչյուր հենք կլինի այդպիսին նաև $\bar{A}$ մատրիցի սյունակներից կազմված համակարգի համար (հատկություն 17.3): Այսպիսով, $\bar{A}$ մատրիցի վերջին B սյունակը գծայնորեն կարտահայտվի A մատրիցի սյունակների համակարգի հենքով, հետևաբար, նաև A-ի բոլոր սյունակներով: Այդ վերլուծության գործակիցներից կազմված $(\alpha_1, \ldots, \alpha_n)$ հաջորդականությունը կլինի (17.5) համակարգի լուծում: □

Հետևություն 17.10: *Եթե* $A_1 = (a_{11}, \ldots, a_{1n})$, *...*, $A_m = (a_{m1}, \ldots, a_{mn})$ n*-տողերի հաջորդականությունը գծայնորեն անկախ է, ապա կամայական* $b_1, \ldots, b_m \in P$ *սկալյարների համար գծային հավասարումների (17.5) համակարգն ունի լուծում:* □

Նշանակելով

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

(17.5) համակարգն ընդունում է հետևյալ համառոտ մատրիցային հավասարման տեսքը՝

$$A \cdot X = B \; : \tag{17.6}$$

Ըստ որում, որպեսզի $(\alpha_1, \ldots, \alpha_n) \in P_n$ n-յակը լինի լուծում (17.5) համակարգի համար անհրաժեշտ է և բավարար, որ $\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix}$ սյունակը լինի լուծում (17.6) մատրիցային հավասարման համար:

17.6. Հենքային ենթամատրից և մատրիցի ռանգ

Դիտարկենք $n \times m$ չափանի կամայական $A = (a_{ij}) \in P^{n \times m}$ մատրից: A մատրիցի մեջ սևեռենք k քանակի տողեր և նույնքան էլ սյունակներ՝ $k \leqslant \min\{n, m\}$: Ընտրված տողերի և սյունակների հատման կետերում գտնվող մատրիցի տարրերից կազմում ենք մի B քառակուսային մատրից (առանց խախտելու տարրերի միմյանց նկատմամբ ունեցած դիրքը), որի կարգը հավասար է k-ի: Այս B մատրիցը կոչվում է սկզբնական A մատրիցի k-**րդ կարգի ենթամատրից** և գրվում է $B \leqslant A$: Եթե ընտրված (սևեռված) տողերի և սյունակների համարներն են $1 \leqslant i_1 < i_2 < \cdots < i_k \leqslant n$ և $1 \leqslant j_1 < j_2 < \cdots < j_k \leqslant m$ թվերը, ապա k-րդ կարգի B ենթամատրիցը երբեմն համառոտ նշանակվում է՝

$$B = A\begin{pmatrix} i_1, i_2, \ldots, i_k \\ j_1, j_2, \ldots, j_k \end{pmatrix},$$

իսկ նրա որոշիչը հաճախ կոչվում է A մատրիցի k-**րդ կարգի մինոր**:

Դիցուք B և C քառակուսային մատրիցները միևնույն $n \times m$-չափանի A մատրիցի ենթամատրիցներ են: C ենթամատրիցը կոչվում է k-րդ կարգի B ենթամատրիցին **երիզող** կամ **շրջափակող**, եթե $B \leqslant C$ և C ենթամատրիցի կարգը հավասար է $k+1$:

A մատրիցի B (քառակուսային) ենթամատրիցը կանվանենք **հենքային**, եթե $det(B) \neq 0$ և B-ին երիզող A-ի բոլոր ենթամատրիցների որոշիչները հավասար են զրոյի կամ B-ն չունի երիզող ենթամատրից ընդհանրապես:

Օրինակ,

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & 3 \end{pmatrix}$$

մատրիցն օժտված է երկու հենքային ենթամատրիցներով՝

$$A\begin{pmatrix} 1,3 \\ 1,2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad A\begin{pmatrix} 1,3 \\ 1,3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix},$$

իսկ միավոր մատրիցի միակ հենքային ենթամատրիցն ինքն է:

Ակնհայտ է, որ զրոյական մատրիցը չի օժտված հենքային ենթամատրիցով:

Լեմմ 17.6: *Յուրաքանչյուր ոչ զրոյական $n \times m$-չափանի A մատրից օժտված է հենքային ենթամատրիցով:*

Ապացուցում: Եթե $A \neq 0$, ապա այն ունի որևէ a ոչ զրոյական տարր: Հնարավոր է երկու դեպք, կամ (a)-ին երիզող 2-րդ կարգի A-ի բոլոր ենթամատրիցներն ունեն զրո որոշիչ կամ գոյություն ունի 2-րդ կարգի (a)-ին երիզող այնպիսի $C_1 \leqslant A$ ենթամատրից, որի որոշիչը $\neq 0$: Առաջին դեպքում $(a) \leqslant A$ ենթամատրիցը կլինի հենքային, իսկ երկրորդ դեպքում սկսում ենք դիտարկել C_1 ենթամատրիցին երիզող A-ի ենթամատրիցները (եթե այդպիսիք գոյություն ունեն): Եթե C_1 ենթամատրիցին երիզող A-ի բոլոր ենթամատրիցներն ունեն զրո որոշիչ, ապա C_1-ը կլինի հենքային ենթամատրից A-ի համար, հակառակ դեպքում՝ գոյություն կունենա C_1-ին երիզող այնպիսի $C_2 \leqslant A$

ենթամատրից, որի որոշիչը $\neq 0$: Վերջավոր թվով նմանատիպ քայլերից հետո, հանգում ենք A-ի որևէ հենքային ենթամատրիցի: $\square$

Հետևյալ բնական թիվը կոչվում է ոչ զրոյական $n \times m$-չափանի A **մատրիցի նշիչ**`

$$ind(A) = \max\{k \in N \mid k \geqslant 1 \text{ և գոյություն ունի } k\text{-րդ կարգի այնպիսի } B \leqslant A \text{ ենթամատրից, որ } det(B) \neq 0\}\ ,$$

այսինքն` մատրիցի նշիչը հավասար է նրա ոչ զրոյական որոշիչ ունեցող ամենամեծ կարգի ենթամատրիցի կարգին:

Լեմմ 17.7: $k = ind(A)$ *նշիչով ոչ զրոյական* $n \times m$*-չափանի* A *մատրիցի ոչ զրոյական որոշիչ ունեցող ցանկացած* k*-րդ կարգի* $B \leqslant A$ *ենթամատրից կլինի հենքային:* $\square$

Հետևյալ արդյունքից նույնպես բխում է, որ ոչ զրոյական A մատրիցի տողային և սյունակային ռանգերը հավասար են (A-ի հենքային ենթամատրիցի կարգին):

Թեորեմ 17.8: *1) Ոչ զրոյական* $n \times m$*-չափանի* A *մատրիցի* B *հենքային ենթամատրիցով անցնող* A*-ի սյունակների համակարգը (հաջորդականությունը) գծայնորեն անկախ է, իսկ այդ համակարգի միջոցով գծայնորեն արտահայտվում է* B *հենքային ենթամատրիցից դուրս գտնվող* A*-ի ցանկացած սյունակ (եթե այդպիսին գոյություն ունի):*

2) Ոչ զրոյական $n \times m$*-չափանի* A *մատրիցի* B *հենքային ենթամատրիցով անցնող* A*-ի տողերի համակարգը գծայնորեն անկախ է, իսկ այդ համակարգի միջոցով գծայնորեն արտահայտվում է* B *հենքային ենթամատրիցից դուրս գտնվող* A*-ի ցանկացած տող (եթե այդպիսին գոյություն ունի):*

Ապացույց: 1) Եթե $A \neq 0$, ապա գոյություն ունի նրա որևէ B հենքային ենթամատրից (լեմմ 17.6): Պնդման մի մասն ակնհայտ է: Իրոք, եթե B հենքային ենթամատրիցով անցնող սյունակների համակարգը լիներ գծայնորեն կախյալ, ապա գծայնորեն կախյալ կլիներ նաև B հենքային ենթամատրիցի սյունակների համակարգը և, հետևաբար, B հենքային ենթամատրիցի որոշիչը կլիներ հավասար զրոյի, որը հակասում է նրա սահմանմանը:

Այժմ ապացուցենք, որ $A \neq 0$ մատրիցի ցանկացած սյունակ գծայնորեն արտահայտվում է նրա B հենքային ենթամատրիցով անցնող սյունակների միջոցով: Պարզության համար ենթադրենք, թե k-րդ կարգի B հենքային ենթամատրիցը գրավում է A մատրիցի վերին ձախ անկյունը՝

$$A = \left(\begin{array}{c|c} a_{11}, \ldots, a_{1k} & \ldots, a_{1m} \\ \ldots \quad \ldots & \ldots \quad \ldots \\ a_{k1}, \ldots, a_{kk} & \ldots, a_{km} \\ \hline \ldots \quad \ldots & \ldots \quad \ldots \\ a_{n1}, \ldots, a_{nk} & , \ldots, a_{nm} \end{array} \right) :$$

Դիտարկենք $(k+1)$-րդ կարգի

$$B_{ij} = \begin{pmatrix} a_{11}, \ldots, a_{1k}, a_{1j} \\ \ldots \quad \ldots \quad \ldots \\ a_{k1}, \ldots, a_{kk}, a_{kj} \\ a_{i1}, \ldots, a_{ik}, a_{ij} \end{pmatrix}$$

մատրիցը, որտեղ $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant m$: Դժվար չէ նկատել, որ i, j նշիչների ցանկացած արժեքների դեպքում՝ $|B_{ij}| = 0$: Իրոք, եթե $1 \leqslant i \leqslant k$ կամ $1 \leqslant j \leqslant k$, ապա $|B_{ij}| = 0$ որպես երկու հավասար տողերով կամ երկու հավասար սյունակներով մատրիցի որոշիչ, իսկ $k < i \leqslant n$ և $k < j \leqslant m$ դեպքում B_{ij}-ն կլինի B հենքային ենթամատրիցին երիզող A-ի ենթամատրից և, հետևաբար, $|B_{ij}| = 0$: Վերլուծելով B_{ij} մատրիցի որոշիչը ըստ իր վերջին տողի տարրերի, կունենանք՝

$$a_{i1}\mathcal{D}_1 + \cdots + a_{ik}\mathcal{D}_k + a_{ij}\mathcal{D} = 0\,,$$

որտեղ $\mathcal{D} = |B| \neq 0$, իսկ $\mathcal{D}_1, \ldots, \mathcal{D}_k$ հանրահաշվական լրացուցիչները կախված չեն i-ից: Հետևաբար,

$$a_{ij} = \left(-\mathcal{D}^{-1}\mathcal{D}_1\right) a_{i1} + \cdots + \left(-\mathcal{D}^{-1}\mathcal{D}_k\right) a_{ik}\,,$$

որտեղից, $i = 1, \ldots, n$ արժեքների դեպքում, հանգում ենք պահանջվող հավասարությանը՝

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} = \left(-\mathcal{D}^{-1}\mathcal{D}_1\right) \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} + \cdots + \left(-\mathcal{D}^{-1}\mathcal{D}_k\right) \begin{pmatrix} a_{1k} \\ \vdots \\ a_{nk} \end{pmatrix} :$$

Ճիշտ նույն եղանակով ապացուցվում է նաև թեորեմի երկրորդ պնդումը: □

Հետևություն 17.11: *Ոչ զրոյական $n \times m$-չափանի մատրիցի տողային և սյունակային ռանգերը հավասար են իր ցանկացած հենքային ենթամատրիցի կարգին:* □

Հետևություն 17.12: *Ոչ զրոյական $n \times m$-չափանի մատրիցի բոլոր հենքային ենթամատրիցներն ունեն նույն կարգը:* □

Հետևություն 17.13: *Ոչ զրոյական $n \times m$-չափանի մատրիցի ռանգը հավասար է իր նշիչին՝ $rank(A) = ind(A)$:* □

Թեորեմ 17.9 (մատրիցի որոշիչի զրո լինելու հայտանիշը): *n-րդ կարգի $A \in P^{n\times n}$ մատրիցի որոշիչը հավասար է զրոյի այն և միայն այն դեպքում, երբ A-ի տողերի (սյունակների) համակարգը գծայնորեն կախյալ է:*

Ապացուցում: Դիցուք $det(A) = 0$: Հնարավոր է երկու դեպք՝ $A = 0$ կամ $A \neq 0$: Առաջին դեպքում պնդումն ակնհայտ է, իսկ երկրորդ դեպքում $n \geqslant 2$ և A-ն օժտված է B հենքային ենթամատրիցով, որի կարգը կլինի փոքր n-ից: Հետևաբար, գոյություն կունենա B հենքային ենթամատրիցից դուրս դտնվող A-ի սյունակ (տող), որն ըստ նախորդ թեորեմի գծայնորեն կարտահայտվի B հենքային ենթամատրիցով անցնող սյունակների (տողերի) միջոցով: Այսպիսով, A մատրիցի սյունակների (տողերի) համակարգը գծայնորեն կախյալ է:

Եվ հակառակը, եթե n-րդ կարգի A մատրիցի սյունակներից (տողերից) կազմված համակարգը գծայնորեն կախյալ է, ապա կամ $A = 0$ և $det(A) = 0$, կամ $A \neq 0$ և A-ի հենքային ենթամատրիցի կարգը կլինի փոքր n-ից: Հետևաբար, այս դեպքում՝ $ind(A) < n$ և $det(A) = 0$ (տես նաև հատկություն 14.18-ը): □

17.7. Գծային (վեկտորական) տարածության հենք և չափողականություն: Ենթատարածություն

Դիցուք Q-ն գծային (վեկտորական) տարածություն է որոշված P դաշտի վրա (պարզության համար կարելի է ենթադրել $P = \mathbb{R}$): Q գծային տարածության տարրերի

$$e_1, e_2, \ldots, e_n \tag{17.7}$$

վերջավոր հաջորդականությունը (համակարգը) կոչվում է Q-ի **հենք** (բազա, բազիս) կամ **կոորդինատական համակարգ**, եթե այն գծայնորեն անկախ է և Q-ի յուրաքանչյուր x տարր (վեկտոր) գծայնորեն արտահայտվում է (17.7)-ի միջոցով: Եթե (17.7)-ը հենք է, ապա նրա տարրերի տարբեր տեղափոխությունների մեջոցով կարող ենք ստանալ ևս $n!$ հատ հենքեր:

Լեմմ 17.8: *Եթե (17.7) հաջորդականությունը հենք է Q գծային տարածության համար և*

$$x = \alpha_1 e_1 + \cdots + \alpha_n e_n\,,$$

$$x = \alpha_1' e_1 + \cdots + \alpha_n' e_n\,,$$

որտեղ $x \in Q$, $\alpha_1, \ldots, \alpha_n, \alpha_1', \ldots, \alpha_n' \in P$, ապա $\alpha_1 = \alpha_1'$, ..., $\alpha_n = \alpha_n'$ (այսինքն՝ գծային տարածության յուրաքանչյուր տարր (վեկտոր) միարժեքորեն է վերլուծվում իր հենքի միջոցով):

Ապացուցում: Եթե

$$\alpha_1 e_1 + \cdots + \alpha_n e_n = \alpha_1' e_1 + \cdots + \alpha_n' e_n\,,$$

ապա

$$(\alpha_1 - \alpha_1')\, e_1 + \cdots + (\alpha_n - \alpha_n')\, e_n = 0\,,$$

որտեղից $\alpha_1 - \alpha_1' = 0$, ..., $\alpha_n - \alpha_n' = 0$, որովհետև $e_1, \ldots, e_n$ համակարգը գծայնորեն անկախ է: Այսպիսով, $\alpha_1 = \alpha_1'$, ..., $\alpha_n = \alpha_n'$: $\square$

Հատկություն 17.6: *Միևնույն Q գծային տարածության բոլոր հենքերը (եթե դրանք գոյություն ունեն) պարունակում են նույն քանակի տարրեր: Այդ թիվը կոչվում է Q գծային տարածության չափողականություն և նշանակվում է $dim(Q)$-ով կամ $dim\,Q$-ով:*

Ապացուցում: Դիցուք (17.7) և

$$f_1, f_2, \ldots, f_m \tag{17.8}$$

հաջորդականությունները միևնույն Q գծային տարածության համար հենքեր են: Քանի որ (17.7)-ը հենք է, ապա յուրաքանչյուր f_i $(i = 1, \ldots, m)$ գծայնորեն կարտահայտվի (17.7)-ի միջոցով: Միաժամանակ (17.8)-ը նույնպես հենք է և յուրաքանչյուր e_j գծայնորեն կարտահայտվի (17.8)-ի միջոցով: Ուստի (17.7) և (17.8) հաջորդականությունները գծայնորեն անկախ են և համարժեք: Հետևաբար, $n = m$ (հատկություն 17.1): □

Օրինակ, $dim\mathbb{R}^n = dim\mathbb{R}_n = n$, $dim\mathbb{R}^{n\times m} = n \cdot m$:

Զրոյական գծային տարածության չափողականությունը ընդունվում է հավասար զրոյի: Եթե $dim Q = n$, ապա Q-ն կոչվում է **n-չափանի գծային տարածություն**: Q գծային տարածությունը կոչվում է **վերջավոր չափանի**, եթե այն n-չափանի է որևէ $n \geqslant 0$ բնական թվի համար: Հակառակ դեպքում, գծային տարածությունը կոչվում է **անվերջ չափանի**:

Հետևություն 17.1-ից բխում է, որ n-չափանի գծային տարածության n-ից շատ թվով տարրեր պարունակող յուրաքանչյուր հաջորդականություն գծայնորեն կախյալ է ($n \geqslant 1$):

Հատկություն 17.7: *n-չափանի Q գծային տարածության n-տարրանի գծայնորեն անկախ յուրաքանչյուր հաջորդականություն Q-ի հենք է:*

Ապացուցում: Եթե տրված Q գծային տարածության $f_1, f_2, \ldots, f_n$ գծայնորեն անկախ հաջորդականությունը Q-ի հենք չլինի, ապա Q գծային տարածության որևէ f տարր գծայնորեն չի արտահայտվի այդ $f_1, f_2, \ldots, f_n$ հաջորդականության միջոցով և, հետևաբար,

$$f_1, f_2, \ldots, f_n, f$$

հաջորդականությունը կլիներ գծայնորեն անկախ, որը հակասում է թեորեմ 17.1-ին: □

Գոյություն ունի գծային տարածություն, որը վերջավոր չափանի չէ: Այդպիսին է, օրինակ, $P[x]$ բազմանդամների գծային տարածությունը, որովհետև այդ գծային տարածության

$$1, x, x^2, \ldots, x^n$$

հաջորդականությունը գծայնորեն անկախ է՝ ցանկացած $n \in \mathbb{N}$ բնական թվի դեպքում:

Թեորեմ 17.10: *Ոչ զրոյական վերջավոր չափանի Q գծային տարածության տարրերի յուրաքանչյուր գծայնորեն անկախ*

$$t_1, t_2, \ldots, t_m \tag{17.9}$$

համակարգ կամ Q-ի հենք է կամ դրան կարելի է ընդլայնել մինչև Q-ի հենքի, այսինքն՝ եթե (17.9)-ը Q-ի հենք չէ, ապա գոյություն կունենան վերջավոր քանակությամբ այնպիսի $a_1, \ldots, a_\ell \in Q$ տարրեր, որ $t_1, \ldots, t_m, a_1, \ldots, a_\ell$ համակարգը Q-ի հենք է: Մասնավորապես, վերջավոր չափանի ոչ զրոյական Q գծային տարածության յուրաքանչյուր ոչ զրոյական տարրից կազմված համակարգ կամ Q-ի հենք է կամ դրան կարելի է ընդլայնել մինչև Q-ի հենքի:

Ապացուցում: Եթե (17.9) համակարգը Q-ի հենք է, ապա պնդումն ապացուցված է: Հակառակ դեպքում, Q-ի որևէ a_1 տարր գծայնորեն չի արտահայտվի (17.9) հաջորդականության միջոցով: Հետևաբար,

$$t_1, t_2, \ldots, t_m, a_1 \tag{17.10}$$

հաջորդականությունը կլինի գծայնորեն անկախ: Եթե այս նոր (17.10) հաջորդականությունը Q-ի հենք է, ապա պնդումն ապացուցված է: Հակառակ դեպքում, նորից գոյություն կունենա Q-ի այնպիսի a_2 տարր, որը գծայնորեն չի արտահայտվի (17.10)-ի միջոցով: Հետևաբար,

$$t_1, t_2, \ldots, t_m, a_1, a_2$$

հաջորդականությունը կլինի գծայնորեն անկախ, և այսպես շարունակ: Վերջավոր թվով նմանատիպ քայլերից հետո կհանգենք Q-ի հենքի, որովհետև $dim\, Q = n > 0$ որևէ n բնական թվի համար, իսկ այդ դեպքում Q-ի $n+1$ տարրեր պարունակող յուրաքանչյուր հաջորդականություն գծայնորեն կախյալ է: □

Հետևություն 17.14: *Յուրաքանչյուր վերջավոր գծային տարածություն վերջավոր չափանի գծային տարածություն է:* □

Թեորեմ 17.11: *Վերջավոր դաշտի կարգը (այսինքն՝ տարրերի քանակը) հավասար է պարզ թվի աստիճանի:*

Ապացուցում: Յուրաքանչյուր $F(+,\cdot)$ վերջավոր դաշտի բնութագրիչը հավասար է որևէ p պարզ թվի, այսինքն՝

$$\begin{aligned}
&e \neq 0\\
&2e = e + e \neq 0,\\
&\dots \quad \dots \quad \dots\\
&(p-1)e = \underbrace{e + \cdots + e}_{p-1} \neq 0,\\
&pe = \underbrace{e + \cdots + e}_{p} = 0,
\end{aligned}$$

որտեղ e-ն F դաշտի միավորն է: $F' = \{0, e, 2e, \dots, (p-1)e\}$ բազմությունը կլինի F-ի ենթադաշտ, որն իզոմորֆ է $\mathbb{Z}_p$ մնացքների դաշտին: Այնուհետև, F-ն իր գործողություններով կարելի է դիտել որպես գծային տարածություն որոշված F' դաշտի վրա: Քանի որ F-ը վերջավոր է, ապա, նախորդ հետևության համաձայն, այն կլինի վերջավոր չափանի գծային տարածություն: Դիցուք $dim(F) = n$: Ակնհայտ է, որ $n \neq 0$, որովհետև $F \neq \{0\}$: Եթե $e_1, \dots, e_n$ համակարգը F-ի հենք է, ապա նրա յուրաքանչյուր x տարր կունենա հետևյալ միարժեք վերլուծությունը (լեմմ՝ 17.8)՝

$$x = \alpha_1 e_1 + \cdots + \alpha_n e_n\,,$$

որտեղ $\alpha_1, \dots, \alpha_n$ սկալյարները պատկանում են F' բազմությանը, որի կարգը հավասար է p-ի: Հետևաբար, $|F| = p^n$: $\square$

Դիցուք Q-ն գծային տարածություն է որոշված P դաշտի վրա: Ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը կոչվում է Q-ի **ենթատարածություն** և գրվում (նշանակվում) է $Q' \leqslant Q$, եթե Q'-ը փակ է գումարման և սկալյարով (ձախից) բազմապատկման նկատմամբ, այսինքն՝

ա) $x, y \in Q' \longrightarrow x + y \in Q'$,

բ) $x \in Q'$, $\alpha \in P \longrightarrow \alpha x \in Q'$:

Այս երկու պայմանները ակնհայտորեն միավորվում են մեկ պայմանի մեջ՝

գ) $x, y \in Q',\ \alpha, \beta \in P \longrightarrow \alpha x + \beta y \in Q'$:

բ) պայմանի մեջ վերցնելով $\alpha = 0$ ստանում ենք՝ $0 \in Q'$, իսկ $\alpha = -1$ դեպքում կունենանք՝ $-x \in Q'$, եթե $x \in Q'$: Հետևաբար, Q' ենթատարածության համար տեղի կունենան գծային տարածության սահմանման բոլոր ութ պայմանները (աքսիոմները): Այսպիսով, Q գծային տարածության յուրաքանչյուր $Q' \leqslant Q$ ենթատարածություն կլինի գծային տարածություն Q-ի գումարման և սկալյարով բազմապատկման գործողությունների նկատմամբ:

Օրինակ, եթե $A \in P^{n\times m}$, ապա բոլոր այն $x \in P^m$ սյունակների բազմությունը, որոնց համար $A \cdot x = 0$, կոչվում է $n \times m$-չափանի A **մատրիցի միջուկ** և նշանակվում է $Ker(A)$-ով՝

$$Ker(A) = \{x \in P^m \mid A \cdot x = 0\} :$$

Հեշտությամբ ստուգվում է, որ $Ker(A)$-ն P^m-ի ենթատարածություն է: Յուրաքանչյուր Q գծային տարածություն օժտված է $Q' = \{0\}$ և $Q' = Q$ ենթատարածություններով:

Լեմմ 17.9: *Եթե Q-ն գծային տարածություն է որոշված P դաշտի վրա և $s_1, s_2, \ldots, s_m \in Q$, ապա*

$$Q' = \{\alpha_1 s_1 + \alpha_2 s_2 + \cdots + \alpha_m s_m \mid \alpha_1 \in P, \alpha_2 \in P, \ldots, \alpha_m \in P\} \subseteq Q$$

ենթաբազմությունը կլինի Q-ի ենթատարածություն: Այս Q' ենթատարածությունը կոչվում է $s_1, s_2, \ldots, s_m \in Q$ տարրերով ծնված **գծային թաղանթ** *և նշանակվում է՝*

$$Q' = \langle s_1, s_2, \ldots, s_m \rangle \quad \textit{կամ} \quad Q' = (s_1, s_2, \ldots, s_m) : \qquad \square$$

Եթե $Q = (s_1, s_2, \ldots, s_m)$, ապա $s_1, s_2, \ldots, s_m$ վերջավոր համակարգը կոչվում է Q գծային տարածության **ծնորդների** (ծնիչների) **համակարգ**, իսկ դրա տարրերը՝ Q-ի ծնորդներ (ծնիչներ) կամ ծնորդ (ծնիչ) տարրեր:

Օրինակ, եթե $e_1, \ldots, e_n$ հաջորդականությունը հենք է Q գծային տարածության համար, ապա $Q = (e_1, \ldots, e_n)$ և նշանակելով $Q' = (e_1, \ldots, e_m)$, որտեղ $1 \leqslant m < n$, կստանանք $dim(Q') = m$ չափողականությամբ ենթատարածություն:

Թեորեմ 17.12: *1) Վերջավոր չափանի Q գծային տարածության յուրաքանչյուր Q' ենթատարածություն ևս վերջավոր չափանի գծային տարածություն է և $dim(Q') \leqslant dim(Q)$, իսկ $Q' \neq Q$ դեպքում՝ $dim(Q') < dim(Q)$;*

2) Որպեսզի գծային տարածությունը լինի վերջավոր չափանի անհրաժեշտ է և բավարար, որ այն օժտված լինի ծնորդների համակարգով;

3) Ոչ զրոյական Q գծային տարածության ծնորդների յուրաքանչյուր համակարգից կարելի է ընտրել Q-ի հենք հանդիսացող ենթահամակարգ:

Ապացուցում: 1) Դիցուք $dim Q = n$: Եթե $Q' = \{0\}$, ապա պնդումն ակնհայտ է: Դիցուք $Q' \neq \{0\}$: Վերցնենք Q'-ի որևէ $f_1 \neq 0$ տարր: Եթե f_1-ից կազմված մեկ տարրանի համակարգը հենք է Q'-ի համար, ապա պնդումն ապացուցված է: Հակառակ դեպքում, գոյություն կունենա այնպիսի $f_2 \in Q'$ տարր, որը գծայնորեն չի արտահայտվում f_1-ի միջոցով: Այդ դեպքում, Q'-ի f_1, f_2 համակարգը կլինի գծայնորեն անկախ: Եթե այս f_1, f_2 համակարգը հենք է Q'-ի համար, ապա պնդումն ապացուցված է: Հակառակ դեպքում, գոյություն կունենա այնպիսի $f_3 \in Q'$ տարր, որը գծայնորեն չի արտահայտվում f_1, f_2 համակարգի միջոցով, և այսպես շարունակ: Վերջավոր թվով նմանատիպ քայլերից հետո կհանգենք Q'-ի հենքի, որովհետև Q'-ի գծայնորեն անկախ յուրաքանչյուր համակարգ կլինի այդպիսին նաև Q-ի համար, իսկ Q գծային տարածության $n+1$ հատ տարրեր պարունակող յուրաքանչյուր հաջորդականություն գծայնորեն կախյալ է:

2) Եթե $dim Q = n > 0$, ապա Q-ի յուրաքանչյուր հենք կլինի ծնորդների համակարգ, իսկ $dim Q = 0$ դեպքում $0 \in Q$ տարրը կլինի $Q = \{0\}$ գծային տարածության ծնորդների համակարգը: Ապացուցենք հակառակը:

Դիցուք $Q \neq \{0\}$ և Q-ն օժտված է ծնորդների համակարգով՝ $Q = (s_1, s_2, \ldots, s_m)$: Նախ նկատենք, որ $s_1, s_2, \ldots, s_m$ ծնորդների համակարգը կլինի ոչ զրոյական: Եթե $s_1, s_2, \ldots, s_m$ համակարգը գծայնորեն անկախ է, ապա այն կլինի հենք Q-ի համար և $dim Q = m$: Հակառակ դեպքում, $s_1, s_2, \ldots, s_m$ համակարգը կլինի գծայնորեն կախյալ և նրա տարրերից որևէ մեկը գծայնորեն կարտահայտվի մյուսների միջոցով: Դիցուք s_m-ը գծայնորեն արտահայտվում է $s_1, s_2, \ldots, s_{m-1}$ համակարգի միջոցով և, հետևաբար, $Q = (s_1, s_2, \ldots, s_{m-1})$: Եթե $s_1, s_2, \ldots, s_{m-1}$ համակարգը գծայնորեն անկախ է, ապա այն կլինի հենք Q-ի համար և $dim Q = m-1$: Հակառակ դեպքում, $s_1, s_2, \ldots, s_{m-1}$ համակարգը կլինի գծայնորեն կախյալ և նրա տարրերից որևէ մեկը գծայնորեն կարտահայտվի մյուսների միջոցով, և այսպես շարունակ: Վերջավոր թվով նմանատիպ քայլերից հետո $s_1, s_2, \ldots, s_m$ համակարգից կառանձնացվի մի ենթահամակարգ որը հենք է Q-ի համար: Այսպիսով, Q գծային տարածությունը կլինի վերջավոր չափանի:

3)-ը բխում է 2)-ի ապացուցումից: □

n-չափանի Q գծային տարածության յուրաքանչյուր $(n-1)$-չափանի ենթատարածություն կոչվում է Q-ի **գերհարթություն** (հիպերհարթություն), իսկ յուրաքանչյուր 1-չափանի ենթատարածություն կոչվում է **ուղիղ գիծ**:

17.8. Գծային հավասարումների համատեղելի համակարգի ընդհանուր լուծում

Ինչպես գիտենք, գծային հավասարումների (17.5) համակարգը կարելի է գրել $A \cdot X = B$ մատրիցային հավասարման տեսքով և $\alpha = (\alpha_1, \ldots, \alpha_n) \in P_n$ n-յակը կլինի լուծում (17.5) համակարգի համար այն և միայն այն դեպքում, երբ $A \cdot \alpha^T = B$: Այսպիսով, գծային հավասարումների համակարգի լուծման ընթացքը կարելի է նկարագրել նաև մատրիցային տեսքով: $A \cdot X = 0$ հավասարումը կոչվում է $A \cdot X = B$ մատրիցային հավասարմանը համապատասխանող **համասեռ մատրիցային հավասարում**: L^A-ով կամ L_n^A-ով նշանակենք $A \cdot X = 0$ համասեռ մատրիցային հավասարման բոլոր լուծումների բազմությունը, այսինքն՝

$$L^A = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in P^n \,\middle|\, A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \right\} :$$

Լեմմ 17.10: *L_n^A-ն P^n-ի ենթատարածություն է՝ ցանկացած $m \times n$-չափանի $A \in P^{m\times n}$ մատրիցի համար: Հետևաբար, L_n^A-ն վերջավոր չափանի գծային տարածություն է և $dim\left(L_n^A\right) \leqslant n$:*

Ապացուցում: Իրոք, նախ նկատենք, որ $L_n^A \neq \emptyset$, որովհետև $0 \in L_n^A$: Եթե $h_1, h_2 \in L_n^A$ և $\alpha \in P$, ապա

$$A\,(h_1 + h_2) = Ah_1 + Ah_2 = 0 + 0 = 0\,,$$

$$A\,(\alpha h_1) = \alpha\,(Ah_1) = \alpha 0 = 0\,;$$

Հետևաբար, $h_1 + h_2 \in L_n^A$ և $\alpha h_1 \in L_n^A$: □

L_n^A վերջավոր չափանի գծային տարածության ցանկացած հենք կոչվում է $A \cdot X = 0$ համասեռ մատրիցային հավասարման **հենքային** կամ **ֆունդամենտալ լուծումների համակարգ**:

Այժմ S^A-ով կամ S_n^A-ով նշանակենք $A \cdot X = B$ մատրիցային հավասարման բոլոր լուծումների բազմությունը, այսինքն՝

$$S_n^A = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \in P^n \,\middle|\, A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = B \right\} :$$

Լեմմ 17.11: *Եթե* $h_1, h_2 \in S_n^A$*, ապա* $h_1 - h_2 \in L_n^A$*:*

Ապացույց: Ըստ պայմանի, $A \cdot h_1 = B$ և $A \cdot h_2 = B$: Հետևաբար,

$$A\,(h_1 - h_2) = Ah_1 - Ah_2 = B - B = 0 \ : \qquad \square$$

Նշանակենք՝ $h + L_n^A = \left\{ h + \mu \,|\, \mu \in L_n^A \right\}$, որտեղ $h \in P^n$:

Թեորեմ 17.13: *Եթե* h_1*-ը* $A \cdot X = B$ *մատրիցային հավասարման որևէ լուծում է, այսինքն՝* $A \cdot h_1 = B$*, ապա*

$$S_n^A = h_1 + L_n^A \ :$$

Ապացույց: $h_1 + L_n^A \subseteq S_n^A$ ներդրումն ակնհայտ է, որովհետև

$$A\,(h_1 + \mu) = Ah_1 + A\mu = B + 0 = B\,,$$

որտեղ $\mu \in L_n^A$: Եվ հակառակը, եթե $h_2 \in S_n^A$, ապա, ըստ նախորդ լեմմի, $h_2 - h_1 = \mu \in L_n^A$ և $h_2 = h_1 + \mu$, այսինքն՝ $S_n^A \subseteq h_1 + L_n^A$: $\square$

***Հետևություն 17.15*:** *Եթե* h_1*-ը* $A \cdot X = B$ *մատրիցային հավասարման որևէ լուծում է, իսկ* $c_1, \ldots, c_k \in L_n^A$ *համակարգը հենք է* L_n^A *գծային տարածության համար, ապա ցանկացած* $h \in S_n^A$ *լուծման համար գոյություն ունեն այնպիսի* $\alpha_1, \ldots, \alpha_k \in P$ *սկալյարներ, որ*

$$h = h_1 + \alpha_1 c_1 + \cdots + \alpha_k c_k \ : \qquad \square$$

Այս $h_1 + \alpha_1 c_1 + \cdots + \alpha_k c_k$ տեսքի լուծումը կոչվում է $A \cdot X = B$ մատրիցային հավասարման **ընդհանուր լուծում**, որտեղ h_1-ը $A \cdot X = B$ հավասարման որևէ լուծում է, $\alpha_1, \ldots, \alpha_k \in P$, իսկ $c_1, \ldots, c_k$ համակարգը $A \cdot X = 0$ համասեռ հավասարման որևէ հենքային կամ ֆունդամենտալ լուծումների համակարգ է:

Սակայն, գործնականում գծային հավասարումների (17.5) համակարգի լուծման ընթացքը շարադրվում է ոչ թե մատրիցային, այլ սովորական տեսքով:

Որոշենք (հաշվենք) L_n^A վերջավոր չափանի գծային տարածության չափողականությունը:

Թեորեմ 17.14: *$dim(L_n^A) = n - r$, որտեղ r-ը A մատրիցի ռանգն է, իսկ n-ը համակարգի անհայտների թիվը:*

Ապացույցում: $r = 0$ դեպքում պնդումն ակնհայտ է: Դիցուք $r > 0$: Գծային հավասարումների (17.5) համակարգին համապատասխանող համասեռ համակարգը (կամ, որ նույնն է, $A \cdot X = 0$ համասեռ մատրիցային հավասարումը) կարելի է գրել նաև հետևյալ մատրիցային տեսքով՝

$$x_1 A_1' + x_2 A_2' + \cdots + x_n A_n' = 0\,, \tag{17.11}$$

որտեղ $A_1', A_2', \ldots, A_n'$-ը A մատրիցի սյունակներն են: $(\alpha_1, \alpha_2, \ldots, \alpha_n) \in P_n$ n-յակը կոչվում է (17.11) հավասարման լուծում, եթե

$$\alpha_1 A_1' + \alpha_2 A_2' + \cdots + \alpha_n A_n' = 0 \ :$$

Ակնհայտ է, որ $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in P_n$ n-յակը կլինի (17.11) հավասարման լուծում այն և միայն այն դեպքում, երբ $\alpha^T = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \in P^n$ սյունակը $A \cdot X = 0$ հավասարման լուծում է (այսինքն՝ $A \cdot \alpha^T = 0$):

Դիցուք $A_1', A_2', \ldots, A_r'$ հաջորդականությունը A մատրիցի սյունակների համակարգի հենքն է: Հետևաբար, $A_{r+1}', \ldots, A_n'$ սյունակները գծայնորեն կարտահայտվեն $A_1', A_2', \ldots, A_r'$ սյունակների միջոցով՝

$$\begin{aligned} A_{r+1}' &= \beta_{r+1,1} A_1' + \cdots + \beta_{r+1,r} A_r'\,, \\ &\ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ A_n' &= \beta_{n,1} A_1' + \cdots + \beta_{n,r} A_r'\,, \end{aligned}$$

այսինքն՝

$$\begin{aligned} &\beta_{r+1,1} A_1' + \cdots + \beta_{r+1,r} A_r' + (-1) A_{r+1}' + 0 A_{r+2}' + \cdots + 0 A_n' = 0\,, \\ &\quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ &\beta_{n,1} A_1' + \cdots + \beta_{n,r} A_r' + 0 A_{r+1}' + 0 A_{r+2}' + \cdots + (-1) A_n' = 0 \ : \end{aligned}$$

Այստեղից բխում է, որ

$$t_{r+1} = \begin{pmatrix} \beta_{r+1,1} \\ \vdots \\ \beta_{r+1,r} \\ -1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \ldots, \ t_n = \begin{pmatrix} \beta_{n,1} \\ \vdots \\ \beta_{n,r} \\ 0 \\ \vdots \\ 0 \\ -1 \end{pmatrix}$$

սյունակները հանդիսանում են $A \cdot X = 0$ հավասարման լուծումներ: Անմիջականորեն ստուգվում է, որ $t_{r+1}, \ldots, t_n$ սյունակների համակարգը գծայնորեն անկախ է: Մնում է ապացուցել, որ $A \cdot X = 0$ հավասարման յուրաքանչյուր $s \in P^n$ լուծում գծայնորեն արտահայտվում է $t_{r+1}, \ldots, t_n$ լուծումների միջոցով: Դիցուք $s = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix}$ և $y = s + \lambda_{r+1} t_{r+1} + \cdots + \lambda_n t_n$, որը նույնպես կլինի լուծում $A \cdot X = 0$ համասեռ հավասարման համար: Ըստ որում, y լուծումը կունենա հետևյալ տեսքը՝

$$y = \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_r \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

որտեղ

$$\begin{gathered} \mu_1 = \lambda_1 + \lambda_{r+1}\beta_{r+1,1} + \cdots + \lambda_n \beta_{n,1}\,, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \mu_r = \lambda_r + \lambda_{r+1}\beta_{r+1,r} + \cdots + \lambda_n \beta_{n,r} \ : \end{gathered}$$

Սակայն, քանի որ y-ը լուծում է $A \cdot X = 0$ հավասարման համար, ապա կունենանք՝

$$\mu_1 A'_1 + \mu_2 A'_2 + \cdots + \mu_r A'_r + 0A'_{r+1} + \cdots + 0A'_n = 0\,,$$

որտեղից $\mu_1 = \mu_2 = \cdots = \mu_r = 0$, որովհետև $A'_1, A'_2, \ldots, A'_r$ համակարգը գծայնորեն անկախ է: Այսպիսով, $y = 0$ և

$$s = (-\lambda_{r+1})\, t_{r+1} + \cdots + (-\lambda_n)\, t_n \ : \qquad \square$$

Վերջում նշենք գծային հավասարումների համակարգի ընդհանուր լուծումը գտնելու հետևյալ ալգորիթմը:

Նախ Կրոնեկեր-Կապելլի թեորեմի օգնությամբ որոշում ենք տրված գծային հավասարումների (17.5) համակարգի լուծելիությունը (համատեղելիությունը): Դիցուք գծային հավասարումների (17.5) համակարգը լուծելի է և դիցուք նրա հիմնական A և ընդլայնված A' մատրիցների ռանգերը հավասար են k-ի: Առանց ընդհանրությունը խախտելու կարելի է ենթադրել, որ համապատասխան հենքային ենթամատրիցը զբաղեցնում է A (և A') մատրիցների վերին ձախ անկյունը: Քանի որ թեորեմ 17.8-ի համաձայն, A' ընդլայնված մատրիցի վերջին $m-k$ տողերից յուրաքանչյուրը գծայնորեն արտահայտվում է նրա առաջին k տողերի միջոցով, ապա գծային հավասարումների (17.5) համակարգի վերջին $m-k$ հավասարումներից յուրաքանչյուրը գծայնորեն կարտահայտվի այդ համակարգի առաջին k հավասարումների միջոցով: Հետևաբար, գծային հավասարումների (17.5) համակարգի լուծումների բազմությունը կհամընկնի հետևյալ համակարգերից յուրաքանչյուրի լուծումների բազմության հետ`

$$\left\{\begin{array}{l|l} a_{11}x_1+\cdots+a_{1k}x_k & +\,a_{1,k+1}x_{k+1}+\cdots+a_{1n}x_n=b_1\,, \\ \cdots\quad\cdots\qquad\cdots\quad\cdots & \cdots\quad\cdots\quad\cdots\quad\cdots \\ a_{k1}x_1+\cdots+a_{kk}x_k & +\,a_{k,k+1}x_{k+1}+\cdots+a_{kn}x_n=b_k\,, \end{array}\right.$$

կամ

$$\begin{cases} a_{11}x_1+\cdots+a_{1k}x_k=b_1-a_{1,k+1}x_{k+1}-\cdots-a_{1n}x_n\,, \\ \cdots\quad\cdots\qquad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots\quad\cdots \\ a_{k1}x_1+\cdots+a_{kk}x_k=b_k-a_{k,k+1}x_{k+1}-\cdots-a_{kn}x_n\ : \end{cases}$$

Այստեղ $x_{k+1},\ldots,x_n$ անհայտներն անվանելով **ազատ անհայտներ** և դրանց տալով կամայական արժեքներ դիտարկվող P դաշտից, լուծում ենք ստացված համակարգը` ըստ $x_1,\ldots,x_k$ անհայտների, որոնք կոչվում են **գլխավոր անհայտներ** (օրինակ, Կրամերի եղանակով, որովհետև համաձայն հենքային ենթամատրիցի սահմանման` $det\begin{pmatrix} a_{11},\ldots,a_{1k} \\ \cdots\ \cdots\ \cdots \\ a_{k1},\ldots,a_{kk}\end{pmatrix} \neq 0$): Միաժամանակ, (17.5) համակարգին համապատասխանող համասեռ համակարգի լուծումը հանգում է հետևյալ համակարգի լուծմանը՝

$$\begin{cases} a_{11}x_1 + \cdots + a_{1k}x_k = -a_{1,k+1}x_{k+1} - \cdots - a_{1n}x_n\,, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ a_{k1}x_1 + \cdots + a_{kk}x_k = -a_{k,k+1}x_{k+1} - \cdots - a_{kn}x_n \ : \end{cases}$$

Ըստ որում,

$$\begin{array}{cccc} x_{k+1} = 1, & x_{k+2} = 0, & \ldots\,, & x_n = 0\,, \\ x_{k+1} = 0, & x_{k+2} = 1, & \ldots\,, & x_n = 0\,, \\ \ldots & \ldots & \ldots & \ldots \\ x_{k+1} = 0, & \ldots, & x_{n-1} = 0, & x_n = 1 \end{array}$$

արժեքներին համապատասխան ստացվող $n-k$ հատ լուծումները կկազմեն համասեռ համակարգի հենքային (ֆունդամենտալ) լուծումների համակարգ: Այնուհետև, ընտրելով (17.5) համակարգի որևէ լուծում, գտնում ենք նաև նրա ընդհանուր լուծումը (հետևություն 17.15):

Որպես օրինակ որոշենք գծային հավասարումների հետևյալ համակարգի ընդհանուր լուծումը՝

$$\begin{cases} 2x_1 + x_2 - x_3 - x_4 + x_5 = 1\,, \\ x_1 - x_2 + x_3 + x_4 - 2x_5 = 0\,, \\ 3x_1 + 3x_2 - 3x_3 - 3x_4 + 4x_5 = 2\,, \\ 4x_1 + 5x_2 - 5x_3 - 5x_4 + 7x_5 = 3 \ : \end{cases} \tag{17.12}$$

Համակարգի ընդլայնված մատրիցը տողերի տարրական ձևափոխությունների օգնությամբ բերենք աստիճանաձև տեսքի.

$$\left(\begin{array}{rrrrr|r} 2 & 1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -2 & 0 \\ 3 & 3 & -3 & -3 & 4 & 2 \\ 4 & 5 & -5 & -5 & 7 & 3 \end{array}\right) \sim \left(\begin{array}{rrrrr|r} 1 & -1 & 1 & 1 & -2 & 0 \\ 2 & 1 & -1 & -1 & 1 & 1 \\ 3 & 3 & -3 & -3 & 4 & 2 \\ 4 & 5 & -5 & -5 & 7 & 3 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{rrrrr|r} 1 & -1 & 1 & 1 & -2 & 0 \\ 0 & 3 & -3 & -3 & 5 & 1 \\ 0 & 6 & -6 & -6 & 10 & 2 \\ 0 & 9 & -9 & -9 & 15 & 3 \end{array}\right) \sim \left(\begin{array}{rrrrr|r} 1 & -1 & 1 & 1 & -2 & 0 \\ 0 & 1 & -1 & -1 & 5/3 & 1/3 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{array}\right) :$$

Այսպիսով, համակարգի հիմնական և ընդլայնված մատրիցների ռանգերը հավասար են 2-ի: Այստեղ, x_1, x_2 անհայտները կլինեն գլխավոր անհայտները, իսկ մնացած x_3, x_4, x_5 անհայտները՝ ազատ անհայտները: Արդյունքում, հանգում ենք հետևյալ համակարգի լուծմանը՝

$$\begin{cases} x_1 - x_2 + x_3 + x_4 - 2x_5 = 0\,, \\ \qquad x_2 - x_3 - x_4 + \dfrac{5}{3}x_5 = \dfrac{1}{3}\,, \end{cases} \tag{17.13}$$

որտեղից՝

$$x_2 = \frac{1}{3} + x_3 + x_4 - \frac{5}{3}x_5\,,$$

$$x_1 = x_2 - x_3 - x_4 + 2x_5 = \frac{1}{3} + x_3 + x_4 - \frac{5}{3}x_5 - x_3 - x_4 + 2x_5 = \frac{1}{3} + \frac{x_5}{3}\,,$$

այսինքն՝ (17.12) համակարգի բոլոր լուծումների բազմությունն է՝

$$\left\{ \left(\frac{1}{3} + \frac{x_5}{3}\,, \frac{1}{3} + x_3 + x_4 - \frac{5}{3}x_5\,, x_3,\, x_4\,, x_5 \right) \middle|\ x_3, x_4, x_5 \in \mathbb{R} \right\} :$$

Հասկանալի է, որ (17.12) համակարգին համապատասխանող

$$\begin{cases} 2x_1 + x_2 - x_3 - x_4 + x_5 = 0\,, \\ x_1 - x_2 + x_3 + x_4 - 2x_5 = 0\,, \\ 3x_1 + 3x_2 - 3x_3 - 3x_4 + 4x_5 = 0\,, \\ 4x_1 + 5x_2 - 5x_3 - 5x_4 + 7x_5 = 0 \end{cases} \tag{17.14}$$

համասեռ համակարգի լուծումների բազմությունն է՝

$$\left\{ \left(\frac{x_5}{3}\,, x_3 + x_4 - \frac{5}{3}x_5\,, x_3,\, x_4\,, x_5 \right) \middle|\ x_3, x_4, x_5 \in \mathbb{R} \right\} :$$

Եթե $x_3 = x_4 = x_5 = 0$, ապա ստանում ենք (17.12) համակարգի $h_1 = \left(\frac{1}{3}, \frac{1}{3}, 0, 0, 0\right)$ լուծումը, իսկ ազատ անհայտների հետևյալ արժեքների դեպքում՝

$$\begin{aligned} x_3 &= 1, \quad x_4 = 0, \quad x_5 = 0\,, \\ x_3 &= 0, \quad x_4 = 1, \quad x_5 = 0\,, \\ x_3 &= 0, \quad x_4 = 0, \quad x_5 = 1\,, \end{aligned}$$

ստանում ենք (17.14) համասեռ համակարգի հենքային (ֆունդամենտալ) լուծումների հետևյալ համակարգը՝

$$c_1 = (0,\, 1,\, 1,\, 0,\, 0)\,,$$

$$c_2 = (0,\, 1,\, 0,\, 1,\, 0)\,,$$

$$c_3 = \left(\frac{1}{3},\, -\frac{5}{3},\, 0,\, 0,\, 1\right)\,:$$

Հետևաբար, (17.12) համակարգի h ընդհանուր լուծումը կունենա հետևյալ տեսքը (հետևություն 17.15)՝

$$h = h_1 + \alpha_1 c_1 + \alpha_2 c_2 + \alpha_3 c_3 =$$

$$= \left(\frac{1}{3},\, \frac{1}{3},\, 0,\, 0,\, 0\right) + \alpha_1 (0,\, 1,\, 1,\, 0,\, 0) + \alpha_2 (0,\, 1,\, 0,\, 1,\, 0) + \alpha_3 \left(\frac{1}{3},\, -\frac{5}{3},\, 0,\, 0,\, 1\right)\,,$$

որտեղ $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{R}$:

17.9. Վեկտորի կոորդինատներ և կոորդինատների ձևափոխությունը հենքի փոփոխության դեպքում

Դիցուք Q-ն կամայական գծային տարածություն է որոշված P դաշտի վրա, իսկ $e_1, e_2, \ldots, e_n$-ը հենք (կոորդինատային համակարգ) է Q-ի համար, որը համառոտ կնշանակենք (e_i)-ով: Ըստ հենքի սահմանման, Q-ի ցանկացած x տարր (վեկտոր) գծայնորեն արտահայտվում է (e_i)-ի միջոցով, այսինքն՝ գոյություն ունեն այնպիսի $\alpha_1, \alpha_2, \ldots, \alpha_n \in P$ սկալյարներ, որ

$$x = \alpha_1 e_1 + \alpha_2 e_2 + \cdots + \alpha_n e_n\ :$$

Այստեղ $\alpha_1, \alpha_2, \ldots, \alpha_n$ սկալյարները որոշվում են միարժեքորեն (լեմմ 17.8) և կոչվում են x **վեկտորի կոորդինատներ** և նշանակվում է $(x)_{(e_i)} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$: x-ի վերլուծությունը համառոտ կարելի է ներկայացնել նաև հետևյալ կերպ՝

$$x = \sum_{i=1}^{n} \alpha_i e_i = (\alpha_1, \ldots, \alpha_n) \bullet \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}\,,$$

որտեղ $\bullet$ բազմապատկումը կատարվում է մատրիցների բազմապատկման եղանակով (օրենքով): Նույն իմաստն ունի նաև $U \bullet e$ կամ $U \bullet a$ արտադրյալը, որտեղ U-ն $m \times n$-չափանի կամայական մատրից է՝ որոշված սկալյարների P դաշտի վրա, իսկ

$$e = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}, \quad a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, \qquad a_1, \ldots, a_n \in Q \ :$$

Լեմմ 17.12: *Եթե U, V մատրիցները $m \times n$-չափանի մատրիցներ են որոշված սկալյարների P դաշտի վրա և $U \bullet e = V \bullet e$, ապա $U = V$:*

Ապացուցում: Համաձայն տրված պայմանի՝

$$u_{i1}e_1 + u_{i2}e_2 + \cdots + u_{in}e_n = v_{i1}e_1 + v_{i2}e_2 + \cdots + v_{in}e_n \, ,$$

$$(u_{i1} - v_{i1})\, e_1 + (u_{i2} - v_{i2})\, e_2 + \cdots + (u_{in} - v_{in})\, e_n = 0 \ :$$

Հետևաբար, $u_{i1} - v_{i1} = 0$, $u_{i2} - v_{i2} = 0$, ..., $u_{in} - v_{in} = 0$ և $u_{i1} = v_{i1}$, $u_{i2} = v_{i2}$, ..., $u_{in} = v_{in}$: □

Լեմմ 17.13: *Q գծային տարածության վեկտորների ցանկացած $a = (a_1, \ldots, a_k)^T$ սյունակի և սկալյարների P դաշտի վրա որոշված կամայական $m \times n$-չափանի $A = (\alpha_{ij})$ ու $n \times k$-չափանի $B = (\beta_{ij})$ մատրիցների համար՝ $A \bullet (B \bullet a) = (A \cdot B) \bullet a$:* □

Դիցուք Q գծային տարածության մեջ $e_1, e_2, \ldots, e_n$ հենքի հետ մեկտեղ ընտրված է նաև մեկ ուրիշ հենք ևս՝ $e'_1, e'_2, \ldots, e'_n$, որը համառոտ կնշանակենք (e'_i)-ով, և դիցուք

$$\begin{aligned} e'_1 &= t_{11}e_1 + \cdots + t_{1n}e_n \, , \\ &\ldots \quad \ldots \quad \ldots \quad \ldots \\ e'_n &= t_{n1}e_1 + \cdots + t_{nn}e_n \, , \end{aligned} \tag{17.15}$$

իսկ

$$\begin{aligned} e_1 &= t'_{11}e'_1 + \cdots + t'_{1n}e'_n \, , \\ &\ldots \quad \ldots \quad \ldots \quad \ldots \\ e_n &= t'_{n1}e'_1 + \cdots + t'_{nn}e'_n \, , \end{aligned} \tag{17.16}$$

որտեղ $\Gamma = (t_{ij})$ և $\Gamma' = (t'_{ij})$ մատրիցները, համապատասխանաբար, կոչվում են (e_i) հենքից (e'_i) հենքին **անցման մատրից** և (e'_i) հենքից (e_i) հենքին անցման մատրից: Օգտվելով վերոհիշյալ $\bullet$ բազմապատկումից, հավասարությունների (17.15) և (17.16) համակարգերը կարելի է գրել մատրիցային տեսքով՝

$$e' = \Gamma \bullet e \quad \text{և} \quad e = \Gamma' \bullet e'\,,$$

որտեղ $e' = \begin{pmatrix} e'_1 \\ \vdots \\ e'_n \end{pmatrix} = (e'_1, \ldots, e'_n)^T$: Հետևաբար, լեմմ 17.13-ի համաձայն,

$$E \bullet e' = e' = \Gamma \bullet (\Gamma' \bullet e') = (\Gamma \cdot \Gamma') \bullet e'\,,$$

$$E \bullet e = e = \Gamma' \bullet (\Gamma \bullet e) = (\Gamma' \cdot \Gamma) \bullet e\,,$$

որտեղից, լեմմ 17.12-ի համաձայն, $E = \Gamma \cdot \Gamma'$, $E = \Gamma' \cdot \Gamma$, այսինքն՝ n-րդ կարգի Γ և Γ' անցման մատրիցները հակադարձելի են ու $\Gamma' = \Gamma^{-1}$: Այսպիսով,

$$e' = \Gamma \bullet e \longrightarrow e = \Gamma^{-1} \bullet e'\ :$$

Այժմ պարզենք, թե ինչպես են փոփոխվում x վեկտորի կոորդինատները (e_i) հենքից (e'_i) հենքին անցման դեպքում.

$$x = \alpha_1 e_1 + \cdots + \alpha_n e_n = (\alpha_1, \ldots, \alpha_n) \bullet \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} =$$

$$(\alpha_1, \ldots, \alpha_n) \bullet e = (\alpha_1, \ldots, \alpha_n) \bullet (\Gamma' \bullet e') = ((\alpha_1, \ldots, \alpha_n) \cdot \Gamma') \bullet e'\,,$$

$$x = \alpha'_1 e'_1 + \cdots + \alpha'_n e'_n = (\alpha'_1, \ldots, \alpha'_n) \bullet \begin{pmatrix} e'_1 \\ \vdots \\ e'_n \end{pmatrix} = (\alpha'_1, \ldots, \alpha'_n) \bullet e'\,,$$

որտեղից

$$((\alpha_1, \ldots, \alpha_n) \bullet \Gamma') \bullet e' = (\alpha'_1, \ldots, \alpha'_n) \bullet e'$$

և, համաձայն լեմմ 17.12-ի, կունենանք՝

$$(\alpha_1, \ldots, \alpha_n) \bullet \Gamma' = (\alpha'_1, \ldots, \alpha'_n)$$

կամ

$$(\alpha_1, \ldots, \alpha_n) = (\alpha'_1, \ldots, \alpha'_n) \bullet (\Gamma')^{-1} = (\alpha'_1, \ldots, \alpha'_n) \bullet \Gamma\,,$$

այսինքն՝
$$\begin{aligned} &\alpha_1 = t_{11}\alpha'_1 + t_{21}\alpha'_2 + \cdots + t_{n1}\alpha'_n\,, \\ &\ldots \quad \ldots \quad \ldots \quad \ldots \\ &\alpha_n = t_{1n}\alpha'_1 + t_{2n}\alpha'_2 + \cdots + t_{nn}\alpha'_n \ : \end{aligned}$$
Այս պատճառով
$$\Gamma^T = \begin{pmatrix} t_{11},\ t_{21},\ \cdots,\ t_{n1} \\ \ldots \quad \ldots \quad \ldots \\ t_{1n},\ t_{2n},\ \cdots,\ t_{nn} \end{pmatrix}$$
մատրիցը կոչվում է **կոորդինատների ձևափոխության մատրից**, որը (e_i) հենքից (e'_i) հենքին անցման մատրիցի շրջվածն է: Նոր (e'_i) կոորդինատային համակարգում x-ի ունեցած կոորդինատները հին կոորդինատներով կարտահայտվեն $\left(\Gamma^T\right)^{-1} = \left(\Gamma^{-1}\right)^T$ մատրիցի օգնությամբ:

Կարևոր է նաև, որ
$$\left((\Gamma_1 \cdot \Gamma_2)^T\right)^{-1} = \left(\Gamma_2^T \cdot \Gamma_1^T\right)^{-1} = \left(\Gamma_1^T\right)^{-1} \cdot \left(\Gamma_2^T\right)^{-1} \ :$$

Թեորեմ 17.15: *Դիցուք Q-ն վերջավոր չափանի գծային տարածություն է՝ $e_1, e_2, \ldots, e_n$ հենքով: Որպեսզի Q-ի տարրերի $a_1, a_2, \ldots, a_k$ հաջորդականությունը լինի գծայնորեն անկախ անհրաժեշտ է և բավարար, որ նրանց կոորդինատներից կազմված $k \times n$-չափանի*
$$A = \begin{pmatrix} (a_1)_{(e_i)} \\ (a_2)_{(e_i)} \\ \vdots \\ (a_k)_{(e_i)} \end{pmatrix}$$
մատրիցի ռանգը լինի հավասար k-ի:

Ապացուցում: Դիցուք
$$\begin{aligned} &(a_1)_{(e_i)} = (\alpha_{11}, \ldots, \alpha_{1n})\ , \\ &(a_2)_{(e_i)} = (\alpha_{21}, \ldots, \alpha_{2n})\ , \\ &\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ &(a_k)_{(e_i)} = (\alpha_{k1}, \ldots, \alpha_{kn})\ , \end{aligned}$$
այսինքն՝ $a_t = \alpha_{t1}e_1 + \cdots + \alpha_{tn}e_n$, որտեղ $t = 1, 2, \ldots, k$: Հետևաբար,

$$\alpha_1 a_1 + \cdots + \alpha_k a_k = 0 \longleftrightarrow$$
$$\alpha_1 (\alpha_{11} e_1 + \cdots + \alpha_{1n} e_n) + \cdots + \alpha_k (\alpha_{k1} e_1 + \cdots + \alpha_{kn} e_n) = 0 \longleftrightarrow$$
$$(\alpha_1 \alpha_{11} + \cdots + \alpha_k \alpha_{k1}) e_1 + \cdots + (\alpha_1 \alpha_{1n} + \cdots + \alpha_k \alpha_{kn}) e_n = 0 \longleftrightarrow$$
$$\alpha_1 \alpha_{11} + \cdots + \alpha_k \alpha_{k1} = 0, \ldots, \alpha_1 \alpha_{1n} + \cdots + \alpha_k \alpha_{kn} = 0 \longleftrightarrow$$
$$\alpha_1 (\alpha_{11}, \ldots, \alpha_{1n}) + \cdots + \alpha_k (\alpha_{k1}, \ldots, \alpha_{kn}) = 0 :$$ □

Հետևություն 17.16: *Դիցուք Q-ն վերջավոր չափանի գծային տարածություն է $e_1, e_2, \ldots, e_n$ հենքով և n-րդ կարգի $A = (a_{ij}) \in P^{n\times n}$ մատրիցն ունի ոչ զրոյական որոշիչ: Եթե*

$$\begin{aligned} e'_1 &= a_{11}e_1 + \cdots + a_{1n}e_n, \\ e'_2 &= a_{21}e_1 + \cdots + a_{2n}e_n, \\ \cdots & \quad \cdots \quad \cdots \quad \cdots \\ e'_n &= a_{n1}e_1 + \cdots + a_{nn}e_n, \end{aligned}$$

ապա Q-ի տարրերի $e'_1, e'_2, \ldots, e'_n$ համակարգը գծայնորեն անկախ է, այսինքն՝ հենք է Q-ի համար: □

17.10. Ենթատարածությունների հատում, գումար և ուղիղ գումար

Դիցուք Q-ն կամայական գծային տարածություն է որոշված P դաշտի վրա, իսկ $Q_1, Q_2 \leqslant Q$: Q_1 և Q_2 ենթաբազմությունների հատումը կոչվում է այդ **ենթատարածությունների հատում**: Նույն եղանակով սահմանվում է նաև ցանկացած թվով ենթատարածությունների հատումը:

Լեմմ 17.14: *1) Եթե $Q_1 \leqslant Q$ և $Q_2 \leqslant Q$, ապա $Q_1 \cap Q_2 \leqslant Q$, այսինքն՝ միևնույն Q գծային տարածության երկու ենթատարածությունների հատումը նորից Q-ի ենթատարածություն է;*

2) Եթե $Q_1 \leqslant Q, \ldots, Q_k \leqslant Q$, ապա $Q_1 \cap \cdots \cap Q_k \leqslant Q$, այսինքն՝ միևնույն Q գծային տարածության վերջավոր թվով ենթատարածությունների հատումը նորից Q-ի ենթատարածություն է;

3) Միևնույն Q գծային տարածության ցանկացած թվով ենթատարածությունների հատումը նորից Q-ի ենթատարածություն է:

Ապացուցում: 1) Ակնհայտ է, որ $Q_1 \cap Q_2 \neq \emptyset$, որովհետև $0 \in Q_1$, $0 \in Q_2$ և, հետևաբար, $0 \in Q_1 \cap Q_2$: Այնուհետև, եթե $x, y \in Q_1 \cap Q_2$ և $\alpha, \beta \in P$, ապա $x, y \in Q_1$, $x, y \in Q_2$ և $\alpha x + \beta y \in Q_1$, $\alpha x + \beta y \in Q_2$, այսինքն՝ $\alpha x + \beta y \in Q_1 \cap Q_2$:

2)-ը և 3)-ը ապացուցվում են նույն եղանակով: □

Հետևություն 17.17: *$Q_1 \cap Q_2 \leqslant Q_1$, $Q_1 \cap Q_2 \leqslant Q_2$ և $Q_1 \cap Q_2$-ը Q-ի այն «ամենամեծ» ենթատարածությունն է, որը միաժամանակ ընկած է Q_1-ի և Q_2-ի մեջ (այսինքն՝ եթե $Q' \leqslant Q$ ենթատարածության համար՝ $Q' \subseteq Q_1$ և $Q' \subseteq Q_2$, ապա $Q' \subseteq Q_1 \cap Q_2$):* □

Q գծային տարածության $Q_1, Q_2 \leqslant Q$ **ենթատարածությունների գումարը** նշանակվում է $Q_1 + Q_2$-ով և սահմանվում է հետևյալ կերպ՝

$$Q_1 + Q_2 = \{u + v \mid u \in Q_1, v \in Q_2\} \ :$$

Ակնհայտ է, որ $Q_1 \subseteq Q_1 + Q_2$, $Q_2 \subseteq Q_1 + Q_2$, $Q_1 + Q_1 = Q_1$ և $Q_1 + Q_2 = Q_2 \longleftrightarrow Q_1 \subseteq Q_2$:

Լեմմ 17.15: *1) Եթե $Q_1 \leqslant Q$ և $Q_2 \leqslant Q$, ապա $Q_1 + Q_2 \leqslant Q$, այսինքն՝ միևնույն Q գծային տարածության երկու ենթատարածությունների գումարը նորից Q-ի ենթատարածություն է;*

2) $Q_1 + Q_2 = Q_2 + Q_1$ և $(Q_1 + Q_2) + Q_3 = Q_1 + (Q_2 + Q_3)$, այսինքն՝ ենթատարածությունների գումարը տեղափոխական է և զուգորդական: □

Հետևաբար, Q գծային տարածության վերջավոր թվով $Q_1, \ldots, Q_k \leqslant Q$ ենթատարածությունների գումարը կախված չէ փակագծերի դասավորությունից (թեորեմ 1.3) և այդ պատճառով կարելի է գրել առանց փակագծերի՝ $Q_1 + \cdots + Q_k$: Այսպիսով, վերջավոր թվով ենթատարածությունների գումարը սահմանվում է հետևյալ կերպ՝

$$Q_1 + \cdots + Q_k = \{u_1 + \cdots + u_k \mid u_1 \in Q_1, \ldots, u_k \in Q_k\},$$

որը կլինի $Q_1, \ldots, Q_k$ ենթատարածությունները պարունակող Q-ի ենթատարածություն և այդ $Q_1 + \cdots + Q_k$ ենթատարածությունը Q-ի այն «ամենափոքր» ենթատարածությունն է, որը միաժամանակ պարունակում է $Q_1, \ldots, Q_k$ ենթատարածությունները (այսինքն՝ եթե $Q' \leqslant Q$ և $Q_1 \subseteq Q'$, ..., $Q_k \subseteq Q'$, ապա $Q_1 + \cdots + Q_k \subseteq Q'$):

Q գծային տարածության վերջավոր թվով ենթատարածությունների $Q_1 + \cdots + Q_k$ գումարը կոչվում է **ուղիղ գումար** և նշանակվում է $Q_1 \oplus \cdots \oplus Q_k$, եթե նրա յուրաքանչյուր $z \in Q_1 + \cdots + Q_k$ տարր միարժեքորեն է ներկայացվում $u_1 + \cdots + u_k$ տեսքով, որտեղ $u_1 \in Q_1, \ldots, u_k \in Q_k$: Ակնհայտ է, որ եթե $Q_1 + \cdots + Q_k$ գումարն ուղիղ է, ապա $Q_1 + Q_2$, $Q_1 + Q_2 + Q_3, \ldots$ գումարները ևս կլինեն ուղիղ գումարներ:

Օրինակներ : 1) $\{0\} + Q = \{0\} \oplus Q$;

2) Հարթությունը դիտելով որպես իր վրա գտնվող վեկտորների գծային տարածություն, իսկ ուղիղը՝ որպես իր վրա գտնվող վեկտորների ենթատարածություն, կարող ենք պնդել, որ հարթությունը հանդիսանում է իր ցանկացած երկու հատվող (բայց ոչ համընկնող) ուղիղների ուղիղ գումար;

3) Եթե $Q \neq \{0\}$, ապա $Q + Q$ գումարը չի լինի ուղիղ գումար, որովհետև, եթե $a \neq 0$ և $a \in Q$, ապա $a + a = b$ և $0 + b = b$, որտեղ $b \in Q$:

Լեմմ 17.16: *Եթե* $Q = Q_1 \oplus \cdots \oplus Q_k$, *իսկ* $Q_i = Q_{i1} \oplus \cdots \oplus Q_{i\ell_i}$, *որտեղ* $i = 1, \ldots, k$, *ապա*

$$Q = Q_{11} \oplus \cdots \oplus Q_{1\ell_1} \oplus \cdots \oplus Q_{k1} \oplus \cdots \oplus Q_{k\ell_k} : \qquad \square$$

Հատկություն 17.8: *Որպեսզի երկու ենթատարածությունների* $Q_1 + Q_2$ *գումարը լինի ուղիղ գումար անհրաժեշտ է և բավարար, որ* $Q_1 \cap Q_2 = \{0\}$*:*

Ապացույց: Եթե $Q_1 + Q_2$ գումարն ուղիղ է և $z \in Q_1 \cap Q_2$, ապա $z + (-z) = 0$, որտեղ $z \in Q_1$, $-z \in Q_2$, և $0 + 0 = 0$: Հետևաբար, $z = 0$: Եվ հակառակը, եթե $Q_1 \cap Q_2 = \{0\}$ և $z = u_1 + u_2 = u_1' + u_2'$, որտեղ $u_1, u_1' \in Q_1$, $u_2, u_2' \in Q_2$, ապա $u_1 - u_1' = u_2' - u_2 \in Q_1 \cap Q_2 = \{0\}$: Հետևաբար, $u_1 - u_1' = 0$ և $u_2 - u_2' = 0$, այսինքն՝ $u_1 = u_1'$ և $u_2 = u_2'$: Ուստի՝ $Q_1 + Q_2 = Q_1 \oplus Q_2$: $\square$

Հատկություն 17.9: *Որպեսզի վերջավոր չափանի* Q *գծային տարածության ոչ զրոյական ենթատարածությունների* $Q_1 + Q_2$ *գումարը լինի ուղիղ գումար անհրաժեշտ է և բավարար, որ* Q_1, Q_2 *ենթատարածությունների հենքերի միավորումը լինի հենք* $Q_1 + Q_2 \leqslant Q$ *ենթատարածության համար:*

Ապացույց: Դիցուք $Q_1 + Q_2 = Q_1 \oplus Q_2$ և դիցուք $e_1, \ldots, e_k$ հաջորդականությունը հենք է Q_1-ի համար, իսկ $f_{k+1}, \ldots, f_n$ հաջորդականությունը հենք է Q_2-ի համար: Ակնհայտ է, որ յուրաքանչյուր $z \in Q_1 + Q_2$ տարր գծայնորեն կարտահայտվի

$e_1, \ldots, e_k, f_{k+1}, \ldots, f_n$ միավորված հաջորդականության միջոցով: Ապացուցենք, որ այդ հաջորդականությունը նաև գծայնորեն անկախ է.

$$\alpha_1 e_1 + \cdots + \alpha_k e_k + \beta_{k+1} f_{k+1} + \cdots + \beta_n f_n = 0,$$

$$\alpha_1 e_1 + \cdots + \alpha_k e_k = (-\beta_{k+1}) f_{k+1} + \cdots + (-\beta_n) f_n \in Q_1 \cap Q_2 :$$

Համաձայն նախորդ հայտանիշի՝ $Q_1 \cap Q_2 = \{0\}$: Հետևաբար, $\alpha_1 e_1 + \cdots + \alpha_k e_k = 0$ և $(-\beta_{k+1}) f_{k+1} + \cdots + (-\beta_n) f_n = 0$: Ուստի՝ $\alpha_1 = \cdots = \alpha_k = 0$, $-\beta_{k+1} = \cdots = -\beta_n = 0$ և $\beta_{k+1} = \cdots = \beta_n = 0$:

Բավարարությունն ակնհայտ է: □

Հետևություն 17.18: *Վերջավոր չափանի Q գծային տարածության երկու ենթատարածությունների $Q_1 \oplus Q_2$ ուղիղ գումարի չափողականությունը հավասար է գումարելի ենթատարածությունների չափողականությունների գումարին՝*

$$dim(Q_1 \oplus Q_2) = dim(Q_1) + dim(Q_2) :$$

Ապացուցում: Եթե $Q_1 = \{0\}$ կամ $Q_2 = \{0\}$, ապա պնդումն ակնհայտ է, իսկ եթե $Q_1 \neq \{0\}$ և $Q_2 \neq \{0\}$, ապա օգտվում ենք նախորդ հատկությունից: □

Հետևություն 17.19: *Վերջավոր չափանի Q գծային տարածության ցանկացած Q' ենթատարածություն օժտված է լրացումով, այսինքն՝ գոյություն ունի Q-ի այնպիսի Q'' ենթատարածություն, որ $Q' \oplus Q'' = Q$:*

Ապացուցում: Քանի որ Q-ն վերջավոր չափանի գծային տարածություն է, ապա Q'-ը ևս կլինի այդպիսին: Եթե $Q' = \{0\}, Q$, ապա $Q'' = Q, \{0\}$: Դիցուք $Q' \neq \{0\}, Q$ և $e_1, \ldots, e_k$ հաջորդականությունը հենք է Q'-ի համար, իսկ $e_1, \ldots, e_k, f_{k+1}, \ldots, f_n$ համակարգը հենք է Q-ի համար: Նշանակելով $Q'' = (f_{k+1}, \ldots, f_n)$ կունենանք՝ $Q = Q' \oplus Q''$: □

Հատկություն 17.10: *Որպեսզի վերջավոր չափանի Q գծային տարածության ոչ զրոյական ենթատարածությունների $Q_1 + \cdots + Q_k$ գումարը լինի ուղիղ գումար անհրաժեշտ է և բավարար, որ $Q_1, \ldots, Q_k$ ենթատարածությունների հենքերի միավորումը լինի հենք $Q_1 + \cdots + Q_k \leqslant Q$ ենթատարածության համար:*

Ապացուցում: Նախորդ հատկության ապացուցման կրկնությունն է: □

Հետևություն 17.20: *Վերջավոր չափանի գծային տարածության ենթատարածությունների $Q_1 \oplus \cdots \oplus Q_k$ ուղիղ գումարի չափողականությունը հավասար է գումարելի ենթատարածությունների չափողականությունների գումարին՝*

$$dim(Q_1 \oplus \cdots \oplus Q_k) = dim(Q_1) + \cdots + dim(Q_k) :$$

Ապացույց: Բավական է պնդումն ապացուցել ոչ զրոյական ենթատարածությունների համար: Իսկ այդ դեպքում պնդումը բխում է նախորդ հատկությունից: □

Դիցուք Q-ն կամայական վերջավոր չափանի ոչ զրոյական գծային տարածություն է, իսկ Q'-ը նրա կամայական ոչ զրոյական ենթատարածություն է: Ինչպես գիտենք, Q'-ը ևս կլինի վերջավոր չափանի և դիցուք $e_1, \ldots, e_k$ համակարգը հենք է Q'-ի համար: Ընդլայնենք (շարունակենք) այդ հենքը մինչև Q-ի հենքի՝

$$e_1, \ldots, e_k, f_{k+1}, \ldots, f_n :$$

Կասենք, որ Q-ի հենքը **համաձայնեցված է** Q' ենթատարածության հետ, եթե այդ հենքը հանդիսանում է Q'-ի որևէ հենքի շարունակությունը (ընդլայնումը):

Օրինակներ: 1) Q-ի ցանկացած ոչ զրոյական Q' ենթատարածության համար գոյություն ունի Q'-ի հետ համաձայնեցված Q-ի հենք:

2) Q գծային տարածության $e_1, \ldots, e_n$ հենքը համաձայնեցված է իր $Q_1 = (e_1)$, ..., $Q_n = (e_n)$ ենթատարածությունների հետ:

Լեմմ 17.17: *Վերջավոր չափանի Q գծային տարածության ցանկացած ոչ զրոյական $Q_1, Q_2 \leqslant Q$ ենթատարածությունների համար գոյություն ունի Q-ի այնպիսի հենք, որը համաձայնեցված է Q_1 և Q_2 ենթատարածությունների հետ:*

Ապացույց: Հնարավոր են հետևյալ երկու դեպքերը. ա) $Q_1 \cap Q_2 = \{0\}$, բ) $Q_1 \cap Q_2 \neq \{0\}$: Նախ պնդումն ապացուցենք առաջին դեպքում: Համաձայն թեորեմ 17.12-ի, Q_1 և Q_2 ենթատարածությունները ևս կլինեն վերջավոր չափանի: Դիցուք $e_1, \ldots, e_k$ համակարգը Q_1-ի հենքն է, իսկ $f_1, \ldots, f_s$ համակարգը Q_2-ի հենքն է: Այժմ բավական է նկատել, որ

$$e_1, \ldots, e_k, f_1, \ldots, f_s \tag{17.17}$$

միավորված համակարգը գծայնորեն անկախ է, որովհետև այդ դեպքում, ինչպես հայտնի է, դրան կարելի է շարունակել մինչև Q-ի հենքի:

Այժմ պնդումն ապացուցենք երկրորդ դեպքում: Ենթադրենք նաև $Q_1 \cap Q_2 \neq Q_1$ և $Q_1 \cap Q_2 \neq Q_2$: Դիցուք $a_1, \ldots, a_k$ համակարգը հենք է $Q_1 \cap Q_2$ ենթատարածության համար, $a_1, \ldots, a_k, b_{k+1}, \ldots, b_s$ համակարգը հենք է Q_1 ենթատարածության համար, իսկ $a_1, \ldots, a_k, c_{k+1}, \ldots, c_t$ համակարգը հենք է Q_2 ենթատարածության համար: Բավական է այժմ նկատել, որ

$$a_1, \ldots, a_k, b_{k+1}, \ldots, b_s, c_{k+1}, \ldots, c_t \tag{17.18}$$

համակարգը գծայնորեն անկախ է:

$Q_1 \cap Q_2 = Q_1$ կամ $Q_1 \cap Q_2 = Q_2$ դեպքում պնդումն ակնհայտ է: □

Թեորեմ 17.16: *Վերջավոր չափանի Q գծային տարածության ցանկացած Q_1 և Q_2 ենթատարածությունների համար՝*

$$dim(Q_1 + Q_2) = dim(Q_1) + dim(Q_2) - dim(Q_1 \cap Q_2) :$$

Ապացուցում: 1) Եթե $Q_1 \cap Q_2 = \{0\}$, ապա $Q_1 + Q_2 = Q_1 \oplus Q_2$ և

$$dim(Q_1 + Q_2) = dim(Q_1 \oplus Q_2) = dim(Q_1) + dim(Q_2) =$$

$$= dim(Q_1) + dim(Q_2) - 0 = dim(Q_1) + dim(Q_2) - dim(Q_1 \cap Q_2);$$

2) Ընդհանուր դեպքում՝ $Q_1 \cap Q_2 \neq \{0\}$: Այստեղ հնարավոր են հետևյալ ենթադեպքերը.

ա) $Q_1 \subseteq Q_2$: Հետևաբար, $Q_1 + Q_2 = Q_2$, $Q_1 \cap Q_2 = Q_1$ և

$$dim(Q_1 + Q_2) = dim(Q_2) = dim(Q_1) + dim(Q_2) - dim(Q_1) =$$

$$= dim(Q_1) + dim(Q_2) - dim(Q_1 \cap Q_2);$$

բ) $Q_2 \subseteq Q_1$: Հանգում է նախորդ դեպքի քննարկմանը:

գ) $Q_1 \not\subseteq Q_2$ և $Q_2 \not\subseteq Q_1$, այսինքն՝ հատում կա, սակայն դրանցից որևէ մեկը չի ընկած մյուսի մեջ: Դիցուք

$$dim(Q_1 \cap Q_2) = k > 0, \quad dim(Q_1) = n > 0, \quad dim(Q_2) = m > 0,$$

որտեղ $k < n$ և $k < m$: Դիցուք $e_1, \ldots, e_k$ հաջորդականությունը հենք է $Q_1 \cap Q_2$ ենթատարածության համար, $e_1, \ldots, e_k, f_{k+1}, \ldots, f_n$

հաջորդականությունը հենք է Q_1 ենթատարածություն համար, իսկ $e_1, \ldots, e_k, g_{k+1}, \ldots, g_m$ հաջորդականությունը հենք է Q_2 ենթատարածության համար: Թեորեմի ապացուցումը կլինի ավարտված, եթե ապացուցենք, որ

$$e_1, \ldots, e_k, f_{k+1}, \ldots, f_n, g_{k+1}, \ldots, g_m \tag{17.19}$$

հաջորդականությունը հենք է $Q_1 + Q_2$ ենթատարածության համար: Ակնհայտ է, որ յուրաքանչյուր $z \in Q_1 + Q_2$ տարր գծայնորեն արտահայտվում է (17.19) հաջորդականության միջոցով: Մնում է ապացուցել, որ (17.19) հաջորդականությունը գծայնորեն անկախ է.

$$\alpha_1 e_1 + \cdots + \alpha_k e_k + \beta_{k+1} f_{k+1} + \cdots + \beta_n f_n + \gamma_{k+1} g_{k+1} + \cdots + \gamma_m g_m = 0,$$

$$\alpha_1 e_1 + \cdots + \alpha_k e_k + \beta_{k+1} f_{k+1} + \cdots + \beta_n f_n = (-\gamma_{k+1}) g_{k+1} + \cdots + (-\gamma_m) g_m \in Q_1 \cap Q_2 :$$

Ուստի՝

$$(-\gamma_{k+1}) g_{k+1} + \cdots + (-\gamma_m) g_m = \delta_1 e_1 + \cdots + \delta_k e_k,$$

$$\delta_1 e_1 + \cdots + \delta_k e_k + \gamma_{k+1} g_{k+1} + \cdots + \gamma_m g_m = 0$$

և $\gamma_{k+1} = \cdots = \gamma_m = 0$ ($= \delta_1 = \cdots = \delta_k$): Հետևաբար,

$$\alpha_1 e_1 + \cdots + \alpha_k e_k + \beta_{k+1} f_{k+1} + \cdots + \beta_n f_n = 0$$

և $\alpha_1 = \cdots \alpha_k = \beta_{k+1} = \cdots = \beta_n = 0$: □

Հետևություն 17.21: *Եթե վերջավոր չափանի Q գծային տարածության Q_1 և Q_2 ենթատարածությունների համար՝*

$$dim(Q_1 + Q_2) = dim(Q_1) + dim(Q_2),$$

ապա ենթատարածությունների $Q_1 + Q_2$ գումարը կլինի ուղիղ գումար:

Ապացուցում: Ըստ նախորդ թեորեմի՝

$$dim(Q_1 + Q_2) = dim(Q_1) + dim(Q_2) - dim(Q_1 \cap Q_2) :$$

Օգտվելով տրված պայմանից կունենանք՝ $dim(Q_1 \cap Q_2) = 0$ և $Q_1 \cap Q_2 = \{0\}$: Մնում է կիրառել ենթատարածությունների $Q_1 + Q_2$ գումարը ուղիղ գումար լինելու հայտանիշը: □

Հետևություն 17.22: *Վերջավոր չափանի Q գծային տարածության ցանկացած Q_1, Q_2 և Q_3 ենթատարածությունների համար՝*

$$dim(Q_1+Q_2+Q_3)=dim(Q_1)+dim(Q_2)+dim(Q_3)-$$

$$-dim(Q_1\cap Q_2)-dim\left((Q_1+Q_2)\cap Q_3\right)\ :$$

Ապացուցում: Համաձայն նախորդ թեորեմի՝

$$dim(Q_1+Q_2+Q_3)=dim\left((Q_1+Q_2)+Q_3\right)=$$

$$=dim(Q_1+Q_2)+dim(Q_3)-dim\left((Q_1+Q_2)\cap Q_3\right)=$$

$$=dim(Q_1)+dim(Q_2)-dim\left(Q_1\cap Q_2\right)+dim(Q_3)-dim\left((Q_1+Q_2)\cap Q_3\right):$$

□

Հետևություն 17.23: *Վերջավոր չափանի Q գծային տարածության ցանկացած $Q_1,\ldots,Q_k$ ենթատարածությունների համար՝*

$$dim(Q_1+\cdots+Q_k)=dim(Q_1)+\cdots+dim(Q_k)-$$

$$-dim(Q_1\cap Q_2)-dim\left((Q_1+Q_2)\cap Q_3\right)-\cdots-dim\left((Q_1+\cdots+Q_{k-1})\cap Q_k\right)\ :$$

Ապացուցում: Վերհանգման եղանակով: □

Q գծային տարածության $Q_1,\ldots,Q_k$ ենթատարածությունները կոչվում են **գծայնորեն անկախ**, եթե

$$x_1+\cdots+x_k=0\longrightarrow x_1=\cdots=x_k=0\,,$$

որտեղ $x_1\in Q_1$, ..., $x_k\in Q_k$:

Հատկություն 17.11: *Որպեսզի վերջավոր թվով ենթատարածությունների $Q_1+\cdots+Q_k$ գումարը լինի ուղիղ գումար անհրաժեշտ է և բավարար, որ $Q_1,\ldots,Q_k$ ենթատարածությունները լինեն գծայնորեն անկախ:*

Ապացուցում: Եթե $Q_1,\ldots,Q_k$ ենթատարածությունները գծայնորեն անկախ են և $z=u_1+\cdots+u_k$, $z=u_1'+\cdots+u_k'$, որտեղ $u_1,u_1'\in Q_1$, ..., $u_k,u_k'\in Q_k$, ապա

$$(u_1-u_1')+\cdots+(u_k-u_k')=0$$

և $u_1 - u_1' = 0$, …, $u_k - u_k' = 0$, որտեղից $u_1 = u_1'$, …, $u_k = u_k'$:

Եվ հակառակը, եթե յուրաքանչյուր $z \in Q_1 + \cdots + Q_k$ տարր միարժեքորեն է վերլուծվում $z = u_1 + \cdots + u_k$ տեսքով, որտեղ $u_1 \in Q_1$, …, $u_k \in Q_k$, և $x_1 + \cdots + x_k = 0$, որտեղ $x_1 \in Q_1$, …, $x_k \in Q_k$, ապա $x_1 = 0$, …, $x_k = 0$, այսինքն՝ $Q_1, \ldots, Q_k$ ենթատարածությունները գծայնորեն անկախ են: □

Հատկություն 17.12: *Որպեսզի վերջավոր թվով ենթատարածությունների $Q_1 + \cdots + Q_k$ գումարը լինի ուղիղ գումար անհրաժեշտ է և բավարար, որ յուրաքանչյուր Q_i ենթատարածության հատումը մնացած ենթատարածությունների գումարի հետ լինի զրոյական՝*

$$Q_i \cap (Q_1 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_k) = \{0\},$$

որտեղ $i = 1, \ldots, k$:

Ապացուցում: Իրոք, եթե գումարն ուղիղ է և $z \in Q_i \cap (Q_1 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_k) = \{0\}$, ապա $z = u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k$ և $z - u_1 - \cdots - +u_{i-1} - u_{i+1} - \cdots - u_k = 0$, որտեղից $z = 0$:

Եվ հակառակը, եթե

$$Q_i \cap (Q_1 + \cdots + Q_{i-1} + Q_{i+1} + \cdots + Q_k) = \{0\},$$

որտեղ $i = 1, \ldots, k$, ապա

$$u_1 + \cdots + u_{i-1} + u_i + u_{i+1} + \cdots + u_k = 0$$

պայմանից կունենանք՝

$$u_i = u_1 + \cdots + u_{i-1} + u_{i+1} + \cdots + u_k,$$

որտեղից $u_i = 0$, $i = 1, \ldots, k$: □

Հատկություն 17.13: *Որպեսզի ենթատարածությունների $Q_1 + \cdots + Q_k$ գումարը լինի ուղիղ գումար անհրաժեշտ է և բավարար, որ սկսած երկրորդից յուրաքանչյուր ենթատարածության հատումը նախորդ ենթատարածությունների գումարի հետ լինի զրոյական, այսինքն՝*

$$Q_1 \cap Q_2 = \{0\}, \;\; (Q_1 + Q_2) \cap Q_3 = \{0\}, \; \ldots \; (Q_1 + \cdots + Q_{k-1}) \cap Q_k = \{0\} :$$

Ապացուցում: Անհրաժեշտությունը բխում է նախորդ պնդումից: Բավարարությունը ապացուցենք վերհանգման եղանակով՝ ըստ k բնական թվի: $k = 2$ դեպքում պնդումն ապացուցված է: ենթադրենք պնդումը ճիշտ է $k-1$ թվով ենթատարածությունների համար և ապացուցենք k թվով ենթատարածությունների համար: Եթե $u_1 + \cdots + u_{k-1} + u_k = 0$, ապա $(Q_1 + \cdots + Q_{k-1}) \cap Q_k = \{0\}$ պայմանից կբխի, որ $u_k = 0$ և $u_1 + \cdots + u_{k-1} = 0$: Համաձայն վերհանգային ենթադրության, կունենանք՝ $u_1 = 0, \ldots, u_{k-1} = 0$: □

Հետևություն 17.24: *Եթե վերջավոր չափանի Q գծային տարածության $Q_1, \ldots, Q_k$ ենթատարածությունների համար՝*

$$dim(Q_1 + \cdots + Q_k) = dim(Q_1) + \cdots + dim(Q_k),$$

ապա ենթատարածությունների $Q_1 + \cdots + Q_k$ գումարը կլինի ուղիղ գումար:

Ապացուցում: Ինչպես գիտենք վերջավոր չափանի Q գծային տարածության դեպքում՝

$$dim(Q_1 + \cdots + Q_k) = dim(Q_1) + \cdots + dim(Q_k) -$$

$$-dim(Q_1 \cap Q_2) - dim((Q_1 + Q_2) \cap Q_3) - \cdots dim((Q_1 + \cdots + Q_{k-1}) \cap Q_k) :$$

Հետևաբար՝

$dim(Q_1 \cap Q_2) = \{0\}$,
$dim((Q_1 + Q_2) \cap Q_3) = \{0\}$,
$\cdots\ \cdots\ \cdots$
$dim((Q_1 + \cdots + Q_{k-1}) \cap Q_k) = \{0\}$,

Ուստի՝ $Q_1 \cap Q_2 = \{0\}$, $(Q_1 + Q_2) \cap Q_3 = \{0\}$, ..., $(Q_1 + \cdots + Q_{k-1}) \cap Q_k = \{0\}$: Մնում է օգտվել նախորդ արդյունքից: □

17.11. Գծային տարածությունների իզոմորֆիզմը (նույնաձևությունը)

Դիցուք Q-ն և Q'-ը երկու գծային տարածություններ են որոշված միևնույն P դաշտի վրա (պարզության համար կարելի է ենթադրել $P = \mathbb{R}$): $\varphi : Q \to Q'$ արտապատկերումը կոչվում է **իզոմորֆիզմ** կամ **նույնաձևություն** Q-ից Q' (կամ Q և Q' գծային տարածությունների միջև), եթե φ-ն բավարարում է հետևյալ երեք պայմաններին.

Ա) φ-ն փոխմիարժեք (բիեկտիվ) արտապատկերում է,

Բ) $\varphi(x+y) = \varphi(x) + \varphi(y)$ բոլոր $x, y \in Q$ տարրերի համար,

Գ) $\varphi(\alpha x) = \alpha\varphi(x)$ ցանկացած $x \in Q$ վեկտորի և ցանկացած $\alpha \in P$ սկալյարի համար:

Վերջին երկու պայմաններն ակնհայտորեն միավորվում են մեկ պայմանի մեջ՝

Դ) $\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y)$ ցանկացած $x, y \in Q$ վեկտորների և ցանկացած $\alpha, \beta \in P$ սկալյարների համար:

Սահմանման Բ) պայմանից բխում է՝ $\varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0)$ և $\varphi(0) = 0'$, որտեղ $0'$-ը Q'-ի զրոն է: Այնուհետև, $0' = \varphi(0) = \varphi(x + (-x)) = \varphi(x) + \varphi(-x)$ և $\varphi(-x) = -\varphi(x)$: Այս երկու հատկությունները հեշտությամբ բխում են նաև սահմանման գ) պայմանից՝ $\alpha = 0$ և $\alpha = -1$ արժեքների դեպքում:

Վերհանգման եղանակով ապացուցվում է նաև

$$\varphi\left(x_1 + \cdots + x_n\right) = \varphi(x_1) + \cdots + \varphi(x_n)$$

հավասարությունը ցանկացած $x_1, \ldots, x_n \in Q$ վեկտորների համար:

Օրինակ, եթե $Q = \mathbb{R}_n$, $Q' = \{f \in \mathbb{R}[x] \mid deg(f) \leqslant n-1$ կամ $f = 0\}$, իսկ $\varphi : (a_0, \ldots, a_{n-1}) \to a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, ապա φ-ն կլինի իզոմորֆիզմ Q գծային տարածությունից Q' գծային տարածության մեջ:

Q և Q' գծային տարածությունները կոչվում են **իզոմորֆ** կամ **նույնաձև** և նշանակվում է $Q \simeq Q'$ կամ $Q \cong Q'$, եթե գոյություն ունի որևէ $\varphi : Q \to Q'$ իզոմորֆիզմ (նույնաձևություն): Սահմանված «$\simeq$» կամ «$\cong$» հարաբերությունը կոչվում է գծային տարածությունների **իզոմորֆության** կամ **նույնաձևության հարաբերություն**:

Լեմմ 17.18: *Գծային տարածությունների նույնաձևության «$\simeq$» հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $Q \simeq Q$ ցանկացած Q գծային տարածության համար;

բ) $Q \simeq Q' \longrightarrow Q' \simeq Q$;

գ) $Q \simeq Q'$, $Q' \simeq Q'' \longrightarrow Q \simeq Q''$:

Ապացուցում: ա) պայմանը բխում է այն փաստից, որ $\varepsilon_Q : Q \to Q$ նույնական արտապատկերումը նույնաձևություն է: բ) պայմանը բխում է այն փաստից, որ եթե $\varphi : Q \to Q'$ արտապատկերումը նույնաձևություն է, ապա այդպիսին է նաև $\varphi^{-1} : Q' \to Q$ արտապատկերումը, որովհետև

$$\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y)$$

պայմանից $x = \varphi^{-1}(x')$, $y = \varphi^{-1}(y')$ արժեքների դեպքում կունենանք՝

$$\varphi\left(\alpha\varphi^{-1}(x') + \beta\varphi^{-1}(y')\right) = \alpha\varphi\left(\varphi^{-1}(x')\right) + \beta\varphi\left(\varphi^{-1}(y')\right)\ ,$$

$$\varphi\left(\alpha\varphi^{-1}(x') + \beta\varphi^{-1}(y')\right) = \alpha x' + \beta y'\ ,$$

$$\alpha\varphi^{-1}(x') + \beta\varphi^{-1}(y') = \varphi^{-1}\left(\alpha x' + \beta y'\right)\ ,$$

որտեղ $x', y' \in Q'$: գ) պայմանը բխում է այն փաստից, որ եթե $\varphi : Q \to Q'$ և $\varphi' : Q' \to Q''$ արտապատկերումները նույնաձևություններ են, ապա այդպիսին կլինի նաև դրանց $\varphi \cdot \varphi' : Q \to Q''$ արտադրյալը, որովհետև այն փոխմիարժեք (բիեկտիվ) արտապատկերում է և

$$\varphi\varphi'(\alpha x + \beta y) = \varphi'\left(\varphi(\alpha x + \beta y)\right) =$$

$$= \varphi'\left(\alpha\varphi(x) + \beta\varphi(y)\right) = \alpha\varphi'\left(\varphi(x)\right) + \beta\varphi'\left(\varphi(y)\right) = \alpha\varphi\varphi'(x) + \beta\varphi\varphi'(y)\ :\ \square$$

Թեորեմ 17.17 (վերջավոր չափանի գծային տարածությունների իզոմորֆության հայտանիշը): *Միևնույն դաշտի վրա որոշված երկու Q և Q' վերջավոր չափանի գծային տարածություններ կլինեն իզոմորֆ (նույնաձև) այն և միայն այն դեպքում, երբ դրանք ունեն նույն չափողականությունը՝*

$$Q \simeq Q' \longleftrightarrow dim(Q) = dim(Q')\ :$$

Ապացուցում: Դիցուք $Q \simeq Q'$, $dim(Q) = n$ և $\varphi : Q \to Q'$ արտապատկերումը նույնաձևություն (իզոմորֆիզմ) է Q և Q' գծային տարածությունների միջև: Եթե $n = 0$, այսինքն՝ $Q = \{0\}$, ապա Q'-ը ևս կլինի զրոյական գծային տարածություն, այսինքն՝ $dim(Q') = 0 = dim(Q)$: Դիցուք $n > 0$ և $e_1, \ldots, e_n$ վեկտորների համակարգը հենք է Q-ի համար: Ապացուցենք, որ $\varphi(e_1), \ldots, \varphi(e_n)$ վեկտորների համակարգը կլինի հենք Q'-ի համար: Իրոք, եթե

$$\alpha_1\varphi(e_1) + \cdots + \alpha_n\varphi(e_n) = 0'\,,$$

ապա

$$\varphi\left(\alpha_1 e_1\right) + \cdots + \varphi\left(\alpha_n e_n\right) = \varphi(0)\,,$$

$$\varphi\left(\alpha_1 e_1 + \cdots + \alpha_n e_n\right) = \varphi(0)\ :$$

Քանի որ φ-ն ներդրող (ինյեկտիվ) է, այստեղից կունենանք՝

$$\alpha_1 e_1 + \cdots + \alpha_n e_n = 0$$

և $\alpha_1 = \cdots = \alpha_n = 0$: Ուստի, $\varphi(e_1), \ldots, \varphi(e_n)$ համակարգը գծայնորեն անկախ է:

Մյուս կողմից, համաձայն φ-ի վերադրող (սյուրեկտիվ) լինելուն, ցանկացած $x' \in Q'$ վեկտորի համար գոյություն կունենա այնպիսի $x \in Q$ վեկտոր, որ $\varphi(x) = x'$: Դիցուք $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$, որտեղ $\alpha_1, \ldots, \alpha_n \in P$: Հետևաբար,

$$x' = \varphi(x) = \varphi\left(\alpha_1 e_1 + \cdots + \alpha_n e_n\right) = \alpha_1 \varphi(e_1) + \cdots + \alpha_n \varphi(e_n) \ :$$

Այսպիսով $dim(Q') = n = dim(Q)$:

Եվ հակառակը, եթե $dim(Q) = dim(Q')$, ապա $Q \simeq Q'$: Իրոք, հնարավոր են հետևյալ երկու դեպքերը.

I) $dim(Q) = dim(Q') = 0$ և այս դեպքում պնդումն ակնհայտ է;

II) $dim(Q) = dim(Q') = n > 0$: Դիցուք $e_1, \ldots, e_n$ ու $f_1, \ldots, f_n$ համակարգերը հենքեր են համապատասխանաբար Q և Q' գծային տարածությունների համար: Այս դեպքում, յուրաքանչյուր $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$ վեկտորի համապատասխան սահմանելով

$$\varphi(x) = \alpha_1 f_1 + \cdots + \alpha_n f_n \in Q' \,,$$

ստանում ենք $\varphi : Q \to Q'$ նույնաձևությունը (իզոմորֆիզմը), որովհետև այն փոխմիարժեք (բիեկտիվ) արտապատկերում է և

$$\varphi(\alpha x + \beta y) = \alpha \varphi(x) + \beta \varphi(y)$$

ցանկացած $x, y \in Q$ վեկտորների և ցանկացած $\alpha, \beta \in P$ սկալյարների համար: $\square$

17.12. Գծային ձևեր (ֆունկցիաներ): Համալուծ տարածություն

Դիցուք Q-ն կամայական գծային տարածություն է որոշված P դաշտի վրա (պարզության համար կարելի է ենթադրել $P = \mathbb{R}$):

$\varphi : Q \to P$ ֆունկցիան (արտապատկերումը) կոչվում է Q-ի **գծային ձև** կամ **գծային ֆունկցիա**, եթե այն բավարարում է հետևյալ պայմաններին.

$$\varphi(x + y) = \varphi(x) + \varphi(y) \,,$$

$$\varphi(\lambda x) = \lambda \varphi(x)$$

ցանկացած $x, y \in Q$ վեկտորների և ցանկացած $\lambda \in P$ սկալյարի համար: Այս երկու պայմանները միավորվում են մեկ պայմանի մեջ՝

$$\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y)$$

ցանկացած $x, y \in Q$ վեկտորների և ցանկացած $\alpha, \beta \in P$ սկալյարների համար: Սահմանումից անմիջապես բխում են $\varphi(0) = 0$ և $\varphi(-x) = -\varphi(x)$ հատկությունները, իսկ վերհանգման եղանակով՝ նաև

$$\varphi(x_1 + \cdots + x_n) = \varphi(x_1) + \cdots + \varphi(x_n)$$

հավասարությունը, որտեղ $x, x_1, \ldots, x_n \in Q$:

Q գծային տարածության բոլոր գծային ձևերի բազմությունը նշանակվում է $L(Q, P)$-ով կամ $Hom(Q, P)$: Ակնհայտ է, որ $Hom(Q, P) \neq \emptyset$, որովհետև $\varphi(x) = 0$ պայմանով որոշվող ֆունկցիան կլինի Q-ի գծային ձև, որը կոչվում է **զրոյական գծային ձև**:

Լեմմ 17.19: *Գծային ձևերի $Hom(Q, P)$ ոչ դատարկ բազմությունը կլինի գծային տարածություն՝ հետևյալ գործողությունների նկատմամբ.*

$$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) + \varphi_2(x),$$

$$(\alpha\varphi)(x) = \alpha \cdot \varphi(x),$$

որտեղ $x \in Q$, $\alpha \in P$, $\varphi, \varphi_1, \varphi_2 \in Hom(Q, P)$:

Ապացուցում: Նախ հեշտությամբ ապացուցվում է, որ $\varphi_1 + \varphi_2 \in Hom(Q, P)$ և $\alpha\varphi \in Hom(Q, P)$, եթե $\varphi, \varphi_1, \varphi_2 \in Hom(Q, P)$ և $\alpha \in P$: Այնուհետև, ստուգվում են գծային տարածության սահմանման ութ պայմանները՝ նշված գործողությունների համար: $\square$

Լեմմ 17.20: *1) Եթե $X \neq \emptyset$, ապա ֆունկցիաների*

$$F(X, P) = \{f \mid f : X \to P\}$$

բազմությունը կլինի գծային տարածություն՝ ֆունկցիաների հետևյալ գումարման և սկալյարով (ձախից) բազմապատկման նկատմամբ.

$$(f_1 + f_2)x = f_1(x) + f_2(x)\,,$$

$$(\alpha f)x = \alpha \cdot f(x)\,,$$

որտեղ $x \in X$, $\alpha \in P$, $f, f_1, f_2 \in F(X, P)$:

2) $Hom(Q, P) \leqslant F(Q, P)$, այսինքն՝ $Hom(Q, P)$-ն $F(Q, P)$ գծային տարածության ենթատարածություն է: $\square$

Օրինակներ: 1) $\varphi : f \to f(x_0)$ ֆունկցիան, որտեղ x_0-ն X-ի սևեռված (ֆիքսված) կետ է, կլինի գծային ձև $F(X, P)$ գծային տարածության համար:

2) $C[a,b]$-ով սովորաբար նշանակվում է $[a,b]$ հատվածի վրա անընդհատ բոլոր իրական ֆունկցիաների բազմությունը: Ակնհայտ է, որ $C[a,b] \leqslant F([a,b], \mathbb{R})$ և

$$\varphi : f \longrightarrow \int_a^b f(x)\, dx$$

ֆունկցիան կլինի գծային ձև $C[a,b]$ գծային տարածության համար:

3) $C^1(\mathbb{R})$-ով նշանակենք $f : \mathbb{R} \to \mathbb{R}$ տեսքի բոլոր այն ֆունկցիաների բազմությունը, որոնք ունեն անընդհատ ածանցյալ: Ակնհայտ է, որ $C^1(\mathbb{R}) \leqslant F(\mathbb{R}, \mathbb{R})$ և

$$\varphi : f \longrightarrow f'(x_0), \qquad x_0 \in \mathbb{R},$$

ֆունկցիան կլինի գծային ձև $C^1(\mathbb{R})$ գծային տարածության համար (x_0-ն սևեռված է):

$Hom(Q, P)$ գծային տարածությունը կոչվում է Q-ի **համալուծ տարածություն** և համառոտ նշանակվում է Q^*-ով՝ $Hom(Q, P) = Q^*$: Q^* տարածության տարրերը երբեմն կոչվում են Q-ի **կովեկտորներ**, իսկ $\varphi(x)$-ը այդ դեպքում կոչվում է φ կովեկտորի և x վեկտորի **սկալյար արտադրյալ**:

Զրոյական գծային ձևը կլինի զրոյական գծային տարածության միակ գծային ձևը: Հաջորդ արդյունքում բնութագրվում են n-չափանի գծային տարածության բոլոր գծային ձևերը՝ $n \geqslant 1$ դեպքում:

Թեորեմ 17.18: *Դիցուք Q-ն $e_1, \ldots, e_n$ հենքով գծային տարածություն է որոշված P դաշտի վրա;*

1) Q-ի յուրաքանչյուր $\varphi : Q \to P$ գծային ձև ունի հետևյալ տեսքը՝

$$\varphi(x) = \alpha_1 a_1 + \cdots + \alpha_n a_n,$$

որտեղ $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$, $a_1 = \varphi(e_1)$, …, $a_n = \varphi(e_n)$;

2) Եվ հակառակը, ցանկացած $a_1, \ldots, a_n \in P$ սկալյարների համար գոյություն ունի միարժեքորեն որոշվող այնպիսի $\varphi : Q \to P$ գծային ձև, որ $\varphi(e_1) = a_1$, …, $\varphi(e_n) = a_n$:

Ապացուցում: 1) պնդումն ակնհայտ է: Ապացուցենք 2) պնդումը: Յուրաքանչյուր $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$ վեկտորի համար սահմանենք՝

$$\varphi(x) = \alpha_1 a_1 + \cdots + \alpha_n a_n \in P\ :$$

Հեշտությամբ ստուգվում են $\varphi(x+y) = \varphi(x) + \varphi(y)$ և $\varphi(\lambda x) = \lambda\varphi(x)$ պայմանները: Ակնհայտ է, որ $\varphi(e_1) = a_1, \ldots, \varphi(e_n) = a_n$: Մնում է ապացուցել φ-ի միակությունը: Դիցուք $\varphi(e_1) = \varphi'(e_1) = a_1$, ..., $\varphi(e_n) = \varphi'(e_n) = a_n$, որտեղ φ'-ը ևս Q-ի գծային ձև է: Այդ դեպքում,

$$\varphi(x) = \alpha_1 a_1 + \cdots + \alpha_n a_n = \alpha_1\varphi'(e_1) + \cdots + \alpha_n\varphi'(e_n) =$$

$$= \varphi'(\alpha_1 e_1) + \cdots + \varphi'(\alpha_n e_n) = \varphi'\left(\alpha_1 e_1 + \cdots + \alpha_n e_n\right) = \varphi'(x)$$

ցանկացած $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$ տարրի համար: Ուստի, $\varphi = \varphi'$: □

***Հետևություն 17.25*:** *Յուրաքանչյուր վերջավոր չափանի Q գծային տարածություն իզոմորֆ է իր համալուծ Q^* տարածությանը՝ $Q \simeq Q^*$:*

Ապացուցում: Եթե $Q = \{0\}$, ապա պնդումն ակնհայտ է: Եթե $dim(Q) = n > 0$ և $e_1, \ldots, e_n$ համակարգը Q-ի հենք է, ապա ըստ նախորդ թեորեմի, Q-ի յուրաքանչյուր φ գծային ձև որոշվում է

$$\varphi(x) = \alpha_1 a_1 + \cdots + \alpha_n a_n$$

բանաձևով, որտեղ $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$, $a_1 = \varphi(e_1)$, ..., $a_n = \varphi(e_n)$: Այժմ $\varphi \to (a_1, \ldots, a_n)$ համապատասխանությունը կլինի իզոմորֆիզմ (նույնաձևություն) Q^* և P_n n-տողերի գծային տարածությունների միջև: Քանի որ $dim(P_n) = n$, ապա $dim(Q^*) = n$: Հետևաբար, $dim(Q^*) = dim(Q)$ և $Q \simeq Q^*$: □

Եթե Q-ն զրոյական գծային տարածություն է, ապա նրա Q^* համալուծ տարածությունը ևս կլինի զրոյական: Դիցուք $e_1, \ldots, e_n$ համակարգը հենք է Q-ի համար: Եթե $\alpha_1, \ldots, \alpha_n$-ը $x \in Q$ վեկտորի կոորդինատներն են սևեռված $e_1, \ldots, e_n$ հենքում, այսինքն՝

$$x = \alpha_1 e_1 + \cdots + \alpha_n e_n\,,$$

ապա $\varepsilon_i(x) = \alpha_i$, $i = 1, \ldots, n$, ֆունկցիաները կոչվում են **կոորդինատային ֆունկցիաներ** ($e_1, \ldots, e_n$ հենքի նկատմամբ) և դրանք կլինեն գծային ձևեր Q-ի համար: Մասնավորապես,

$$\varepsilon_i(e_j) = \left\{ \begin{array}{ll} 1, & \textbf{եթե } i = j\,, \\ 0, & \textbf{եթե } i \neq j \end{array} \right. = \delta_{ij} \qquad \text{(Կրոնեկերի սիմվոլը (նշանը))} \ :$$

Այս նշանակումների դեպքում տեղի ունի հետևյալ արդյունքը:

Թեորեմ 17.19: *$\varepsilon_1, \ldots, \varepsilon_n$ հաջորդականությունը կլինի հենք Q^* համալուծ տարածության համար, որը կոչվում է Q գծային տարածության $e_1, \ldots, e_n$ հենքին* **համալուծ հենք***:*

Ապացուցում: Նախ ապացուցենք, որ $\varepsilon_1, \ldots, \varepsilon_n$ հաջորդականությունը գծայնորեն անկախ է: Իրոք, եթե

$$\beta_1\varepsilon_1 + \cdots + \beta_n\varepsilon_n = \mathcal{O}\,,$$

որտեղ $\mathcal{O} : Q \to P$ ֆունկցիան որոշվում է $\mathcal{O}(x) = 0$ պայմանով ($x \in Q$), ապա ցանկացած $x \in Q$ վեկտորի համար կունենանք՝

$$(\beta_1\varepsilon_1 + \cdots + \beta_n\varepsilon_n)\,(x) = \mathcal{O}(x) = 0\,,$$

$$\beta_1\varepsilon_1(x) + \cdots + \beta_n\varepsilon_n(x) = 0 \ :$$

Այստեղ վերցնելով $x = e_i$, կունենանք՝

$$\beta_1\varepsilon_1(e_i) + \cdots + \beta_n\varepsilon_n(e_i) = 0\,,$$

$$\beta_1 0 + \cdots + \beta_{i-1}0 + \beta_i 1 + \beta_{i+1}0 + \cdots + \beta_n 0 = 0\,,$$

այսինքն՝ $\beta_i = 0$ ցանկացած $i = 1, \ldots, n$ արժեքների դեպքում:

Մնում է ապացուցել, որ ցանկացած $f \in Q^*$ գծային ձև գծայնորեն արտահայտվում է $\varepsilon_1, \ldots, \varepsilon_n$ գծային ձևերի միջոցով: Կամայական $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$ վեկտորի համար, հաշվենք $f(x)$-ը՝

$$f(x) = f\left(\alpha_1 e_1 + \cdots + \alpha_n e_n\right) = \alpha_1 f(e_1) + \cdots + \alpha_n f(e_n) =$$

$$f_1\alpha_1 + \cdots + f_n\alpha_n = f_1\varepsilon_1(x) + \cdots + f_n\varepsilon_n(x) = \left(f_1\varepsilon_1 + \cdots + f_n\varepsilon_n\right)(x)\,,$$

որտեղ $f_i = f(e_i)$, $i = 1, \ldots, n$: Ուստի,

$$f = f_1\varepsilon_1 + \cdots + f_n\varepsilon_n \ : \qquad \square$$

Մասնավորապես, $Q \simeq Q^{**} = (Q^*)^*$, որովհետև $Q \simeq Q^*$, $Q^* \simeq Q^{**}$: Սակայն $Q \simeq Q^{**}$ նույնաձևությունը կարելի է հաստատել նաև բնական ճանապարհով: Իրոք, ցանկացած $x \in Q$ վեկտորի համապատասխան սահմանելով $f_x : Q^* \to P$ ֆունկցիան, որտեղ

$$f_x(\varphi) = \varphi(x)\,, \qquad \varphi \in Q^*\,,$$

կստանանք գծային ձև, այսինքն՝ $f_x \in Hom(Q^*, P) = Q^{**}$:

Թեորեմ 17.20: *Վերջավոր չափանի Q գծային տարածության դեպքում $\Phi : x \to f_x$ արտապատկերումը կլինի իզոմորֆիզմ (նույնաձևություն) Q և Q^{**} գծային տարածությունների միջև:*

Ապացուցում: Իրոք, Q-ի ցանկացած φ գծային ձևի համար՝

$$f_{x+y}(\varphi) = \varphi(x+y) = \varphi(x) + \varphi(y) = f_x(\varphi) + f_y(\varphi) = (f_x + f_y)(\varphi)\,,$$

$$f_{\lambda x}(\varphi) = \varphi(\lambda x) = \lambda\varphi(x) = \lambda f_x(\varphi) = (\lambda f_x)(\varphi)\,,$$

այսինքն՝ $f_{x+y} = f_x + f_y$, $f_{\lambda x} = \lambda f_x$ և

$$\Phi(x+y) = f_{x+y} = f_x + f_y = \Phi(x) + \Phi(y)\,,$$

$$\Phi(\lambda x) = f_{\lambda x} = \lambda f_x = \lambda\Phi(x)\,,$$

որտեղ $x, y \in Q$, $\lambda \in P$: Մնում է ապացուցել, որ $\Phi : x \to f_x$ արտապատկերումը փոխմիարժեք (բիեկտիվ) է: $Q = \{0\}$ դեպքում այն ակնհայտ է: դիցուք $dim(Q) = n > 0$ և $e_1, \ldots, e_n$ համակարգը հենք է Q-ի համար, իսկ $\varepsilon_1, \ldots, \varepsilon_n$ համակարգը համապատասխան համալուծ հենքն է Q^*-ում: Այդ դեպքում՝

$$f_{e_i}(\varepsilon_j) = \varepsilon_j(e_i) = \delta_{ij}$$

և, համաձայն նախորդ թեորեմի, $f_{e_1}, \ldots f_{e_n}$ համակարգը կլինի հենք Q^{**}-ի համար, որը Q^* տարածության $\varepsilon_1, \ldots, \varepsilon_n$ հենքի համալուծն է: Հետևաբար, եթե $x \in Q$ և $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$, ապա

$$\Phi(x) = \Phi\left(\alpha_1 e_1 + \cdots + \alpha_n e_n\right) = \alpha_1\Phi(e_1) + \cdots + \alpha_n\Phi(e_n) = \alpha_1 f_{e_1} + \cdots + \alpha_n f_{e_n} \ :$$

Այստեղից բխում է, որ Φ-ը փոխմիարժեք (բիեկտիվ) է, որովհետև

$$x \neq y \longrightarrow \Phi(x) \neq \Phi(y)$$

և ցանկացած $g \in Q^{**}$, $g = \alpha_1 f_{e_1} + \cdots + \alpha_n f_{e_n}$ տարրի համար $\Phi(x) = g$, որտեղ $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$: □

17.13. Քանորդ (կամ ֆակտոր) -տարածություններ

Դիցուք Q-ն կամայական գծային տարածություն է որոշված P դաշտի վրա, իսկ Q'-ը Q-ի կամայական ենթատարածություն է: Նշանակենք՝

$$Q/_{Q'} = \{x + Q' \mid x \in Q\},$$

որտեղ

$$x + Q' = \{x + u \mid u \in Q'\} \subseteq Q$$

ենթաբազմությունը կոչվում է x վեկտորի **հարակից դաս ըստ** Q' **ենթատարածության** կամ **գծային բազմաձևություն**: x-ը կոչվում է $x+Q'$ **հարակից դասի ներկայացուցիչ**:

Օրինակ, $0 + Q' = Q' = x + Q'$, եթե $x \in Q'$: Եթե $t \in x + Q'$, ապա $t + Q' = x + Q'$:

Այսպիսով, միևնույն հարակից դասը կարող է ունենալ տարբեր ներկայացուցիչներ:

Լեմմ 17.21 (հարակից դասերի հավասարության հայտանիշը): *Հետևյալ պնդումները համարժեք են.*

1) $x + Q' = y + Q'$,

2) $x - y \in Q'$,

3) $(x + Q') \cap (y + Q') \neq \emptyset$,

որտեղ $x, y \in Q$:

Ապացուցում: 1)$\to$ 2): Քանի որ $0 \in Q'$, ապա $x = x + 0 \in x + Q'$: Հետևաբար, $x \in y + Q'$, $x = y + u$, $u \in Q'$ և $x - y = u \in Q'$:

2)$\to$ 3): $x \in x + Q'$, իսկ $x - y \in Q'$ պայմանից բխում է $x - y = u$, որտեղ $u \in Q'$: Հետևաբար, $x = y + u \in y + Q'$: Այսպիսով, $x \in (x + Q') \cap (y + Q')$, այսինքն՝ $(x + Q') \cap (y + Q') \neq \emptyset$:

3)$\to$ 1): Գոյություն ունի $z \in (x+Q') \cap (y+Q')$: Հետևաբար, $z \in x+Q'$ և $z \in y + Q'$, այսինքն՝ $z = x + u$ և $z = y + v$, որտեղ $u, v \in Q'$: Ուստի, $x + u = y + v$, որտեղից

$$x = y + (v - u) = y + a,$$

$$y = x + (u - v) = x + (-a),$$

որտեղ $a = v - u \in Q'$: Այժմ ապացուցենք $x + Q' = y + Q'$ հավասարությունը: Դիցուք $t \in x+Q'$: Հետևաբար, $t = x+w = y+a+w = y + w' \in y + Q'$, որտեղ $w \in Q'$, $w' = a + w \in Q'$: Նույն եղանակով ապացուցվում է $y + Q' \subseteq x + Q'$ ներդրումը: $\square$

Հետևություն 17.26: $(a + x) + Q' = a + Q'$, *եթե* $x \in Q'$, $a \in Q$: □

Հետևություն 17.27: *Բոլոր հարակից դասերի* $^{Q}/_{Q'} = \{x + Q' \mid x \in Q\}$ *բազմությունը կազմում է* Q*-ի տրոհում, այսինքն՝* Q*-ի յուրաքանչյուր տարր պատկանում է միարժեքորեն որոշվող որևէ հարակից դասի:* □

Հետևություն 17.28: *Հետևյալ պնդումները համարժեք են.*

1') $x + Q' \neq y + Q'$,

2') $x - y \notin Q'$,

3') $(x + Q') \cap (y + Q') = \emptyset$,

որտեղ $x, y \in Q$ □

Թեորեմ 17.21(հարակից դասերի հավասարության ընդհանուր հայտանիշը): *Q գծային տարածության $H_1, H_2 \leqslant Q$ ենթատարածությունների համար՝*

$$x + H_1 = y + H_2 \longleftrightarrow H_1 = H_2, \quad x - y \in H_1 = H_2,$$

որտեղ $x, y \in Q$:

Ապացուցում: Եթե $x + H_1 = y + H_2$, ապա $x \in y + H_2$, $y \in x + H_1$: Հետևաբար, $x = y + h''$, $y = x + h'$, որտեղ $h' \in H_1$, $h'' \in H_2$: Ուստի $x - y \in H_1 \cap H_2$ և $y - x \in H_1 \cap H_2$: Այժմ ապացուցենք $H_1 \subseteq H_2$ ներդրումը (նույն եղանակով կապացուցվի նաև $H_2 \subseteq H_1$ ներդրումը): Դիցուք $h_1 \in H_1$: Հետևաբար $x + h_1 \in x + H_1 = y + H_2$ և $x + h_1 = y + h^*$, որտեղ $h^* \in H_2$: Ուստի, $h_1 = (y - x) + h^* \in H_2$: □

Այժմ

$$^{Q}/_{Q'} = \{x + Q' \mid x \in Q\}$$

բազմության մեջ ներմուծենք **հարակից դասերի գումարման** և **հարակից դասը սկալյարով** (ձախից) **բազմապատկման** հետևյալ գործողությունները.

$$(x + Q') + (y + Q') = (x + y) + Q'\ ,$$

$$\lambda(x + Q') = \lambda x + Q'\ ,$$

որտեղ $x, y \in Q$ և $\lambda \in P$: Նախ նկատենք, որ սահմանված գումարման և սկալյարով բազմապատկման արդյունքները կախված չեն հարակից դասերում ներկայացուցիչների ընտրությունից:

Լեմմ 17.22: *Եթե $x+Q'=x'+Q'$ և $y+Q'=y'+Q'$, ապա $(x+y)+Q'=(x'+y')+Q'$ և $\lambda x+Q'=\lambda x'+Q'$ ցանկացած $\lambda\in P$ սկալյարի համար:*

Ապացուցում: Օգտվենք հարակից դասերի հավասարության հայտանիշից: Եթե $x+Q'=x'+Q'$ և $y+Q'=y'+Q'$, ապա $x-x'\in Q'$, $y-y'\in Q'$ և $(x+y)-(x'+y')=(x-x')+(y-y')\in Q'$, $\lambda x-\lambda x'=\lambda(x-x')\in Q'$: Հետևաբար,

$$(x+y)+Q'=(x'+y')+Q',$$

$$\lambda x+Q'=\lambda x'+Q' :$$ □

Թեորեմ 17.22: *Եթե Q-ն գծային տարածություն է որոշված P դաշտի վրա և $Q'\leqslant Q$, ապա ${}^{Q}/_{Q'}=\{x+Q' \mid x\in Q\}$ բազմությունը ևս կլինի գծային տարածություն որոշված P դաշտի վրա՝ հարակից դասերի գումարման և հարակից դասը սկալյարով (ձախից) բազմապատկման վերոհիշյալ գործողությունների նկատմամբ: Այս գծային տարածությունը կոչվում է Q գծային տարածության քանորդ-տարածություն կամ ֆակտոր-տարածություն ըստ $Q'\leqslant Q$ ենթատարածության:*

Ապացուցում: Հեշտությամբ ստուգվում են գծային տարածության սահմանման բոլոր ութ աքսիոմները, այսինքն՝ ցանկացած $x,y,z\in Q$ տարրերի և ցանկացած $\alpha,\beta\in P$ սկալյարների համար տեղի ունեն հետևյալ ութ հավասարությունները.

(1) $((x+Q')+(y+Q'))+(z+Q')=(x+Q')+((y+Q')+(z+Q'))$;
(2) $(x+Q')+(y+Q')=(y+Q')+(x+Q')$;
(3) $(x+Q')+(0+Q')=(0+Q')+(x+Q')=x+Q'$;
(4) $(x+Q')+(-x+Q')=(-x+Q')+(x+Q')=0+Q'$;
(5) $\alpha(\beta(x+Q'))=\alpha\beta(x+Q')$;
(6) $\alpha((x+Q')+(y+Q'))=\alpha(x+Q')+\alpha(y+Q')$;
(7) $(\alpha+\beta)(x+Q')=\alpha(x+Q')+\beta(x+Q')$;
(8) $1(x+Q')=x+Q'$: □

Թեորեմ 17.23: *Եթե Q-ն վերջավոր չափանի գծային տարածություն է և $dim(Q)=n$, իսկ $Q'\leqslant Q$ և $dim(Q')=m$, ապա ${}^{Q}/_{Q'}$ քանորդ-տարածությունը ևս կլինի վերջավոր չափանի և $dim\left({}^{Q}/_{Q'}\right)=n-m$:*

Ապացուցում: 1. Եթե $Q' = \{0\}$, ապա $x + Q' = \{x\}$, իսկ

$$^{Q}/_{Q'} = \{\,\{x\} \mid x \in Q\}\ :$$

Այստեղ ևս հնարավոր է երկու ենթադեպք՝ $Q = \{0\}$ կամ $Q \neq \{0\}$: Առաջին ենթադեպքում՝ $dim\left(^{Q}/_{Q'}\right) = 0 = dim(Q) - dim(Q')$: Երկրորդ ենթադեպքում, եթե $e_1, \ldots, e_n$ հաջորդականությունը հենք է Q-ի համար, ապա $\{e_1\}, \ldots, \{e_n\}$ հաջորդականությունը կլինի հենք $^{Q}/_{Q'}$ քանորդ-տարածության համար, այսինքն՝ $dim\left(^{Q}/_{Q'}\right) = n = dim(Q) - dim(Q')$: Եթե $Q' = Q$, ապա $Q/Q' = \{Q\}$ և $dim(Q/Q') = 0 = n - n = dim\,Q - dim\,Q'$:

2. Դիցուք $Q' \neq \{0\}; Q$: Ինչպես գիտենք, Q'-ը ևս կլինի վերջավոր չափանի գծային տարածություն և դիցուք $f_1, \ldots, f_m$ հաջորդականությունը հենք է Q'-ի համար $(m < n)$: Շարունակենք (ընդլայնենք) $f_1, \ldots, f_m$ գծայնորեն անկախ հաջորդականությունը մինչև Q-ի հենքի՝

$$f_1, \ldots, f_m, f_{m+1}, \ldots, f_n\ :$$

Այդ դեպքում, դժվար չէ ապացուցել, որ հարակից դասերի

$$f_{m+1} + Q', \ldots, f_n + Q'$$

հաջորդականությունը կլինի հենք $^{Q}/_{Q'}$ քանորդ-տարածության համար: Հետևաբար, $dim\left(^{Q}/_{Q'}\right) = n - m$: □

Սահմանենք (կառուցենք) $\pi : Q \to {^{Q}/_{Q'}}$ արտապատկերումը հետևյալ կերպ՝

$$\pi(x) = x + Q'\,, \qquad x \in Q\ :$$

Այս արտապատկերումը կոչվում է **բնական** կամ **քանորդ** (ֆակտոր) **արտապատկերում**:

Լեմմ 17.23: *Ցանկացած $x, y \in Q$ տարրերի և ցանկացած $\lambda \in P$ սկալյարի համար՝*

$$\pi(x + y) = \pi(x) + \pi(y)\,,$$

$$\pi(\lambda x) = \lambda \pi(x)\ :$$ □

Երբեմն π նշանակման փոխարեն անհրաժեշտ է լինում օգտվել $\pi_{Q'}$ նշանակումից:

Լեմմ 17.24: $\pi_{Q'}(x) = Q' \longleftrightarrow x \in Q'$*:* □

Ակնհայտ է, որ $\pi_{Q'}$ բնական արտապատկերումը միշտ վերադրող (սյուրեկտիվ) է:

Լեմմ 17.25: *$\pi_{Q'}$ բնական արտապատկերումը կլինի ներդրող (ինյեկտիվ) այն և միայն այն դեպքում, երբ Q' ենթատարածությունը զրոյական է $(Q' = \{0\})$: Հետևաբար, $\pi_{Q'}$ բնական արտապատկերումը կլինի նույնաձևություն (իզոմորֆիզմ) այն և միայն այն դեպքում, երբ Q' ենթատարածությունը զրոյական է:* □

17.14. Գծային արտապատկերումներ: Գծային արտապատկերման միջուկի և պատկերի կապը

Դիցուք Q-ն և S-ը գծային տարածություններ են որոշված միևնույն P դաշտի վրա (պարզության համար կարելի է ենթադրել $P = \mathbb{R}$): $\varphi : Q \to S$ արտապատկերումը կոչվում է **գծային արտապատկերում** Q գծային տարածությունից S գծային տարածության մեջ, եթե տեղի ունեն հետևյալ երկու պայմանները.

$$\varphi(x + y) = \varphi(x) + \varphi(y)\,,$$

$$\varphi(\alpha x) = \alpha\varphi(x)$$

ցանկացած $x, y \in Q$ տարրերի (վեկտորների) և ցանկացած $\alpha \in P$ սկալյարի համար: Այս երկու պայմաններն ակնհայտորեն միավորվում են մեկ պայմանի մեջ՝

$$\varphi(\alpha x + \beta y) = \alpha\varphi(x) + \beta\varphi(y)$$

ցանկացած $x, y \in Q$ տարրերի և ցանկացած $\alpha, \beta \in P$ սկալյարների համար: Այս սահմանումը տարբերվում է գծային տարածությունների իզոմորֆիզմի (նույնաձևության) սահմանումից նրանով, որ այստեղ չի պահանջվում արտապատկերման փոխմիարժեք (բիեկտիվ) լինելը:

$\varphi : Q \to Q$ տեսքի գծային արտապատկերումը կոչվում է նաև Q գծային տարածության **գծային ձևափոխություն** կամ **գծային օպերատոր**:

Օրինակներ: 1) Ածանցման

$$(f + g)' = f' + g'\,,$$

$$(\alpha f)' = \alpha f'$$

հայտնի կանոնները նշանակում են, որ $f \to f'$ արտապատկերումը գծային արտապատկերում է.

ա) $P[x]$ բազմանդամների գծային տարածությունից իր մեջ;

բ) $C^1[a,b]$ գծային տարածությունից $C[a,b]$ գծային տարածության մեջ, որտեղ $C[a,b]$-ն $[a,b]$ հատվածում անընդհատ բոլոր ֆունկցիաների, իսկ $C^1[a,b]$-ն $[a,b]$ հատվածում անընդհատ ածանցյալ ունեցող բոլոր ֆունկցիաների բազմությունն է;

2) $\varphi : (\alpha_1, \ldots, \alpha_n) \to (\alpha_1, \ldots, \alpha_{n-1})$ արտապատկերումը կլինի գծային արտապատկերում P_n-ից P_{n-1}-ի մեջ (մասնավորապես, $\mathbb{R}_n$-ից $\mathbb{R}_{n-1}$-ի մեջ);

3) $\varphi : (\alpha_1, \ldots, \alpha_n) \to (\alpha_1, \ldots, \alpha_{n-1}, 0)$ արտապատկերումը կլինի P_n-ի գծային ձևափոխություն (մասնավորապես, $\mathbb{R}_n$-ի գծային ձևափոխություն);

4) Յուրաքանչյուր $\pi_{Q'} : Q \to {}^{Q}\!/_{Q'}$ բնական արտապատկերում գծային արտապատկերում է;

5) $\varphi : f \to \int\limits_a^b f(x)\,dx$ արտապատկերումը կլինի գծայի արտապատկերում $C[a,b]$-ից $\mathbb{R}$-ի մեջ (որպես գծային տարածություններ՝ որոշված $\mathbb{R}$-ի վրա):

Լեմմ 17.26: *Յուրաքանչյուր $\varphi : Q \to S$ գծային արտապատկերման համար՝*

$$\varphi(0) = 0\,,$$

$$\varphi(-x) = -\varphi(x)\,,$$

$$\varphi(x-y) = \varphi(x) - \varphi(y)\,,$$

$$\varphi(x_1 + \ldots + x_n) = \varphi(x_1) + \ldots + \varphi(x_n)$$

ցանկացած x, y, $x_1, \ldots, x_n \in Q$ տարրերի համար: □

Հետևյալ արդյունքում բնութագրվում են բոլոր $\varphi : Q \to S$ գծային արտապատկերումները, երբ Q-ն n-չափանի գծային տարածություն է ($n > 0$):

Թեորեմ 17.24: *Դիցուք Q-ն $e_1, \ldots, e_n$ հենքով գծային տարածություն է;*

1) Յուրաքանչյուր $\varphi : Q \to S$ գծային արտապատկերում որոշվում է հետևյալ կերպ՝

$$\varphi(x) = \alpha_1 a_1 + \cdots + \alpha_n a_n\,,$$

որտեղ $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$, $a_1 = \varphi(e_1)$, ..., $a_n = \varphi(e_n)$*;*

2) Եվ հակառակը, ցանկացած $a_1, \ldots, a_n \in S$ *վեկտորների համար գոյություն ունի միարժեքորեն որոշվող այնպիսի* $\varphi : Q \to S$ *գծային արտապատկերում, որ* $\varphi(e_1) = a_1$, ..., $\varphi(e_n) = a_n$*:*

Ապացուցում: 1) պնդումն ակնհայտ է: Ապացուցենք 2) պնդումը: Յուրաքանչյուր $x \in Q$, $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$ վեկտորի համար սահմանենք՝

$$\varphi(x) = \alpha_1 a_1 + \cdots + \alpha_n a_n \in S :$$

Հեշտությամբ ստուգվում են $\varphi(x + y) = \varphi(x) + \varphi(y)$ և $\varphi(\lambda x) = \lambda\varphi(x)$ պայմանները: Ակնհայտ է, որ $\varphi(e_1) = a_1$, ..., $\varphi(e_n) = a_n$: Մնում է նաև նկատել φ-ի միակությունը: □

Կամայական $\varphi : Q \to S$ գծային արտապատկերման համար

$$Im(\varphi) = \{\varphi(x) \mid x \in Q\} = \varphi(Q) \subseteq S$$

ենթաբազմությունը կոչվում է φ-ի **պատկեր**, իսկ

$$Ker(\varphi) = \{x \in Q \mid \varphi(x) = 0\} \subseteq Q$$

ենթաբազմությունը կոչվում է φ-ի **միջուկ** կամ **կորիզ**: Օրինակ, $Ker\left(\pi_{Q'}\right) = Q'$, իսկ $Im\left(\pi_{Q'}\right) = {}^{Q}\!/_{Q'}$: Հետևաբար, յուրաքանչյուր ենթատարածություն հանդիսանում է որևէ գծային արտապատկերման միջուկ ($Q' = Ker(\pi_{Q'})$): Սակայն այստեղ միակություն չկա:

Լեմմ 17.27: *Յուրաքանչյուր* $\varphi : Q \to S$ *գծային արտապատկերման պատկերը և միջուկը ենթատարածություններ են, այսինքն՝* $Im(\varphi) \leqslant S$ *և* $Ker(\varphi) \leqslant Q$*:*

Ապացուցում: Օրինակ, ապացուցենք երկրորդը: Եթե $x, y \in Ker(\varphi)$, այսինքն՝ $\varphi(x) = 0$ և $\varphi(y) = 0$, ապա

$$\varphi(x + y) = \varphi(x) + \varphi(y) = 0 + 0 = 0\,,$$

$$\varphi(\alpha x) = \alpha\varphi(x) = \alpha 0 = 0\,,$$

այսինքն՝ $x + y \in Ker(\varphi)$ և $\alpha x \in Ker(\varphi)$ ցանկացած $\alpha \in P$ սկալյարի համար: □

Լեմմ 17.28: *1) Որպեսզի $\varphi : Q \to S$ գծային արտապատկերումը լինի ներդրող (ինյեկտիվ) անհրաժեշտ է և բավարար, որ $Ker(\varphi) = \{0\}$;*

2) Որպեսզի $\varphi : Q \to S$ գծային արտապատկերումը լինի վերադրող (սյուրեկտիվ) անհրաժեշտ է և բավարար, որ $Im(\varphi) = S$:

Ապացուցում: 1) Եթե $\varphi : Q \to S$ գծային արտապատկերումը ներդրող է, ապա $Ker(\varphi) = \{0\}$, որովհետև $\varphi(0) = 0$, այսինքն՝ $\{0\} \subseteq Ker(\varphi)$ և

$$x \neq 0 \longrightarrow \varphi(x) \neq \varphi(0) = 0\,, \qquad x \in Q\ :$$

Եվ հակառակը, եթե $Ker(\varphi) = \{0\}$, ապա

$$\varphi(x) = \varphi(y) \longrightarrow \varphi(x) - \varphi(y) = 0 \longrightarrow \varphi(x-y) = 0 \longrightarrow$$

$$x - y \in Ker(\varphi) = \{0\} \longrightarrow x - y = 0 \longrightarrow x = y\,,$$

այսինքն՝ φ-ն ներդրող (ինյեկտիվ) է: □

Թեորեմ 17.25: *Եթե Q-ն վերջավոր չափանի գծային տարածություն է, ապա յուրաքանչյուր $\varphi : Q \to S$ գծային արտապատկերման դեպքում $Im(\varphi)$-ն և $Ker(\varphi)$-ն նույնպես կլինեն վերջավոր չափանի գծային տարածություններ և*

$$dim(Ker(\varphi)) + dim(Im(\varphi)) = dim(Q)\ :$$

Հետևաբար, $Q = Ker(\varphi) \oplus H$, որտեղ $H \leqslant Q$ ենթատարածությունն իզոմորֆ է $Im(\varphi)$-ին: $dim(Im(\varphi))$-ն կոչվում է φ գծային արտապատկերման **ռանգ**, *իսկ $dim(Ker(\varphi))$-ն՝* **արատ**:

Ապացուցում: Դիցուք $dim(Q) = n$: Հնարավոր է երկու դեպք՝ $Ker(\varphi) = \{0\}$ կամ $Ker(\varphi) \neq \{0\}$: Առաջին դեպքում պնդումն ակնհայտ է, որովհետև այդ դեպքում՝ $Im(\varphi) \simeq Q$, հետևաբար, $dim(Im(\varphi)) = dim(Q)$:

Դիցուք $Ker(\varphi) \neq \{0\}$ և վեկտորների $e_1, \ldots, e_k$ հաջորդականությունը հենք է $Ker(\varphi) \leqslant Q$ ենթատարածության համար: Եթե այստեղ $Ker(\varphi) = Q$, ապա $Im(\varphi) = \{0\}$ և պնդումը կլինի ճիշտ: Հակառակ դեպքում՝ $Ker(\varphi) \neq Q$: Այս դեպքում շարունակենք (ընդլայնենք) $e_1, \ldots, e_k$ հաջորդականությունը մինչև Q-ի հենքի՝

$$e_1, \ldots, e_k, f_{k+1}, \ldots, f_n\ :$$

Ապացուցենք, որ $\varphi(f_{k+1}),\ldots,\varphi(f_n)$ հաջորդականությունը հենք է $Im(\varphi)\leqslant Q$ ենթատարածության համար: Իրոք, յուրաքանչյուր $y\in Im(\varphi)$ տարրի համար գոյություն ունի այնպիսի $x\in Q$, $x=\alpha_1e_1+\cdots+\alpha_ke_k+\alpha_{k+1}f_{k+1}+\cdots+\alpha_nf_n$, որ $\varphi(x)=y$: Հետևաբար,

$$y=\alpha_{k+1}\varphi(f_{k+1})+\cdots+\alpha_n\varphi(f_n)\ :$$

Մնում է ապացուցել $\varphi(f_{k+1}),\ldots,\varphi(f_n)$ հաջորդականության գծայնորեն անկախությունը: Իրոք, եթե

$$\gamma_{k+1}\varphi(f_{k+1})+\cdots+\gamma_n\varphi(f_n)=0\,,$$

ապա $\gamma_{k+1}f_{k+1}+\cdots+\gamma_nf_n\in Ker(\varphi)$: Հետևաբար,

$$\gamma_{k+1}f_{k+1}+\cdots+\gamma_nf_n=\beta_1e_1+\cdots+\beta_ke_k\ ,$$

$$\gamma_{k+1}f_{k+1}+\cdots+\gamma_nf_n+(-\beta_1)e_1+\cdots+(-\beta_k)e_k=0$$

և $\gamma_{k+1}=\cdots=\gamma_n=-\beta_1=\cdots=-\beta_k=0$: Այսպիսով, $dim(Im(\varphi))=n-k=dim(Q)-dim(Ker(\varphi))$: □

Որպես հետևություն, այս թեորեմից նորից ստացվում է քանորդ-տարածության չափողականության վերաբերյալ թեորեմը, եթե որպես գծային արտապատկերում վերցնենք $\pi_{Q'}\ :\ Q\to {}^{Q}/_{Q'}$ բնական արտապատկերումը: Իրոք, եթե Q-ն վերջավոր չափանի գծային տարածություն է, ապա

$$dim\,(Ker\,(\pi_{Q'}))+dim\,(Im\,(\pi_{Q'}))=dim(Q)\,,$$

որտեղ $Ker\,(\pi_{Q'})=Q'$, $Im\,(\pi_{Q'})={}^{Q}/_{Q'}$: Ուստի

$$dim\left({}^{Q}/_{Q'}\right)=dim(Q)-dim(Q')\ :$$

Ապացուցված թեորեմից որպես հետևություն ստացվում է նաև գծային հավասարումների համասեռ համակարգի լուծումների L^A տարածության չափողականության վերաբերյալ թեորեմը (թեորեմ 17.14): Այդ նպատակով նախ նկատենք, որ յուրաքանչյուր $m\times n$-չափանի $A=(a_{ij})\in P^{m\times n}$ մատրից կարելի է դիտել նաև որպես գծային արտապատկերում P^n-ից P^m-ի մեջ՝

$$A\ :\ \begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}\longrightarrow A\cdot\begin{pmatrix}\alpha_1\\ \vdots\\ \alpha_n\end{pmatrix}\,,$$

քանի որ ցանկացած $x, y \in P^n$ սյունակների և ցանկացած $\alpha \in P$ սկալյարի համար տեղի ունեն հետևյալ երկու հավասարությունները.

$$A(x+y) = A(x) + A(y)\,,$$

$$A(\alpha x) = \alpha A(x)\ :$$

Քանի որ $Ker(A) \leqslant P^n$ և $Im(A) \leqslant P^m$, ապա $Ker(A)$ և $Im(A)$ ենթատարածությունները վերջավոր չափանի գծային տարածություններ են: Ակնհայտ է նաև, որ $Ker(A) = L^A$: Հետևաբար, $dim(Ker(A)) = dim\left(L^A\right)$:

Թեորեմ 17.26: *Յուրաքանչյուր $m \times n$-չափանի A մատրիցի համար՝ $dim(Im(A)) = rank(A)$:*

Ապացուցում: Եթե $A'_1, A'_2, \ldots, A'_n$ սյունակները A մատրիցի սյունակներն են, ապա

$$Im(A) = \left\{ A \cdot \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \,\middle|\, \alpha_1, \ldots, \alpha_n \in P \right\} =$$

$$= \{\alpha_1 A'_1 + \alpha_2 A'_2 + \cdots + \alpha_n A'_n \mid \alpha_1, \ldots, \alpha_n \in P\} = (A'_1, A'_2, \ldots, A'_n)\ ,$$

այսինքն՝ $Im(A)$-ն համընկնում է $A'_1, A'_2, \ldots, A'_n$ սյունակների գծային թաղանթի հետ: Հետևաբար, $Im(A)$-ի չափողականությունը կհամընկնի $A'_1, A'_2, \ldots, A'_n$ հաջորդականության ռանգի հետ, ինչը հենց A մատրիցի ռանգն է: □

Այսպիսով, $dim\left(L^A\right) + rank(A) = n$ և $dim\left(L^A\right) = n - rank(A)$:

Թեորեմ 17.27: *Եթե Q և S գծային տարածությունները n-չափանի գծային տարածություններ են, այսինքն՝ $dim(Q) = dim(S) = n$, ապա յուրաքանչյուր $\varphi : Q \to S$ գծային արտապատկերման համար հետևյալ հատկությունները համարժեք են.*

1) φ-ն ներդրող (ինյեկտիվ) է;

2) φ-ն վերադրող (սյուրեկտիվ) է;

3) φ-ն փոխմիարժեք (բիեկտիվ) է:

Ապացուցում: 1)$\to$ 2): Եթե φ-ն ներդրող (ինյեկտիվ) է, ապա $\ker(\varphi) = \{0\}$ և

$$dim(Ker(\varphi)) + dim(Im(\varphi)) = dim(Q) = n$$

բանաձևից կստանանք՝ $dim(Im(\varphi)) = n = dim(S)$: Հետևաբար, $Im(\varphi) = S$, այսինքն՝ φ-ն վերադրող (սյուրեկտիվ) է:

Նույն եղանակով ապացուցվում է նաև 2)→ 3) պնդումը: □

Լեմմ 17.29: *Երկու գծային արտապատկերումների արտադրյալը (եթե այն գոյություն ունի) նորից գծային արտապատկերում է, այսինքն՝ եթե $\varphi : Q \to S$ և $\mu : S \to V$ արտապատկերումները գծային արտապատկերումներ են, ապա $\varphi \cdot \mu : Q \to V$ արտադրյալը ևս կլինի գծային արտապատկերում:*

Ապացուցում: Իրոք,

$$\varphi\mu(\alpha x + \beta y) = \mu(\varphi(\alpha x + \beta y)) =$$

$$= \mu(\alpha\varphi(x) + \beta\varphi(y)) = \alpha\mu(\varphi x) + \beta\mu(\varphi y) = \alpha((\varphi\mu)x) + \beta((\varphi\mu)y) \ : \ \square$$

Անցնենք գծային արտապատկերման միջուկի և պատկերի կապին ընդհանուր դեպքում, այսինքն՝ կամայական Q և S գծային տարածությունների դեպքում, որտեղ չի ենթադրվում դիտարկվող գծային տարածությունների վերջավոր չափանի լինելը:

Հետևյալ արդյունքում յուրաքանչյուր վերադրող (սյուրեկտիվ) գծային արտապատկերում բնութագրվում է նաև իզոմորֆիզմ (նույնաձևություն) հանդիսացող արտադրիչի ճշտությամբ: Ավելի ճիշտ, յուրաքանչյուր վերադրող գծային արտապատկերում նույնաձևություն հանդիսացող արտադրիչի ճշտությամբ համընկնում է բնական արտապատկերման հետ:

Թեորեմ 17.28 (գծային արտապատկերման միջուկի և պատկերի կապը ընդհանուր դեպքում): *Դիցուք Q-ն և S-ը կամայական գծային տարածություններ են: Այդ դեպքում յուրաքանչյուր վերադրող (սյուրեկտիվ) $\varphi : Q \to S$ գծային արտապատկերման համար՝ $S \simeq Q/_{Q'}$, որտեղ $Q' = Ker(\varphi)$: Ավելի ճշգրիտ, յուրաքանչյուր վերադրող (սյուրեկտիվ) $\varphi : Q \to S$ գծային արտապատկերման համար, որտեղ $Ker(\varphi) = Q'$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\mu : S \to {}^{Q}/_{Q'}$ իզոմորֆիզմ (նույնաձևություն), որ $\pi = \varphi \cdot \mu$, այսինքն՝ տեղափոխական է գծային արտապատկերումների հետևյալ եռանկյունը՝*

$$\begin{tikzcd} Q \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & S \arrow[d, "\mu"] \\ & {}^{Q}\!/_{Q'} \end{tikzcd} ,$$

որտեղ π-ն բնական արտապատկերումն է ($\pi(x) = x + Q'$):

Ապացուցում: Ցանկացած $y \in S$ վեկտորի համար գոյություն ունի այնպիսի $x \in Q$ վեկտոր, որ $\varphi(x) = y$: Սահմանենք՝ $\mu(y) = x + Q'$, որտեղ $\varphi(x) = y$: Նախ նկատենք, որ $\mu(y)$-ը կախված չէ $\varphi(x) = y$ հավասարությանը բավարարող x-ի ընտրությունից: Իրոք, եթե նաև $\varphi(x_1) = y$, ապա $\varphi(x) = \varphi(x_1)$, այսինքն՝ $\varphi(x - x_1) = 0$, $x - x_1 \in Ker(\varphi) = Q'$ և $x + Q' = x_1 + Q'$ (լեմմ 17.21):

Ակնհայտ է, որ μ-ն վերադրող (սյուրեկտիվ) է, ապացուցենք նրա ներդրող (ինյեկտիվ) լինելը: Դիցուք $\mu(y) = \mu(z)$, որտեղ $y = \varphi(x)$, իսկ $z = \varphi(t)$, որտեղ $x, t \in Q$: Հետևաբար, $x + Q' = t + Q'$, $x - t \in Q' = Ker(\varphi)$, $\varphi(x - t) = 0$, $\varphi(x) - \varphi(t) = 0$, $\varphi(x) = \varphi(t)$ և $y = z$: Այժմ ապացուցենք, որ μ-ն գծային արտապատկերում է:

Դիցուք $y, z \in S$ և $\varphi(x) = y$, $\varphi(t) = z$, որտեղ $x, t \in Q$: Այդ դեպքում, $y + z = \varphi(x) + \varphi(t) = \varphi(x + t)$, $\varphi(\lambda x) = \lambda\varphi(x) = \lambda y$: Հետևաբար,

$$\mu(y + z) = (x + t) + Q' = (x + Q') + (t + Q') = \mu(y) + \mu(z)\,,$$

$$\mu(\lambda y) = \lambda x + Q' = \lambda(x + Q') = \lambda\mu(y)$$

ցանկացած $\lambda \in P$ սկալյարի համար: Ստուգենք $\pi = \varphi \cdot \mu$ հավասարությունը: Իրոք, ըստ μ-ի սահմանենք՝ $\mu(y) = x + Q'$, որտեղ $\varphi(x) = y$: Ուստի, $\mu(\varphi(x)) = \pi(x)$, $(\varphi \cdot \mu)x = \pi(x)$ և $\varphi \cdot \mu = \pi$: Ի վերջո, ապացուցենք μ-ի միակությունը: Եթե $\pi = \varphi \cdot \mu$ և $\pi = \varphi \cdot \mu'$, ապա $\varphi \cdot \mu = \varphi \cdot \mu'$, այսինքն՝ $(\varphi \cdot \mu)x = (\varphi \cdot \mu')x$ ցանկացած $x \in Q$ վեկտորի համար: Այսպիսով, $\mu(\varphi x) = \mu'(\varphi x)$ և $\mu(y) = \mu'(y)$ ցանկացած $y \in S$ վեկտորի համար: □

Թեորեմ 17.29 (գծային արտապատկերման միջուկի և պատկերի ընդհանրացված կապը): *Դիցուք Q-ն, S_1-ը և S_2-ը կամայական գծային տարածություններ են: Այդ դեպքում, կամայական φ_1 :*

$Q \to S_1$ *և* $\varphi_2 : Q \to S_2$ *վերադրող (սյուրեկտիվ) գծային արտապատկերումների համար, որտեղ* $Ker(\varphi_1) \subseteq Ker(\varphi_2)$*, գոյություն ունի միարժեքորեն որոշվող այնպիսի* $\varphi_3 : S_1 \to S_2$ *վերադրող գծային արտապատկերում, որ* $\varphi_1 \cdot \varphi_3 = \varphi_2$*, այսինքն՝ տեղափոխական է գծային արտապատկերումների հետևյալ եռանկյանը՝*

$$\begin{tikzcd} Q \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & S_1 \arrow[d, "\varphi_3"] \\ & S_2 \end{tikzcd} \quad :$$

Ընդ որում, φ_3*-ը կլինի իզոմորֆիզմ այն և միայն այն դեպքում, երբ* $Ker(\varphi_1) = Ker(\varphi_2)$*:*

Ապացուցում: Տես թեորեմ 0.9-ի ապացուցումը: □

Նկատենք նաև, որ գծային արտապատկերումների միջուկի և պատկերի վերաբերյալ ապացուցված առաջին թեորեմը բխում է նաև երկրորդ թեորեմից:

17.15. Գծային արտապատկերումների գծային տարածություն: Գծային արտապատկերման մատրից: Գծային ձևափոխության որոշիչ և հետք

Դիցուք Q-ն և S-ը կամայական գծային տարածություններ են որոշված միևնույն P դաշտի վրա, իսկ $X \neq \emptyset$: Նշանակենք՝

$Hom(Q, S) = \{\varphi : Q \to S \,|\, \varphi$-ն գծային արտապատկերում է $\} \neq \emptyset$,

$F(X, S) = \{f \,|\, f : X \to S\} \neq \emptyset$:

Լեմմ 17.30: $Hom(Q, S)$ *բազմությունը կլինի գծային տարածություն որոշված* P*-ի վրա՝ գծային արտապատկերումների հետևյալ գումարման և սկալյարով (ձախից) բազմապատկման նկատմամբ.*

$$(\varphi_1 + \varphi_2)x = \varphi_1(x) + \varphi_2(x)\,,$$

$$(\alpha\varphi)x = \alpha\varphi(x)\,,$$

որտեղ $x \in Q$, $\alpha \in P$, $\varphi, \varphi_1, \varphi_2 \in Hom(Q, S)$*:*

Ապացուցում: Իրոք, նախ նկատենք, որ $\varphi_1+\varphi_2 \in Hom(Q,S)$ և $\alpha\varphi \in Hom(Q,S)$, եթե $\varphi,\varphi_1,\varphi_2 \in Hom(Q,S)$, $\alpha \in P$.

$$(\varphi_1+\varphi_2)(\beta x+\gamma y) = \varphi_1(\beta x+\gamma y)+\varphi_2(\beta x+\gamma y) =$$

$$= \varphi_1(\beta x)+\varphi_1(\gamma y)+\varphi_2(\beta x)+\varphi_2(\gamma y) =$$

$$= \beta\varphi_1(x)+\gamma\varphi_1(y)+\beta\varphi_2(x)+\gamma\varphi_2(y) =$$

$$= \beta\left(\varphi_1(x)+\varphi_2(x)\right)+\gamma\left(\varphi_1(y)+\varphi_2(y)\right) =$$

$$= \beta\left(\left(\varphi_1+\varphi_2\right)(x)\right)+\gamma\left(\left(\varphi_1+\varphi_2\right)(y)\right)\ ,$$

$$(\alpha\varphi)(\beta x+\gamma y) = \alpha\varphi(\beta x+\gamma y) =$$

$$= \alpha\left(\beta\varphi(x)+\gamma\varphi(y)\right) = \alpha\beta\varphi(x)+\alpha\gamma\varphi(y) =$$

$$= \beta(\alpha\varphi(x))+\gamma(\alpha\varphi(y)) = \beta\left((\alpha\varphi)x\right)+\gamma\left((\alpha\varphi)y\right)\ :$$

Մնում է ստուգել գծային տարածության սահմանման ութ աքսիոմները: □

$Hom(Q,Q)$-ի համար գործածվում է նաև $End(Q)$ նշանակումը:

Լեմմ 17.31: *$F(X,S)$ բազմությունը կլինի գծային տարածություն որոշված P-ի վրա՝ ֆունկցիաների հետևյալ գումարման և սկալյարով (ձախից) բազմապատկման նկատմամբ.*

$$(f_1+f_2)(x) = f_1(x)+f_2(x),$$

$$(\alpha f)(x) = \alpha f(x),$$

որտեղ $x \in X$, $\alpha \in P$, $f,f_1,f_2 \in F(X,S)$: Ըստ որում՝ $Hom(Q,S) \leqslant F(Q,S)$: □

Դիցուք Q-ն և S-ը վերջավոր չափանի ոչ զրոյական գծային տարածություններ են՝ $dim(Q)=n>0$, $dim(S)=m>0$: Եթե $e_1,\ldots,e_n$ համակարգը հենք է Q-ի համար, $f_1,\ldots,f_m$ համակարգը հենք է S-ի համար, իսկ $\varphi : Q \to S$ արտապատկերումը գծային արտապատկերում է և

$$\begin{array}{l} \varphi(e_1) = \alpha_{11}f_1+\alpha_{12}f_2+\cdots+\alpha_{1m}f_m\ , \\ \ldots\ \ldots\ \ldots\ \ldots \\ \varphi(e_n) = \alpha_{n1}f_1+\alpha_{n2}f_2+\cdots+\alpha_{nm}f_m\ , \end{array} \qquad (17.20)$$

ապա այս վերլուծությունների գործակիցներից կազմված $n \times m$-չափանի

$$A = \begin{pmatrix} \alpha_{11}, \ldots, \alpha_{1m} \\ \ldots \quad \ldots \quad \ldots \\ \alpha_{n1}, \ldots, \alpha_{nm} \end{pmatrix} \in P^{n \times m}$$

մատրիցը կոչվում է φ **գծային արտապատկերման մատրից**՝ սևեռված (e_i) և (f_j) հենքերի նկատմամբ:

Ընդունելով՝

$$e = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}, \quad f = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}, \quad \varphi(e) = \begin{pmatrix} \varphi e_1 \\ \vdots \\ \varphi e_n \end{pmatrix}$$

և օգտվելով $\bullet$ արտադրյալից, (17.20) հավասարությունների համակարգը ընդունում է հետևյալ համառոտ մատրիցային տեսքը՝

$$\varphi(e) = A \bullet f \ :$$

Այս դեպքում, φ գծային արտապատկերման A մատրիցը նշանակվում է նաև $\left(\varphi_e^f\right)$-ով կամ համառոտ (φ)-ով:

Եթե $Q = S$, իսկ $e = f$, ապա (φ_e^e) մատրիցը կոչվում է $\varphi : Q \to Q$ գծային ձևափոխության մատրից $e_1, \ldots, e_n$ հենքի նկատմամբ: Այսպիսով, n-րդ կարգի $A \in P^{n \times n}$ մատրիցը կոչվում է n-չափանի Q գծային տարածության $\varphi : Q \to Q$ **գծային ձևափոխության մատրից** $e_1, \ldots, e_n$ հենքի նկատմամբ, եթե

$$\varphi(e) = A \bullet e \ :$$

Պարզ է, որ Q և S վերջավոր չափանի գծային տարածություններում հենքերի փոփոխության դեպքում $\varphi : Q \to S$ գծային արտապատկերման մատրիցի չափողականությունը չի փոխվի: Սակայն պարզվում է, որ հենքերի փոփոխության դեպքում չի փոխվում նաև $\varphi : Q \to S$ գծային արտապատկերման մատրիցի ռանգը: Ավելի ճիշտ տեղի ունի հետևյալ արդյունքը:

Թեորեմ 17.30: *Դիցուք Q-ն և S-ը վերջավոր չափանի գծային տարածություններ են՝ որոշված միևնույն P դաշտի վրա: Q գծային տարածության ցանկացած (e_i) հենքի, S գծային տարածության* *ցանկացած (f_j) հենքի և կամայական $\varphi : Q \to S$ գծային արտապատկերման համար՝*

$$rank\left(\varphi_e^f\right) = dim(Im(\varphi)):$$

*Ապացուցում:*Քանի որ $Im(\varphi) \leqslant S$ ենթատարածությունը համընկնում է $\varphi e_1, \ldots, \varphi e_n$ հաջորդականության գծային թաղանթի հետ՝

$$Im(\varphi) = (\varphi(e_1), \ldots, \varphi(e_n)),$$

ապա մնում է նկատել, որ $\varphi(e_1), \ldots, \varphi(e_n)$ հաջորդականության ռանգը համընկնում է $\left(\varphi_e^f\right)$ մատրիցի ռանգի հետ: Դրա համար, նշանակելով $\left(\varphi_e^f\right)$ մատրիցի տողերը՝ $[\varphi(e_1)], \ldots, [\varphi(e_n)]$, ապացուցենք, որ $\varphi(e_{i_1}), \ldots, \varphi(e_{i_k})$ հաջորդականությունը կլինի գծայնորեն կախյալ այն և միայն այն դեպքում, երբ $[\varphi(e_{i_1})], \ldots, [\varphi(e_{i_k})]$ հաջորդականությունը գծայնորեն կախյալ է: Իրոք՝

$\alpha_1\varphi(e_{i_1}) + \cdots + \alpha_k\varphi(e_{i_k}) = 0 \longleftrightarrow$

$\alpha_1\left(a_{i_1,1}f_1 + \cdots + a_{i_1,m}f_m\right) + \cdots + \alpha_k\left(a_{i_k,1}f_1 + \cdots + a_{i_k,m}f_m\right) = 0 \longleftrightarrow$

$\left(\alpha_1 a_{i_1,1} + \cdots + \alpha_k a_{i_k,1}\right)f_1 + \cdots + \left(\alpha_1 a_{i_1,m} + \cdots + \alpha_k a_{i_k,m}\right)f_m = 0 \longleftrightarrow$

$$\left\{\begin{array}{l} \alpha_1 a_{i_1,1} + \cdots + \alpha_k a_{i_k,1} = 0, \\ \cdots\ \cdots\ \cdots \\ \alpha_1 a_{i_1,m} + \cdots + \alpha_k a_{i_k,m} = 0, \end{array}\right. \longleftrightarrow$$

$\alpha_1\left(a_{i_1,1}, \ldots, a_{i_1,m}\right) + \cdots + \alpha_k\left(a_{i_k,1}, \ldots, a_{i_k,m}\right) = (0, \ldots, 0) \longleftrightarrow$

$\alpha_1[\varphi(e_{i_1})] + \cdots + \alpha_k[\varphi(e_{i_k})] = (0, \ldots, 0):$

Հետևաբար, $\varphi(e_{i_1}), \ldots, \varphi(e_{i_k})$ հաջորդականությունը կլինի գծայնորեն անկախ այն և միայն այն դեպքում, երբ $[\varphi(e_{i_1})], \ldots, [\varphi(e_{i_k})]$ հաջորդականությունը գծայնորեն անկախ է: Արդյունքում $\varphi(e_{i_1}), \ldots, \varphi(e_{i_k})$ հաջորդականությունը կլինի հենք այն և միայն այն դեպքում, երբ $[\varphi(e_{i_1})], \ldots, [\varphi(e_{i_k})]$ հաջորդականությունը հենք է: □

Հետևություն 17.29: *$\varphi : Q \to S$ գծային արտապատկերման ռանգը հավասար է Q-ի ցանկացած (e_i) և S-ի ցանկացած (f_j) հենքերի նկատմամբ նրա ունեցած մատրիցի ռանգին:* □

Թեորեմ 17.31: *Դիցուք Q-ն և S-ը ոչ զրոյական վերջավոր չափանի գծային տարածություններ են՝ որոշված միևնույն P դաշտի վրա: Եթե*

Q-ն n-չափանի է՝ $e_1, \ldots, e_n$ հենքով, իսկ S-ը m-չափանի է՝ $f_1, \ldots, f_m$ հենքով, ապա

$$\Phi : \varphi \longrightarrow \left(\varphi_e^f\right)$$

արտապատկերումը կլինի իզոմորֆիզմ (նույնածնություն) $Hom(Q,S)$ և $P^{n\times m}$ գծային տարածությունների միջև: Մասնավորապես, $dim(Hom(Q,S)) = n \cdot m = dim(Q) \cdot dim(S)$, իսկ $dim(Hom(Q,Q)) = n^2$:

Ապացուցում: Ցանկացած $\lambda \in P$ սկալյարի համար՝

$$\begin{aligned}
&(\lambda\varphi)e_1 = \lambda\varphi(e_1) = \lambda\alpha_{11}f_1 + \lambda\alpha_{12}f_2 + \cdots + \lambda\alpha_{1m}f_m\,,\\
&\ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\\
&(\lambda\varphi)e_n = \lambda\varphi(e_n) = \lambda\alpha_{n1}f_1 + \lambda\alpha_{n2}f_2 + \cdots + \lambda\alpha_{nm}f_m\,,
\end{aligned}$$

այսինքն՝ $\Phi(\lambda\varphi) = \lambda\Phi(\varphi)$: Եթե $\psi \in Hom(Q,S)$ և

$$\begin{aligned}
&\psi(e_1) = \beta_{11}f_1 + \beta_{12}f_2 + \cdots + \beta_{1m}f_m\,,\\
&\ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\\
&\psi(e_n) = \beta_{n1}f_1 + \beta_{n2}f_2 + \cdots + \beta_{nm}f_m\,,
\end{aligned}$$

ապա

$$\begin{aligned}
&(\varphi+\psi)e_1 = \varphi(e_1) + \psi(e_1) =\\
&\qquad = (\alpha_{11}+\beta_{11})\,f_1 + (\alpha_{12}+\beta_{12})\,f_2 + \cdots + (\alpha_{1m}+\beta_{1m})\,f_m\,,\\
&\ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\\
&(\varphi+\psi)e_n = \varphi(e_n) + \psi(e_n) =\\
&\qquad = (\alpha_{n1}+\beta_{n1})\,f_1 + (\alpha_{n2}+\beta_{n2})\,f_2 + \cdots + (\alpha_{nm}+\beta_{1m})\,f_m\,,
\end{aligned}$$

Այսինքն՝ $\Phi(\varphi+\psi) = \Phi(\varphi) + \Phi(\psi)$: Մնում է նկատել $\Phi : Hom(Q,S) \to P^{n\times m}$ արտապատկերման փոխմիարժեք (բիեկտիվ) լինելը՝ ելնելով թեորեմ 17.24-ից: $\square$

Դիցուք Q-ն, S-ը և V-ն վերջավոր չափանի ոչ զրոյական գծային տարածություններ են՝ որոշված միևնույն P դաշտի վրա: Դիցուք Q-ն n-չափանի է՝ $e_1, \ldots, e_n$ հենքով, S-ը m-չափանի է՝ $f_1, \ldots, f_m$ հենքով, իսկ V-ն k-չափանի է՝ $g_1, \ldots, g_k$ հենքով, իսկ $\varphi : Q \to S$ և $\psi : S \to V$ արտապատկերումները կամայական գծային արտապատկերումներ են: Նշված (սևեռված) հենքերի նկատմամբ φ, ψ և $\varphi \cdot \psi$ գծային արտապատկերումների մատրիցները համապատասխանաբար նշանակենք (φ)-ով, (ψ)-ով և $(\varphi \cdot \psi)$-ով:

Թեորեմ 17.32: $(\varphi\cdot\psi)=(\varphi)\cdot(\psi)$*:*

Ապացույց: Դիցուք $(\varphi)=A$, $(\psi)=B$, $(\varphi\cdot\psi)=C$: Հետևաբար, A, B և C մատրիցները համապատասխանաբար կլինեն $n\times m$-չափանի, $m\times k$-չափանի և $n\times k$-չափանի: Ըստ սահմանման՝ $\varphi(e)=A\bullet f$, $\psi(f)=B\bullet g$, $(\varphi\cdot\psi)e=C\bullet g$, որտեղ

$$e=\begin{pmatrix}e_1\\ \vdots\\ e_n\end{pmatrix},\quad f=\begin{pmatrix}f_1\\ \vdots\\ f_m\end{pmatrix},\quad g=\begin{pmatrix}g_1\\ \vdots\\ g_k\end{pmatrix},\quad \varphi(e)=\begin{pmatrix}\varphi e_1\\ \vdots\\ \varphi e_n\end{pmatrix},$$

$$\psi(f)=\begin{pmatrix}\psi f_1\\ \vdots\\ \psi f_m\end{pmatrix},\quad (\varphi\cdot\psi)e=\begin{pmatrix}(\varphi\cdot\psi)e_1\\ \vdots\\ (\varphi\cdot\psi)e_n\end{pmatrix}=\begin{pmatrix}\psi(\varphi e_1)\\ \vdots\\ \psi(\varphi e_n)\end{pmatrix}=\psi(\varphi e)\ :$$

Ընդհանրապես, եթե $y=\begin{pmatrix}y_1\\ \vdots\\ y_n\end{pmatrix}$, ապա $\psi(y)=\begin{pmatrix}\psi y_1\\ \vdots\\ \psi y_n\end{pmatrix}$:
Մասնավորապես, $\psi(A\bullet f)=A\bullet\psi(f)$: Ուստի,

$$\psi(\varphi e)=C\bullet g\,,$$

$$\psi(A\bullet f)=C\bullet g\,,$$

$$A\bullet\psi(f)=C\bullet g\,,$$

$$A\bullet(B\bullet g)=C\bullet g\,,$$

$$(A\cdot B)\bullet g=C\bullet g\,,$$

և $A\cdot B=C$ (լեմմ 17.12): □

Տեսնենք, թե ինչ օրենքով է փոխվում գծային արտապատկերման մատրիցը՝ հենքերի փոփոխության դեպքում:

Թեորեմ 17.33: *Դիցուք $\varphi\in Hom(Q,S)$, որտեղ Q-ն P դաշտի վրա որոշված n-չափանի գծային տարածություն է $e_1,\ldots,e_n$ և $e_1',\ldots,e_n'$ հենքերով, իսկ S-ը P դաշտի վրա որոշված m-չափանի գծային տարածություն է $f_1,\ldots,f_m$ և $f_1',\ldots,f_m'$ հենքերով: Եթե*

$$\varphi(e)=A\bullet f\,,$$

$$\varphi(e') = B \bullet f' \,,$$
$$e' = T \bullet e \,,$$
$$f' = \Gamma \bullet f \,,$$

որտեղ $A, B \in P^{n\times m}$, $T \in P^{n\times n}$, $\Gamma \in P^{m\times m}$, $e = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$, $e' = \begin{pmatrix} e'_1 \\ \vdots \\ e'_n \end{pmatrix}$, $f = \begin{pmatrix} f_1 \\ \vdots \\ f_m \end{pmatrix}$, $f' = \begin{pmatrix} f'_1 \\ \vdots \\ f'_m \end{pmatrix}$, *ապա* $B = T \cdot A \cdot \Gamma^{-1}$*:*

Ապացուցում: Իրոք, ինչպես գիտենք, T և Γ մատրիցները հակադարձելի են: $\varphi(e') = \varphi(T \bullet e) = T \bullet \varphi(e) = T \bullet (A \bullet f) = (T \cdot A) \bullet f$: Մյուս կողմից, $\varphi(e') = B \bullet f' = B \bullet (\Gamma \bullet f) = (B \cdot \Gamma) \bullet f$: Հետևաբար $(B \cdot \Gamma) \bullet f = (T \cdot A) \bullet f$ և $B \cdot \Gamma = T \cdot A$ (լեմմ 17.12), որտեղից՝ $B = T \cdot A \cdot \Gamma^{-1}$: □

Ապացուցված թեորեմից նորից է բխում A և B մատրիցների ռանգերի հավասարությունը (թեորեմ 17.30):

Մասնավորապես, ստանում ենք գծային ձևափոխության մատրիցի փոփոխության հետևյալ օրենքը՝ հենքի փոփոխության դեպքում:

Հետևություն 17.30: *Դիցուք* $\varphi \in Hom(Q, Q)$, *որտեղ* Q*-ն* P *դաշտի վրա որոշված* n*-չափանի գծային տարածություն է* $e_1, \ldots, e_n$ *և* $e'_1, \ldots, e'_n$ *հենքերով: Եթե* $\varphi(e) = A \bullet e$, $\varphi(e') = B \bullet e'$, $e' = T \bullet e$, *որտեղ* $A, B, T \in P^{n\times n}$, *ապա* $B = T \cdot A \cdot T^{-1}$*:*

Ապացուցում: Բխում է նախորդ հատկությունից $f = e$, $f' = e'$ դեպքում: □

Երկու $A \in P^{n\times n}$ և $B \in P^{n\times n}$ մատրիցներ կոչվում են **նման** և գրվում է $A \sim B$, եթե գոյություն ունի այնպիսի $T \in P^{n\times n}$ հակադարձելի մատրից, որ $B = T \cdot A \cdot T^{-1}$: Այս «$\sim$» հարաբերությունը կոչվում է **մատրիցների նմանության հարաբերություն**:

Լեմմ 17.32: *Մատրիցների նմանության հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $A \sim A$ *ցանկացած* $A \in P^{n\times n}$ *մատրիցի համար;*

բ) $A \sim B \longrightarrow B \sim A$*;*

գ) $A \sim B$, $B \sim C \longrightarrow A \sim C$*:*

Ապացուցում: ա) Քանի որ $A = E \cdot A \cdot E^{-1}$, որտեղ E-ն n-րդ կարգի միավոր մատրիցն է, ապա $A \sim A$: բ) Եթե $A \sim B$, ապա $B = T \cdot A \cdot T^{-1}$ որևէ $T \in P^{n\times n}$ հակադարձելի մատրիցի համար: Հետևաբար, $A = T^{-1} \cdot B \cdot (T^{-1})^{-1}$: գ) Եթե $A \sim B$ և $B \sim C$, ապա գոյություն ունեն այնպիսի $T_1, T_2 \in P^{n\times n}$ հակադարձելի մատրիցներ, որ $B = T_1 \cdot A \cdot T_1^{-1}$, $C = T_2 \cdot A \cdot T_2^{-1}$: Հետևաբար, $C = T_2T_1AT_1^{-1}T_2^{-1} = (T_2T_1)A(T_2T_1)^{-1}$: □

Քանի որ նման մատրիցների որոշիչները հավասար են, ապա կարելի է ներմուծել հետևյալ հասկացությունը:

Եթե $dim(Q) = n > 0$, ապա $\varphi \in Hom(Q, Q)$ գծային **ձևափոխության որոշիչը** սահմանվում է որպես Q գծային տարածության ցանկացած $e_1, \ldots, e_n$ հենքում φ գծային ձևափոխության մատրիցի որոշիչ և նշանակվում է $det(\varphi)$-ով:

Քառակուսային $A \in P^{n\times n}$ **մատրիցի հետք** է կոչվում նրա գլխավոր անկյունագծի բոլոր տարրերի գումարը և նշանակվում է $tr(A)$-ով՝

$$tr(A) = a_{11} + a_{22} + \cdots + a_{nn} \in P\,,$$

որտեղ $A = (a_{ij})$ (trace – հետք):

Լեմմ 17.33: *$A \to tr(A)$ արտապատկերումը հանդիսանում է $P^{n\times n}$ գծային տարածության գծային ձև, այսինքն՝*

$$tr(A + B) = tr(A) + tr(B)\,,$$

$$tr(\lambda A) = \lambda\, tr(A)$$

ցանկացած $A, B \in P^{n\times n}$ մատրիցների և ցանկացած $\lambda \in P$ սկալյարի համար: □

Լեմմ 17.34: *Ցանկացած $A, B \in P^{n\times n}$ մատրիցների համար՝ $tr(A \cdot B) = tr(B \cdot A)$:*

Ապացուցում: Եթե $A = (a_{ij})$, $B = (b_{ij})$, $A \cdot B = C = (c_{ij})$, $B \cdot A = D = (d_{ij})$, ապա

$$c_{ii} = a_{i1}b_{1i} + a_{i2}b_{2i} + \cdots + a_{in}b_{ni}\,,$$

$$d_{ii} = b_{i1}a_{1i} + b_{i2}a_{2i} + \cdots + b_{in}a_{ni}\,,$$

որտեղ $i = 1, \ldots, n$: Հետևաբար,

$$tr(A \cdot B) = c_{11} + c_{22} + \cdots + c_{nn} =$$

$$= a_{11}b_{11} + a_{12}b_{21} + \cdots + a_{1n}b_{n1} + \cdots$$

$$+ a_{n1}b_{1n} + a_{n2}b_{2n} + \cdots + a_{nn}b_{nn} =$$

$$= b_{11}a_{11} + \cdots + b_{1n}a_{n1} + \cdots + b_{n1}a_{1n} + \cdots + b_{nn}a_{nn} =$$

$$= d_{11} + d_{22} + \cdots + d_{nn} = tr(B \cdot A) \ : \qquad \square$$

Թեորեմ 17.34: *Նման մատրիցների հետքերը հավասար են:*

Ապացույց: Օգտվենք վերջին լեմմից: Եթե $B = T \cdot A \cdot T^{-1}$, ապա

$$tr(B) = tr\left((TA)T^{-1}\right) = tr\left(T^{-1}(TA)\right) =$$

$$= tr\left(\left(T^{-1}T\right)A\right) = tr(EA) = tr(A) : \qquad \square$$

Հանգում ենք հետևյալ գաղափարին:

Եթե $dim(Q) = n > 0$, ապա $\varphi \in Hom(Q, Q)$ գծային **ձևափոխության հետքը** սահմանվում է որպես Q գծային տարածության ցանկացած $e_1, \ldots, e_n$ հենքում φ գծային ձևափոխության մատրիցի հետք և նշանակվում է $tr(\varphi)$-ով:

17.16. Գծային հանրահաշիվներ: Գծային հանրահաշիվների իզոմորֆիզմը: Քելիի թեորեմը զուգորդական և միավորով գծային հանրահաշիվների համար

Հաճախ անհրաժեշտություն է առաջանում դիտարկել այնպիսի գծային (վեկտորական) տարածություններ Q (որոշված տրված P դաշտի վրա), որտեղ բացի գումարման և սկալյարով բազմապատկման գործողություններից, առկա է նաև Q-ի վրա (մեջ) որոշված բազմապատկման գործողություն, որը կապված է Q-ի գումարման և սկալյարով բազմապատկման գործողությունների հետ հետևյալ բնական նույնություններով՝

$$x(y+z) = xy + xz, \quad (y+z)x = yx + zx,$$

$$(\alpha x) \cdot y = x \cdot (\alpha y) = \alpha(x \cdot y)$$

ցանկացած $x, y, z \in Q$ տարրերի և ցանկացած $\alpha \in P$ սկալյարի համար: Հանգում ենք հետևյալ բնական գաղափարին:

$Q(+,\cdot)$ օղակը կոչվում է **գծային հանրահաշիվ**՝ որոշված P դաշտի վրա (նկատմամբ), եթե $Q(+)$-ը գծային տարածություն է որոշված P-ի վրա և բոլոր $x, y \in Q$ տարրերի և ցանկացած $\alpha \in P$ սկալյարի համար տեղի ունի

$$\alpha(x \cdot y) = (\alpha x) \cdot y = x \cdot (\alpha y)$$

հավասարությունը: Այս դեպքում Q բազմությունը կոչվում է նաև գծային հանրահաշիվ՝ որոշված P դաշտի վրա:

Օրինակ, P դաշտի տարրերով (այսինքն P-ի վրա որոշված) n-րդ կարգի բոլոր մատրիցների $P^{n\times n}$ բազմությունը գծային հանրահաշիվ է որոշված P դաշտի վրա, $P[x]$ բազմանդամների բազմությունը նույնպես: Կոմպլեքս թվերի $\mathbb{C}$ բազմությունը գծային հանրահաշիվ է՝ որոշված իրական թվերի $\mathbb{R}$ դաշտի վրա: Ընդհանուր դեպքում, եթե P դաշտը Q դաշտի ենթադաշտն է, ապա Q-ն կլինի գծային հանրահաշիվ՝ որոշված P դաշտի վրա:

Լեմմ 17.35: *Եթե Q -ն գծային տարածություն է որոշված P դաշտի վրա, ապա Q-ի բոլոր գծային ձևափոխությունների*

$$Hom(Q,Q) = \{\varphi : Q \to Q | \ \varphi\text{-ն գծային արտապատկերում է}\}$$

գծային տարածությունը կդառնա գծային հանրահաշիվ՝ որոշված P-ի վրա, եթե սահմանենք նաև $\varphi_1 \cdot \varphi_2$ արտադրյալը որպես արտապատկերումների արտադրյալ՝

$$(\varphi_1 \cdot \varphi_2)(x) = \varphi_2(\varphi_1 x),$$

որտեղ $x \in Q$, $\varphi_1, \varphi_2 \in Hom(Q,Q)$:

Ապացուցում: Իրոք, ինչպես գիտենք $Hom(Q,Q)$-ն գծային տարածություն է հետևյալ գործողությունների նկատմամբ՝

$$(\varphi_1 + \varphi_2)(x) = \varphi_1(x) = +\varphi_2(x),$$

$$(\alpha\varphi)(x) = \alpha\varphi(x),$$

որտեղ $x \in Q$, $\varphi, \varphi_1, \varphi_2 \in Hom(Q,Q)$: Հայտնի է նաև, որ $\varphi_1 \cdot \varphi_2 \in Hom(Q,Q)$, եթե $\varphi_1, \varphi_2 \in Hom(Q,Q)$: Այնուհետև,

$$(\alpha(\varphi_1 \cdot \varphi_2))(x) = \alpha((\varphi_1 \cdot \varphi_2)(x)) = \alpha(\varphi_2(\varphi_1(x))),$$

$$((\alpha\varphi_1)\cdot\varphi_2)(x) = \varphi_2((\alpha\varphi_1)(x)) = \varphi_2(\alpha(\varphi_1(x))) = \alpha(\varphi_2(\varphi_1(x))),$$

$$(\varphi_1\cdot(\alpha\varphi_2))(x) = (\alpha\varphi_2)(\varphi_1(x)) = \alpha(\varphi_2(\varphi_1(x)))$$

ցանկացած $x \in Q$ տարրի համար:

Հետևաբար,

$$\alpha(\varphi_1\cdot\varphi_2) = (\alpha\varphi_1)\cdot\varphi_2 = \varphi_1\cdot(\alpha\varphi_2)$$

ցանկացած $\alpha \in P$ սկալյարի և ցանկացած $\varphi_1, \varphi_2 \in Hom(Q,Q)$ գծային ձևափոխությունների համար: Հեշտությամբ ստուգվում են նաև՝

$$(\varphi_1+\varphi_2)\cdot\varphi_3 = \varphi_1\varphi_3 + \varphi_2\varphi_3,$$

$$\varphi_1(\varphi_2+\varphi_3) = \varphi_1\varphi_2 + \varphi_1\varphi_3$$

հավասարությունները՝ ցանկացած $\varphi_1, \varphi_2, \varphi_3 \in Hom(Q,Q)$ գծային ձևափոխությունների համար: □

Գծային հանրահաշիվը կոչվում է n-չափանի, եթե այն որպես գծային տարածություն n-չափանի է ($n \geqslant 0$):

Գծային հանրահաշիվը կոչվում է՝

ա) վերջավոր չափանի, եթե այն որպես գծային տարածություն վերջավոր չափանի է;

բ) զրոյական, եթե այն որպես գծային տարածություն զրոյական է, այսինքն մեկ տարրանի է: Հակառակ դեպքում, գծային հանրահաշիվը կոչվում է ոչ զրոյական;

գ) զուգորդական, եթե այն որպես օղակ զուգորդական է;

դ) միավորով (օժտված), եթե այն որպես օղակ միավորով (օժտված) օղակ է:

Դիցուք Q-ն գծային հանրահաշիվ է որոշված P դաշտի վրա: Ոչ դատարկ $H \subseteq Q$ ենթաբազմությունը կոչվում է Q գծային հանրահաշվի ենթահանրահաշիվ, եթե այն Q-ի ենթատարածություն է և ենթաօղակ: Հետևաբար, գծային հանրահաշվի ենթահանրահաշիվը նաև կլինի գծային հանրահաշիվ:

Q գծային հանրահաշվի H ենթահանրահաշիվը կոչվում է Q-ի աջ (ձախ) իդեալ, եթե ցանկացած $a \in H$ և ցանկացած $b \in Q$ տարրերի համար $a\cdot b \in H$ (համապատասխանաբար $b\cdot a \in H$): H ենթահանրահաշիվը կոչվում է Q-ի իդեալ և նշանակվում է $H \trianglelefteq Q$, եթե այն միաժամանակ Q-ի ձախ և աջ իդեալ է: Դիցուք $H_1 \trianglelefteq Q$ և $H_2 \trianglelefteq Q$:

Սահմանենք՝

$$H_1 + H_2 = \{x + y \,|\, x \in H_1, y \in H_2\},$$

$$H_1 - H_2 = \{x - y \,|\, x \in H_1, y \in H_2\},$$

Հեշտությամբ ստուգվում է, որ $H_1 - H_2 = H_1 + H_2 \trianglelefteq Q$ և $H_1 \cap H_2 \trianglelefteq Q$:

Եթե $H \trianglelefteq Q$, ապա

$$Q/\,H = \{x + H \,|\, x \in Q\}$$

քանորդ-տարածությունը վերածվում է գծային հանրահաշվի՝ սահմանելով.

$$(x + H) \cdot (y + H) = (x \cdot y) + H, \quad x, y \in Q :$$

Հաճախ $(x \cdot y)$-ի փոխարեն, ինչպես և օղակներում, համառոտ գրվում է xy: Նախ նկատենք, որ այս հավասարությամբ իրոք սահմանվում է գործողություն, այսինքն բազմապատկման արդյունքը կախված չէ արտադրիչներում ներկայացուցիչների ընտրությունից՝

$$x + H = x' + H, \;\; y + H = y' + H \longrightarrow (x \cdot y) + H = (x' \cdot y') + H,$$

որտեղ $x, x', y, y' \in Q$:

Իրոք, $x' = x + h_1$, $y' = y + h_2$, որտեղ $h_1, h_2 \in H$: Հետևաբար,

$$x' \cdot y' = (x + h_1) \cdot (y + h_2) = xy + xh_2 + h_1 y + h_1 h_2 :$$

Իդեալի սահմանման համաձայն՝ $xh_2 + h_1 y + h_1 h_2 = h$ տարրը պատկանում է H-ին: Այնուհետև, $x'y' - xy = h$ և հետևաբար՝

$$(x' \cdot y') + H = (x \cdot y) + H$$

համաձայն գծային տարածություններում ապացուցված՝ հարակից դասերի հավասարության հայտանիշի:

Մնում է ստուգել սահմանված բազմապատկման գործողության հետ կապված գծային հանրահաշվի պայմանները (նույնությունները)՝

$$(x + H)((y + H) + (z + H)) = (x + H)(y + H) + (x + H)(z + H),$$

$$((y + H) + (z + H))(x + H) = (y + H)(x + H) + (z + H)(x + H),$$

$$\alpha((x+H)(y+H)) = (\alpha(x+H))(y+H) = (x+H)(\alpha(y+H))$$

ցանկացած $x, y, z \in Q$ և ցանկացած $\alpha \in P$ տարրերի համար: Ստացված $Q/_H$ գծային հանրահաշիվը կոչվում է Q գծային հանրահաշվի քանորդ-հանրահաշիվ կամ ֆակտոր-հանրահաշիվ ըստ $H \trianglelefteq Q$ իդեալի:

Դիցուք Q-ն և Q'-ը կամայական երկու գծային հանրահաշիվներ են՝ որոշված միևնույն P դաշտի վրա: $\varphi : Q \to Q'$ արտապատկերումը կոչվում է **գծային արտապատկերում՝** Q **գծային հանրահաշվից** Q' **գծային հանրահաշիվի մեջ**, կամ համառոտ՝ գծային հանրահաշիվների գծային արտապատկերում, եթե

$$\varphi(x+y) = \varphi(x) + \varphi(y),$$

$$\varphi(\alpha x) = \alpha\varphi(x),$$

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

ցանկացած $x, y \in Q$ տարրերի և ցանկացած $\alpha \in P$ սկալյարի համար: Օրինակ, $\pi(x) = x + H$ բնական արտապատկերումը կլնի գծային արտապատկերում Q գծային հանրահաշվից $Q/_H$ քանորդ-հանրահաշվի մեջ, որտեղ $H \trianglelefteq Q$: Հեշտությամբ ապացուցվում է, որ երկու (հետևաբար և վերջավոր թվով) գծային արտապատկերումների արտադրյալը նորից գծային արտապատկերում է (եթե այն գոյություն ունի):

Ինչպես և գծային տարածությունների դեպքում՝

$$Im(\varphi) = \{\varphi(x) \,|\, x \in Q\} = \varphi(Q) \subseteq Q'$$

ենթաբազմությունը կոչվում է φ գծային **արտապատկերման պատկեր**, իսկ

$$Ker(\varphi) = \{x \in Q \,|\, \varphi(x) = 0\} \subseteq Q$$

ոչ դատարկ ենթաբազմույունը կոչվում է φ գծային **արտապատկերման միջուկ**: Սակայն այժմ հեշտությամբ ապացուցվում է ավելին, որ

1) $Im(\varphi)$-ն Q' գծային հանրահաշվի ենթահանրահաշիվ է;

2) $Ker(\varphi)$-ն Q գծային հանրահաշվի իդեալ է:

Գծային հանրահաշիվների $\varphi : Q \to Q'$ գծային արտապատկերումը կոչվում է գծային հանրահաշիվների **իզոմորֆիզմ** կամ **նույնաձևություն**, եթե φ-ն նաև բիեկտիվ (փոխմիարժեք) արտապատկերում է: Եթե

$\varphi : Q \to Q'$ արտապատկերումները գծային հանրահաշիվների նույնաձևություն է, ապա $\varphi^{-1} : Q' \to Q$ արտապատկերումը ևս կլինի այդպիսին: Երկու (հետևաբար և վերջավոր թվով) նույնաձևությունների արտադրյալը նորից նույնաձևություն է (եթե այն գոյություն ունի):

Երկու Q և Q' գծային հանրահաշիվներ կոչվում են **իզոմորֆ** կամ **նույնաձև** և գրվում է $Q \simeq Q'$ (կամ $Q \cong Q'$), եթե գոյություն ունի որևէ $\varphi : Q \to Q'$ իզոմորֆիզմ (նույնաձևություն): Այս «$\simeq$» (կամ «$\cong$») հարաբերությունը կոչվում է գծային հանրահաշիվների **իզոմորֆության** կամ **նույնաձևության** հարաբերություն:

Լեմմ 17.36: *Գծային հանրահաշիվների նույնաձևություն (իզոմորֆություն) հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $Q \simeq Q$ ցանկացած Q գծային հանրահաշվի համար;

բ) $Q \simeq Q' \to Q' \simeq Q$;

գ) $Q \simeq Q'$, $Q' \simeq Q'' \to Q \simeq Q''$: □

Հետևյալ արդյունքների օգնությամբ բացահայտվում են գծային արտապատկերումների միջուկի և պատկերի կապը՝ գծային հանրահաշիվների դեպքում:

Թեորեմ 17.35: *Դիցուք Q-ն և Q'-ը կամայական գծային հանրահաշիվներ են: Այդ դեպքում, գծային հանրահաշիվների յուրաքանչյուր վերադրող (սյուրեկտիվ) $\varphi : Q \to Q'$ գծային արտապատկերման համար՝ $Q' \simeq Q/_H$, որտեղ $H = Ker(\varphi)$: Ավելի ճշգրիտ, յուրաքանչյուր վերադրող (սյուրեկտիվ) $\varphi : Q \to Q'$ գծային արտապատկերման համար, որտեղ $Ker(\varphi) = H$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\mu : Q' \to Q/_H$ իզոմորֆիզմ (նույնաձևություն), որ $\varphi \cdot \mu = \pi$, այսինքն՝ տեղափոխական է գծային արտապատկերումների հետևյալ եռանկյունը՝*

$$\begin{tikzcd}
Q \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & Q' \arrow[d, "\mu"] \\
 & Q/_H
\end{tikzcd},$$

որտեղ π-ն բնական արտապատկերում է $(\pi(x) = x + H)$:

Ապացուցում: Գծային տարածությունների գծային արտապատկերումների վերաբերյալ ապացուցված համապատասխան թեորեմի ապացույցին մնում է միայն ավելացնել հետևյալ հավասարությունը՝

$$\mu(x' \cdot y') = \mu(x') \cdot \mu(y')$$

ցանկացած $x', y' \in Q'$ տարրերի համար:

Դիցուք $x' = \varphi(x)$, $y' = \varphi(y)$, որտեղ $x, y \in Q$: Այդ դեպքում, $x' \cdot y' = \varphi(x) \cdot \varphi(y) = \varphi(x \cdot y)$: Հետևաբար,

$$\mu(x' \cdot y') = (x \cdot y) + H = (x + H) \cdot (y + H) = \mu(x') \cdot \mu(y') : \qquad \square$$

Թեորեմ 17.36: *Դիցուք Q-ն, Q_1-ը և Q_2-ը կամայական գծային հանրահաշիվներ են: Այդ դեպքում, գծային հանրահաշիվների ցանկացած վերադրող (սյուրեկտիվ) $\varphi_1 : Q \to Q_1$ և $\varphi_2 : Q \to Q_2$ գծային արտապատկերումների համար, որտեղ $Ker(\varphi_1) \subseteq Ker(\varphi_2)$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\varphi_3 : Q_1 \to Q_2$ վերադրող գծային արտապատկերում, որ $\varphi_1 \cdot \varphi_3 = \varphi_2$, այսինքն՝ տեղափոխական է գծային արտապատկերումների հետևյալ եռանկյունը՝*

$$\begin{tikzcd} Q \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & Q_1 \arrow[d, "\varphi_3"] \\ & Q_2 \end{tikzcd} \quad :$$

Ըստ որում, φ_3-ը կլինի նույնածնություն (իզոմորֆիզմ) այն և միայն այն դեպքում, երբ $Ker(\varphi_1) = Ker(\varphi_2)$:

Ապացուցում: Տես գծային տարածությունների գծային արտապատկերումների վերաբերյալ համապատասխան թեորեմի ապացուցումը: $\square$

Այժմ բնութագրենք Q գծային տարածության բոլոր գծային ձևափոխությունների $Hom(Q, Q)$ գծային հանրահաշիվը՝ իզոմորֆիզմի ճշտությամբ, եթե Q-ն վերջավոր չափանի գծային տարածություն է: Եթե

Q-ն զրոյական գծային տարածություն է, այսինքն՝ $dim(Q) = 0$, ապա ակնհայտ է, որ $Hom(Q, Q)$ գծային հանրահաշիվը ևս կլինի զրոյական, իսկ n-չափանի Q գծային տարածության համար տեղի ունի հետևյալ արդյունքը, եթե $n \geqslant 1$:

Թեորեմ 17.37: *Եթե Q-ն $e_1, \ldots, e_n$ հենքով n-չափանի գծային տարածություն է՝ որոշված P դաշտի վրա, ապա*

$$\Phi \,:\, \varphi \longrightarrow (\varphi_e^e)$$

արտապատկերումը կլինի նույնածնություն (իզոմորֆիզմ) $Hom(Q, Q)$ և $P^{n\times n}$ գծային հանրահաշիվների միջև, այսինքն՝

$$Hom(Q, Q) \simeq P^{n\times n} \,:$$

Ապացուցում: Բխում է նախորդ վերնագրի արդյունքներից: □

Հաջորդ արդյունքը կոչվում է Քելիի թեորեմ՝ զուգորդական և միավորով (օժտված) գծային հանրահաշիվների համար, որում իզոմորֆիզմի ճշտությամբ բնութագրվում է կամայական վերջավոր չափանի զուգորդական և միավորով (օժտված) գծային հանրահաշիվ:

Թեորեմ 17.38 (Քելի): *P դաշտի վրա որոշված յուրաքանչյուր զուգորդական և միավորով (օժտված) n-չափանի գծային հանրահաշիվ իզոմորֆ է n-րդ կարգի մատրիցների $P^{n\times n}$ գծային հանրահաշվի որևէ ենթահանրահաշվի:*

Ապացուցում: Դիցուք Q-ն n-չափանի գծային հանրահաշիվ է՝ որոշված P դաշտի վրա: Յուրաքանչյուր $a \in Q$ տարրի համար սահմանենք $\varphi_a \in Hom(Q, Q)$ արտապատկերումը՝ հետևյալ կերպ.

$$\varphi_a(x) = x \cdot a, \quad x \in Q \,:$$

Հեշտությամբ ստուգվում է, որ

$$\varphi_Q = \{\varphi_a \mid a \in Q\} \subseteq Hom(Q, Q)$$

ենթաբազմությունը կլինի $Hom(Q, Q)$ գծային հանրահաշվի ենթահանրահաշիվ, իսկ $\Phi \,:\, a \to \varphi_a$ արտապատկերումը կլինի Q և φ_Q գծային հանրահաշիվների իզոմորֆիզմ: Մնում է օգտվել նախորդ թեորեմից: □

Կասենք, որ Q գծային հանրահաշիվը ներդրվում է Q' գծային հանրահաշվի մեջ, եթե գոյություն ունի գծային հանրահաշիվների որևէ ներդրող (ինյեկտիվ) $\varphi : Q \to Q'$ գծային արտապատկերում:

Վերջին թեորեմը կարելի է վերաձևակերպել հետևյալ կերպ:

Թեորեմ 17.39 (Քելի): *P դաշտի վրա որոշված յուրաքանչյուր զուգորդական և միավորով (օժտված) n-չափանի գծային հանրահաշիվ ներդրվում է n-րդ կարգի մատրիցների $P^{n\times n}$ գծային հանրահաշվի մեջ:* □

17.17. Երկգծային ձևեր: Երկգծային ձևի մատրից և ռանգ

Դիցուք Q-ն գծային տարածություն է՝ որոշված P դաշտի վրա, իսկ

$$Q \times Q = \{(x, y) \,|\, x, y \in Q\} \ :$$

Եթե $f : Q \times Q \to P$ արտապատկերման դեպքում՝ $f : (x, y) \to z$, ապա գրվում է $f(x, y) = z$, որտեղ $x, y \in Q$, $z \in P$: $f(x, y)$ արտահայտության մեջ x-ը կոչվում է նաև առաջին արգումենտ (կոորդինատ), իսկ y-ը՝ երկրորդ: $f : Q \times Q \to P$ արտապատկերումը (ֆունկցիան) կոչվում է Q գծային տարածության **երկգծային ձև**, եթե f-ը գծային է իր յուրաքանչյուր արգումենտի նկատմամբ, այսինքն՝

ա) $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$, $f(\alpha x, y) = \alpha f(x, y)$,

բ) $f(x, y_1 + y_2) = f(x, y_1) + f(x, y_2)$, $f(x, \alpha y) = \alpha f(x, y)$,

որտեղ $x, y, x_1, x_2, y_1, y_2 \in Q$, $\alpha \in P$: Սահմանման ա) պայմանը կարելի է փոխարինել

$$f(\alpha x_1 + \beta x_2, y) = \alpha f(x_1, y) + \beta f(x_2, y)$$

պայմանով, իսկ բ) պայմանը՝

$$f(x, \alpha y_1 + \beta y_2) = \alpha f(x, y_1) + \beta f(x, y_2)$$

պայմանով, որտեղ $x, y, x_1, x_2, y_1, y_2 \in Q$, $\alpha, \beta \in P$: Սահմանումից բխում է, որ $f(0, y) = f(x, 0) = 0$, $f(-x, y) = f(x, -y) = -f(x, y)$, իսկ վերիանգման եղանակով ապացուցվում են նաև հետևյալ

$$f(x_1 + \cdots + x_n, y) = f(x_1, y) + \cdots + f(x_n, y)\,,$$

$$f(x, y_1 + \cdots + y_n) = f(x, y_1) + \cdots + f(x, y_n)$$

հավասարությունները՝ ցանկացած $x, y, x_1, \ldots, x_n, y_1, \ldots, y_n \in Q$ տարրերի համար:

$P = \mathbb{R}$ դեպքում երկգծային ձևը կոչվում է **իրական**, իսկ $P = \mathbb{C}$ դեպքում՝ **կոմպլեքս**:

Միևնույն Q գծային տարածության երկու f և g երկգծային ձևեր կոչվում են հավասար և գրվում է $f = g$, եթե $f(x, y) = g(x, y)$ ցանկացած $x, y \in Q$ տարրերի համար:

Օրինակներ: 1) $f(x, y) = 0$ $(x, y \in Q)$ հավասարությունով որոշվող ֆունկցիան կլինի երկգծային ձև ցանկացած Q գծային տարածության համար: Այս երկգծային ձևը կոչվում է **զրոյական**: Հակառակ դեպքում, երկգծային ձևը կոչվում է **ոչ զրոյական**:

2) Հարթության բոլոր երկրաչափական վեկտորների գծային տարածության համար՝

$$f\left(\bar{a}, \bar{b}\right) = |\bar{a}|\,|\bar{b}| \cos\left(\widehat{\bar{a}, \bar{b}}\right)$$

սկալյար արտադրյալը երկգծային ձև է:

3) $Q = P_2$ գծային տարածության համար՝

$$f\left((\alpha_1, \alpha_2), (\beta_1, \beta_2)\right) = det\begin{pmatrix} \alpha_1, & \alpha_2 \\ \beta_1, & \beta_2 \end{pmatrix} \in P$$

օրենքով որոշվող ֆունկցիան կլինի երկգծային ձև:

4) $Q = C[a, b]$ գծային տարածության համար՝

$$f(f_1, f_2) = \int\limits_a^b g(x) f_1(x) f_2(x)\, dx$$

օրենքով որոշվող ֆունկցիան կլինի երկգծային ձև (այստեղ $g \in C[a, b]$ ֆունկցիան սևեռված է և կոչվում է **ինտեգրալային կորիզ**):

5) $Q = P^{n \times n}$ գծային տարածության համար՝

$$f(A, B) = tr(A \cdot B) \in P$$

օրենքով որոշված ֆունկցիան կլինի երկգծային ձև:

Լեմմ 17.37: *P դաշտի վրա որոշված Q գծային տարածության բոլոր երկգծային ձևերի բազմությունը գծային տարածություն է որոշված* *նույն դաշտի վրա՝ երկգծային ձևերի հետևյալ գումարման և սկալյարով բազմապատկման նկատմամբ.*

$$(f+g)(x,y) = f(x,y) + g(x,y)\,,$$

$$(\lambda f)(x,y) = \lambda f(x,y)$$

ցանկացած $x, y \in Q$ տարրերի և ցանկացած $\lambda \in P$ սկալյարի համար: □

Այս գծային տարածությունը կոչվում է Q գծային տարածության **երկգծային ձևերի տարածություն** և նշանակվում է $Hom(Q,Q;P)$-ով: Եթե Q գծային տարածությունը զրոյական է, ապա ակնհայտ է, որ նրա երկգծային ձևերի $Hom(Q,Q;P)$ տարածությունը ևս կլինի զրոյական:

Թեորեմ 17.40: *n-չափանի Q գծային տարածության երկգծային ձևերի $Hom(Q,Q;P)$ տարածությունը կլինի n^2-չափանի:*

Ապացուցում: $n = 0$ դեպքում պնդումն ակնհայտ է: Դիցուք $dim(Q) = n > 0$ և դիցուք $e_1, \ldots, e_n$ համակարգը Q-ի հենք է: Եթե $x, y \in Q$ և $x = x_1e_1 + \cdots + x_ne_n$, $y = y_1e_1 + \cdots + y_ne_n$, ապա ցանկացած f երկգծային ձևի համար կունենանք՝

$$f(x,y) = f\left(x_1e_1 + \cdots + x_ne_n, y_1e_1 + \cdots + y_ne_n\right) =$$

$$f\left(x_1e_1, y_1e_1 + \cdots + y_ne_n\right) + \cdots + f\left(x_ne_n, y_1e_1 + \cdots + y_ne_n\right) =$$

$$= f\left(x_1e_1, y_1e_1\right) + \cdots + f\left(x_1e_1, y_ne_n\right) +$$

$$\cdots + f\left(x_ne_n, y_1e_1\right) + \cdots + f\left(x_ne_n, y_ne_n\right) =$$

$$= x_1y_1f\left(e_1,e_1\right) + \cdots + x_1y_nf\left(e_1,e_n\right) + \cdots$$

$$+x_ny_1f\left(e_n,e_1\right) + \cdots + x_ny_nf\left(e_n,e_n\right) =$$

$$= \sum_{i,j=1}^{n} x_iy_jf(e_i,e_j) = \sum_{i,j=1}^{n} x_iy_ja_{ij}\,, \qquad (17.21)$$

որտեղ $a_{ij} = f(e_i, e_j)$, $i,j = 1, \ldots, n$: Այս հավասարությունը կոչվում է f երկգծային ձևի **ներկայացում** $e_1, \ldots, e_n$ հենքի նկատմամբ (հենքում): Ներմուծելով հետևյալ երկգծային ձևերը՝

$$\ell_{ij}(x,y) = x_iy_j\,,$$

որտեղ $i, j = 1, \ldots, n$, $x = x_1e_1 + \cdots + x_ne_n$, $y = y_1e_1 + \cdots + y_ne_n$, կունենանք՝

$$f(x, y) = \sum_{i,j=1}^{n} a_{ij}\ell_{ij}(x, y)\,,$$

այսինքն՝

$$f = \sum_{i,j=1}^{n} a_{ij}\ell_{ij}\ :$$

Մնում է ապացուցել, որ ℓ_{ij} երկգծային ձևերի համակարգը գծայնորեն անկախ է: Իրոք, եթե

$$\alpha_{11}\ell_{11} + \alpha_{12}\ell_{12} + \cdots + \alpha_{nn}\ell_{nn} = 0\,,$$

ապա

$$\alpha_{11}\ell_{11}(x, y) + \alpha_{12}\ell_{12}(x, y) + \cdots + \alpha_{nn}\ell_{nn}(x, y) = 0$$

ցանկացած $x, y \in Q$ տարրերի համար: Այստեղ վերցնելով $x = e_i$, $y = e_j$, նախ կստանանք՝

$$\ell_{ks}(e_i, e_j) = \begin{cases} 1\,, & \text{եթե}\ \ k = i, s = j, \\ 0\,, & \text{հակառակ դեպքում :} \end{cases}$$

Հետևաբար, $\alpha_{ij} \cdot 1 = 0$, որտեղ 1-ը դաշտի միավորն է: Ուստի, $\alpha_{ij} = 0$ բոլոր $i, j = 1, \ldots, n$ արժեքների դեպքում: Այսպիսով, $\ell_{11}, \ldots, \ell_{1n}, \ldots, \ell_{n1}, \ldots, \ell_{nn}$ համակարգը հենք է Q-ի երկգծային ձևերի տարածության համար, այսինքն՝ Q-ի երկգծային ձևերի տարածությունը կլինի n^2-չափանի: $\square$

(17.21) հավասարության a_{ij} գործակիցներից կազմված

$$A = \begin{pmatrix} a_{11}, \ldots, a_{1n} \\ \ldots\ \ \ldots\ \ \ldots \\ a_{n1}, \ldots, a_{nn} \end{pmatrix} \in P^{n\times n}$$

մատրիցը կոչվում է f **երկգծային ձևի** մատրից՝ $e_1, \ldots, e_n$ հենքի նկատմամբ կամ f երկգծային ձևի **Գրամի մատրից**:

Եթե մեկ տարրանի մատրիցը նույնականացնենք իր տարրի հետ և նշանակենք՝

$$X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \quad Y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix},$$

ապա (17.21) հավասարությունը կարելի է գրել հետևյալ տեսքով՝

$$f(x,y) = X^T AY \ :$$

Վերցնենք Q-ի մեկ այլ հենք՝ $e_1', \ldots, e_n'$ և դիցուք

$$\begin{aligned} e_1' &= t_{11}e_1 + \cdots + t_{1n}e_n \,, \\ \ldots \ \ldots & \ \ldots \ \ldots \\ e_n' &= t_{n1}e_1 + \cdots + t_{nn}e_n \,, \end{aligned}$$

իսկ

$$\begin{aligned} x &= x_1'e_1' + \cdots + x_n'e_n' \,, \\ y &= y_1'e_1' + \cdots + y_n'e_n' \ : \end{aligned}$$

Նշանակենք $e_1, \ldots, e_n$ հենքից $e_1', \ldots, e_n'$ հենքին անցման մատրիցը՝

$$\Gamma = \begin{pmatrix} t_{11}, \ldots, t_{1n} \\ \ldots \ \ldots \ \ldots \\ t_{n1}, \ldots, t_{nn} \end{pmatrix}$$

և որոշենք f երկգծային ձևի $A' = \left(a_{ij}'\right)$ մատրիցը $e_1', \ldots, e_n'$ հենքի նկատմամբ:

$$f(x,y) = \sum_{i,j=1}^{n} x_i'y_j' f\left(e_i', e_j'\right) = \sum_{i,j=1}^{n} x_i'y_j'a_{ij}' \,,$$

որտեղ

$$\begin{aligned} a_{ij}' = f\left(e_i', e_j'\right) &= f\left(t_{i1}e_1 + \cdots + t_{in}e_n, t_{j1}e_1 + \cdots + t_{jn}e_n\right) = \\ &= t_{i1}t_{j1}f(e_1,e_1) + \cdots + t_{i1}t_{jn}f(e_1,e_n) + \cdots \\ &+ t_{in}t_{j1}f(e_n,e_1) + \cdots + t_{in}t_{jn}f(e_n,e_n) = \\ &= t_{i1}t_{j1}a_{11} + \cdots + t_{i1}t_{jn}a_{1n} + \cdots + t_{in}t_{j1}a_{n1} + \cdots + t_{in}t_{jn}a_{nn} = \\ &= t_{i1}\left(a_{11}t_{j1} + \cdots + a_{1n}t_{jn}\right) + \cdots + t_{in}\left(a_{n1}t_{j1} + \cdots + a_{nn}t_{jn}\right) \,; \end{aligned}$$

Հետևաբար՝

$$\begin{pmatrix} a_{11}', \ldots, a_{1n}' \\ \ldots \ \ldots \ \ldots \\ a_{n1}', \ldots, a_{nn}' \end{pmatrix} = \Gamma A \Gamma^T \ :$$

Հանգում ենք հետևյալ արդյունքին.

Թեորեմ 17.41: *Եթե A-ն Q գծային տարածության f երկգծային ձևի մատրիցն է $e_1, \ldots, e_n$ հենքի նկատմամբ, ապա $e_1', \ldots, e_n'$ հենքի նկատմամբ f-ի ունեցած A' մատրիցը որոշվում է հետևյալ կերպ՝*

$$A' = \Gamma A \Gamma^T \,,$$

որտեղ Γ-ն $e_1, \ldots, e_n$ հենքից $e_1', \ldots, e_n'$ հենքին անցման հակադարձելի մատրիցն է: □

Քանի որ A և $\Gamma A \Gamma^T$ մատրիցների ռանգերը հավասար են (որովհետև Γ և Γ^T մատրիցները հակադարձելի են (հետևություն 17.9)), ապա հանգում ենք երկգծային ձևի ռանգի հետևյալ գաղափարին:

Q գծային տարածության f **երկգծային ձևի ռանգ** ասելով հասկացվում է Q-ի ցանկացած հենքի նկատմամբ նրա ունեցած մատրիցի ռանգը և նշանակվում է $rank(f)$-ով:

Երկու $A, B \in P^{n \times n}$ մատրիցներ կոչվում են **կոնգրուենտ** և գրվում է $A \approx B$, եթե գոյություն ունի այնպիսի $\Gamma \in P^{n \times n}$ հակադարձելի մատրից, որ

$$B = \Gamma A \Gamma^T \,,$$

որտեղ Γ^T-ն Γ-ի շրջված մատրիցն է: Այս «$\approx$» հարաբերությունը կոչվում է **մատրիցների կոնգրուենտության հարաբերություն**:

Լեմմ 17.38: *Մատրիցների կոնգրուենտության հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $A \approx A$ ցանկացած $A \in P^{n \times n}$ մատրիցի համար;

բ) $A \approx B \longrightarrow B \approx A$;

գ) $A \approx B$, $B \approx C \longrightarrow A \approx C$: □

Հանրահաշվի կիրառություններում հաճախ հանդիպում է նաև հետևյալ ավելի ընդհանուր գաղափարը:

Դիցուք Q_1-ը, Q_2-ը և Q-ն միևնույն P դաշտի վրա որոշված գծային տարածություններ են, իսկ

$$Q_1 \times Q_2 = \{(x, y) \,|\, x \in Q_1, y \in Q_2\} \,:$$

Եթե $f : Q_1 \times Q_2 \to Q$ արտապատկերման դեպքում՝ $f : (x, y) \to z$, ապա գրվում է $z = f(x, y)$, որտեղ $x \in Q_1$, $y \in Q_2$, $z \in Q$: $f(x, y)$ արտահայտության մեջ x-ը կոչվում է f-ի առաջին արգումենտ, իսկ y-ը՝ երկրորդ: $f : Q_1 \times Q_2 \to Q$ արտապատկերումը (ֆունկցիան) կոչվում է

Q_1, Q_2, Q գծային տարածությունների **երկգծային արտապատկերում**, եթե f-ը գծային է իր յուրաքանչյուր արգումենտի նկատմամբ: Եթե $Q_1 = Q_2 = Q$, ապա Q_1, Q_2, Q գծային տարածությունների f երկգծային արտապատկերումը կընդունի հետևյալ տեսքը՝ $f : Q \times Q \to Q$: Այս դեպքում f-ը կոչվում է Q գծային տարածության **երկգծային ձևափոխություն**: Q_1, Q_2, Q գծային տարածությունների բոլոր երկգծային արտապատկերումների բազմությունը նշանակվում է $Hom(Q_1, Q_2; Q)$-ով, իսկ Q գծային տարածության բոլոր երկգծային ձևափոխությունների բազմությունը՝ $Hom(Q, Q; Q)$-ով:

Եթե $Q_1 = Q_2$, իսկ $Q = P$, ապա երկգծային արտապատկերման գաղափարը հանգում է երկգծային ձևի հասկացությանը:

Թեորեմ 17.42: *1) Միևնույն P դաշտի վրա որոշված Q_1, Q_2, Q գծային տարածությունների բոլոր երկգծային արտապատկերումների $Hom(Q_1, Q_2; Q)$ բազմությունը և Q գծային տարածության բոլոր երկգծային ձևափոխությունների $Hom(Q, Q; Q)$ բազմությունը գծային տարածություններ են (որոշված նույն P դաշտի վրա)՝ երկգծային արտապատկերումների հետևյալ գումարման և սկալյարով բազմապատկման նկատմամբ.*

$$(f + g)(x, y) = f(x, y) + g(x, y),$$

$$(\lambda f)(x, y) = \lambda f(x, y) :$$

2) Եթե Q_1, Q_2, Q գծային տարածությունները վերջավոր չափանի են, ապա այդպիսին կլինի նաև $Hom(Q_1, Q_2; Q)$ գծային տարածությունը և

$$dim\,(Hom(Q_1, Q_2; Q)) = dim(Q_1) \cdot dim(Q_2) \cdot dim(Q) :$$

3) $Hom(Q_1, Q_2; Q)$ գծային տարածությունը կլինի $f : Q_1 \times Q_2 \to Q$ տեսքի բոլոր ֆունկցիաների գծային տարածության ենթատարածություն: □

Նույն եղանակով սահմանվում է նաև n-գծային արտապատկերման գաղափարը:

Դիցուք $Q_1, \ldots, Q_n$ և Q գծային տարածությունները որոշված են միևնույն P դաշտի վրա, իսկ

$$Q_1 \times \cdots \times Q_n = \{(x_1, \ldots, x_n) \,|\, x_1 \in Q_1, \ldots, x_n \in Q_n\} :$$

Եթե $f : Q_1 \times \cdots \times Q_n \to Q$ արտապատկերման դեպքում՝ $f : (x_1, \ldots, x_n) \to z$, ապա գրվում է $z = f(x_1, \ldots, x_n)$, որտեղ $x_1 \in Q_1, \ldots, x_n \in Q_n$, $z \in Q$: $f(x_1, \ldots, x_n)$ արտահայտության մեջ x_i-ն կոչվում է f-ի i-րդ արգումենտ, որտեղ $i = 1, \ldots, n$: $f : Q_1 \times \cdots \times Q_n \to Q$ արտապատկերումը (ֆունկցիան) կոչվում է $Q_1, \ldots, Q_n, Q$ գծային տարածությունների n**-գծային արտապատկերում**, եթե f-ը գծային է իր յուրաքանչյուր արգումենտի նկատմամբ: Եթե $Q_1 = \cdots = Q_n = Q$, ապա f-ը կոչվում է Q գծային տարածության n-գծային ձևափոխություն:

$Q_1, \ldots, Q_n, Q$ գծային տարածությունների բոլոր n-գծային արտապատկերումների բազմությունը նշանակվում է $Hom(Q_1, \ldots, Q_n; Q)$-ով, իսկ Q գծային տարածության բոլոր n-գծային ձևափոխությունների բազմությունը՝ $Hom(\underbrace{Q, \ldots, Q}_{n}; Q)$-ով:

Տեղի ունի նաև հետևյալ ընդհանուր արդյունքը:

Թեորեմ 17.43: *1) Միևնույն P դաշտի վրա որոշված $Q_1, \ldots, Q_n, Q$ գծային տարածությունների բոլոր n-գծային արտապատկերումների $Hom(Q_1, \ldots, Q_n; Q)$ բազմությունը և Q գծային տարածության բոլոր n-գծային ձևափոխությունների $Hom(\underbrace{Q, \ldots, Q}_{n}; Q)$ բազմությունը գծային տարածություններ են (որոշված նույն P դաշտի վրա)՝ n-գծային արտապատկերումների հետևյալ գումարման և սկալյարով բազմապատկման նկատմամբ.*

$$(f + g)(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n),$$

$$(\lambda f)(x_1, \ldots, x_n) = \lambda f(x_1, \ldots, x_n) :$$

2) Եթե $Q_1, \ldots, Q_n, Q$ գծային տարածությունները վերջավոր չափանի են, ապա այդպիսին կլինի նաև $Hom(Q_1, \ldots, Q_n; Q)$ գծային տարածությունը և

$$dim\,(Hom(Q_1, \ldots, Q_n; Q)) = dim(Q_1) \cdots dim(Q_n) \cdot dim(Q) :$$

3) $Hom(Q_1, \ldots, Q_n; Q)$ գծային տարածությունը կլինի $f : Q_1 \times \cdots \times Q_n \to Q$ տեսքի բոլոր ֆունկցիաների գծային տարածության ենթատարածություն: □

17.18. Սիմետրիկ և շեղսիմետրիկ երկգծային ձևեր: Երկգծային ձևի միջուկ: Ենթատարածության օրթոգոնալ լրացում

Դիցուք Q-ն գծային տարածություն է՝ որոշված P դաշտի վրա: Q-ի f երկգծային ձևը կոչվում է.

ա) **սիմետրիկ**, եթե

$$f(x,y)=f(y,x)$$

ցանկացած $x,y\in Q$ տարրերի համար;

բ) **շեղսիմետրիկ**, եթե

$$f(x,y)=-f(y,x)$$

ցանկացած $x,y\in Q$ տարրերի համար;

գ) **սիմետրիկ ըստ զրոյի**, եթե

$$f(x,y)=0\longleftrightarrow f(y,x)=0\,,$$

որտեղ $x,y\in Q$:

Օրինակ, եթե f երկգծային ձևը սիմետրիկ կամ շեղսիմետրիկ է, ապա այն սիմետրիկ է ըստ զրոյի:

Q գծային տարածության x և y տարրերը կոչվում են **օրթոգոնալ** f **երկգծային ձևի նկատմամբ** և գրվում է $x\perp y$, եթե $f(x,y)=0$:

Օրինակ, եթե P դաշտում $1+1\neq 0$, որտեղ 1-ը P-ի միավորն է, ապա յուրաքանչյուր x վեկտոր օրթոգոնալ է իրեն $(x\perp x)$ ցանկացած f շեղսիմետրիկ երկգծային ձևի նկատմամբ: Իրոք, $f(x,x)=-f(x,x)$, $f(x,x)+f(x,x)=0$, $(1+1)f(x,x)=0$, որտեղ $1+1\neq 0$: Հետևաբար, $f(x,x)=0$:

Եթե f-ը սիմետրիկ է ըստ զրոյի, ապա

$$x\perp y\longleftrightarrow y\perp x\ :$$

Ակնհայտ է, որ f երկգծային ձևը կլինի սիմետրիկ այն և միայն այն դեպքում, երբ ցանկացած $e_1,\ldots,e_n$ հենքի նկատմամբ նրա ունեցած A մատրիցը լինի սիմետրիկ, այսինքն՝ $A^T=A$: Իրոք,

$$f(x,y)=f(y,x)\longleftrightarrow a_{ij}=f(e_i,e_j)=f(e_j,e_i)=a_{ji}\ :$$

Այնուհետև, f երկգծային ձևը կլինի շեղսիմետրիկ այն և միայն այն դեպքում, երբ ցանկացած $e_1, \ldots, e_n$ հենքի նկատմամբ նրա ունեցած A մատրիցը լինի շեղսիմետրիկ, այսինքն՝ $A^T = -A$:

Լեմմ 17.39: *1) Q գծային տարածության սիմետրիկ երկգծային ձևերի բազմությունը Q-ի երկգծային ձևերի տարածության ենթատարածություն է;*

2) Q գծային տարածության շեղսիմետրիկ երկգծային ձևերի բազմությունը Q-ի երկգծային ձևերի տարածության ենթատարածություն է: □

Թեորեմ 17.44: *Եթե P դաշտում $1+1 \neq 0$, ապա P-ի վրա որոշված Q գծային տարածության երկգծային ձևերի տարածությունը հավասար է իր սիմետրիկ երկգծային ձևերի ենթատարածության և շեղսիմետրիկ երկգծային ձևերի ենթատարածության ուղիղ գումարին:*

Ապացուցում: Նշանակենք՝ $2 = 1+1 \neq 0$, որտեղ 1-ը P դաշտի միավորն է: Նախ նկատենք, որ յուրաքանչյուր f երկգծային ձև կարելի է ներկայացնել որևէ սիմետրիկ երկգծային ձևի և որևէ շեղսիմետրիկ երկգծային ձևի գումարի տեսքով, որովհետև

$$f(x,y) = 2^{-1}\left(f(x,y) + f(y,x)\right) + 2^{-1}\left(f(x,y) - f(y,x)\right),$$

որտեղ նշանակելով՝

$$f_1(x,y) = 2^{-1}\left(f(x,y) + f(y,x)\right), \quad f_2(x,y) = 2^{-1}\left(f(x,y) - f(y,x)\right),$$

ստանում ենք f_1 սիմետրիկ և f_2 շեղսիմետրիկ երկգծային ձևերը, որոնց համար $f = f_1 + f_2$: Մյուս կողմից, եթե երկգծային ձևը միաժամանակ սիմետրիկ է և շեղսիմետրիկ, ապա այն զրոյական է: Իրոք, եթե $f(x,y) = f(y,x)$ և $f(x,y) = -f(y,x)$, ապա $f(y,x) = -f(y,x)$, այսինքն՝ $2f(y,x) = 0$, որտեղ $2 \neq 0$: Հետևաբար, $f(y,x) = 0$ ցանկացած $x, y \in Q$ տարրերի համար: □

***Հետևություն 17.31*:** *Իրական երկգծային ձևերի տարածությունը հավասար է իր սիմետրիկ երկգծային ձևերի ենթատարածության և շեղսիմետրիկ երկգծային ձևերի ենթատարածության ուղիղ գումարին:* □

Հետևություն 17.32: *Կոմպլեքս երկգծային ձևերի տարածությունը հավասար է իր սիմետրիկ երկգծային ձևերի ենթատարածության և շեղսիմետրիկ երկգծային ձևերի ենթատարածության ուղիղ գումարին:*

□

Թեորեմ 17.45: *1) n-չափանի Q գծային տարածության սիմետրիկ երկգծային ձևերի տարածության չափողականությունը հավասար է $C_n^2 + n = \frac{1}{2}n(n+1)$-ի, որի համար որպես հենք կարելի է դիտարկել հետևյալ*

$$\ell_{ij}(x,y) = x_i y_j + x_j y_i, \quad \ell_{ii}(x,y) = x_i y_i$$

սիմետրիկ երկգծային ձևերի հաջորդականությունը, որտեղ $i,j = 1,\ldots,n$ և $i<j$:

2) Եթե P դաշտում $1+1 \neq 0$, ապա P-ի վրա որոշված n-չափանի Q գծային տարածության շեղսիմետրիկ երկգծային ձևերի տարածության չափողականությունը հավասար է $C_n^2 = \frac{n(n-1)}{2}$-ի, որի համար որպես հենք կարելի է դիտարկել

$$q_{ij} = x_i y_j - x_j y_i$$

շեղսիմետրիկ երկգծային ձևերի հաջորդականությունը, որտեղ $i,j = 1,\ldots,n$ և $i<j$:

Ապացուցում: 1) $n=0$ դեպքում պնդումն ակնհայտ է: Եթե $n>0$ և $e_1,\ldots,e_n$ համակարգը հենք է Q-ի համար, ապա Q-ի յուրաքանչյուր f սիմետրիկ երկգծային ձևի համար կունենանք՝

$$f(x,y) = \sum_{i<k} a_{ik}\left(x_i y_k + x_k y_i\right) + \sum_{i=1}^{n} a_{ii} x_i y_i\,,$$

որտեղ $x = x_1e_1 + \cdots + x_ne_n$, $y = y_1e_1 + \cdots + y_ne_n$, $a_{ij} = f(e_i,e_j) = f(e_j,e_i) = a_{ji}$: Ըստ որում,

$$\ell_{ik}(x,y) = x_i y_k + x_k y_i\,, \quad i<k\,,$$
$$\ell_{ii}(x,y) = x_i y_i$$

բանաձևերով որոշվող ℓ_{ik}, ℓ_{ii} $(i<k)$ երկգծային ձևերը սիմետրիկ են և գծայնորեն անկախ, որոնց թիվը հավասար է $C_n^2 + n = \frac{n(n-1)}{2} + n$-ի:

2) n-չափանի գծային տարածության շեղսիմետրիկ երկգծային ձևերի տարածության չափողականությունը, համաձայն նախորդ թեորեմի, կլինի հավասար՝ $n^2 - \dfrac{n(n+1)}{2} = \dfrac{n(n-1)}{2}$: Յուրաքանչյուր f շեղսիմետրիկ երկգծային ձևի համար կունենանք՝

$$f(x,y) = \sum_{i<k} a_{ik}\left(x_i y_k - x_k y_i\right)\,,$$

որովհետև $a_{ii}=0$, իսկ $a_{ki}=-a_{ik}$, եթե $i\neq k$: Մնում է նկատել, որ

$$q_{ik}(x,y) = x_i y_k - x_k y_i\,, \qquad i<k\,,$$

բանաձևով որոշվող q_{ik} երկգծային ձևերը շեղսիմետրիկ են և գծայնորեն անկախ, որոնց թիվը հավասար է $C_n^2 = \dfrac{n(n-1)}{2}$-ի: □

Q գծային տարածության f **երկգծային ձևի միջուկ** (կորիզ) է կոչվում

$$Ker(f) = \{y\in Q \mid f(x,y)=0\,,\forall x\in Q\}\subseteq Q$$

ենթաբազմությունը: Քանի որ $0\in Ker(f)$, ապա $Ker(f)\neq\emptyset$: Ավելի ճիշտ կլիներ $Ker(f)$-ը անվանել f-ի ձախ միջուկ (համանման եղանակով սահմանելով f-ի աջ միջուկը): Սակայն վերջավոր չափանի Q գծային տարածության դեպքում ստացվող ձախ և աջ միջուկները կհամընկնեն իզոմորֆիզմի ճշտությամբ: Այդ պատճառով, մենք ուսումնասիրում ենք դրանցից միայն մեկը:

Լեմմ 17.40: *$Ker(f)\leqslant Q$, այսինքն՝ $Ker(f)$-ը Q-ի ենթատարածություն է:*

Ապացույց: Եթե $y_1,y_2\in Ker(f)$, ապա ցանկացած $x\in Q$ տարրի համար՝ $f(x,y_1)=0=f(x,y_2)$: Հատևաբար,

$$f\left(x,\alpha y_1+\beta y_2\right) = \alpha f(x,y_1)+\beta f(x,y_2) = 0\,,$$

այսինքն՝ $\alpha y_1+\beta y_2\in Ker(f)$ ցանկացած $\alpha,\beta\in P$ սկալյարների համար: □

f երկգծային ձևը կոչվում է **չվերասերված**, եթե $Ker(f)=\{0\}$: Հակառակ դեպքում f երկգծային ձևը կոչվում է **վերասերված**:

Լեմմ 17.41: *Եթե Q-ն գծային տարածություն է $e_1,\ldots,e_n$ հենքով, ապա*

$$Ker(f) = \{y\in Q \mid f(e_i,y)=0\,,i=1,\ldots,n\}\ :$$

Ապացուցում: Ցանկացած $x \in Q$ տարրի համար, որտեղ $x = x_1e_1 + \cdots + x_ne_n$ և $f(e_i, y) = 0$, $i = 1, \ldots, n$, կունենանք՝

$$f(x, y) = f(x_1e_1 + \cdots + x_ne_n, y) = x_1f(e_1, y) + \cdots + x_nf(e_n, y) = 0: \quad \Box$$

Միաժամանակ, եթե $y = y_1e_1 + \cdots + y_ne_n \in Ker(f)$, ապա $f(e_i, y) = 0$ պայմանը կունենա հետևյալ տեսքը՝

$$f(e_i, y) = f(e_i, y_1e_1 + \cdots + y_ne_n) = y_1f(e_i, e_1) + \cdots + y_nf(e_i, e_n) =$$

$$= a_{i1}y_1 + \cdots + a_{in}y_n = 0 \ :$$

Հետևաբար, $i = 1, \ldots, n$ դեպքում հանգում ենք գծային հավասարումների հետևյալ համասեռ համակարգին.

$$\begin{cases} a_{11}y_1 + \cdots + a_{1n}y_n = 0\,, \\ \ldots \ \ldots \ \ldots \\ a_{n1}y_1 + \cdots + a_{nn}y_n = 0\,, \end{cases} \tag{17.22}$$

որտեղ

$$A = \begin{pmatrix} a_{11}, \ldots, a_{1n} \\ \ldots \ \ldots \ \ldots \\ a_{n1}, \ldots, a_{nn} \end{pmatrix}$$

մատրիցը f երկգծային ձևի մատրիցն է $e_1, \ldots, e_n$ հենքի նկատմամբ: Ինչպես գիտենք, (17.22) համակարգի լուծումների L_A գծային տարածության համար՝

$$dim(L_A) = n - rank(A) \ :$$

Սակայն, $L_A \simeq Ker(f)$, որովհետև $\Phi : y \to \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ արտապատկերումը կլինի իզոմորֆիզմ՝ $\Phi : Ker(f) \to L_A$: Հետևաբար, $dim(L_A) = dim(Ker(f))$: Այսպիսով, հանգում ենք հետևյալ արդյունքին:

Թեորեմ 17.46: *n-չափանի Q գծային տարածության ցանկացած f երկգծային ձևի համար՝*

$$dim\,(Ker(f)) = n - rank(f),$$

որտեղ $n \geqslant 1$: $\Box$

Q գծային տարածության f երկգծային ձևի նկատմամբ $U \leqslant Q$ ենթատարածության **օրթոգոնալ լրացում** է կոչվում

$$U^{\perp} = \{y \in Q \,|\, f(x,y) = 0\,, \forall x \in U\} \subseteq Q$$

ենթաբազմությունը: Օրինակ, $Q^{\perp} = Ker(f)$:

Լեմմ 17.42: *Ցանկացած $U \leqslant Q$ ենթատարածության համար $U^{\perp} \leqslant Q$:* □

Թեորեմ 17.47: *Եթե Q-ն վերջավոր չափանի գծային տարածություն է և $U \leqslant Q$, ապա*

$$dim\left(U^{\perp}\right) \geqslant dim(Q) - dim(U) \ :$$

Ապացուցում: Եթե $U = \{0\}$, Q, ապա պնդումը ճիշտ է, որովհետև $U = \{0\}$ դեպքում՝ $U^{\perp} = Q$ և $dim\left(U^{\perp}\right) = dim\,(Q)$, իսկ $U = Q$ դեպքում կունենանք՝ $dim(U^{\perp}) \geqslant 0$: Դիցուք $U \neq \{0\}$, Q և դիցուք $e_1, \ldots, e_k$ համակարգը հենք է U-ի համար: Լրացնենք $e_1, \ldots, e_k$ համակարգը մինչև Q-ի հենքի՝ $e_1, \ldots, e_k, e_{k+1}, \ldots, e_n$:

Ակնհայտ է, որ

$$y \in U^{\perp} \longleftrightarrow f(e_i, y) = 0\,, \qquad i = 1, \ldots, k \ :$$

Եթե $y = y_1 e_1 + \cdots + y_n e_n \in U^{\perp}$, ապա $f(e_i, y) = 0$, $i = 1, \ldots, k$, հավասարություններից կունենանք՝

$$\begin{cases} a_{11}y_1 + \cdots + a_{1n}y_n = 0\,, \\ \ldots \ \ldots \ \ldots \\ a_{k1}y_1 + \cdots + a_{kn}y_n = 0\,, \end{cases} \tag{17.23}$$

և հակառակը, որտեղ $a_{ij} = f(e_i, e_j)$: Նշանակելով՝

$$B = \begin{pmatrix} a_{11}, \ldots, a_{1n} \\ \ldots \ \ldots \ \ldots \\ a_{k1}, \ldots, a_{kn} \end{pmatrix} \ ,$$

իսկ L_B-ով (17.23) համասեռ համակարգի լուծումների տարածությունը, կունենանք՝ $B \leqslant A$ և

$$dim(L_B) = n - rank(B) \ :$$

Սակայն, $U^{\perp} \simeq L_B$, որովհետև $\Phi : y \to \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ արտապատկերումը կլինի իզոմորֆիզմ՝ $\Phi : U^{\perp} \to L_B$: Հետևաբար, $dim\left(U^{\perp}\right) = dim(L_B)$: Միաժամանակ, $rank(B) \leqslant k$: Այսպիսով,

$$dim\left(U^{\perp}\right) = n - rank(B) \geqslant n - k = dim(Q) - dim(U) : \qquad \square$$

Հետևություն 17.33: *Եթե վերջավոր չափանի Q գծային տարածության f երկգծային ձևը չվերասերված է, այսինքն՝ $Ker(f) = \{0\}$ և $U \leqslant Q$, ապա*

$$dim\left(U^{\perp}\right) = dim(Q) - dim(U) \ :$$

Ապացույց: Եթե $dim(Q) = n$, ապա

$$dim\left(Ker(f)\right) = n - rank(f)\,,$$

որտեղ $rank(f) = rank(A)$, իսկ A-ն f-ի մատրիցն է Q-ի սևեռված հենքի նկատմամբ: Քանի որ այստեղ՝ $dim\left(Ker(f)\right) = 0$, ապա $n = rank(A)$: Հետևաբար, նախորդ թեորեմի ապացուցման ընթացքում նշանակված $B \leqslant A$ ենթամատրիցի տողերը կլինեն գծայնորեն անկախ, այսինքն՝ $rank(B) = k = dim(U)$: Ուստի,

$$dim\left(U^{\perp}\right) = n - k = dim(Q) - dim(U) : \qquad \square$$

Հետևություն 17.34: *Եթե վերջավոր չափանի Q գծային տարածության f երկգծային ձևը չվերասերված է ու սիմետրիկ ըստ զրոյի և $U \leqslant Q$, ապա*

$$\left(U^{\perp}\right)^{\perp} = U \ :$$

Ապացույց: Օգտվելով նախորդ հետևության մեջ ապացուցված բանաձևից, նախ կունենանք՝

$$dim\left(U^{\perp}\right)^{\perp} = n - (n-k) = k = dim(U)\,,$$

որտեղ $dim(Q) = n$, իսկ $dim(U) = k$: Սակայն, $U \subseteq \left(U^{\perp}\right)^{\perp}$, որովհետև եթե $x \in U$, ապա ցանկացած $y \in U^{\perp}$ տարրի համար՝ $f(x,y) = 0$: Ուստի, $f(y,x) = 0$ ցանկացած $y \in U^{\perp}$ տարրի համար: Հետևաբար, $x \in \left(U^{\perp}\right)^{\perp}$:

$\square$

17.19. Քառակուսային ձևեր: Իներցիայի օրենքը: Սիլվեստրի հայտանիշը: Քառակուսային ձևի բերումը կանոնական տեսքի

Դիցուք P դաշտում $1+1 \neq 0$, որտեղ 1-ը P-ի միավորն է (օրինակ, $P=\mathbb{R}$ կամ $P=\mathbb{C}$, բայց $P \neq \mathbb{Z}_2$), և դիցուք Q-ն գծային տարածություն է որոշված P դաշտի վրա, իսկ $f: Q \times Q \to P$ արտապատկերումը Q-ի սիմետրիկ երկգծային ձև է: f սիմետրիկ երկգծային ձևին համապատասխանող **քառակուսային ձև** է կոչվում այն $f^*: Q \to P$ արտապատկերումը, որը որոշվում է հետևյալ կերպ՝

$$f^*(x) = f(x,x)$$

ցանկացած $x \in Q$ տարրի (վեկտորի) համար: $q: Q \to P$ արտապատկերումը կոչվում է Q-ի քառակուսային ձև, եթե գոյություն ունի Q-ի այնպիսի f սիմետրիկ երկգծային ձև, որ $q = f^*$: Այդ դեպքում, f սիմետրիկ երկգծային ձևը կոչվում է q-ի **բևեռային ձև**:

Եթե $P=\mathbb{R}$, ապա q քառակուսային ձևը կոչվում է **իրական**, իսկ $P=\mathbb{C}$ դեպքում q-ն կոչվում է **կոմպլեքս** քառակուսային ձև:

Լեմմ 17.43: *Եթե q-ն քառակուսային ձև է և $q = f^*$, ապա Q գծային տարածության f սիմետրիկ երկգծային ձևը որոշվում է հետևյալ կերպ՝*

$$f(x,y) = 2^{-1}\left(q(x+y) - q(x) - q(y)\right), \tag{17.24}$$

որտեղ $2 = 1+1 \in P$, $x, y \in Q$: Այսինքն՝ քառակուսային ձևով նրա բևեռային ձևը վերականգնվում է միարժեքորեն:

Ապացուցում: Իրոք, օգտվելով f երկգծային ձևի սիմետրիկությունից, կունենանք՝

$$2^{-1}\left(q(x+y)-q(x)-q(y)\right) = 2^{-1}\left(f(x+y,x+y)-f(x,x)-f(y,y)\right) =$$
$$= 2^{-1}\left(f(x,x)+f(x,y)+f(y,x)+f(y,y)-f(x,x)-f(y,y)\right) =$$
$$= 2^{-1}\left(2f(x,y)\right) = f(x,y): \qquad \square$$

Թեորեմ 17.48: *Q գծային տարածության բոլոր քառակուսային ձևերի բազմությունը գծային տարածություն է հետևյալ գործողությունների նկատմամբ՝*

$$(q_1+q_2)x = q_1(x) + q_2(x),$$

$$(\lambda q)x = \lambda q(x)\,,$$

որտեղ $x \in Q$, $\lambda \in P$*:*

$\Phi : f \to f^*$ *արտապատկերումը կլինի իզոմորֆիզմ (նույնածնություն) Q գծային տարածության բոլոր սիմետրիկ երկգծային ձևերի տարածությունից նրա բոլոր քառակուսային ձևերի տարածության մեջ: Հետևաբար, n-չափանի Q գծային տարածության բոլոր քառակուսային ձևերի գծային տարածության չափողականությունը հավասար է* $C_n^2 + n = \dfrac{n(n+1)}{2}$*-ի:*

Ապացուցում: Q-ի քառակուսային ձևերի ոչ դատարկ բազմությունը ֆունկցիաների $F(Q,P)$ գծային տարածության ենթատարածություն է: Իրոք, եթե $q_1 = f_1^*$ և $q_2 = f_2^*$, որտեղ f_1-ը և f_2-ը Q-ի սիմետրիկ երկգծային ձևեր են, ապա ցանկացած $x \in Q$ տարրի համար՝

$$(q_1 + q_2)x = q_1(x) + q_2(x) = f_1^*(x) + f_2^*(x) =$$

$$f_1(x,x) + f_2(x,x) = (f_1 + f_2)(x,x) = (f_1 + f_2)^* x\,,$$

որտեղ $f_1 + f_2$-ը Q-ի սիմետրիկ երկգծային ձև է, իսկ եթե $q = f^*$, որտեղ f-ը Q-ի սիմետրիկ երկգծային ձև է, ապա ցանկացած $x \in Q$ տարրի և ցանկացած $\lambda \in P$ սկալյարի համար կունենանք՝

$$(\lambda q)x = \lambda q(x) = \lambda f^*(x) = \lambda f(x,x) = (\lambda f)(x,x) = (\lambda f)^*(x)\,,$$

որտեղ λf-ը ևս Q-ի սիմետրիկ երկգծային ձև է: Այսպիսով, $q_1 + q_2$-ը և λq-ն քառակուսային ձևեր են: Միաժամանակ, ապացուցվեց

$$(f_1 + f_2)^* = f_1^* + f_2^*\,,$$

$$(\lambda f)^* = \lambda f^*$$

հավասարությունները Q-ի ցանկացած f, f_1, f_2 սիմետրիկ երկգծային ձևերի և ցանկացած $\lambda \in P$ սկալյարի համար, այսինքն՝

$$\Phi\,(f_1 + f_2) = \Phi(f_1) + \Phi(f_2)\,,$$

$$\Phi(\lambda f) = \lambda \Phi(f)\ :$$

Մնում է նկատել, որ $\Phi : f \to f^*$ արտապատկերումը փոխմիարժեք (բիեկտիվ) է և օգտվել թեորեմ 17.45-ից: Իրոք, Φ արտապատկերման սյուրեկտիվությունն ակնհայտ է, իսկ ինյեկտիվությունը բխում է նախորդ լեմմից՝

$$f^* = g^* \longrightarrow f^*(x) = g^*(x), \quad f^*(y) = g^*(y), \quad f^*(x+y) = g^*(x+y) \longrightarrow$$

$$2^{-1}\left(f^*(x+y) - f^*(x) - f^*(y)\right) = 2^{-1}\left(g^*(x+y) - g^*(x) - g^*(y)\right) \longrightarrow$$

$$f(x,y) = g(x,y) \longrightarrow f = g : \qquad \square$$

Q վերջավոր չափանի գծային տարածության $e_1, \ldots, e_n$ հենքը կոչվում է **օրթոգոնալ** $f : Q \times Q \to P$ երկգծային ձևի նկատմամբ, եթե $f(e_i, e_j) = 0$, որտեղ $i \neq j$, $i, j = 1, \ldots, n$: Այդպիսի հենքի նկատմամբ f երկգծային ձևը կունենա հետևյալ ներկայացումը՝

$$f(x,y) = a_{11}x_1y_1 + a_{22}x_2y_2 + \cdots + a_{nn}x_ny_n \,, \qquad (17.25)$$

որը կոչվում է f երկգծային ձևի **կանոնական տեսք**, այսինքն՝ օրթոգոնալ հենքի նկատմամբ f-ի մատրիցը կլինի անկյունագծային տեսքի: Այս դեպքում, ոչ զրոյական $a_{ii} = f(e_i, e_i)$ գործակիցների թիվը կլինի հավասար f-ի ռանգին:

Թեորեմ 17.49: *n-չափանի ($n \geqslant 1$) Q գծային տարածության ցանկացած f սիմետրիկ երկգծային ձևի նկատմամբ գոյություն ունի Q-ի օրթոգոնալ հենք:*

Ապացուցում: Պնդումն ապացուցենք վերհանգման եղանակով՝ ըստ $dim(Q) = n$ բնական թվի: $n = 1$ դեպքում պնդումը ճիշտ է: Դիցուք $n > 1$ և n-ից փոքր չափողականություն ունեցող գծային տարածությունների համար պնդումը ճիշտ է: Եթե f սիմետրիկ երկգծային ձևը զրոյական է, ապա պնդումն ակնհայտ է, որովհետև $f(x,y) = 0$ դեպքում նաև $f(e_i, e_j) = 0$ ($x, y \in Q$): Դիցուք $f \neq 0$, այսինքն գոյություն ունեն այնպիսի $x, y \in Q$ տարրեր, որ $f(x,y) \neq 0$: (17.24) բանաձևի համաձայն, այդ դեպքում, $q = f^* \neq 0$, այսինքն՝ գոյություն կունենա այնպիսի $s_1 \in Q$ տարր, որ $q(s_1) = f(s_1, s_1) \neq 0$:

Ակնհայտ է, որ $s_1 \neq 0$ և, հետևաբար, s_1-ը գծայնորեն անկախ համակարգ է:

Նշանակենք $U = (s_1) \leqslant Q$ և նկատենք, որ $U \cap U^{\perp} = \{0\}$: Իրոք, եթե $x \in U \cap U^{\perp}$, ապա $x = \lambda s_1$ և $x \perp s_1$, այսինքն՝ $f(\lambda s_1, s_1) = 0$,

$\lambda f(s_1, s_1) = 0$ և $\lambda = 0$, որովհետև $f(s_1, s_1) \neq 0$: Հետևաբար, $x = 0$: Ըստ թեորեմ 17.47-ի,

$$dim(Q) \leqslant dim(U) + dim\left(U^{\perp}\right) - dim\left(U \cap U^{\perp}\right) = dim\left(U + U^{\perp}\right) :$$

Մյուս կողմից, քանի որ $U + U^{\perp} \leqslant Q$, ապա

$$dim\left(U + U^{\perp}\right) \leqslant dim\,(Q) :$$

Այսպիսով,

$$dim\,(Q) = dim\left(U + U^{\perp}\right)$$

և $Q = U \oplus U^{\perp}$: Քանի որ $dim(U) = 1$, $dim(Q) = n$, ապա $dim\left(U^{\perp}\right) = n - 1$ և, համաձայն վերհանգման ենթադրության, $U^{\perp} \leqslant Q$ ենթատարածությունը կունենա $s_2, \ldots, s_n$ օրթոգոնալ հենք f-ի նկատմամբ (որպես $U^{\perp}$ ենթատարածության սիմետրիկ երկգծային ձևի): Հետևաբար, այս հենքին ավելացնելով s_1-ը կստանանք Q-ի $s_1, s_2, \ldots, s_n$ օրթոգոնալ հենքը f-ի նկատմամբ: □

Հետևություն 17.35: *n-չափանի ($n \geqslant 1$) Q գծային տարածության ցանկացած f սիմետրիկ երկգծային ձևի համար գոյություն ունի Q-ի այնպիսի հենք, որի նկատմամբ f-ն ունի կանոնական տեսք, այսինքն՝ որի նկատմամբ f-ի մատրիցը կլինի անկյունագծային տեսքի:* □

n-չափանի ($n \geqslant 1$) Q գծային տարածության f սիմետրիկ երկգծային ձևի A մատրիցը $e_1, \ldots, e_n$ հենքում կոչվում է նաև $q = f^*$ **քառակուսային ձևի մատրից** նույն հենքում: A մատրիցի ռանգը կոչվում է նաև $q = f^*$ քառակուսային ձևի ռանգ:

Հետևություն 17.36: *n-չափանի ($n \geqslant 1$) Q գծային տարածության ցանկացած $q = f^*$ քառակուսային ձևի համար գոյություն ունի Q-ի այնպիսի $e_1, \ldots, e_n$ հենք, որի նկատմամբ q-ի մատրիցը կլինի անկյունագծային տեսքի: Ավելի ճիշտ այդպիսի հենքի նկատմամբ՝*

$$q(x) = q(e_1)x_1^2 + q(e_2)x_2^2 + \cdots + q(e_n)x_n^2\,,$$

որտեղ $x \in Q$, $x = x_1e_1 + \cdots + x_ne_n$, $q(e_i) = f(e_i, e_i)$, $i = 1, \ldots, n$: □

Եթե $e_1, \ldots, e_n$ հենքն այնպիսին է, որ Q գծային տարածության ցանկացած x տարրի (վեկտորի) համար՝

$$q(x) = a_1x_1^2 + \cdots + a_nx_n^2\,,$$

որտեղ $x = x_1e_1 + \cdots + x_ne_n$, $a_i \in P$, $i = 1, \ldots, n$, ապա կասենք, որ q քառակուսային ձևը $e_1, \ldots, e_n$ հենքի նկատմամբ ունի **կանոնական տեսք**: Այս դեպքում, ոչ զրոյական $a_i = q(e_i)$ գործակիցների թիվը կլինի հավասար q-ի ռանգին:

Հետևություն 17.37: *Ցանկացած $A \in P^{n\times n}$ սիմետրիկ մատրից կոնգրուենտ է որևէ $B \in P^{n\times n}$ անկյունագծային մատրիցի:*

Ապացուցում: Եթե $A = (a_{ij})$, $A^T = A$ և Q-ն $c_1, \ldots, c_n$ հենքով գծային տարածություն է որոշված P դաշտի վրա, ապա ցանկացած $x, y \in Q$, $x = x_1c_1 + \cdots + x_nc_n$, $y = y_1c_1 + \cdots + y_nc_n$ տարրերի համար սահմանելով

$$f(x, y) = \sum_{i,j=1}^{n} a_{ij}x_iy_j \,,$$

կստանանք $f : Q \times Q \to P$ սիմետրիկ երկգծային ձևը, որի մատրիցը $c_1, \ldots, c_n$ հենքի նկատմամբ կլինի հենց A-ն: Ըստ ապացուցված թեորեմի, գոյություն ունի Q-ի այնպիսի $e_1, \ldots, e_n$ հենք, որն օրթոգոնալ է կառուցված f սիմետրիկ երկգծային ձևի նկատմամբ: f-ի B մատրիցը $e_1, \ldots, e_n$ հենքում կլինի անկյունագծային տեսքի և A ու B մատրիցները կլինեն կոնգրուենտ՝ համաձայն թեորեմ 17.41-ի: □

Հետևություն 17.38: *n-չափանի ($n \geqslant 1$) Q գծային տարածության ցանկացած q քառակուսային ձևի համար գոյություն ունի Q-ի այնպիսի հենք, որի նկատմամբ q քառակուսային ձևն ունի կանոնական տեսք: Համառոտ, ցանկացած քառակուսային ձև կարելի է բերել կանոնական տեսքի:* □

Նշենք $f^*(x) = f(x, x) = \sum\limits_{i,j=1}^{n} a_{i,j}x_ix_j$ տեսքով տրված քառակուսային ձևը կանոնական տեսքի բերելու հետևյալ գործնական եղանակը (ալգորիթմը): Հնարավոր է երկու դեպք:

I) Տրված քառակուսային ձևի մեջ $a_{11} = a_{22} = \cdots = a_{nn} = 0$, իսկ որևէ $a_{ij} \neq 0$, որտեղ $i \neq j$: Որոշակիության համար դիցուք $a_{1,2} \neq 0$: Ընտրենք այնպիսի հենք, որում x-ի $z_1, z_2, \ldots, z_n$ կոորդինատները կապված են սկզբնական $x_1, x_2, \ldots, x_n$ կոորդինատների հետ հետևյալ կերպ՝

$$\begin{aligned} x_1 &= z_1 - z_2 \\ x_2 &= z_1 + z_2, \\ x_3 &= z_3, \\ &\vdots \\ x_n &= z_n, \end{aligned}$$

որտեղ կոորդինատների ձևափոխության մատրիցն ունի ոչ զրոյական որոշիչ՝

$$\begin{vmatrix} 1 & -1 & 0 & \dots & 0 \\ 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{vmatrix} = 1 + 1 \neq 0 \ :$$

Այդ դեպքում տրված քառակուսային ձևի $2a_{12}x_1x_2$ անդամը կընդունի հետևյալ տեսքը.

$$2a_{12}x_1x_2 = 2a_{12}(z_1 - z_2)(z_1 + z_2) = 2a_{12}z_1^2 - 2a_{12}z_2^2\,,$$

այսինքն՝ քառակուսային ձևում այժմ վեկտորի որևէ կոորդինատի քառակուսու գործակիցը տարբեր է զրոյից ($2 = 1 + 1 \neq 0$);

II) Տրված քառակուսային ձևում $a_{11}, a_{22}, \dots, a_{nn}$ գործակիցներից որևէ մեկը տարբեր է զրոյից: Դիցուք $a_{11} \neq 0$: Այդ դեպքում՝

$$f(x, x) - a_{11}^{-1}\left(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n\right)^2 = g$$

տարբերությունը կպարունակի միայն $x_2, x_3, \dots, x_n$ կոորդինատներով անդամներ: Որտեղից՝

$$f(x, x) = a_{11}^{-1}\left(a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n\right)^2 + g \ :$$

Նշանակելով՝

$$\begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n, \\ y_2 &= x_2, \\ &\vdots \\ y_n &= x_n, \end{aligned}$$

կստանանք՝

$$f(x,x) = a_{11}^{-1} y_1^2 + g,$$

որտեղ g քառակուսային ձևը պարունակում է միայն $y_2, \ldots, y_n$ կոորդինատներով անդամներ:

Այնուհետև I) կամ II) դեպքերում նշված ձևափոխությունները կիրառվում են g քառակուսային ձևի նկատմամբ, և այսպես շարունակ: Այսպիսով, վերջավոր թվով քայլերից հետո կհանգենք տրված $f(x,x)$ քառակուսային ձևի կանոնական տեսքին:

Նկատենք նաև, որ $1+1=0$ պայմանին բավարարող դաշտի դեպքում, հետևություն 17.38-ը ընդհանուր դեպքում տեղի չունի: Օրինակ, $\mathbb{Z}_2$ դաշտի դեպքում $f(x,x) = x_1 x_2$ տեսքի քառակուսային ձևը հնարավոր չէ բերել կանոնական տեսքի, որովհետև եթե որևէ հենքում $f(x,x) = x_1 x_2$ քառակուսային ձևն ունենա կանոնական տեսք, ապա մի կողմից՝

$$\begin{aligned} x_1 &= b_{11} y_1 + b_{12} y_2, \\ x_2 &= b_{21} y_1 + b_{22} y_2, \end{aligned}$$

որտեղ

$$\begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix} = b_{11} b_{22} - b_{12} b_{21} \neq 0\,,$$

իսկ մյուս կողմից՝

$$\begin{aligned} f(x,x) = x_1 x_2 = (b_{11} y_1 + b_{12} y_2)(b_{21} y_1 + b_{22} y_2) = \\ = b_{11} b_{21} y_1^2 + (b_{11} b_{22} + b_{12} b_{21}) y_1 y_2 + b_{12} b_{22} y_2^2, \end{aligned}$$

որտեղ $b_{11} b_{22} + b_{12} b_{21} = 0$: Հետևաբար, $b_{11} b_{22} - b_{12} b_{21} = 0$, որովհետև $\mathbb{Z}_2$ դաշտում՝ $a = -a$: Հակասություն:

Դիցուք $P = \mathbb{C}$ (այսինքն՝ դիտարկենք կոմպլեքս երկգծային և քառակուսային ձևեր): Այդ դեպքում, «նորմավորելով» $e_1, \ldots, e_n$ հենքային վեկտորները, (17.25) հավասարության ոչ զրոյական a_{ii} գործակիցները կարելի է դարձնել 1: Իրոք, անցնենք մեկ այլ $e'_1, \ldots, e'_n$ հենքի՝

$$e'_i = \begin{cases} \left(\sqrt{a_{ii}}\right)^{-1} e_i, & \text{եթե } a_{ii} \neq 0\,, \\ e_i, & \text{եթե } a_{ii} = 0\,, \end{cases}$$

որտեղ $\sqrt{a_{ii}}$-ով նշանակված է $z^2 = a_{ii}$ հավասարման երկու կոմպլեքս լուծումներից որևէ մեկը: Ուստի, $e_1, \ldots, e_n$ օրթոգոնալ հենքից $e'_1, \ldots, e'_n$ հենքին անցման Γ մատրիցը կլինի անկյունագծային մատրից, որի գլխավոր անկյունագծի յուրաքանչյուր տարր հավասար է $\left(\sqrt{a_{ii}}\right)^{-1}$-ի կամ 1-ի: Այսպիսով, $det(\Gamma) \neq 0$ և $e'_1, \ldots, e'_n$ համակարգը կլինի հենք դիտարկվող Q գծային տարածության համար (հետևություն 17.16): Ըստ որում, ստացված $e'_1, \ldots, e'_n$ հենքը ևս կլինի օրթոգոնալ, որովհետև

$$f\left(e'_i, e'_j\right) = \alpha_{ij} f(e_i, e_j) = 0\,, \qquad i \neq j\,,$$

իսկ

$$f\left(e'_i, e'_i\right) = \begin{cases} 1\,, & \text{եթե } a_{ii} \neq 0\,, \\ 0\,, & \text{եթե } a_{ii} = 0\ : \end{cases}$$

Հանգում ենք հետևյալ արդյունքին:

Հետևություն 17.39: *Կոմպլեքս թվերի դաշտի վրա որոշված n-չափանի ($n \geqslant 1$) Q գծային տարածության յուրաքանչյուր f սիմետրիկ երկգծային ձևի համար գոյություն ունի Q-ի այնպիսի $e'_1, \ldots, e'_n$ (օրթոգոնալ) հենք, որ ցանկացած $x, y \in Q$, $x = x_1 e'_1 + \cdots + x_n e'_n$, $y = y_1 e'_1 + \cdots + y_n e'_n$ տարրերի (վեկտորների) համար՝*

$$f(x, y) = x_1 y_1 + \cdots + x_r y_r\,, \qquad r \leqslant n\,,$$

որտեղ r-ը f-ի ռանգն է: □

Հետևություն 17.40: *Կոմպլեքս թվերի դաշտի վրա որոշված n-չափանի ($n \geqslant 1$) Q գծային տարածության ցանկացած q քառակուսային ձևի համար գոյություն ունի Q-ի այնպիսի $e'_1, \ldots, e'_n$ հենք, որ յուրաքանչյուր $x \in Q$, $x = x_1 e'_1 + \cdots + x_n e'_n$ տարրի (վեկտորի) համար՝*

$$q(x) = x_1^2 + \cdots + x_r^2\,, \qquad r \leqslant n\,,$$

որտեղ r-ը q-ի ռանգն է: □

Դիցուք $P = \mathbb{R}$ (այսինքն՝ դիտարկենք իրական երկգծային և քառակուսային ձևեր): Այս դեպքում «նորմավորելով» $e_1, \ldots, e_n$ հենքային վեկտորները, (17.25) հավասարության ոչ զրոյական a_{ii}

գործակիցները կարելի է դարձնել 1 կամ -1: Իրոք, այս դեպքում անցնում ենք այն $e'_1, \dots, e'_n$ հենքին, որտեղ

$$e'_i = \begin{cases} \left(\sqrt{|a_{ii}|}\right)^{-1} e_i, & \text{եթե } a_{ii} \neq 0\,, \\ e_i, & \text{եթե } a_{ii} = 0 \ : \end{cases}$$

Հանգում ենք հետևյալ արդյունքին:

Հետևություն 17.41: *Իրական թվերի դաշտի վրա որոշված n-չափանի ($n \geqslant 1$) Q գծային տարածության յուրաքանչյուր f սիմետրիկ երկգծային ձևի համար գոյություն ունի Q-ի այնպիսի $e'_1, \dots, e'_n$ (օրթոգոնալ) հենք, որ ցանկացած $x, y \in Q$, $x = x_1e'_1 + \dots + x_ne'_n$, $y = y_1e'_1 + \dots + y_ne'_n$ տարրերի (վեկտորների) համար՝*

$$f(x,y) = x_1y_1 + \dots + x_ky_k - x_{k+1}y_{k+1} - \dots - x_{k+\ell}y_{k+\ell}\,, \quad k+\ell \leqslant n\,, \quad (17.26)$$

որտեղ $k + \ell = rank(f)$: □

f իրական սիմետրիկ երկգծային ձևի (17.26) տեսքը կոչվում է նրա **նորմալ տեսք**, իսկ համապատասխան մատրիցը՝ **նորմալ մատրից**: Այսպիսով, նորմալ մատրից է կոչվում այն անկյունագծային մատրիցը, որն ունի հետևյալ ընդհանուր տեսքը՝

$$\begin{pmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & \text{\Huge 0} & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & 0 & & \\ & \text{\Huge 0} & & & & & & \ddots & \\ & & & & & & & & 0 \end{pmatrix} :$$

Հետևություն 17.42: *Ցանկացած $A \in \mathbb{R}^{n\times n}$ սիմետրիկ մատրից կոնգրուենտ է որևէ $B \in \mathbb{R}^{n\times n}$ նորմալ մատրիցի:* □

Հետևություն 17.43: *Իրական թվերի դաշտի վրա որոշված n-չափանի ($n \geqslant 1$) Q գծային տարածության ցանկացած q քառակուսային ձևի համար գոյություն ունի Q-ի այնպիսի $e'_1, \dots, e'_n$ հենք, որ յուրաքանչյուր $x \in Q$, $x = x_1e'_1 + \dots + x_ne'_n$ տարրի (վեկտորի) համար՝*

$$q(x) = x_1^2 + \dots + x_k^2 - x_{k+1}^2 - \dots - x_{k+\ell}^2\,, \quad k+\ell \leqslant n\,, \qquad (17.27)$$

որտեղ $k + \ell = rank(q)$*:* □

(17.27) հավասարությունը կոչվում է q իրական քառակուսային ձևի **նորմալ տեսք**, $e'_1, \ldots, e'_n$ հենքը՝ նորմալ հենք, իսկ k և ℓ թվերը կոչվում են q քառակուսային ձևի **դրական** և **բացասական նշիչներ** նշված հենքի նկատմամբ: (k, ℓ) զույգը կոչվում է q-ի **նշիչ** կամ **սիգնատուրա** նշված հենքի նկատմամբ:

Իրական թվերի դաշտի վրա որոշված Q գծային տարածության q քառակուսային ձևը կոչվում է **դրական որոշյալ** (**բացասական որոշյալ**) $Q_1 \leqslant Q$ ենթատարածության վրա, եթե $q(x) > 0$ (համապատասխանաբար, $q(x) < 0$) ցանկացած ոչ զրոյական $x \in Q_1$ տարրի (վեկտորի) համար ($q(0) = 0$): $Q_1 = Q$ ենթատարածության վրա դրական որոշյալ (բացասական որոշյալ) քառակուսային ձևը կոչվում է Q-ի դրական որոշյալ (բացասական որոշյալ) քառակուսային ձև:

Լեմմ 17.44: *Դիցուք Q-ն վերջավոր չափանի իրական գծային տարածություն է: **Եթե** (k, ℓ)-ը $q : Q \to \mathbb{R}$ իրական քառակուսային ձևի նշիչն (սիգնատուրան) է $e'_1, \ldots, e'_n$ նորմալ հենքի նկատմամբ և $Q_1 = (e'_1, \ldots, e'_k)$, իսկ $Q_2 = \left(e'_{k+1}, \ldots, e'_{k+\ell}\right)$, ապա q-ն կլինի դրական որոշյալ Q_1 ենթատարածության վրա և բացասական որոշյալ Q_2 ենթատարածության վրա:* □

Լեմմ 17.45: *Դիցուք Q-ն վերջավոր չափանի իրական գծային տարածություն է: **Եթե** (k, ℓ)-ը $q : Q \to \mathbb{R}$ իրական քառակուսային ձևի նշիչն (սիգնատուրան) է և q-ն դրական որոշյալ (բացասական որոշյալ) է $U \leqslant Q$ ենթատարածության վրա, ապա $dim(U) \leqslant k$ (համապատասխանաբար, $dim(U) \leqslant \ell$):*

Ապացուցում: Դիցուք $dim(Q) = n$ և (k, ℓ)-ը q իրական քառակուսային ձևի նշիչն (սիգնատուրան) է $e'_1, \ldots, e'_n$ նորմալ հենքի նկատմամբ, իսկ $Q_1 = (e'_1, \ldots, e'_k)$, $Q'_1 = \left(e'_{k+1}, \ldots, e'_n\right)$: **Եթե** $x \in U \cap Q'_1$ և $x \neq 0$, ապա $x \in U$, $x \in Q'_1$ և մի կողմից՝ $q(x) > 0$, իսկ մյուս կողմից՝ $q(x) \leqslant 0$: Հակասություն:

Հետևաբար, $U \cap Q'_1 = \{0\}$: Դիտարկենք $U + Q'_1 \leqslant Q$ ենթատարածությունը: Մի կողմից՝ $dim\,(U + Q'_1) \leqslant dim(Q) = n$, իսկ մյուս կողմից՝ $dim\,(U + Q'_1) = dim(U) + dim(Q'_1) - dim\,(U \cap Q'_1) = dim(U) + n - k - 0$: Ուստի, $dim(U) \leqslant k$: Ճիշտ նույն եղանակով կապացուցվի U-ի վրա բացասական որոշյալ քառակուսային ձևի դեպքը: □

Թեորեմ 17.50 (Իրական քառակուսային ձևի իներցիայի օրենքը): *Իրական քառակուսային ձևի նշիչը (սիգնատուրան) կախված չէ վերջավոր չափանի իրական գծային տարածության մեջ նորմալ հենքի ընտրությունից:*

Ապացուցում: Դիցուք q իրական քառակուսային ձևը մի նորմալ հենքի նկատմամբ ունի (k,ℓ) նշիչը (սիգնատուրան), իսկ մեկ այլ նորմալ հենքի նկատմամբ՝ (k',ℓ') նշիչը, որտեղ $rank(q)=k+\ell=k'+\ell'$: Պահանջվում է ապացուցել $(k,\ell)=(k',\ell')$ հավասարությունը: Իրոք, եթե $k<k'$, ապա $\ell>\ell'$, որը հակասում է վերջին լեմմին: Նույնպիսի հակասության ենք հանգում նաև $k>k'$ դեպքում: Հետևաբար, $k=k'$, որտեղից բխում է նաև $\ell=\ell'$ հավասարությունը: □

Լեմմ 17.46: *Որպեսզի վերջավոր չափանի Q իրական գծային տարածության q քառակուսային ձևը լինի դրական որոշյալ անհրաժեշտ է և բավարար, որ նրա նշիչը (սիգնատուրան) լինի $(n,0)$ տեսքի, որտեղ $n=dim(Q)>0$:*

Ապացուցում: Դիցուք $dim\,(Q)=n>0$: *Բավարարությունն* ակնհայտ է, որովհետև, եթե Q-ի $e_1,\dots,e_n$ նորմալ հենքում՝

$$q(x)=x_1^2+\cdots+x_n^2\,,$$

որտեղ $x=x_1e_1+\cdots+x_ne_n$, ապա $q(x)>0$, եթե $x\neq 0$, $x\in Q$:

Անհրաժեշտություն: Դիցուք Q-ի $e_1,\dots,e_n$ նորմալ հենքում q դրական որոշյալ քառակուսային ձևն ունի հետևյալ տեսքը՝

$$q(x)=x_1^2+\cdots+x_k^2-x_{k+1}^2-\cdots-x_{k+\ell}^2\,,$$

որտեղ $x=x_1e_1+\cdots+x_ne_n$, $k+\ell=rank(q)\leqslant n$: Եթե $\ell>0$, ապա ընտրելով $x=0e_1+\cdots+0e_k+e_{k+1}+\cdots+e_n\neq 0$, կունենանք՝

$$q(x)=\underbrace{0^2+\cdots+0^2}_{k}-\underbrace{1^2-\cdots-1^2}_{\ell}<0\,,$$

որը հակասում է q-ի սահմանմանը: Հետևաբար, $\ell=0$, այսինքն՝ q-ի նշիչը (սիգնատուրան) կունենա $(k,0)$ տեսքը: Եթե այստեղ $k<n$, ապա x-ի նույն ընտրության դեպքում, կունենանք՝ $q(x)=0$, որը նույնպես հակասում է q-ի սահմանմանը: Այսպիսով՝ $k=n$: □

Հետևություն 17.44: *Վերջավոր չափանի Q իրական գծային տարածության q դրական որոշյալ քառակուսային ձևի համար՝ $rank(q) = dim(Q)$:* □

Լեմմ 17.47: *Եթե վերջավոր չափանի Q իրական գծային տարածության q քառակուսային ձևը դրական որոշյալ է, ապա Q-ի ցանկացած հենքի նկատմամբ q-ի ունեցած մատրիցի որոշիչը դրական է:*

Ապացուցում: Նախորդ լեմմից բխում է, որ Q-ի նորմալ հենքի նկատմամբ q-ի A մատրիցի որոշիչը հավասար է 1-ի: Սակայն, ցանկացած հենքի նկատմամբ q-ի ունեցած B մատրիցը կոնգրուենտ է A-ին, այսինքն՝ գոյություն ունի այնպիսի հակադարձելի C մատրից, որ

$$B = CAC^T \ :$$

Հետևաբար, B և A մատրիցների որոշիչները կունենան նույն նշանը, որովհետև $det(B) = det(CAC^T) = det(C)det(A)det(C^T) = (det(C))^2 > 0$: □

Դիցուք Q-ն n-չափանի իրական գծային տարածություն է $e_1, \ldots, e_n$ հենքով, f-ը Q-ի սիմետրիկ երկգծային ձև է, իսկ

$$A = \begin{pmatrix} a_{11}, \ \ldots, \ a_{1n} \\ \ldots \ \ \ldots \ \ \ldots \\ a_{n1}, \ \ldots, \ a_{nn} \end{pmatrix} \in \mathbb{R}^{n \times n}$$

մատրիցը f-ի մատրիցն է $e_1, \ldots, e_n$ հենքում, այսինքն՝ $a_{ij} = f(e_i, e_j) \in \mathbb{R}$: Ըստ սահմանման, A-ն կլինի նաև $q = f^*$ քառակուսային ձևի մատրիցը նույն հենքում: Եթե $1 \leqslant k \leqslant n$, ապա

$$\delta_k = det \begin{pmatrix} a_{11}, \ \ldots, \ a_{1k} \\ \ldots \ \ \ldots \ \ \ldots \\ a_{k1}, \ \ldots, \ a_{kk} \end{pmatrix}$$

որոշիչը կոչվում է A մատրիցի k-րդ **գլխավոր** կամ **անկյունագծային** մինոր: Մասնավորապես, $\delta_1 = a_{11}$, իսկ $\delta_n = |A|$: $\delta_1, \ldots, \delta_n$ որոշիչները կոչվում են նաև $q = f^*$ քառակուսային ձևի գլխավոր կամ անկյունագծային մինորներ՝ $e_1, \ldots, e_n$ հենքի նկատմամբ:

Թեորեմ 17.51 (Սիլվեստրի հայտանիշը): *Դիցուք Q-ն n-չափանի իրական գծային տարածություն է:*

1) Եթե Q-ի $q = f^*$ քառակուսային ձևը դրական որոշյալ է, ապա ցանկացած հենքի նկատմամբ նրա ունեցած բոլոր անկյունագծային մինորները կլինեն դրական;

2) Եթե $q = f^*$ քառակուսային ձևի Q-ի որևէ հենքի նկատմամբ ունեցած բոլոր անկյունագծային մինորները դրական են, ապա q-ն կլինի դրական որոշյալ:

Ապացույց: 1)-ը ապացուցենք վերհանգման եղանակով՝ ըստ n-ի: $n = 1$ դեպքում պնդումն ակնհայտ է, որովհետև այս դեպքում՝ $x = x_1e_1$ ցանկացած $x \in Q$ տարրի (վեկտորի) համար և $q = f^*$ քառակուսային ձևի համար կունենանք՝

$$q(x) = f(x, x) = f(x_1e_1, x_1e_1) = f(e_1, e_1)x_1^2 = a_{11}x_1^2 \ :$$

Դիցուք պնդումը ճիշտ է n-ից փոքր չափողականություն ունեցող գծային տարածությունների համար և դիցուք

$$q(x) = f(x, x) = \sum_{i,j=1}^{n} a_{ij}x_ix_j \ ,$$

որտեղ $x = x_1e_1 + \cdots + x_ne_n$, $a_{ij} = f(e_i, e_j)$, իսկ $e_1, \ldots, e_n$-ը Q-ի ցանկացած հենք է: Նշանակենք $Q' = (e_1, \ldots, e_{n-1})$ և գրենք՝

$$q(x) = \sum_{i,j=1}^{n-1} a_{ij}x_ix_j + 2\sum_{i=1}^{n-1} a_{in}x_ix_n + a_{nn}x_n^2 \ :$$

Ակնհայտ է, որ $dim(Q') = n - 1$ և

$$q'(x') = \sum_{i,j=1}^{n-1} a_{ij}x_ix_j$$

բանաձևով որոշվող $q' : Q \to \mathbb{R}$ արտապատկերումը կլինի Q'-ի քառակուսային ձև, որտեղ $x' \in Q'$, $x' = x_1e_1 + \cdots + x_{n-1}e_{n-1}$: Ակնհայտ է նաև, որ այս q' քառակուսային ձևը դրական որոշյալ է, որովհետև եթե $q'(x') \leqslant 0$ որևէ $x' \in Q'$, $x' = x_1e_1 + \cdots + x_{n-1}e_{n-1} \neq 0$ տարրի համար, ապա $q(x) \leqslant 0$, որտեղ $x = x_1e_1 + \cdots + x_{n-1}e_{n-1} + 0x_n \neq 0$: Ըստ վերհանգման ենթադրության q'-ի բոլոր $\delta_1, \ldots, \delta_{n-1}$ անկյունագծային մինորները կլինեն դրական, իսկ δ_n-ի դրական լինելը բխում է նախորդ լեմմից:

2) Դիցուք $q = f^*$ քառակուսային ձևի որևէ $e_1, \ldots, e_n$ հենքում ունեցած բոլոր $\delta_1, \ldots, \delta_n = |A|$ անկյունագծային մինորները դրական են: Պահանջվում է ապացուցել, որ այդ դեպքում q-ն դրական որոշյալ է: Այս պնդումը նույնպես կապացուցենք վերհանգման եղանակով՝ ըստ n-ի: $n = 1$ դեպքում այն ակնհայտ է: Դիցուք պնդումը ճիշտ է n-ից փոքր բնական թվերի դեպքում և

$$q(x) = f(x, x) = \sum_{i,j=1}^{n-1} a_{ij} x_i x_j + 2 \sum_{i=1}^{n-1} a_{in} x_i x_n + a_{nn} x_n^2 ,$$

որտեղ $x = x_1 e_1 + \cdots + x_n e_n$, $a_{ij} = f(e_i, e_j)$: Եթե $Q' = (e_1, \ldots, e_{n-1})$, ապա $dim(Q') = n - 1$, $Q = Q' \oplus (e_n)$ և վերհանգման ենթադրության համաձայն՝

$$q'(x') = \sum_{i,j=1}^{n-1} a_{ij} x_i x_j$$

բանաձևով որոշվող $q' : Q' \to \mathbb{R}$ քառակուսային ձևը կլինի դրական որոշյալ, որտեղ $x' \in Q'$, $x' = x_1 e_1 + \cdots + x_{n-1} e_{n-1}$: Հետևաբար, q'-ը Q'-ի որևէ $e'_1, \ldots, e'_{n-1}$ հենքում կունենա հետևյալ նորմալ տեսքը (լեմմ 17.46)՝

$$q'(x') = (x'_1)^2 + \cdots + \left(x'_{n-1}\right)^2 ,$$

որտեղ $x' = x'_1 e'_1 + \cdots + x'_{n-1} e'_{n-1}$: Դիտարկենք Q-ի $e'_1, \ldots, e'_{n-1}, e'_n$ հենքը, որտեղ $e'_n = e_n$: Այս հենքի նկատմամբ՝

$$q(x) = (x'_1)^2 + \cdots + \left(x'_{n-1}\right)^2 +$$

$$+2 \left(b_{1n} x'_1 x'_n + b_{2n} x'_2 x'_n + \cdots + b_{n-1,n} x'_{n-1} x'_n\right) + a_{nn} \left(x'_n\right)^2 ,$$

որտեղ $x = x'_1 e'_1 + \cdots + x'_{n-1} e'_{n-1} + x'_n e'_n$, $b_{ij} = f\left(e'_i, e'_j\right)$: Այնուհետև,

$$q(x) = (x'_1 + b_{1n} x'_n)^2 + (x'_2 + b_{2n} x'_n)^2 + \cdots + \left(x'_{n-1} + b_{n-1,n} x'_n\right)^2 + b \left(x'_n\right)^2 ,$$

որտեղ $b = a_{nn} - b_{1n}^2 - b_{2n}^2 - \cdots - b_{n-1,n}^2$: Այժմ կատարենք անցում $e'_1, \ldots, e'_n$ հենքից այնպիսի $e''_1, \ldots, e''_n$ հենքի, որի նկատմամբ $x = x''_1 e''_1 + \cdots + x''_n e''_n$ վեկտորի կոորդինատները որոշվում են հետևյալ կերպ՝

$$\begin{aligned}
x''_1 &= x'_1 + b_{1n} x'_n , \\
x''_2 &= x'_2 + b_{2n} x'_n , \\
&\ldots \quad \ldots \quad \ldots \quad \ldots \\
x''_{n-1} &= x'_{n-1} + b_{n-1,n} x'_n , \\
x''_n &= \qquad\qquad\quad x'_n ;
\end{aligned}$$

Այստեղ, x-ի $x'_1, \ldots, x'_n$ կոորդինատներից $x''_1, \ldots, x''_n$ կոորդինատներին անցման

$$B = \begin{pmatrix} 1,\ 0,\ \ldots,\ 0,\ b_{1n} \\ 0,\ 1,\ \ldots,\ 0,\ b_{2n} \\ \ldots\ \ \ldots\ \ \ldots\ \ \ldots \\ 0,\ 0,\ \ldots,\ 1,\ b_{n-1,n} \\ 0,\ 0,\ \ldots,\ 0,\ 1 \end{pmatrix}$$

մատրիցի որոշիչը հավասար է 1-ի: Հետևաբար, B-ն հակադարձելի է և $\left(B^{-1}\right)^T = (t_{ij})$ մատրիցը կլինի $e'_1, \ldots, e'_n$ հենքից նոր $e''_1, \ldots, e''_n$ հենքին անցման մատրիցը, այսինքն՝

$$\begin{aligned} e''_1 &= t_{11}e'_1 + \cdots + t_{1n}e'_n\,, \\ &\ldots\ \ \ldots\ \ \ldots\ \ \ldots \\ e''_n &= t_{n1}e'_1 + \cdots + t_{nn}e'_n\ : \end{aligned}$$

Արդյունքում, ընտրված $e''_1, \ldots, e''_n$ հենքի նկատմամբ կունենանք՝

$$q(x) = (x''_1)^2 + \cdots + \left(x''_{n-1}\right)^2 + b\,(x''_n)^2\ ,$$

այսինքն՝ q-ի $e''_1, \ldots, e''_n$ հենքի նկատմամբ ունեցած Δ մատրիցի որոշիչը կլինի հավասար b-ի: Սակայն, Δ և սկզբնական A մատրիցները կոնգրուենտ են: Հետևաբար, դրանց որոշիչները կունենան նույն նշանը, այսինքն՝ $b > 0$ և q քառակուսային ձևը կլինի դրական որոշյալ: □

17.20. Էվկլիդյան (էվկլիդեսյան) տարածություններ: Պյութագորասի թեորեմը, Կոշի-Բունյակովսկու անհավասարությունը: Օրթոգոնալացման ընթացքը: Էվկլիդյան տարածությունների իզոմորֆիզմը

Q իրական գծային տարածության $f : Q \times Q \to \mathbb{R}$ սիմետրիկ երկգծային ձևը կոչվում է **դրական որոշյալ**, եթե դրան համապատասխանող $f^* : Q \to \mathbb{R}$ քառակուսային ձևը դրական որոշյալ է: Q իրական գծային տարածության ցանկացած $f : Q \times Q \to \mathbb{R}$ սիմետրիկ և դրական որոշյալ երկգծային ձև կոչվում է Q-ի (վրա որոշված) **սկալյար արտադրյալ**, այսինքն՝ $f : Q \times Q \to \mathbb{R}$ արտապատկերումը (ֆունկցիան) կոչվում է Q-ի սկալյար արտադրյալ, եթե այն բավարարում է հետևյալ պայմաններին.

ա) $f(x_1 + x_2, y) = f(x_1, y) + f(x_2, y)$,

$f(\alpha x, y) = \alpha f(x, y)$
ցանկացած $x, y, x_1, x_2 \in Q$ տարրերի (վեկտորների) և ցանկացած $\alpha \in \mathbb{R}$ սկալյարի համար (գծայնության պայման՝ ըստ առաջին արգումենտի);

բ) $f(x, y) = f(y, x)$
ցանկացած $x, y \in Q$ տարրերի (վեկտորների) համար (համաչափության կամ սիմետրիկության պայման);

գ) $f(x, x) > 0$ ցանկացած ոչ զրոյական $x \in Q$ տարրի (վեկտորի) համար ($f(0, 0) = 0$), այսինքն՝ $f(x, x) \geqslant 0$ ցանկացած $x \in Q$ վեկտորի համար և $f(x, x) = 0 \longleftrightarrow x = 0$ (դրական որոշյալության պայման):

Նկատենք, որ եթե f-ը սկալյար արտադրյալ է, ապա

$$f(x, 0) = f(0, x) = 0,$$

$$f(-x, y) = f(x, -y) = -f(x, y),$$

$$f(x_1 - x_2, y) = f(x_1, y) - f(x_2, y) :$$

Q իրական գծային տարածությունն իր կամայական f սկալյար արտադրյալի հետ մեկտեղ կոչվում է **էվկլիդյան** կամ **էվկլիդեսյան տարածություն** և նշանակվում է (Q, f)-ով կամ համառոտ Q-ով: Եթե (Q, f)-ը էվկլիդյան տարածություն է, ապա Q-ն կոչվում է էվկլիդյան տարածություն՝ f սկալյար արտադրյալով կամ f սկալյար արտադրյալի նկատմամբ: Q գծային տարածության տարրերը (վեկտորները) կոչվում են նաև (Q, f) էվկլիդյան տարածության տարրեր (վեկտորներ): Q գծային տարածության հենքը կոչվում է նաև հենք (Q, f) էվկլիդյան տարածության համար, իսկ (Q, f)-ի չափողականություն ասելով հասկացվում է Q-ի չափողականությունը: Մասնավորապես, (Q, f) էվկլիդյան տարածությունը կկոչվի n-չափանի, եթե n-չափանի է Q գծային տարածությունը:

(Q, f) էվկլիդյան տարածության տարրերի համակարգը կոչվում է գծայնորեն կամ գծորեն կախյալ (անկախ), եթե այդ համակարգը գծայնորեն կախյալ (անկախ) է Q գծային տարածության մեջ:

Եթե $Q' \subseteq Q$, ապա յուրաքանչյուր $f : Q \times Q \to \mathbb{R}$ արտապատկերում մակածում է արտապատկերում՝ $Q' \times Q' \to \mathbb{R}$, որը սովորաբար նշանակվում է նույն f տառով: Հետևաբար, եթե (Q, f)-ը էվկլիդյան տարածություն է և $Q' \leqslant Q$, ապա (Q', f)-ը նույնպես կլինի էվկլիդյան տարածություն: Այս պատճառով, Q գծային տարածության յուրաքանչյուր $Q' \leqslant Q$ ենթատարածություն կոչվում է նաև (Q, f) էվկլիդյան տարածության ենթատարածություն:

Էվկլիդյան տարածությունը կոչվում է **զրոյական**, եթե այն որպես գծային տարածություն զրոյական է, այսինքն՝ մեկ տարրանի է: Հակառակ դեպքում էվկլիդյան տարածությունը կոչվում է ոչ զրոյական:

Հետևյալ հատկությունները բխում են նախորդ երկու վերնագրերի ընդհանուր գաղափարներից և արդյունքներից:

Հատկություն 17.14: *Սկալյար արտադրյալը չվերասերված երկգծային ձև է:*

Ապացույց: Իրոք, ըստ սահմանման, f սկալյար արտադրյալի համար՝

$$Ker(f) = \{y \in Q \mid f(x, y) = 0, \forall x \in Q\} :$$

Հետևաբար, $x = y$ դեպքում կունենանք $f(y, y) = 0$ և $y = 0$: Այսպիսով, $Ker(f) = \{0\}$: □

Հատկություն 17.15: *Վերջավոր չափանի (Q, f) էվկլիդյան տարածության ցանկացած $U \leqslant Q$ ենթատարածության համար՝*

$$(U^\perp)^\perp = U, \text{ (Դե Մորգանի հավասարություն (նույնություն))}$$

որտեղ $U^\perp$-ը U-ի օրթոգոնալ լրացումն է f-ի նկատմամբ:

Ապացույց: f սկալյար արտադրյալը չվերասերված և սիմետրիկ երկգծային ձև է: Հետևաբար և սիմետրիկ է ըստ զրոյի, իսկ այս դեպքի համար պնդումն ապացուցված է (հետևություն 17.34): □

Թեորեմ 17.52: *Վերջավոր չափանի Q էվկլիդյան տարածությունը հավասար է իր ցանկացած $U \leqslant Q$ ենթատարածության և դրա օրթոգոնալ լրացման ուղիղ գումարին՝*

$$Q = U \oplus U^\perp :$$

Ապացույց: Չվերասերված երկգծային ձևի դեպքում ունենք՝ $dim(U^\perp) = dim(Q) - dim(U)$, այսինքն՝ $dim(Q) = dim(U) + dim(U^\perp)$: Սակայն այս դեպքում նաև՝ $U \cap U^\perp = \{0\}$, որովհետև, եթե $x \in U \cap U^\perp$, ապա $x \in U$ և $x \in U^\perp$: Հետևաբար, $f(x, x) = 0$ և $x = 0$: Ուստի,

$$dim(Q) = dim(U) + dim(U^\perp) - dim(U \cap U^\perp) = dim(U + U^\perp),$$

և քանի որ $U + U^\perp \leqslant Q$, ապա $Q = U + U^\perp$, որտեղ $U \cap U^\perp = \{0\}$: Այսպիսով, $Q = U \oplus U^\perp$: □

Հատկություն 17.16: *Վերջավոր չափանի ոչ զրոյական Q էվկլիդյան տարածությունն ունի օրթոգոնալ հենք իր f սկալյար արտադրյալի նկատմամբ:*

Ապացուցում: f սկալյար արտադրյալը սիմետրիկ երկգծային ձև է, իսկ այդ դեպքում պնդումն ապացուցված է (թեորեմ 17.49): □

(Q, f) էվկլիդյան տարածության x և y տարրերը (վեկտորները) կոչվում են **օրթոգոնալ** և գրվում է $x \perp y$, եթե $f(x, y) = 0$, իսկ տարրերի (վեկտորների) $x_1, \ldots, x_k$ համակարգը կոչվում է **օրթոգոնալ**, եթե $f(x_i, x_j) = 0$, որտեղ $i \neq j$ և $i, j = 1, \ldots, k$, այսինքն՝ երբ $x_1, \ldots, x_k$ համակարգի վեկտորները զույգ առ զույգ օրթոգոնալ են:

Լեմմ 17.48 (հիմնական): *(Q, f) էվկլիդյան տարածության ոչ զրոյական տարրերի յուրաքանչյուր $a_1, \ldots, a_k$ օրթոգոնալ համակարգ գծայնորեն անկախ է:*

Ապացուցում (վերհանգման եղանակ): $k = 1$ դեպքում պնդումն ակնհայտ է, որովհետև մեկ ոչ զրոյական տարրից կազմված համակարգը գծայնորեն անկախ է: Ենթադրենք $k > 1$ և պնդումն ճիշտ է $k - 1$ թվով ոչ զրոյական տարրերի դեպքում ու ապացուցենք k թվով ոչ զրոյական տարրերի համար: Դիցուք

$$\alpha_1 a_1 + \cdots + \alpha_{k-1} a_{k-1} + \alpha_k a_k = 0 :$$

Հետևաբար,

$$f(\alpha_1 a_1 + \cdots + \alpha_{k-1} a_{k-1} + \alpha_k a_k, a_k) = f(0, a_k) = 0,$$

որտեղից՝

$$\alpha_1 f(a_1, a_k) + \cdots + \alpha_{k-1} f(a_{k-1}, a_k) + \alpha_k f(a_k, a_k) = 0$$

և $\alpha_k f(a_k, a_k) = 0$, որտեղ $f(a_k, a_k) > 0$: Ուստի, $\alpha_k = 0$: Արդյունքում՝

$$\alpha_1 a_1 + \cdots + \alpha_{k-1} a_{k-1} = 0$$

և, համաձայն վերհանգման ենթադրության, $\alpha_1 = \cdots = \alpha_{k-1} = 0$: □

Հետևություն 17.45: *n-չափանի էվկլիդյան տարածության n հատ ոչ զրոյական տարրերից կազմված յուրաքանչյուր օրթոգոնալ համակարգ հենք է:* □

(Q, f) էվկլիդյան տարածության տարրերի $a_1, \ldots, a_m \in Q$ հաջորդականությունը կոչվում է **նորմավորված**, եթե $f(a_i, a_i) = 1$ ցանկացած $i = 1, \ldots, m$ արժեքների դեպքում: Հաջորդականությունը կոչվում է **օրթոնորմավորված (կամ օրթոնորմալ)** , եթե այն օրթոգոնալ է և նորմավորված: Հենքը կոչվում է օրթոնորմավորված (կամ օրթոնորմալ) , եթե այն նաև օրթոնորմավորված հաջորդականություն է:

Հատկություն 17.17: *Վերջավոր չափանի ոչ զրոյական* (Q, f) *էվկլիդյան տարածությունն ունի օրթոնորմավորված հենք:*

Ապացուցում: Նախորդ հատկության համաձայն Q-ն ունի օրթոգոնալ հենք: Դիցուք Q-ի $e_1, \ldots, e_n$ հենքն այդպիսին է: Այդ դեպքում $e_1, \ldots, e_n$ հաջորդականության յուրաքանչյուր տարր կլինի ոչ զրոյական, իսկ

$$e_1' = \frac{e_1}{\sqrt{f(e_1, e_1)}}, \ldots, e_n' = \frac{e_n}{\sqrt{f(e_n, e_n)}}$$

հաջորդականությունը կլինի օրթոնորմավորված: Հետևաբար, $e_1', \ldots, e_n'$ հաջորդականությունը կլինի օրթոնորմավորված հենք՝ համաձայն վերջին լեմմի: □

Եթե f-ը սկալյար արտադրյալ է, ապա $f(x, y)$-ը ընդունված է համառոտ նշանակել (x, y)-ով: Այդ դեպքում, (x, x)-ը կոչվում է (x-ի) սկալյար քառակուսի:

Օրինակներ: 1) Հարթության վրա (մեջ) գտնվող բոլոր երկրաչափական վեկտորների գծային տարածությունը էվկլիդյան տարածություն է

$$(x, y) = |x| \cdot |y| \cdot \cos(\widehat{x, y})$$

սկալյար արտադրյալով:

2) $\mathbb{R}_n$ գծային տարածությունը էվկլիդյան տարածություն է

$$(x, y) = x_1 y_1 + \cdots + x_n y_n$$

սկալյար արտադրյալով, որտեղ $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n)$: $\mathbb{R}^n$-ը ևս էվկլիդյան տարածություն է նույն սկալյար արտադրյալի նկատմամբ՝

$(x, y) = x_1 y_1 + \cdots + x_n y_n$, եթե $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$:

3) $[a,b] \subseteq \mathbb{R}$ հատվածում ($a < b$) անընդհատ ֆունկցիաների $C[a,b]$ գծային տարածությունը էվկլիդյան տարածություն է

$$(f,g) = \int_a^b f(x)\,g(x)\,dx$$

սկալյար արտադրյալով: Իրական գործակիցներով բոլոր բազմանդամների (կամ n-ը չգերազանցող աստիճան ունեցող բոլոր բազմանդամների) գծային տարածությունը էվկլիդյան տարածություն է նշված սկալյար արտադրյալի նկատմամբ:

4) $e_1, \ldots, e_n$ հենքով յուրաքանչյուր n-չափանի Q իրական գծային տարածություն էվկլիդյան տարածություն է

$$(x,y) = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$$

սկալյար արտադրյալով, որտեղ $x = \alpha_1 e_1 + \cdots + \alpha_n e_n$, $y = \beta_1 e_1 + \cdots + \beta_n e_n$:

Էվկլիդյան տարածության մեջ սահմանվում է նրա վեկտորի (տարրի) երկարության կամ նորմի, ինչպես նաև երկու վեկտորների կազմած անկյան գաղափարները, որոնք երկրաչափական վեկտորների դեպքում հանգում են դպրոցական դասընթացից հայտնի համապատասխան հասկացություններին: Դիցուք Q-ն էվկլիդյան տարածություն է, $x \in Q$ տարրի (վեկտորի) **երկարությունը** կամ **նորմը** նշանակվում է $|x|$-ով և սահմանվում է հետևյալ կերպ.

$$|x| = \sqrt{(x,x)}\ :$$

Հետևաբար,

ա) $|x| \geqslant 0$ ցանկացած $x \in Q$ տարրի (վեկտորի) համար: Ըստ որում, $|x| = 0$ այն և միայն այն դեպքում, երբ $x = 0$;

բ) $|-x| = |x|$ ցանկացած $x \in Q$ տարրի (վեկտորի) համար;

գ) $|\alpha x| = |\alpha| \cdot |x|$ ցանկացած $x \in Q$ տարրի (վեկտորի) և ցանկացած $\alpha \in \mathbb{R}$ սկալյարի համար, որտեղ $|\alpha| = \sqrt{\alpha^2}$:

Պյութագորասի թեորեմը: *Եթե Q էվկլիդյան տարածության x և y վեկտորները (տարրերը) օրթոգոնալ են, ապա*

$$|x \pm y|^2 = |x|^2 + |y|^2\ :$$

Ապացուցում: Իրոք, եթե $(x,y)=0$, ապա

$$|x+y|^2=(x+y,x+y)=(x,x)+(x,y)+(y,x)+(y,y)=$$

$$=(x,x)+(y,y)=|x|^2+|y|^2:$$

Այնուհետև, եթե $(x,y)=0$, ապա $(x,-y)=-(x,y)=0$ և

$$|x-y|^2=|x+(-y)|^2=|x|^2+|-y|^2=|x|^2+|y|^2: \qquad \square$$

Պյութագորասի ընդհանրացված թեորեմը: *Եթե Q էվկլիդյան տարածության վեկտորների (տարրերի) $x_1,\ldots,x_k$ համակարգը օրթոգոնալ է, ապա*

$$|x_1+\cdots+x_k|^2=|x_1|^2+\cdots+|x_k|^2:$$

Ապացուցում (վերհանգման եղանակ): $k=1,2$ դեպքում պնդումը ճիշտ է: Ենթադրենք $k>2$ և պնդումը ճիշտ է k-ից քիչ թվով վեկտորների համար: Նկատելով x_k և $x_1+\cdots+x_{k-1}$ վեկտորների օրթոգոնալությունը ($(x_k,x_1+\cdots+x_{k-1})=(x_k,x_1)+\cdots+(x_k,x_{k-1})=0+\cdots+0=0$) և օգտվելով նախորդ թեորեմից, կունենանք՝

$$|x_1+\cdots+x_k|^2=|(x_1+\cdots+x_{k-1})+x_k|^2=$$

$$=|x_1+\cdots+x_{k-1}|^2+|x_k|^2=|x_1|^2+\cdots|x_{k-1}|^2+|x_k|^2: \qquad \square$$

Թեորեմ 17.53 (Կոշի-Բունյակովսկու անհավասարությունը): *Q էվկլիդյան տարածության ցանկացած $x,y\in Q$ վեկտորների (տարրերի) համար՝*

$$|(x,y)|\leqslant|x|\cdot|y|\,,$$

որի ձախ մասում իրական թվի մոդուլն է: Ըստ որում, հավասարությունը տեղի կունենա այն և միայն այն դեպքում, երբ x, y համակարգը գծայնորեն կախյալ է:

Ապացուցում: Եթե x, y համակարգը գծայնորեն կախյալ է, ապա $y=\lambda x$ կամ $x=\lambda y$: Դիցուք $y=\lambda x$: Այդ դեպքում՝

$$|(x,y)|=|(x,\lambda x)|=|\lambda|\cdot|(x,x)|=|\lambda|\cdot|x|^2=$$

$$= |x| \cdot (|\lambda| \cdot |x|) = |x| \cdot |y| \ :$$

Նույն արդյունքը կստացվի նաև $x = \lambda y$ դեպքում: Եթե x, y համակարգը գծայնորեն անկախ է, ապա այն կլինի հենք $x, y \in Q$ տարրերով ծնված $\langle x, y \rangle$ գծային թաղանթի համար: Q-ի սկալյար արտադրյալը լինելով սիմետրիկ և դրական որոշյալ երկգծային ձև, այդպիսին կլինի նաև $Q' = \langle x, y \rangle$ ենթատարածության համար: Սակայն սկալյար արտադրյալի մատրիցը x, y հենքի նկատմամբ կլինի՝

$$\begin{pmatrix} (x,x)\,, & (x,y) \\ (x,y)\,, & (y,y) \end{pmatrix},$$

որի որոշիչը կլինի խիստ դրական (լեմմ 17.51): Հետևաբար, $(x,x)(y,y) - (x,y)^2 > 0$, $(x,x)(y,y) > (x,y)^2$, որտեղից՝ $\sqrt{(x,y)^2} < \sqrt{(x,x)}\sqrt{(y,y)}$:

Երկրորդ ապացուցում: Եթե x, y համակարգը գծայնորեն անկախ է, ապա $x \neq 0$ և $tx + y \neq 0$ ցանկացած $t \in \mathbb{R}$ իրական թվի դեպքում: Ուստի՝ $(x,x) > 0$ և

$$|tx + y|^2 = (tx + y, tx + y) = t^2(x,x) + 2t(x,y) + (y,y) > 0 \ :$$

Հետևաբար, ստացված քառակուսի եռանդամի դիսկրիմինանտը կլինի բացասական՝

$$\mathcal{D} = (x,y)^2 - (x,x)(y,y) = (x,y)^2 - |x|^2|y|^2 < 0 \ : \qquad \square$$

Հետևություն 17.46 (Եռանկյան անհավասարությունը): *Q էվկլիդյան տարածության ցանկացած $x, y \in Q$ վեկտորների (տարրերի) համար՝*

$$|x \pm y| \leqslant |x| + |y| \ :$$

Ապացուցում: Իրոք,

$$|x+y|^2 = (x+y, x+y) = (x,x) + (x,y) + (y,x) + (y,y) =$$

$$= |x|^2 + 2(x,y) + |y|^2 \leqslant |x|^2 + 2|x| \cdot |y| + |y|^2 = (|x| + |y|)^2 \ :$$

Հետևաբար, $\sqrt{|x+y|^2} \leqslant \sqrt{(|x| + |y|)^2}$ և $|x+y| \leqslant |x| + |y|$: Այնուհետև,

$$|x - y| = |x + (-y)| \leqslant |x| + |-y| = |x| + |y| \ : \qquad \square$$

Հետևություն 17.47: *Էվկլիդյան տարածության ցանկացած* x, y *վեկտորների համար՝*

$$|x \pm y| \geqslant |x| - |y| :$$

Ապացուցում: Բխում է եռանկյան անհավասարությունից: Իրոք,

$$|x| = |(x-y)+y| \leqslant |x-y| + |y|,$$

որտեղից $|x-y| \geqslant |x| - |y|$, իսկ

$$|x+y| = |x-(-y)| \geqslant |x| - |-y| = |x| - |y| : \qquad \square$$

Էվկլիդյան տարածության մեջ

$$\rho(x,y) = |x-y| \geqslant 0$$

մեծությունը կոչվում է x և y **վեկտորների** (տարրերի) **հեռավորություն**:

Հետևություն 17.48: Q *էվկլիդյան տարածության մեջ սահմանված* $\rho : Q \times Q \to \mathbb{R}$ *արտապատկերումը բավարարում է մետրիկայի աքսիոմներին, այսինքն՝*

M_1) $\rho(x,y) \geqslant 0$ ցանկացած $x, y \in Q$ վեկտորների համար և $\rho(x,y) = 0 \longleftrightarrow x = y$;

M_2) $\rho(x,y) = \rho(y,x)$ ցանկացած $x, y \in Q$ վեկտորների համար;

M_3) $\rho(x,z) \leqslant \rho(x,y) + \rho(y,z)$ ցանկացած $x, y, z \in Q$ վեկտորների համար:

Ապացուցում: M_1) և M_2) հատկությունները ակնհայտ են և բխում են նորմի սահմանումից: M_3) հատկությունը բխում է եռանկյան անհավասարությունից՝

$$\rho(x,z) = |x-z| = |(x-y)+(y-z)| \leqslant$$

$$\leqslant |x-y| + |y-z| = \rho(x,y) + \rho(y,z) \ : \qquad \square$$

Հետևություն 17.49: Q *էվկլիդյան տարածության ցանկացած* $x, y \in Q$ *ոչ զրոյական վեկտորների (տարրերի) համար՝*

$$-1 \leqslant \frac{(x,y)}{|x| \cdot |y|} \leqslant 1 \ : \qquad \square$$

Հետևաբար, էվկլիդյան տարածության x և y ոչ զրոյական վեկտորների (տարրերի) կազմած $\widehat{x,y}$ **անկյունը** կարելի է սահմանել հետևյալ բանաձևով՝

$$\cos(\widehat{x,y}) = \frac{(x,y)}{|x|\cdot|y|}\,, \qquad 0 \leqslant \widehat{x,y} \leqslant \pi :$$

Կոսինուսների թեորեմը: *Q էվկլիդյան տարածության ցանկացած ոչ զրոյական $x, y \in Q$ վեկտորների (տարրերի) համար՝*

$$|x-y|^2 = |x|^2 + |y|^2 - 2|x|\,|y|cos\varphi,$$

որտեղ $\varphi = \widehat{x,y}$:

Ապացույց: Իրոք,

$$|x-y|^2 = (x-y, x-y) = (x,x) + (y,y) - 2(x,y) = |x|^2 + |y|^2 - 2|x|\,|y|cos\varphi :$$

□

Q էվկլիդյան տարածության վեկտորների (տարրերի) $a_1, \ldots, a_k$ համակարգի համար

$$G(a_1,\ldots,a_k) = \begin{pmatrix} (a_1,a_1), & \ldots, & (a_1,a_k) \\ \ldots & \ldots & \ldots & \ldots \\ (a_k,a_1), & \ldots, & (a_k,a_k) \end{pmatrix} \in \mathbb{R}^{k\times k}$$

մատրիցը կոչվում է **Գրամի մատրից**: Կոշի-Բունյակովսկու անհավասարությունը հանդիսանում է հետևյալ արդյունքի մասնավոր դեպքը:

Թեորեմ 17.54: *Q էվկլիդյան տարածության $a_1, \ldots, a_k$ վեկտորների (տարրերի) ցանկացած համակարգի համար՝*

$$det\,(G(a_1,\ldots,a_k)) \geqslant 0\ :$$

Ըստ որում, հավասարությունը տեղի կունենա այն և միայն այն դեպքում, երբ $a_1, \ldots, a_k$ համակարգը գծայնորեն կախյալ է:

Ապացույց: Եթե $a_1, \ldots, a_k$ համակարգը գծայնորեն կախյալ է, այսինքն՝ $\lambda a_1 + \cdots + \lambda_k a_k = 0$, որտեղ որևէ $\lambda_i \neq 0$, ապա

$$\begin{cases} \lambda_1(a_1,a_1) + \cdots + \lambda_k(a_1,a_k) = 0\,, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ \lambda_1(a_k,a_1) + \cdots + \lambda_k(a_k,a_k) = 0\ : \end{cases}$$

Այս հավասարությունների համակարգից ստանում ենք $\lambda_1 G_1 + \cdots + \lambda_k G_k = 0$ գծային կախվածությունը $G(a_1, \ldots, a_k)$ մատրիցի $G_1, \ldots, G_k$ սյունակների միջև: Հետևաբար, $det\,(G(a_1, \ldots, a_k)) = 0$: Եթե $a_1, \ldots, a_k$ համակարգը գծայնորեն անկախ է, ապա այն կլինի հենք $\langle a_1, \ldots, a_k \rangle \leqslant Q$ գծային թաղանթի համար, իսկ Q-ի սկալյար արտադրյալը կլինի այդպիսին նաև $\langle a_1, \ldots, a_k \rangle$ ենթատարածության համար, որի դրական որոշյալությունից բխում է $det\,(G(a_1, \ldots, a_k)) > 0$ անհավասարությունը: □

Կարող ենք ասել, որ էվկլիդյան տարածության վեկտորների համակարգը կոչվում է **օրթոնորմալ** կամ **օրթոնորմավորված**, եթե այն օրթոգոնալ է, իսկ վեկտորներից յուրաքանչյուրի երկարությունը հավասար է 1-ի՝ $|a_i| = 1$, $i = 1, \ldots, n$, այսինքն՝ $(a_i, a_j) = \delta_{ij}$, որտեղ δ_{ij}-ն Կրոնեկերի սիմվոլն է:

Լեմմ 17.49: *Որպեսզի էվկլիդյան տարածության $e_1, \ldots, e_n$ հենքը լինի օրթոնորմալ անհրաժեշտ է և բավարար, որ նրա նկատմամբ էվկլիդյան տարածության սկալյար արտադրյալն ունենա հետևյալ ներկայացումը՝*

$$(x, y) = x_1 y_1 + \cdots + x_n y_n\,,$$

որտեղ $x = x_1 e_1 + \cdots + x_n e_n$, $y = y_1 e_1 + \cdots + y_n e_n$: □

Լեմմ 17.50: *Որպեսզի էվկլիդյան տարածության $e_1, \ldots, e_n$ հենքը լինի օրթոնորմալ անհրաժեշտ է և բավարար, որ նրա նկատմամբ էվկլիդյան տարածության կամայական x տարրի սկալյար քառակուսին ունենա հետևյալ ներկայացումը՝*

$$(x, x) = x_1^2 + \cdots + x_n^2\,,$$

որտեղ $x = x_1 e_1 + \cdots + x_n e_n$:

Ապացուցում: Անհրաժեշտությունն ակնհայտ է: Ապացուցենք բավարարությունը: Նախ նկատենք, որ $(e_i, e_i) = 1$, այսինքն՝ $|e_i| = 1$, $i = 1, \ldots, n$: Մնում է ապացուցել $(e_i, e_j) = 0$ հավասարությունը, որտեղ $i \neq j$: Իրոք, քանի որ $(e_i + e_j, e_i + e_j) = 1^2 + 1^2 = 2$, ապա $(e_i, e_i) + 2(e_i, e_j) + (e_j, e_j) = 2$ և $(e_i, e_j) = 0$, որտեղ $i \neq j$: □

Ինչպես նկատեցինք վերևում, յուրաքանչյուր ոչ զրոյական վերջավոր չափանի էվկլիդյան տարածություն օժտված է օրթոնորմալ հենքերով: Սակայն էվկլիդյան տարածություններում օրթոնորմալ հենքի կառուցման պարզագույն եղանակը ստացվում է, այսպես կոչված, օրթոգոնալացման ընթացքի (պրոցեսի) արդյունքում, որը կոչվում է նաև Գրամ-Շմիդտի օրթոգոնալացման ընթացք:

Օրթոգոնալացման ընթացքը: Դիցուք $f_1, \ldots, f_m$ համակարգը (հաջորդականությունը) Q էվկլիդյան տարածության կամայական գծայնորեն անկախ համակարգ է: Ընտրենք $e_1 = f_1$, իսկ

$$e_2 = f_2 + \alpha e_1\,,$$

ըստ որում, α թիվն ընտրում ենք այնպես, որ e_1 և e_2 վեկտորները լինեն օրթոգոնալ՝

$$\begin{aligned}&(e_1, e_2) = 0\,,\\&(e_1, f_2 + \alpha e_1) = 0\,,\\&(e_1, f_2) + \alpha(e_1, e_1) = 0\,,\end{aligned}$$

որտեղից

$$\alpha = -\frac{(e_1, f_2)}{(e_1, e_1)}\,,$$

որտեղ $(e_1, e_1) \neq 0$, որովհետև $e_1 = f_1 \neq 0$: Քանի որ f_1, f_2 համակարգը գծայնորեն անկախ է, ապա $e_2 \neq 0$: Դիցուք $e_1, \ldots, e_{m-1}$ ոչ զրոյական վեկտորներն արդեն կառուցված են այնպես, որ դրանցից յուրաքանչյուրն օրթոգոնալ է իր բոլոր նախորդ վեկտորներին: Կառուցենք

$$e_m = f_m + \lambda_1 e_1 + \cdots + \lambda_{m-1} e_{m-1}$$

և $\lambda_1, \ldots, \lambda_{m-1}$ թվերն ընտրենք այնպես, որ e_m-ը լինի օրթոգոնալ $e_1, \ldots, e_{m-1}$ վեկտորներից յուրաքանչյուրին, այսինքն՝

$$(e_m, e_i) = 0\,,$$

$$(f_m, e_i) + \lambda_i(e_i, e_i) = 0\,,$$

որտեղից

$$\lambda_i = -\frac{(f_m, e_i)}{(e_i, e_i)}\,,$$

որտեղ $(e_i, e_i) \neq 0$, որովհետև $e_i \neq 0$, $i = 1, \ldots, m-1$: Քանի որ սկզբնական $f_1, \ldots, f_m$ համակարգը գծայնորեն անկախ է, ապա $e_m \neq 0$: Ստացված ոչ զրոյական վեկտորների $e_1, \ldots, e_m$ օրթոգոնալ համակարգը, համաձայն հիմնական լեմմի, կլինի գծայնորեն անկախ: Հետևաբար, եթե վեկտորների սկզբնական $f_1, \ldots, f_m$ համակարգը հենք է Q էվկլիդյան տարածության համար, ապա կառուցված $e_1, \ldots, e_m$ համակարգը կլինի օրթոգոնալ հենք Q-ի համար: Եթե այժմ «նորմավորենք» ստացված $e_1, \ldots, e_m$ հենքը, «բաժանելով» դրանցից յուրաքանչյուրն իր երկարության վրա, ապա ստացված

$$e_1' = \frac{e_1}{|e_1|} \ldots, e_m' = \frac{e_m}{|e_m|}$$

համակարգն արդեն կլինի օրթոնորմալ հենք Q էվկլիդյան տարածության համար:

Նկատենք նաև, որ եթե $f_1, \ldots, f_m$ գծայնորեն անկախ համակարգի սկզբի k վեկտորները լինեին օրթոգոնալ, ապա օրթոգոնալացման ընթացքի արդյունքում կստանայինք՝ $e_1 = f_1$, ..., $e_k = f_k$, իսկ եթե բացի այդ սկզբի k վեկտորներից յուրաքանչյուրի երկարությունը լիներ հավասար 1-ի, ապա կստանայինք՝ $e_1' = f_1$, ..., $e_k' = f_k$: Այսպիսով, որպես օրթոգոնալացման ընթացքի հետևանք, հանգում ենք հետևյալ արդյունքին:

Թեորեմ 17.55: *1) Վերջավոր չափանի Q էվկլիդյան տարածության յուրաքանչյուր ոչ զրոյական վեկտոր կամ Q-ի հենք է կամ դրան կարելի է ընդգրկել Q-ի որևէ օրթոգոնալ հենքում;*

2) Վերջավոր չափանի Q էվկլիդյան տարածության 1 երկարությամբ յուրաքանչյուր վեկտոր կամ Q-ի հենք է կամ դրան կարելի է ընդգրկել Q-ի որևէ օրթոնորմալ հենքում;

3) Վերջավոր չափանի Q էվկլիդյան տարածության վեկտորների ցանկացած օրթոգոնալ համակարգ կամ Q-ի օրթոգոնալ հենք է կամ դրան կարելի է շարունակել (ընդլայնել) մինչև Q-ի օրթոգոնալ հենքի;

4) Վերջավոր չափանի Q էվկլիդյան տարածության վեկտորների ցանկացած օրթոնորմալ համակարգ կամ Q-ի օրթոնորմալ հենք է կամ դրան կարելի է շարունակել (ընդլայնել) մինչև Q-ի օրթոնորմալ հենքի:

□

Հատկություն 17.18: *Վերջավոր չափանի էվկլիդյան տարածության մեկ օրթոնորմալ հենքից մյուս օրթոնորմալ հենքին անցման մատրիցը օրթոգոնալ է:*

Ապացույց: Դիցուք Q էվկլիդյան տարածության մեջ տրված են $e_1, \ldots, e_n$ և $e'_1, \ldots, e'_n$ օրթոնորմալ հենքերը և դիցուք՝

$$e'_1 = t_{11}e_1 + \cdots + t_{1n}e_n\,,$$

$$\ldots\ \ldots\ \ldots\ \ldots$$

$$e'_n = t_{n1}e_1 + \cdots + t_{nn}e_n\ :$$

Պահանջվում է ապացուցել, որ $\Gamma = (t_{ij}) \in \mathbb{R}^{n\times n}$ մատրիցը օրթոգոնալ է, այսինքն՝

$$\Gamma \cdot \Gamma^T = \Gamma^T \cdot \Gamma = E_n\ :$$

Այս պայմանը բխում է հետևյալ հավասարություններից.

$$(e'_i, e'_i) = t_{i1}^2 + \cdots + t_{in}^2 = 1\,,$$

$$(e'_i, e'_j) = t_{i1}t_{j1} + \cdots + t_{in}t_{jn} = 0 \qquad i \neq j\,,$$

որտեղ $i, j = 1, \ldots, n$: □

Անցնենք էվկլիդյան տարածությունների իզոմորֆիզմին (նույնաձևությանը):

Դիցուք Q-ն և Q'-ը էվկլիդյան տարածություններ են: $\varphi : Q \to Q'$ արտապատկերումը կոչվում է **իզոմորֆիզմ** կամ **նույնաձևություն** Q-ից Q', եթե

ա) φ-ն իզոմորֆիզմ (նույնաձևություն) է Q և Q' գծային տարածությունների միջև;

բ) $(\varphi x, \varphi y) = (x, y)$ ցանկացած $x, y \in Q$ վեկտորների (տարրերի) համար:

Սահմանման վերջին պայմանը կարելի է փոխարինել ավելի թույլ պայմանով՝ $(\varphi x, \varphi x) = (x, x)$ ցանկացած $x \in Q$ վեկտորի համար: Իրոք,

$$(\varphi(x+y), \varphi(x+y)) = (x+y, x+y) \longrightarrow (\varphi x, \varphi y) = (x, y)\ :$$

Եթե $\varphi : Q \to Q'$ արտապատկերումը իզոմորֆիզմ է, ապա $\varphi^{-1} : Q' \to Q$ արտապատկերումը նս կլինի իզոմորֆիզմ: Էվկլիդյան տարածությունների իզոմորֆիզմների արտադրյալը նորից կլինի իզոմորֆիզմ (եթե այն գոյություն ունի):

Երկու Q և Q' էվկլիդյան տարածություններ կոչվում են **իզոմորֆ** կամ **նույնաձև** և գրվում է $Q \simeq Q'$ կամ $Q \cong Q'$, եթե գոյություն ունի որևէ $\varphi : Q \to Q'$ իզոմորֆիզմ: Այս «$\simeq$» հարաբերությունը կոչվում է **էվկլիդյան տարածությունների իզոմորֆության** կամ **նույնաձևության հարաբերություն**:

Լեմմ 17.51: *Էվկլիդյան տարածությունների իզոմորֆության հարաբերությունը համարժեքության հարաբերություն է, այսինքն՝*

ա) $Q \simeq Q$ ցանկացած Q էվկլիդյան տարածության համար;

բ) $Q \simeq Q' \longrightarrow Q' \simeq Q$;

գ) $Q \simeq Q'$, $Q' \simeq Q'' \longrightarrow Q \simeq Q''$: □

Թեորեմ 17.56 (Վերջավոր չափանի էվկլիդյան տարածությունների իզոմորֆության հայտանիշը): *Որպեսզի երկու վերջավոր չափանի էվկլիդյան տարածություններ լինեն իզոմորֆ (նույնաձև) անհրաժեշտ է և բավարար, որ դրանց չափողականությունները լինեն հավասար.*

$$Q \simeq Q' \longleftrightarrow dim(Q) = dim(Q') :$$

Ապացույց: Անհրաժեշտությունը բխում է վերջավոր չափանի գծային տարածությունների իզոմորֆության հայտանիշից, իսկ բավարարությունը բխում է վերջավոր չափանի էվկլիդյան տարածություններում օրթոնորմալ հենքի գոյությունից: Իրոք, դիցուք $dim(Q) = dim(Q') = n$: Եթե $n = 0$, ապա երկու Q և Q' էվկլիդյան տարածությունները կլինեն զրոյական, հետևաբար, և իզոմորֆ (նույնաձև): Եթե $n > 0$, ապա n-չափանի Q և Q' էվկլիդյան տարածություններում գոյություն կունենան համապատասխանաբար $e_1, \ldots, e_n$ և $e'_1, \ldots, e'_n$ օրթոնորմալ հենքեր: Սահմանենք $\varphi : Q \to Q'$ արտապատկերումը

$$\varphi(x) = x_1 e'_1 + \cdots + x_n e'_n \in Q'$$

բանաձևով, որտեղ $x \in Q$, $x = x_1 e_1 + \cdots + x_n e_n$: Ակնհայտ է, որ սահմանված φ արտապատկերումը կլինի իզոմորֆիզմ Q և Q' էվկլիդյան տարածությունների միջև: Այսպիսով, $Q \simeq Q'$: □

17.21. Գծային ձևափոխության ինվարիանտ ենթատարածություն, սեփական արժեք, սեփական վեկտոր, բացասող բազմանդամ,բնութագրիչ բազմանդամ: Համիլտոն-Քելիի թեորեմը

Հենքի փոփոխության միջոցով գծային ձևափոխության մատրիցը հաճախ կարելի է բերել ավելի պարզ տեսքի: Մասնավորապես, այդպիսի հնարավորություն է ընձեռնվում, եթե գծային տարածությունն օժտված է ինվարիանտ ենթատարածությամբ (կամ ենթատարածություններով):

Դիցուք P-ն կամայական դաշտ է, իսկ Q-ն գծային տարածություն է որոշված P-ի վրա (մասնավորապես, կարելի է վերցնել $P = \mathbb{R}$ կամ $P = \mathbb{C}$): Դիցուք Q'-ը Q-ի ենթատարածություն է, իսկ $\varphi : Q \to Q$ արտապատկերումը Q-ի գծային ձևափոխություն է, այսինքն`

$$\varphi(x+y) = \varphi(x) + \varphi(y)\,,$$

$$\varphi(\alpha x) = \alpha\varphi(x)$$

ցանկացած $x, y \in Q$ վեկտորների և ցանկացած $\alpha \in P$ սկալյարի համար:

Q-ի բոլոր գծային ձևափոխությունների տարածությունը, ինչպես գիտենք, նշանակվում է $End(Q)$-ով կամ $Hom(Q,Q)$-ով, որի չափողականությունը հավասար է n^2, եթե Q-ն n-չափանի է (թեորեմ 17.31):

$Q' \leqslant Q$ ենթատարածությունը կոչվում է ինվարիանտ $\varphi : Q \to Q$ գծային ձևափոխության նկատմամբ կամ φ-ի **ինվարիանտ ենթատարածություն**, եթե $\varphi(x) \in Q'$ ցանկացած $x \in Q'$ վեկտորի համար, այսինքն` $\varphi(Q') \subseteq Q'$: Համառոտ, Q'-ը կոչվում է նաև φ-ինվարիանտ ենթատարածություն:

Օրինակներ: 1) Ցանկացած Q գծային տարածության $Q' = \{0\}$ և $Q' = Q$ ենթատարածություններն ինվարիանտ են յուրաքանչյուր $\varphi : Q \to Q$ գծային ձևափոխության նկատմամբ;

2) Եթե Q գծային տարածության $\varphi_\lambda : Q \to Q$ գծային ձևափոխությունը որոշվում է $\varphi_\lambda(x) = \lambda x$, $x \in Q$, օրենքով, ապա Q-ի ցանկացած $Q' \leqslant Q$ ենթատարածություն կլինի φ_λ-ինվարիանտ: φ_λ գծային ձևափոխությունը կոչվում է λ **գործակցով նմանություն**:

Եթե $Q' \leqslant Q$ ենթատարածությունը φ-ինվարիանտ ենթատարածություն է, ապա φ-ն կարելի է դիտել որպես գծային ձևափոխություն նաև Q' գծային տարածության համար` $\varphi : Q' \to Q'$:

$\lambda \in P$ սկալյարը կոչվում է $\varphi \in Hom(Q,Q)$ գծային ձևափոխության **սեփական արժեք**, եթե գոյություն ունի այնպիսի ոչ զրոյական $x \in Q$ վեկտոր, որ $\varphi(x) = \lambda x$: Այդ դեպքում, ոչ զրոյական $x \in Q$ վեկտորը կոչվում է λ սեփական արժեքին համապատասխանող φ-ի **սեփական վեկտոր**: Ոչ զրոյական $x \in Q$ վեկտորը կոչվում է $\varphi \in Hom(Q,Q)$ գծային ձևափոխության սեփական վեկտոր, եթե այն հանդիսանում է φ-ի որևէ λ սեփական արժեքին համապատասխանող սեփական վեկտոր: Գծային ձևափոխության բոլոր սեփական արժեքների բազմությունը կոչվում է դրա **սպեկտր** (լուսակ):

Զուգահեռ ներմուծվում է նաև մատրիցի սեփական վեկտորի և սեփական արժեքի գաղափարները: Եթե $A \in P^{n\times n}$ մատրիցի համար՝ $A \cdot x = \lambda x$, որտեղ $x \in P^{n\times 1}$, $x \neq 0$ և $\lambda \in P$, ապա x-ը կոչվում է A մատրիցի **սեփական վեկտոր**, իսկ λ սկալյարը դրա **սեփական արժեք**:

Օրինակ: Քանի որ $(e^{\lambda x})' = \lambda e^{\lambda x}$, ապա $e^{\lambda x}$ ֆունկցիան ածանցման գծային ձևափոխության սեփական վեկտոր է և այստեղ յուրաքանչյուր λ իրական թիվ սեփական արժեք է:

$x \in Q$ վեկտորը կոչվում է $\varphi \in Hom(Q,Q)$ գծային ձևափոխության **անշարժ կետ**, եթե $\varphi(x) = x$: Եթե այստեղ $x \neq 0$, ապա այն կոչվում է φ-ի ոչ զրոյական անշարժ կետ:

Օրինակ, $\mathbb{R}_3$-ի յուրաքանչյուր $x = (\alpha, 0, 0)$ վեկտոր կլինի $\varphi_1 : (\alpha_1, \alpha_2, \alpha_3) \to (\alpha_1, 0, 0)$ գծային ձևափոխության անշարժ կետը:

Լեմմ 17.52: *Որպեսզի $1 \in P$ սկալյարը լինի $\varphi \in Hom(Q,Q)$ գծային ձևափոխության սեփական արժեք անհրաժեշտ է և բավարար, որ φ գծային ձևափոխությունն ունենա ոչ զրոյական անշարժ կետ:* $\square$

Լեմմ 17.53: *Սևեռված $\lambda \in P$ սկալյարին համապատասխանող φ-ի բոլոր սեփական վեկտորների բազմությունը զրոյական վեկտորի հետ մեկտեղ կազմում է ենթատարածություն, որը համընկնում է $Ker(\varphi - \lambda\varepsilon) \leqslant Q$ ենթատարածության հետ, որտեղ ε-ը Q-ի նույնական արտապատկերումն է: Հետևաբար, այդ ենթատարածության չափողականությունը կլինի հավասար $n - rank(\varphi - \lambda\varepsilon)$ թվին, եթե $n = dim(Q)$:*

Ապացուցում: Իրոք,

$$\varphi(x) = \lambda x \longleftrightarrow (\varphi - \lambda\varepsilon)x = 0,$$

որտեղ $x \in Q$: $\square$

$Ker(\varphi - \lambda\varepsilon)$ ենթատարածությունը կոչվում է λ–ին համապատասխանող φ-ի սեփական ենթատարածություն:

Թեորեմ 17.57: *$\varphi \in Hom(Q, Q)$ գծային ձևափոխության զույգ առ զույգ միմյանցից տարբեր $\lambda_1, \ldots, \lambda_k \in P$ սեփական արժեքներին համապատասխանող φ-ի սեփական ենթատարածությունները գծայնորեն անկախ են ($\lambda_i \neq \lambda_j$, եթե $i \neq j$):*

Ապացուցում (վերհանգման եղանակ): $k = 1$ դեպքում պնդումն ակնհայտ է: Դիցուք $k > 1$ և k-ից քիչ թվով սեփական ենթատարածությունների համար պնդումը ճիշտ է: Եթե

$$v_1 + \cdots + v_{k-1} + v_k = 0, \tag{17.28}$$

որտեղ $v_i \in Ker(\varphi - \lambda_i\varepsilon)$, $i = 1, \ldots, k$, ապա

$$\begin{aligned} &\varphi(v_1 + \cdots + v_{k-1} + v_k) = \varphi(0) = 0, \\ &\varphi(v_1) + \cdots + \varphi(v_{k-1}) + \varphi(v_k) = 0, \\ &\lambda_1 v_1 + \cdots + \lambda_{k-1} v_{k-1} + \lambda_x v_k = 0 : \end{aligned}$$

Ստացված հավասարությունից հանելով (17.28)-ը բազմապատկած λ_k-ով, կստանանք՝ $(\lambda_1 - \lambda_k)v_1 + \cdots + (\lambda_{k-1} - \lambda_k)v_{k-1} = 0$, որտեղից, համաձայն վերհանգման ենթադրության կունենանք՝ $(\lambda_i - \lambda_k)v_i = 0$ և $v_i = 0$, $i = 1, \ldots, k-1$: Այժմ (17.28)-ից կունենանք նաև $v_k = 0$: □

Հատկություն 17.19: *1) Եթե ոչ զրոյական $x \in Q$ վեկտորը $\varphi \in Hom(Q, Q)$ գծային ձևափոխության սեփական վեկտորն է, ապա $(x) \leqslant Q$ ենթատարածությունը կլինի Q-ի φ-ինվարիանտ ենթատարածություն;*

2) Եվ հակառակը, եթե Q'-ը Q-ի 1-չափանի φ-ինվարիանտ ենթատարածություն է, ապա յուրաքանչյուր ոչ զրոյական $x \in Q'$ վեկտոր կլինի $\varphi \in Hom(Q, Q)$ գծային ձևափոխության սեփական վեկտոր:

Ապացուցում: 1) Եթե $\varphi(x) = \lambda x$ և $y \in (x)$, այսինքն՝ $y = \alpha x$, ապա $\varphi(y) = \varphi(\alpha x) = \alpha\varphi(x) = (\alpha\lambda)x \in (x)$: Ուստի, մեկ տարրով ծնված (x) գծային թաղանթը Q-ի φ-ինվարիանտ ենթատարածություն է:

2) Եթե $dim(Q') = 1$ և e-ն Q'-ի հենքն է, ապա $Q' = (e)$: Դիցուք $x \in Q'$ և $x \neq 0$: Հետևաբար, $x = \beta e$, $\varphi(e) \in Q'$, այսինքն՝ $\varphi(e) = \gamma e$ և

$$\varphi(x) = \beta\varphi(e) = (\beta\gamma)e = \gamma(\beta e) = \gamma x :$$ □

Կդիտարկենք մատրիցներ որոշված $P[x]$ բազմանդամների օղակի վրա, այսինքն՝ մատրիցներ, որոնց տարրերը P-ից վերցրած գործակիցներով բազմանդամներ են, ինչպես նաև մատրիցներ՝ որոշված գծային ձևափոխությունների $Hom(Q,Q)$ օղակի վրա: Այդպիսի մատրիցների որոշիչներն օժտված են թվային տարրերով մատրիցների որոշիչների ընդհանուր հատկություններով:

Սահմանենք բազմանդամի արժեքի գաղափարը՝ տրված գծային ձևափոխության վրա: Դիցուք $f \in P[x]$, $f = a_0 + a_1x + \cdots + a_nx^n$, իսկ $\varphi \in Hom(Q,Q)$: Q գծային տարածության

$$f(\varphi) = a_0\varepsilon + a_1\varphi + \cdots + a_n\varphi^n = a_0\varepsilon + (a_1\varepsilon)\varphi + \cdots + (a_n\varepsilon)\varphi^n = \\ = a_0\varepsilon + \varphi(a_1\varepsilon) + \cdots + \varphi^n(a_n\varepsilon)$$

գծային ձևափոխությունը կոչվում է f **բազմանդամի արժեք** φ **գծային ձևափոխության վրա**, որտեղ ε-ը Q-ի նույնական արտապատկերումն է, իսկ $\varphi^k = \underbrace{\varphi \cdot \varphi \cdots \varphi}_{k}$, $(\varphi_1 \cdot \varphi_2)(t) = \varphi_2(\varphi_1 t)$, $(\varphi_1 + \varphi_2)(t) = \varphi_1(t) + \varphi_2(t)$, $t \in Q$:

Լեմմ 17.54: *1) Եթե $f = g$, ապա $f(\varphi) = g(\varphi)$;*
2) Եթե $f = g + h$, ապա $f(\varphi) = g(\varphi) + h(\varphi)$;
3) Եթե $f = g \cdot h$, ապա $f(\varphi) = g(\varphi) \cdot h(\varphi)$: □

Մասնավորապես, $f_{ij} \in P[x]$, $i,j = 1,\ldots,n$, բազմանդամներից կազմված n-րդ կարգի (f_{ij}) մատրիցի որոշիչի արժեքը $\varphi \in Hom(Q,Q)$ գծային ձևափոխության վրա կարելի է հաշվել հետևյալ կերպ՝

$$(det(f_{ij}))\,(\varphi) = det\,(f_{ij}(\varphi))\,,$$

որովհետև

$$\left(\sum_{\sigma \in S_n} sgn\,\sigma \cdot f_{1,\sigma(1)} \cdots f_{n,\sigma(n)}\right)(\varphi) = \sum_{\sigma \in S_n} sgn\,\sigma \cdot f_{1,\sigma(1)}(\varphi) \cdots f_{n,\sigma(n)}(\varphi) :$$

$A - xE$ մատրիցը կոչվում է $A = (a_{ij}) \in P^{n \times n}$ մատրիցի **բնութագրիչ մատրից**, որտեղ

$$A - xE = \begin{pmatrix} a_{11} - x, & a_{12}, & \ldots, & a_{1n} \\ a_{21}, & a_{22} - x, & \ldots, & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n1}, & a_{n2}, & \ldots, & a_{nn} - x \end{pmatrix},$$

իսկ $det(A - xE)$ որոշիչը կոչվում է A մատրիցի **բնութագրիչ բազմանդամ**՝ $det(A - xE) \in P[x]$:

Օրինակ, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ դեպքում, $det(A - xE) = det \begin{pmatrix} a-x, & b \\ c & d-x \end{pmatrix} = x^2 - (a+d)x + (ad-bc) = x^2 - tr(A)x + det(A)$:
Նկատենք, որ $A \in P^{n\times n}$ մատրիցի բնութագրիչ բազմանդամը x-ից կախված n-րդ աստիճանի բազմանդամ է՝

$$det(A - xE) = (-1)^n x^n + (-1)^{n-1} tr(A) x^{n-1} + \cdots + det(A) \ :$$

Լեմմ 17.55: *Նման մատրիցների բնութագրիչ բազմանդամները հավասար են, այսինքն՝*

$$A \sim B \longrightarrow det(A - xE) = det(B - xE) \ :$$

Ապացույց: Եթե $A \sim B$, ապա գոյություն ունի այնպիսի $T \in P^{n\times n}$ հակադարձելի մատրից, որ $B = T \cdot A \cdot T^{-1}$: Հետևաբար,

$$det(A - xE) = det\left(T^{-1}BT - xE\right) = det\left(T^{-1}(B - xE)T\right) =$$

$$det\left(T^{-1}\right) det(B - xE) det(T) = det\left(T^{-1} \cdot T\right) det(B - xE) = det(B - xE) \ :$$

□

Հանգում ենք հետևյալ գաղափարին:

Վերջավոր չափանի Q գծային տարածության φ **գծային ձևափոխության բնութագրիչ բազմանդամ** ասելով կհասկանանք Q-ի ցանկացած $e_1, \ldots, e_n$ հենքում φ-ի ունեցած մատրիցի բնութագրիչ բազմանդամը:

$f \in P[x]$ բազմանդամը կոչվում է $\varphi \in Hom(Q, Q)$ գծային ձևափոխությանը **բացասող** կամ **զրո դարձնող**, եթե $f(\varphi) = 0$, որտեղ 0-ն Q գծային տարածության զրոյական գծային ձևափոխությունն է, այսինքն՝ $0(x) = 0$ ցանկացած $x \in Q$ վեկտորի համար: Եթե f բազմանդամը φ գծային ձևափոխությանը բացասող բազմանդամ է, ապա համառոտ կասենք նաև, որ f-ը բացասում է φ-ին: Ակնհայտ է, որ զրոյական բազմանդամը բացասում է բոլոր գծային ձևափոխություններին:

Լեմմ 17.56: *Եթե $f, g \in P[x]$ բազմանդամները $\varphi \in Hom(Q, Q)$ գծային ձևափոխությանը բացասող բազմանդամներ են, ապա $f+g$, $f-g$, $f \cdot h$, λf*

բազմանդամները ևս կլինեն φ-ին բացասող բազմանդամներ ($h \in P[x]$, $\lambda \in P$) *այսինքն՝ φ-ին բացասող բոլոր բազմանդամների բազմությունը $P[x]$ գծային հանրահաշվի իդեալ է:* $\square$

Թեորեմ 17.58: *P դաշտի վրա որոշված վերջավոր չափանի Q գծային տարածության յուրաքանչյուր $\varphi \in Hom(Q,Q)$ գծային ձևափոխության համար գոյություն ունի φ-ին բացասող ոչ զրոյական $f \in P[x]$ բազմանդամ:*

Ապացուցում: Եթե $dim(Q) = 0$, ապա $Q = \{0\}$ և Q-ի միակ գծային ձևափոխությունը զրոյականն է, որին բացասում է առանց ազատ անդամի յուրաքանչյուր ոչ զրոյական $f \in P[x]$ բազմանդամ: Դիցուք $dim(Q) = n > 0$: Այս դեպքում, $dim(Hom(Q,Q)) = n^2$: Հետևաբար, $Hom(Q,Q)$ գծային տարածության n^2+1 թվով տարրեր պարունակող յուրաքանչյուր հաջորդականություն գծայնորեն կախյալ է: Մասնավորապես, եթե $\varphi \in Hom(Q,Q)$, ապա

$$\varepsilon, \varphi, \varphi^2, \ldots, \varphi^{n^2}$$

հաջորդականությունը կլինի գծայնորեն կախյալ, այսինքն՝

$$\alpha_0\varepsilon + \alpha_1\varphi + \alpha_2\varphi^2 + \cdots + \alpha_{n^2}\varphi^{n^2} = 0\,,$$

որտեղ որևէ $\alpha_i \neq 0$: Այսպիսով, ոչ զրոյական

$$f = \alpha_0 + \alpha_1 x + \cdots + \alpha_{n^2}x^{n^2} \in P[x]$$

բազմանդամը բացասում է φ-ին: $\square$

Իրականում, քիչ հետո կապացուցենք Համիլտոն-Քելիի թեորեմը, որի համաձայն n-չափանի Q գծային տարածության յուրաքանչյուր $\varphi \in Hom(Q,Q)$ գծային ձևափոխության համար գոյություն ունի φ-ին բացասող n-րդ աստիճանի բազմանդամ:

Ոչ զրոյական $f \in P[x]$ բազմանդամը կոչվում է $\varphi \in Hom(Q,Q)$ գծային ձևափոխության **փոքրագույն** կամ **մինիմալ** բազմանդամ, եթե f-ը բացասում է φ-ին և φ-ին բացասող ոչ զրոյական բազմանդամների մեջ ունի փոքրագույն աստիճան, այսինքն՝

ա) $f(\varphi) = 0$,

բ) $g(\varphi) = 0$, $g \in P[x]$, $g \neq 0 \longrightarrow deg(f) \leqslant deg(g)$:

Նախորդ թեորեմից բխում է, որ յուրաքանչյուր $\varphi \in Hom(Q,Q)$ գծային ձևափոխության համար փոքրագույն բազմանդամ միշտ գոյություն ունի: Ակնհայտ է նաև, որ եթե f-ը φ-ի համար փոքրագույն բազմանդամ է, ապա λf-ը ևս կլինի φ-ի փոքրագույն բազմանդամ:

Լեմմ 17.57: *1) Եթե f-ը φ-ի փոքրագույն բազմանդամ է և $g(\varphi) = 0$, այսինքն՝ g-ն բացասում է φ-ին, ապա g-ն բաժանվում է f-ի վրա: 2) Մասնավորապես, միևնույն φ գծային ձևափոխության երկու f_1, f_2 փոքրագույն բազմանդամներ տարբերվում են ոչ զրոյական սկալյարով, այսինքն՝ $f_1 = \lambda f_2$, որտեղ $\lambda \in P$, $\lambda \neq 0$:*

Ապացուցում: 1) Օգտվենք բազմանդամների մնացորդով բաժանման թեորեմից՝

$$g = fq + r,$$

որտեղ $r = 0$ կամ $deg(r) < deg(f)$: Ապացուցենք, որ այստեղ $r = 0$: Ենթադրելով հակառակը ստանում ենք հակասություն: Իրոք, եթե $r \neq 0$, ապա $deg(r) < deg(f)$ և

$$r(\varphi) = g(\varphi) - f(\varphi)q(\varphi) = 0 :$$

2) Երկու f_1, f_2 փոքրագույն բազմանդամների համար կունենանք՝ $deg(f_1) = deg(f_2)$ և $f_1 = f_2 q$, $q \neq 0$: Հետևաբար, $deg(q) = 0$ և $q = \lambda \in P$, $\lambda \neq 0$: □

Թեորեմ 17.59: *$\varphi \in Hom(Q,Q)$ գծային ձևափոխության $f \in P[x]$ փոքրագույն բազմանդամի արմատները (P դաշտում) և φ-ի սեփական արժեքները համընկնում են:*

Ապացուցում: Դիցուք $\lambda \in P$ սկալյարը φ-ի սեփական արժեք է, այսինքն՝ գոյություն ունի այնպիսի ոչ զրոյական $t \in Q$ վեկտոր, որ $\varphi(t) = \lambda t$ կամ $(\varphi - \lambda\varepsilon)t = 0$: Ապացուցենք $f(\lambda) = 0$ հավասարությունը: Քանի որ $\varphi(t) = \lambda t$, ապա

$$\begin{aligned}
&\varphi^2(t) = \varphi(\varphi(t)) = \varphi(\lambda t) = \lambda\varphi(t) = \lambda^2 t\,,\\
&\ldots\ \ldots\ \ldots\ \ldots\\
&\varphi^k(t) = \lambda^k t\ :
\end{aligned}$$

Հետևաբար, յուրաքանչյուր $h \in P[x]$, $h = a_0 + a_1 x + \cdots + a_k x^k$ բազմանդամի համար,

$$h(\varphi) = a_0\varepsilon + a_1\varphi + \cdots + a_k\varphi^k,$$

$$h(\varphi)(t) = a_0 t + a_1 \lambda t + \cdots a_k \lambda^k t = \left(a_0 + a_1 \lambda + \cdots a_k \lambda^k\right) t = h(\lambda) t \ :$$

Եթե $h = f$, ապա $f(\varphi) = 0$ և $f(\lambda)t = 0$, որտեղից $f(\lambda) = 0$, որովհետև $t \neq 0$:

Ապացուցենք հակառակը, այսինքն՝ եթե $f(\lambda) = 0$, $\lambda \in P$, ապա λ-ն կլինի φ-ի սեփական արժեք: Իրոք, քանի որ $f(\lambda) = 0$, ապա $f = (x-\lambda)q$, որտեղ $deg(q) < deg(f)$ կամ $q = c \in P$, $c \neq 0$, եթե $deg(f) = 1$: Երկու դեպքում էլ՝ $q(\varphi) \neq 0$, այսինքն՝ գոյություն ունի այնպիսի $t \in Q$, $t \neq 0$, որ $t_1 = q(\varphi)(t) \neq 0$: Հետևաբար,

$$0 = f(\varphi) = (\varphi - \lambda\varepsilon) \cdot q(\varphi) = q(\varphi) \cdot (\varphi - \lambda\varepsilon),$$

$$(\varphi - \lambda\varepsilon)(q(\varphi)(t)) = 0,$$

$$(\varphi - \lambda\varepsilon)(t_1) = 0,$$

$$\varphi(t_1) - \lambda t_1 = 0,$$

$$\varphi(t_1) = \lambda t_1,$$

այսինքն՝ λ-ն կլինի φ գծային ձևափոխության սեփական արժեք: $\square$

Հետևություն 17.50: *Կոմպլեքս գծային տարածության յուրաքանչյուր φ գծային ձևափոխություն ունի գոնե մեկ հատ սեփական վեկտոր, հետևաբար նաև գոնե մեկ հատ 1-չափանի φ-ինվարիանտ ենթատարածություն:* $\square$

Սակայն իրական գծային տարածության գծային ձևափոխությունը կարող է չունենալ սեփական վեկտոր (օրինակ, հարթության պտույտը $\alpha \neq 0, \pi$ անկյան տակ):

Թեորեմ 17.60: *Դիցուք Q-ն վերջավոր չափանի գծային տարածություն է: Որպեսզի $\lambda \in P$ սկալյարը լինի $\varphi \in Hom(Q,Q)$ գծային ձևափոխության սեփական արժեք անհրաժեշտ է և բավարար, որ λ-ն լինի φ-ի բնութագրիչ բազմանդամի արմատ:*

Ապացուցում: Դիցուք $e_1, \ldots, e_n$ հաջորդականությունը Q-ի հենք է: Եթե λ-ն φ-ի սեփական արժեք է, ապա գոյություն ունի այնպիսի ոչ զրոյական $t \in Q$ վեկտոր, որ $\varphi(t) = \lambda t$ կամ՝ $(\varphi - \lambda\varepsilon)t = 0$: Նշանակելով φ-ի մատրիցը $e_1, \ldots, e_n$ հենքում $A = (a_{ij})$-ով, իսկ $t = t_1 e_1 + \cdots + t_n e_n$, կստանանք՝

$$t_1 \varphi e_1 + \cdots + t_n \varphi e_n = \lambda t_1 e_1 + \cdots + \lambda t_n e_n,$$

$$t_1 (a_{11}e_1 + \cdots + a_{1n}e_n) + \cdots + t_n (a_{n1}e_1 + \cdots + a_{nn}e_n) = \lambda t_1 e_1 + \cdots + \lambda t_n e_n,$$

կամ՝

$$\begin{aligned} &a_{11}t_1 + \cdots + a_{n1}t_n = \lambda t_1, \\ &\ \ \cdots\ \ \cdots\ \ \cdots\ \ \cdots \\ &a_{1n}t_1 + \cdots + a_{nn}t_n = \lambda t_n, \end{aligned}$$

այսինքն՝

$$\begin{cases} (a_{11} - \lambda)\, t_1 + \cdots + a_{n1}t_n = 0, \\ \ \ \cdots\ \ \cdots\ \ \cdots\ \ \cdots\ \ \cdots \\ a_{1n}t_1 + \cdots + (a_{nn} - \lambda)\, t_n = 0 \end{cases}$$

համասեռ համակարգն ունի ոչ զրոյական $(t_1, \ldots, t_n)$ լուծում: Ուստի, համակարգի $B = A^T - \lambda E$ հիմնական մատրիցի որոշիչը կլինի զրո: Հետևաբար, $B^T = (A^T)^T - \lambda E^T = A - \lambda E$ և $det(B^T) = det(B) = 0$, այսինքն՝ $det(A - \lambda E) = 0$:

Այսպիսով, λ-ն φ-ի բնութագրիչ բազմանդամի արմատ է: Հակադարձ քայլերով ապացուցվում է նաև հակառակ պնդումը: □

Դիտարկենք կոմպլեքս թվերով $n \times m$-չափանի $A = (a_{ij})$ մատրիցը, այսինքն՝ $A \in \mathbb{C}^{n \times m}$: $\bar{A} = (\bar{a}_{ij})$ մատրիցը, որտեղ $\bar{a}_{ij}$-ը a_{ij} կոմպլեքս թվի համալուծն է, կոչվում է A մատրիցի **համալուծ մատրից**: Նշանակենք՝

$$A^* = \left(\bar{A}\right)^T = \overline{(A^T)}\ :$$

Հետևյալ հատկություններն ակնհայտ են.

1. $(A^*)^* = A$;
2. Եթե $A + B$ գումարը որոշված է, ապա $(A + B)^* = A^* + B^*$;
3. Եթե $A \cdot B$ արտադրյալը որոշված է, ապա $(A \cdot B)^* = B^* \cdot A^*$;
4. $(\alpha B)^* = \bar{\alpha} B^*$;
5. Եթե A-ն հակադարձելի է, ապա A^*-ը ևս կլինի հակադարձելի և $(A^*)^{-1} = (A^{-1})^*$:

Ներմուծենք կոմպլեքս թվերով մատրիցների հետևյալ կարևոր դասը:

Կոմպլեքս թվերով n-րդ կարգի A մատրիցը կոչվում է **հերմիտյան**, եթե $A^* = A$: Օրինակ, իրական թվերով ցանկացած սիմետրիկ մատրից կլինի հերմիտյան:

Թեորեմ 17.61: *Հերմիտյան մատրիցի բոլոր (կոմպլեքս) սեփական արժեքներն իրական թվեր են: Մասնավորապես, իրական թվերով* *ցանկացած սիմետրիկ մատրից ունի միայն իրական սեփական արժեքներ:*

Ապացուցում: Իրոք, եթե λ կոմպլեքս թիվը $A \in \mathbb{C}^{n\times n}$ հերմիտյան մատրիցի սեփական արժեքն է, ապա $Ax = \lambda x$, որտեղ $x \in \mathbb{C}^{n\times 1}$, $x \neq 0$: Որտեղից, $x^*A^* = \bar{\lambda}x^*$, այսինքն՝ $x^*A = \bar{\lambda}x^*$: Ուստի, $x^*Ax = \bar{\lambda}x^*x$ և $x^*Ax = x^*\lambda x = \lambda x^*x$: Այսպիսով, $\bar{\lambda}x^*x = \lambda x^*x$ և $(\bar{\lambda} - \lambda)x^*x = 0$, որտեղ $x^*x \neq 0$, որովհետև $x \neq 0$: Հետևաբար, $\bar{\lambda} - \lambda = 0$ և $\bar{\lambda} = \lambda$: $\square$

Կդիտարկենք մատրիցներ, որի տարրերը գծային ձևափոխություններ են: Դիցուք $\varphi \in Hom(Q, Q)$, իսկ

$$P[\varphi] = \{f(\varphi) \mid f \in P[x]\} \subseteq Hom(Q, Q) :$$

Գծային ձևափոխությունների $P[\varphi]$ բազմությունը միավորով օժտված զուգորդական և տեղափոխական օղակ է՝ գծային ձևափոխությունների գումարման և բազմապատկման նկատմամբ, ըստ որում՝

$$f_1(\varphi) + f_2(\varphi) = (f_1 + f_2)\varphi,$$

$$f_1(\varphi) \cdot f_2(\varphi) = (f_1 \cdot f_2)\varphi :$$

Մասնավորապես, $a\varepsilon \cdot \varphi = a\varphi$, $a_1\varepsilon \cdot a_2\varepsilon \cdots a_n\varepsilon = (a_1 \cdot a_2 \cdots a_n)\,\varepsilon$, $a_1\varepsilon + a_2\varepsilon + \cdots + a_n\varepsilon = (a_1 + a_2 + \cdots + a_n)\,\varepsilon$, որտեղ $a, a_1, \ldots, a_n \in P$: Եթե

$$A = \begin{pmatrix} f_{11}(\varphi), & \ldots, & f_{1n}(\varphi) \\ \ldots & \ldots & \ldots \\ f_{n1}(\varphi), & \ldots, & f_{nn}(\varphi) \end{pmatrix},$$

այսինքն՝ A մատրիցը $P[\varphi]$ օղակի վրա որոշված n-րդ կարգի մատրից է, ապա սահմանվում է նաև A-ի որոշիչը՝ մեզ ծանոթ եղանակով.

$$det(A) = \sum_{\sigma \in S_n} sgn(\sigma) \cdot f_{1,\sigma(1)}(\varphi) \cdots f_{n,\sigma(n)}(\varphi) \in P[\varphi];$$

Այս որոշիչների համար մնում են ուժի մեջ սովորական որոշիչների ընդհանուր հատկությունները: Այսպիսի մատրիցների նկատմամբ (հետ) սովորական եղանակով սահմանում ենք նաև գումարման, բազմապատկման և $f(\varphi)$-ով բազմապատկման գործողություններ:

Մասնավորապես, այստեղ նույնպես սահմանվում է A-ի $A^\vee$ կցորդ մատրիցը (տես 14.8 վերնագիրը), որի համար՝

$$A \cdot A^\vee = A^\vee \cdot A = \begin{pmatrix} det(A) & & 0 \\ & \ddots & \\ 0 & & det(A) \end{pmatrix} :$$

$P[\varphi]^{n\times n}$-ով նշանակենք բոլոր այն n-րդ կարգի մատրիցների բազմությունը, որոնց տարրերը պատկանում են $P[\varphi]$ բազմությանը (օղակին): Եթե $A \in P[\varphi]^{n\times n}$, $A = (f_{ij}(\varphi))$ և $a_1, \ldots, a_n \in Q$, ապա սահմանվում է $\circ$ գործողությունը հետևյալ կերպ՝

$$A \circ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} f_{11}(\varphi)(a_1) + \cdots + f_{1n}(\varphi)(a_n) \\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots\ \ldots \\ f_{n1}(\varphi)(a_1) + \cdots + f_{nn}(\varphi)(a_n) \end{pmatrix} :$$

Լեմմ 17.58: *Եթե* $A, B \in P[\varphi]^{n\times n}$ *և* $a_1, \ldots, a_n \in Q$, *ապա*

$$(A \cdot B) \circ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = A \circ \left(B \circ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \right) : \qquad \square$$

Եթե $\varphi \in Hom(Q, Q)$ և $f \in P[x]$, $f = a_0 + a_1 x + \cdots + a_n x^n$, ապա կասենք, որ φ-ն f-ի արմատ է, եթե f-ը բացասում է φ-ին՝

$$f(\varphi) = 0\,,$$

այսինքն՝

$$a_0\varepsilon + a_1\varphi + \cdots + a_n\varphi^n = 0 :$$

Թեորեմ 17.62 (Համիլտոն-Քելի): *Ոչ զրոյական վերջավոր չափանի Q գծային տարածության յուրաքանչյուր $\varphi \in Hom(Q, Q)$ գծային ձևափոխություն իր բնութագրիչ բազմանդամի արմատ է:*

Ապացուցում: Դիցուք $e_1, \ldots, e_n$ հաջորդականությունը Q-ի հենք է, իսկ $A = (a_{ij})$ մատրիցը φ-ի մատրիցն է նշված հենքում: Պահանջվում է ապացուցել, որ φ-ն $det(A - xE)$ բազմանդամի արմատ է: Քանի որ

$$\begin{aligned} \varphi e_1 &= a_{11}e_1 + \cdots + a_{1n}e_n\,, \\ \ldots\ \ldots&\ \ldots\ \ldots\ \ldots \\ \varphi e_n &= a_{n1}e_1 + \cdots + a_{nn}e_n\,, \end{aligned}$$

ապա

$$\begin{cases} (a_{11}\varepsilon-\varphi)\,e_1+(a_{12}\varepsilon)\,e_2+\cdots+(a_{1n}\varepsilon)\,e_n=0, \\ \ \ldots\ \ \ldots\ \ \ldots\ \ \ldots\ \ \ldots\ \ \ldots\ \ \ldots \\ (a_{n1}\varepsilon)\,e_1+(a_{n2}\varepsilon)\,e_2+\cdots+(a_{nn}\varepsilon-\varphi)\,e_n=0: \end{cases}$$

Դիտարկելով գծային ձևափոխություններից կազմված հետևյալ մատրիցը՝

$$B=\begin{pmatrix} a_{11}\varepsilon-\varphi, & a_{12}\varepsilon, & \ldots, & a_{1n}\varepsilon \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1}\varepsilon, & a_{n2}\varepsilon, & \ldots, & a_{nn}\varepsilon-\varphi \end{pmatrix},$$

կունենանք՝

$$B\circ\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}=0:$$

Հետևաբար,

$$B^{\vee}\circ\left(B\circ\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}\right)=B^{\vee}\circ 0=0,$$

$$(B^{\vee}\cdot B)\circ\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}=0,$$

$$\begin{pmatrix} det(B) & & 0 \\ & \ddots & \\ 0 & & det(B) \end{pmatrix}\circ\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}=0,$$

այսինքն՝

$$\begin{cases} det(B)(e_1)=0\,, \\ \ldots\ \ \ldots\ \ \ldots \\ det(B)(e_n)=0\ : \end{cases}$$

Ուստի, ցանկացած $x\in Q$, $x=x_1e_1+\cdots+x_ne_n$ վեկտորի համար,

$$det(B)(x)=x_1det(B)(e_1)+\cdots+x_ndet(B)(e_n)=0\,,$$

այսինքն՝ $det(B) = 0$: Մնում է նկատել, որ $det(B)$-ն հենց φ գծային ձևափոխության բնութագրիչ բազմանդամի արժեքն է φ-ի վրա՝

$$0 = det(B) = (det(A - xE))\,(\varphi) : \qquad \square$$

Այժմ սահմանենք բազմանդամի արժեքի գաղափարը տրված n-րդ կարգի մատրիցի վրա: Դիցուք $f \in P[x]$ և $f = a_0 + a_1x + \cdots a_mx^m$, իսկ $A \in P^{n\times n}$: Հետևյալ n-րդ կարգի մատրիցը՝

$$\begin{aligned} f(A) &= a_0E + a_1A + \cdots + a_mA^m = \\ &= a_0E + (a_1E)A + \cdots + (a_mE)A^m = \\ &= a_0E + A(a_1E) + \cdots + A^m(a_mE) \end{aligned}$$

կոչվում է f **բազմանդամի արժեք** A **մատրիցի վրա**, որտեղ E-ն n-րդ կարգի միավոր մատրիցն է, իսկ $A^m = \underbrace{A \cdot A \cdots A}_{m}$: Եթե $f(A) = 0$, որտեղ 0-ն n-րդ կարգի զրոյական մատրիցն է, ապա f բազմանդամը կոչվում է A **մատրիցին բացասող բազմանդամ**, կամ A-ն կոչվում է f-ի արմատ: Ինչպես և գծային ձևափոխությունների դեպքում, նույն եղանակով կարելի է ապացուցել, որ յուրաքանչյուր n-րդ կարգի A մատրից հանդիսանում է որևէ ոչ զրոյական f բազմանդամի արմատ, որի աստիճանը $\leqslant n^2$: Սակայն Համիլտոն-Քելիի թեորեմից բխում է նաև հետևյալ արդյունքը:

Հետևություն 17.51: *Յուրաքանչյուր $A \in P^{n\times n}$ մատրից իր բնութագրիչ բազմանդամի արմատ է, այսինքն՝ եթե*

$$f = (-1)^n x^n + (-1)^{n-1} b_1 x^{n-1} + \cdots + b_n$$

բազմանդամը A-ի բնութագրիչ բազմանդամն է, ապա

$$(-1)^n A^n + (-1)^{n-1} b_1 A^{n-1} + \cdots + b_n E = 0 :$$

Ապացուցում: Օգտվենք նախորդ թեորեմից և կիրառենք թեորեմ 17.37-ը: $\square$

17.22. Անկյունագծային մատրիցով գծային ձևափոխություններ: Գծային տարածության վերլուծումը ինվարիանտ ենթատարածությունների ուղիղ գումարի: Արմատային ենթատարածություններ: Ժորդանյան մատրիցներ: Ժորդանյան հենք

Դիցուք Q-ն գծային տարածություն է որոշված P դաշտի վրա:

Լեմմ 17.59: *Եթե* $\lambda_1, \lambda_2, \ldots, \lambda_k \in P$ *սկալյարները* $\varphi \in Hom(Q, Q)$ *գծային ձևափոխության զույգ առ զույգ միմյանցից տարբեր սեփական արժեքներ են (այսինքն՝* $\lambda_i \neq \lambda_j$, *եթե* $i \neq j$*), իսկ* $u_1, u_2, \ldots, u_k \in Q$ *ոչ զրոյական վեկտորները դրանց համապատասխան սեփական վեկտորներ են, ապա* $u_1, u_2, \ldots, u_k$ *համակարգը գծայնորեն անկախ է:*

Ապացուցում (վերհանգման եղանակ): $k = 1$ դեպքում պնդումն ակնհայտ է: Ենթադրենք պնդումը ճիշտ է k-ից քիչ թվով սեփական արժեքների դեպքում, ապացուցենք k-ի համար: Դիցուք

$$\alpha_1 u_1 + \cdots + \alpha_{k-1} u_{k-1} + \alpha_k u_k = 0; \tag{17.29}$$

Հետևաբար,

$$\varphi\left(\alpha_1 u_1 + \cdots + \alpha_{k-1} u_{k-1} + \alpha_k u_k\right) = \varphi(0) = 0,$$

$$\alpha_1 \varphi(u_1) + \cdots + \alpha_{k-1} \varphi(u_{k-1}) + \alpha_k \varphi(u_k) = 0,$$

$$\alpha_1 \lambda_1 u_1 + \cdots + \alpha_{k-1} \lambda_{k-1} u_{k-1} + \alpha_k \lambda_k u_k = 0 : \tag{17.30}$$

(17.29) հավասարությունը ձախից բազմապատկենք λ_k-ով և հանենք (17.30)-ից՝

$$\alpha_1(\lambda_1 - \lambda_k) u_1 + \cdots + \alpha_{k-1}(\lambda_{k-1} - \lambda_k) u_{k-1} = 0;$$

Քանի որ, ըստ վերհանգման ենթադրության, $u_1, u_2, \ldots, u_{k-1}$ համակարգը գծայնորեն անկախ է, ապա

$$\alpha_1(\lambda_1 - \lambda_k) = \cdots = \alpha_{k-1}(\lambda_{k-1} - \lambda_k) = 0,$$

որտեղից $\alpha_1 = \cdots = \alpha_{k-1} = 0$, որովհետև $\lambda_i - \lambda_k \neq 0$, եթե $i \neq k$: Որից հետո, (17.29) հավասարությունից կունենանք՝ $\alpha_k u_k = 0$, որտեղ $u_k \neq 0$: Հետևաբար, նաև $\alpha_k = 0$: □

***Հետևություն 17.52*:** *1) Եթե $dim(Q) = n > 0$ և $\varphi \in Hom(Q,Q)$ գծային ձևափոխությունն ունի n հատ զույգ առ զույգ միմյանցից տարբեր $\lambda_1, \lambda_2, \ldots, \lambda_n \in P$ սեփական արժեքները, ապա դրանց համապատասխան $u_1, u_2, \ldots, u_n \in Q$ սեփական վեկտորների համակարգը կլինի Q-ի հենք, իսկ այդ հենքում φ գծային ձևափոխության A մատրիցը կունենա անկյունագծային տեսք՝*

$$A = \begin{pmatrix} \lambda_1 & & \text{\Large 0} \\ & \lambda_2 & \\ & & \ddots & \\ \text{\Large 0} & & & \lambda_n \end{pmatrix} :$$

2) Եվ հակառակը, եթե n-չափանի $(n > 0)$ Q գծային տարածության $e_1, \ldots, e_n$ հենքում $\varphi \in Hom(Q,Q)$ գծային ձևափոխության մատրիցն ունի անկյունագծային տեսք, ապա $e_1, \ldots, e_n$ հենքը կազմված է φ-ի սեփական վեկտորներից: □

Դիցուք Q-ն n-չափանի գծային տարածություն է, $\varphi \in Hom(Q,Q)$, Q_1-ը Q-ի φ-ինվարիանտ ենթատարածություն է, $Q = Q_1 \oplus Q_2$ և $e_1, \ldots, e_k$ համակարգը Q_1-ի հենք է, իսկ $e_1, \ldots, e_k, e_{k+1}, \ldots, e_n$ համակարգը Q-ի հենք է: Քանի որ $\varphi e_1, \ldots, \varphi e_k \in Q_1$, ապա

$$\begin{aligned}
&\varphi e_1 = \alpha_{11} e_1 + \cdots + \alpha_{1k} e_k + 0 e_{k+1} + \cdots + 0 e_n, \\
&\quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
&\varphi e_k = \alpha_{k1} e_1 + \cdots + \alpha_{kk} e_k + 0 e_{k+1} + \cdots + 0 e_n, \\
&\varphi e_{k+1} = \alpha_{k+1,1} e_1 + \cdots + \alpha_{k+1,k} e_k + \alpha_{k+1,k+1} e_{k+1} + \cdots + \alpha_{k+1,n} e_n, \\
&\quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
&\varphi e_n = \alpha_{n1} e_1 + \cdots + \alpha_{nk} e_k + \alpha_{n,k+1} e_{k+1} + \cdots + \alpha_{n,n} e_n,
\end{aligned}$$

այսինքն՝ φ գծային ձևափոխության մատրիցը նշված հենքում կունենա հետևյալ տեսքը՝

$$\begin{array}{cc} & \quad k \\ k & \left(\begin{array}{c|c} A_1 & 0 \\ \hline A_2 & A_3 \end{array}\right) \end{array},$$

որտեղ A_1-ը φ գծային ձևափոխության մատրիցն է Q_1-ի $e_1,\ldots,e_k$ հենքում, իսկ 0-ով նշանակված է $(k,n-k)$-չափանի զրոյական մատրիցը:

Դիցուք Q-ն n-չափանի գծային տարածություն է, $\varphi \in Hom(Q,Q)$, $Q = Q_1 \oplus Q_2$, որտեղ $Q_1, Q_2 \leqslant Q$ ենթատարածությունները φ-ինվարիանտ են: Եթե $e_1,\ldots,e_k$ համակարգը հենք է Q_1-ի համար, իսկ $f_1,\ldots,f_m$ համակարգը հենք է Q_2-ի համար, ապա $e_1,\ldots,e_k,f_1,\ldots,f_m$ համակարգը կլինի հենք Q-ի համար $(k+m=n)$ և φ-ի մատրիցը այդ հենքում կունենա հետևյալ տեսք՝

$$\left(\begin{array}{c|c} A_1 & 0 \\ \hline 0 & A_2 \end{array}\right),$$

որտեղ A_1-ը φ-ի մատրիցն է Q_1-ի $e_1,\ldots,e_k$ հենքում, իսկ A_2-ը φ-ի մատրիցն է Q_2-ի $f_1,\ldots,f_m$ հենքում: Հետևյալ տեսքի

$$\left(\begin{array}{cccc} A_1 & & 0 & \\ & A_2 & & \\ & & A_3 & \\ 0 & & & \ddots \end{array}\right):$$

քառակուսային մատրիցը կոչվում է **քվազիանկյունագծային** մատրից, որտեղ գլխավոր անկյունագծի երկայնքով դասավորված վանդակները քառակուսային մատրիցներ են, իսկ դրանցից դուրս գտնվող բոլոր տարրերը զրոներ են: Մասնավորապես, յուրաքանչյուր անկյունագծային մատրից քվազիանկյունագծային է:

Լեմմ 17.60: *Դիցուք Q-ն ոչ զրոյական n-չափանի գծային տարածություն է: Որպեսզի $\varphi \in Hom(Q,Q)$ գծային ձևափոխության մատրիցը Q-ի որևէ հենքում ունենա քվազիանկյունագծային տեսք անհրաժեշտ է և բավարար, որ Q-ն վերլուծվի իր ոչ զրոյական φ-ինվարիանտ ենթատարածությունների ուղիղ գումարի: Մասնավորապես, $\varphi \in$*

$Hom(Q,Q)$ գծային ձևափոխության մատրիցը Q-ի որևէ հենքում կունենա անկյունագծային տեսք այն և միայն այն դեպքում, երբ Q-ն վերլուծվում է իր 1-չափանի φ-ինվարիանտ ենթատարածությունների ուղիղ գումարի: □

m-րդ կարգի մատրիցը կոչվում է (m-րդ կարգի) **ժորդանյան վանդակ**, եթե այն ունի հետևյալ տեսքը՝

$$G_m(\lambda) = \begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} :$$

Այսպիսի ժորդանյան վանդակը կոչվում է նաև λ-ին համապատասխանող ժորդանյան վանդակ: Մասնավորապես, $G_1(\lambda) = (\lambda)$, իսկ

$$G_2(\lambda) = \begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}, G_3(\lambda) = \begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix} :$$

Քվազիանկյունագծային մատրիցը կոչվում է **ժորդանյան մատրից**, եթե նրա գլխավոր անկյունագծի երկայնքով դասավորված բոլոր վանդակները ժորդանյան վանդակներ են: Մասնավորապես, յուրաքանչյուր անկյունագծային մատրից ժորդանյան մատրից է, որի բոլոր ժորդանյան վանդակներն ունեն 1 կարգ:

Q գծային տարածության $e_1, \ldots, e_n$ հենքը կոչվում է $\varphi \in Hom(Q,Q)$ գծային ձևափոխության **ժորդանյան հենք**, եթե φ-ի մատրիցը $e_1, \ldots, e_n$ հենքի նկատմամբ ժորդանյան մատրից է: Տրված գծային ձևափոխության ժորդանյան հենքի գոյության և կառուցման հարցը համարվում է գծային տարածությունների ուսումնասիրության հիմնական խնդիրներից մեկը:

Թեորեմ 17.63: *Եթե $\varphi \in Hom(Q,Q)$ գծային ձևափոխության $f \in P[x]$ բացասող բազմանդամը հավասար է երկու փոխադարձաբար պարզ բազմանդամների արտադրյալի, այսինքն՝*

$$f = f_1 \cdot f_2, \quad \textit{որտեղ} \quad (f_1, f_2) = 1\,,$$

և $Q_1 = Ker\,(f_1(\varphi))$, $Q_2 = Ker\,(f_2(\varphi))$, *ապա* $Q_1, Q_2 \leqslant Q$ *ենթատարածությունները կլինեն* φ*-ինվարիանտ և*

$$Q = Q_1 \oplus Q_2 \ :$$

Ապացուցում: Ցանկացած $x \in Q$ տարրի համար՝

$$x \in Q_i \longleftrightarrow f_i(\varphi)(x) = 0, \qquad i = 1, 2 :$$

Նախ ապացուցենք $\varphi(Q_i) \subseteq Q_i$ ներդրումը, որտեղ $i = 1, 2$: Իրոք, եթե $x \in Q_i$, ապա

$$f_i(\varphi)(\varphi(x)) = (\varphi \cdot f_i(\varphi))\,(x) = (f_i(\varphi) \cdot \varphi)\,(x) = \varphi\,(f_i(\varphi)(x)) = \varphi(0) = 0 :$$

Քանի որ $(f_1, f_2) = 1$, ապա գոյություն ունեն այնպիսի $g_1, g_2 \in P[x]$ բազմանդամներ, որ

$$f_1 g_1 + f_2 g_2 = 1 :$$

Հետևաբար,

$$f_1(\varphi) g_1(\varphi) + f_2(\varphi) g_2(\varphi) = \varepsilon$$

և ցանկացած $x \in Q$ վեկտորի համար՝

$$(f_1(\varphi) g_1(\varphi))\,(x) + (f_2(\varphi) g_2(\varphi))\,(x) = x,$$

որտեղ $x_1 = (f_2(\varphi) g_2(\varphi))\, x \in Q_1$, իսկ $x_2 = (f_1(\varphi) g_1(\varphi))\, x \in Q_2$: Իրոք,

$$f_1(\varphi)(x_1) = f_1(\varphi)\,((f_2(\varphi) g_2(\varphi))\,(x)) = (f_2(\varphi) g_2(\varphi) f_1(\varphi))\,(x) =$$

$$= (f_1(\varphi) f_2(\varphi) g_2(\varphi))\,(x) = g_2(\varphi)\,((f_1(\varphi) \cdot f_2(\varphi))\,(x)) =$$

$$= g_2(\varphi)\,(f(\varphi)(x)) = g_2(\varphi)(0) = 0 :$$

Նույնպիսի քայլերով ստացվում է նաև $x_2 \in Q_2$ ներդրումը: Այսպիսով, յուրաքանչյուր $x \in Q$ տարրի համար գոյություն ունեն այնպիսի $x_1 \in Q_1$ և $x_2 \in Q_2$ տարրեր, որ $x = x_1 + x_2$: Մնում է ապացուցել, որ $Q_1 \cap Q_2 = \{0\}$: Իրոք, եթե $x \in Q_1 \cap Q_2$, ապա $x \in Q_1$ և $x \in Q_2$, այսինքն՝ $f_i(\varphi)(x) = 0$, $i = 1, 2$: Հետևաբար,

$$x = (f_1(\varphi) g_1(\varphi))\,(x) + (f_2(\varphi) g_2(\varphi))\,(x) =$$

$$= g_1(\varphi)\,(f_1(\varphi)(x)) + g_2(\varphi)\,(f_2(\varphi)(x)) = g_1(\varphi)(0) + g_2(\varphi)(0) = 0 + 0 = 0 : \ \square$$

Վերհանգման եղանակով ապացուցվում է նաև հետևյալ ընդհանուր արդյունքը:

Թեորեմ 17.64: *Եթե $\varphi \in Hom(Q,Q)$ գծային ձևափոխության $f \in P[x]$ բացասող բազմանդամը հավասար է զույգ առ զույգ փոխադարձաբար պարզ բազմանդամների արտադրյալի, այսինքն՝*

$$f = f_1 \cdot f_2 \cdots f_k, \quad \text{որտեղ} \quad (f_i, f_j) = 1, \;\; \text{եթե } i \neq j,$$

և $Q_i = Ker\,(f_i(\varphi))$, $i = 1, \ldots, k$, ապա $Q_i \leqslant Q$ ենթատարածությունները φ-ինվարիանտ են և

$$Q = Q_1 \oplus Q_2 \oplus \cdots \oplus Q_k : \qquad \square$$

***Հետևություն 17.53*:** *Եթե $\varphi \in Hom(Q,Q)$ գծային ձևափոխության $f \in P[x]$ բնութագրիչ բազմանդամը ներկայացվում է*

$$f = (x-\lambda_1)^{s_1}(x-\lambda_2)^{s_2}\cdots(x-\lambda_k)^{s_k}$$

տեսքով, որտեղ $\lambda_1, \lambda_2, \ldots, \lambda_k \in P$, $\lambda_i \neq \lambda_j$, եթե $i \neq j$, և

$$Q_i = \{x \in Q \,|\, (\varphi - \lambda_i\varepsilon)^{s_i}(x) = 0\}, \quad i = 1, \ldots, k,$$

ապա $Q_i \leqslant Q$ ենթատարածությունները կլինեն φ-ինվարիանտ և

$$Q = Q_1 \oplus Q_2 \oplus \cdots \oplus Q_k:$$

Ապացուցում: Համաձայն Համիլտոն-Քելիի թեորեմի՝ $f(\varphi) = 0$: $\square$

Հանգում ենք հետևյալ գաղափարին:

Դիցուք $\varphi \in Hom(Q,Q)$: $a \in Q$ վեկտորը կոչվում է $\lambda \in P$ սկալյարին համապատասխանող **արմատային φ-վեկտոր**, եթե գոյություն ունի այնպիսի m բնական թիվ, որ $(\varphi - \lambda\varepsilon)^m(a) = 0$: λ սկալյարին համապատասխանող բոլոր արմատային φ-վեկտորների բազմությունը նշանակենք Q_λ^φ-ով կամ համառոտ Q_λ-ով: Քանի որ $0 \in Q_\lambda$, ապա $Q_\lambda \neq \emptyset$ ցանկացած $\lambda \in P$ սկալյարի համար: $a \in Q$ վեկտորը կոչվում է **արմատային վեկտոր**, եթե $a \in Q_\lambda$ որևէ $\lambda \in P$ սկալյարի համար: Օրինակ, յուրաքանչյուր սեփական վեկտոր արմատային վեկտոր է:

Լեմմ 17.61: *Q_λ-ն Q-ի φ-ինվարիանտ ենթատարածություն է ցանկացած $\lambda \in P$ սկալյարի համար: Հետևաբար, $Q_\lambda \leqslant Q$ ենթատարածությունը կլինի ինվարիանտ նաև $\varphi - \mu\varepsilon$ և $(\varphi - \mu\varepsilon)^m$ գծային ձևափոխությունների նկատմամբ, որտեղ $\mu \in P$, իսկ $m \in \mathbb{N}$: Այս Q_λ ենթատարածությունը կոչվում է λ-ին համապատասխանող* **արմատային ենթատարածություն***:*

Ապացուցում: Եթե $a_1, a_2 \in Q_\lambda$, ապա գոյություն ունեն այնպիսի k_1, k_2 բնական թվեր, որ $(\varphi - \lambda\varepsilon)^{k_1}(a_1) = 0$ և $(\varphi - \lambda\varepsilon)^{k_2}(a_2) = 0$: Նշանակենք՝ $k = \max\{k_1, k_2\}$: Այդ դեպքում $(\varphi - \lambda\varepsilon)^k(a_i) = 0$, որտեղ $i = 1, 2$, և

$$(\varphi - \lambda\varepsilon)^k(a_1 + a_2) = (\varphi - \lambda\varepsilon)^k(a_1) + (\varphi - \lambda\varepsilon)^k(a_2) = 0 + 0 = 0 :$$

Միաժամանակ,

$$(\varphi - \lambda\varepsilon)^{k_1}(\alpha a_1) = \alpha\left((\varphi - \lambda\varepsilon)^{k_1}(a_1)\right) = \alpha 0 = 0 :$$

Մնում է ապացուցել $Q_\lambda \leqslant Q$ ենթատարածության φ-ինվարիանտությունը: Դիցուք $a \in Q_\lambda$ և $(\varphi - \lambda\varepsilon)^k(a) = 0$: Հետևաբար,

$$(\varphi - \lambda\varepsilon)^k(\varphi a) = \left(\varphi \cdot (\varphi - \lambda\varepsilon)^k\right)(a) = \left((\varphi - \lambda\varepsilon)^k \cdot \varphi\right)(a) =$$

$$= \varphi\left((\varphi - \lambda\varepsilon)^k(a)\right) = \varphi(0) = 0,$$

այսինքն՝ $\varphi a \in Q_\lambda$ □

Լեմմ 17.62 (արմատային ենթատարածության ոչ զրոյական լինելու հայտանիշը): *Որպեսզի Q_λ-ն լինի ոչ զրոյական ենթատարածություն անհրաժեշտ է և բավարար, որ λ-ն լինի φ-ի սեփական արժեք:*

Ապացուցում: Եթե $a \in Q_\lambda$, $a \neq 0$, ապա

$$(\varphi - \lambda\varepsilon)^m(a) = 0$$

որևէ m բնական թվի համար: Ակնհայտ է, որ $m > 0$ և դիցուք m_0-ն այս պայմանին բավարարող փոքրագույն բնական թիվն է: $m_0 = 1$ դեպքում a-ն կլինի λ-ին համապատասխանող սեփական վեկտոր, իսկ $m_0 > 1$ դեպքում կունենաք՝

$$0 = (\varphi - \lambda\varepsilon)^{m_0}(a) = (\varphi - \lambda\varepsilon)\left((\varphi - \lambda\varepsilon)^{m_0 - 1}(a)\right) = (\varphi - \lambda\varepsilon)(a_1),$$

որտեղ $a_1 = (\varphi - \lambda\varepsilon)^{m_0 - 1}(a) \neq 0$, այսինքն՝ a_1-ը կլինի λ-ին համապատասխանող սեփական վեկտոր:

Եվ հակառակը, եթե λ-ն φ-ի սեփական արժեք է, ապա գոյություն ունի այնպիսի $a \in Q$, $a \neq 0$, վեկտոր, որ $\varphi(a) = \lambda a$, այսինքն՝ $(\varphi - \lambda\varepsilon)a = 0$ և $a \in Q_\lambda$, որտեղ $a \neq 0$: □

Հետևյալ արդյունքն ապացուցվում է վերհանգման եղանակով (տես թեորեմ 17.57-ի ապացուցումը):

Թեորեմ 17.65: *$\varphi \in Hom(Q,Q)$ գծային ձևափոխության զույգ առ զույգ միմյանցից տարբեր $\lambda_1,\ldots,\lambda_k$ սեփական արժեքներին համապատասխանող արմատային ենթատարածությունները գծայնորեն անկախ են ($\lambda_i \neq \lambda_j$, եթե $i \neq j$):* □

Թեորեմ 17.66: *Եթե $\varphi \in Hom(Q,Q)$ գծային ձևափոխության $f \in P[x]$ բնութագրիչ բազմանդամը ներկայացվում է*

$$f = (x-\lambda_1)^{s_1}(x-\lambda_2)^{s_2}\cdots(x-\lambda_k)^{s_k}$$

տեսքով, որտեղ $\lambda_1,\lambda_2,\ldots,\lambda_k \in P$, $\lambda_i \neq \lambda_j$, եթե $i \neq j$, ապա

$$Q = Q_{\lambda_1} \oplus Q_{\lambda_2} \oplus \cdots \oplus Q_{\lambda_k} :$$

Ապացուցում: Հաշվի առնելով հետևություն 17.53-ում կատարված Q_i նշանակումները, բավական է ապացուցել, որ $Q_i = Q_{\lambda_i}$, որտեղ $i = 1,\ldots,k$: Ակնհայտ է, որ $Q_i \subseteq Q_{\lambda_i}$: Հակառակ ներդրումն ապացուցենք, օրինակ, $i=1$ դեպքում:

Դիցուք $a \in Q_{\lambda_1} \subseteq Q$: Համաձայն հետևություն 17.53-ի, գոյություն ունեն այնպիսի $a_1 \in Q_1$, $a_2 \in Q_2$, …, $a_k \in Q_k$ վեկտորներ, որ $a = a_1+a_2+\cdots+a_k$: Նշանակելով՝ $a' = a_2+\cdots+a_k$, կունենանք՝ $a = a_1+a'$ կամ $a' = a-a_1 \in Q_{\lambda_1}$, որովհետև $a_1 \in Q_1 \subseteq Q_{\lambda_1}$: Հետևաբար, գոյություն կունենա այնպիսի m բնական թիվ, որ

$$(\varphi-\lambda_1\varepsilon)^m(a') = 0,$$

որտեղ $a' = a_2+\cdots+a_k \in Q_2\oplus\cdots\oplus Q_k$: Այնուհետև, քանի որ

$$((\varphi-\lambda_2\varepsilon)^{s_2}\cdots(\varphi-\lambda_k\varepsilon)^{s_k})\,a_i = 0, \qquad i=2,\ldots,k,$$

ապա

$$((\varphi-\lambda_2\varepsilon)^{s_2}\cdots(\varphi-\lambda_k\varepsilon)^{s_k})\,(a_2+\cdots+a_k) = 0,$$

այսինքն՝

$$((\varphi-\lambda_2\varepsilon)^{s_2}\cdots(\varphi-\lambda_k\varepsilon)^{s_k})\,(a') = 0 :$$

Նշանակելով $g_1 = (x-\lambda_1)^m$ և $g_2 = (x-\lambda_2)^{s_2}\cdots(x-\lambda_k)^{s_k}$, կունենանք՝ $g_1(\varphi)(a') = 0$, $g_2(\varphi)(a') = 0$ և $(g_1,g_2) = 1$, այսինքն՝ գոյություն կունենան այնպիսի $g_1', g_2' \in P[x]$ բազմանդամներ, որ $g_1g_1' + g_2g_2' = 1$ կամ $g_1(\varphi)g_1'(\varphi) + g_2(\varphi)g_2'(\varphi) = \varepsilon$: Հաշվենք a'-ը.

$$a' = \varepsilon(a') = (g_1(\varphi)g_1'(\varphi) + g_2(\varphi)g_2'(\varphi))\,(a') =$$

$$= (g_1(\varphi)g_1'(\varphi))\,(a') + (g_2(\varphi)g_2'(\varphi))\,(a') =$$

$$= g_1'(\varphi)\,(g_1(\varphi)(a')) + g_2'(\varphi)\,(g_2(\varphi)(a')) = 0 + 0 = 0:$$

Այսպիսով, $a = a_1 + a' = a_1 + 0 = a_1 \in Q_1$: □

Դիցուք Q-ն վերջավոր չափանի գծային տարածություն է որոշված P դաշտի վրա, $\varphi \in Hom(Q,Q)$, $\lambda \in P$, $a \in Q_\lambda$: Այդ դեպքում

$$\min\{m \in \mathbb{N}\,|\,(\varphi - \lambda\varepsilon)^m(a) = 0\}$$

բնական թիվը[17] կոչվում է a **արմատային վեկտորի բարձրություն** և նշանակվում է $|a|$-ով: Օրինակ, $|0| = 0$: Ցանկացած $i = 0,1,2,\ldots$ բնական թվի համար սահմանենք՝

$$H_i = \{a \in Q_\lambda|\ |a| \leqslant i\} \subseteq Q_\lambda:$$

Ակնհայտ է, որ $H_0 \subseteq H_1 \subseteq H_2 \subset \cdots$

Լեմմ 17.63: *$H_i \leqslant Q_\lambda$ ցանկացած i բնական թվի համար: Մասնավորապես, $H_0 \leqslant H_1 \leqslant H_2 \leqslant \cdots \leqslant Q_\lambda$:*

Ապացուցում: Եթե $x, y \in H_i$, ապա ցանկացած $\alpha, \beta \in P$ սկալյարների համար՝

$$(\varphi - \lambda\varepsilon)^i(\alpha x + \beta y) = \alpha\left((\varphi - \lambda\varepsilon)^i(x)\right) + \beta\left((\varphi - \lambda\varepsilon)^i(y)\right) =$$

$$= \alpha 0 + \beta 0 = 0 + 0 = 0: \qquad \square$$

Կգրենք $H_i < H_j$, եթե $H_i \leqslant H_j$ և $H_i \neq H_j$:

Լեմմ 17.64: *Գոյություն ունի այնպիսի $i \geqslant 0$ բնական թիվ, որ $H_i = H_{i+1}$:*

Ապացուցում: Ենթադրելով հակառակը, կստանանք՝ $H_i \leqslant H_{i+1}$, որտեղ $H_i \neq H_{i+1}$, $i \in \mathbb{N}$, այսինքն՝ վերջավոր չափանի Q_λ գծային տարածության մեջ կունենանք անվերջ թվով միմյանցից տարբեր ենթատարածությունների աճող շղթա՝ $H_0 < H_1 < H_2 < \cdots < H_i < H_{i+1} < \cdots$: □

Լեմմ 17.65: *Եթե $H_i = H_{i+1}$, ապա $H_i = H_{i+j}$ ցանկացած j բնական թվի համար:*

[17] Այստեղ զրոն ևս համարվում է բնական թիվ:

Ապացուցում: Ապացուցենք $H_i = H_{i+2}$ հավասարությունը (նույն եղանակով ստացվում են մնացած հավասարությունները): Քանի որ $H_i = H_{i+1}$, ապա ցանկացած $a \in H_{i+1}$ վեկտորի համար՝

$$(\varphi - \lambda\varepsilon)^{i+1}(a) = 0 \longleftrightarrow (\varphi - \lambda\varepsilon)^{i}(a) = 0 :$$

Դիցուք $a \in H_{i+2}$: Այդ դեպքում՝ $(\varphi - \lambda\varepsilon)a \in H_{i+1}$ և

$$0 = (\varphi - \lambda\varepsilon)^{i+2}(a) = (\varphi - \lambda\varepsilon)^{i+1}\left((\varphi - \lambda\varepsilon)(a)\right) =$$

$$= (\varphi - \lambda\varepsilon)^{i}\left((\varphi - \lambda\varepsilon)(a)\right) = (\varphi - \lambda\varepsilon)^{i+1}(a),$$

այսինքն՝ $a \in H_{i+1} = H_i$: □

Հանգում ենք հետևյալ արդյունքին:

Լեմմ 17.66: *Եթե*

$$m = \min\left\{i \in \mathbb{N} \,|\, H_i = H_{i+1}\right\},$$

ապա $H_0 < H_1 < H_2 < \cdots < H_{m-1} < H_m = Q_\lambda$*:* □

Լեմմ 17.67: *Եթե $Q' \leqslant Q$ և $e_1, \ldots, e_s$ հաջորդականությունը հենք է Q'-ի համար, իսկ $e_1, \ldots, e_s, f_1, \ldots, f_t$ հաջորդականությունը հենք է Q-ի համար, ապա Q'-ի ցանկացած $e'_1, \ldots, e'_s$ հենքի համար $e'_1, \ldots, e'_s, f_1, \ldots, f_t$ հաջորդականությունը կլինի հենք Q-ի համար:*

Ապացուցում: Եթե $Q'' = \langle f_1, \ldots, f_t \rangle$, ապա $Q = Q' \oplus Q''$: □

Իրականում, այս հատկությունը կապված է **հարաբերական հենքի** հասկացության հետ:

$a_1, a_2, \ldots, a_k \in Q$ հաջորդականությունը (համակարգը) կոչվում է **հարաբերական գծայնորեն անկախ ըստ** $H \leqslant Q$ **ենթատարածության** կամ $H \leqslant Q$ ենթատարածության նկատմամբ, եթե $a_1 + H$, $a_2 + H$, ..., $a_k + H$ համակարգը գծայնորեն անկախ է $Q/_H$ քանորդ-տարածության մեջ:

$a_1, a_2, \ldots, a_n \in Q$ համակարգը կոչվում է **հարաբերական հենք ըստ** $H \leqslant Q$ **ենթատարածության** կամ $H \leqslant Q$ ենթատարածության նկատմամբ, եթե $a_1 + H$, $a_2 + H$, ..., $a_n + H$ համակարգը հենք է $Q/_H$ քանորդ-տարածության համար: Հետևյալ պնդումներն ակնհայտ են:

Որպեսզի վեկտորների $a_1, a_2, \ldots, a_k \in Q$ համակարգը լինի հարաբերական գծայնորեն անկախ ըստ $H \leqslant Q$ ենթատարածության անհրաժեշտ է և բավարար, որ ցանկացած $\alpha_1, \alpha_2, \ldots, \alpha_k \in P$ սկալյարների համար՝

$$\alpha_1 a_1 + \alpha_2 a_2 + \cdots \alpha_k a_k \in H \longleftrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_k = 0 :$$

Որպեսզի վեկտորների $a_1, a_2, \ldots, a_k \in Q$ համակարգը լինի հարաբերական գծայնորեն անկախ ըստ $H \leqslant Q$ ենթատարածության անհրաժեշտ է և բավարար, որ H-ի ցանկացած $e_1, \ldots, e_t$ հենքի համար $e_1, \ldots, e_t, a_1, a_2, \ldots, a_k$ համակարգը լինի գծայնորեն անկախ: Հետևաբար, որպեսզի վեկտորների $a_1, a_2, \ldots, a_n \in Q$ համակարգը լինի հարաբերական հենք ըստ $H \leqslant Q$ ենթատարածության անհրաժեշտ է և բավարար, որ H-ի ցանկացած $e_1, \ldots, e_t$ հենքի համար

$$e_1, \ldots, e_t, a_1, \ldots, a_n$$

համակարգը լինի հենք Q-ի համար:

Թեորեմ 17.67 (հիմնական): *Դիցուք Q-ն n-չափանի գծային տարածություն է որոշված P դաշտի վրա $(n > 0)$: **Եթե** $\varphi \in Hom(Q, Q)$ գծային ձևափոխության $f \in P[x]$ բնութագրիչ բազմանդամը ներկայացվում է*

$$f = (x - \lambda_1)^{s_1} (x - \lambda_2)^{s_2} \cdots (x - \lambda_k)^{s_k}$$

*տեսքով, որտեղ $\lambda_1, \lambda_2, \ldots, \lambda_k \in P$, $\lambda_i \neq \lambda_j$, **եթե** $i \neq j$, ապա գոյություն ունի Q-ի այնպիսի հենք, որում φ-ի մատրիցը ժորդանյան է, այսինքն՝ Q-ում գոյություն ունի φ գծային ձևափոխության ժորդանյան հենք:*

Ապացուցում: Ըստ հետևություն 17.53-ի, $Q = Q_1 \oplus Q_2 \oplus \cdots \oplus Q_k$, որտեղ $Q_i = Ker\left((\varphi - \lambda_i \varepsilon)^{s_i}\right) = Q_{\lambda_i}$ (թեորեմ 17.66), $\varphi(Q_i) \subseteq Q_i$: Նշանակենք՝ $Q_{\lambda_i} = Q_\lambda$ և դիտարկենք համապատասխան H_j ենթատարածությունները: Դիցուք՝

$$m = \min\{j \in \mathbb{N} \mid H_j = H_{j+1}\} :$$

Այդ դեպքում (լեմմ 17.66), $Q_\lambda = H_m$: Նշանակենք g_λ-ով φ գծային ձևափոխության սահմանափակումը $Q_\lambda = H_m \leqslant Q$ ենթատարածության վրա՝ $g_\lambda = \varphi|_{Q_\lambda} : Q_\lambda \to Q_\lambda$: Կստանանք՝ $g_\lambda \in Hom(Q_\lambda, Q_\lambda)$: Ունենք՝

$$H_0 < H_1 < H_2 < \cdots < H_m = Q_\lambda,$$

որտեղ $H_i = \left\{a \in Q_\lambda | \, (g_\lambda - \lambda\varepsilon)^i(a) = 0\right\}$: Եթե $g = g_\lambda - \lambda\varepsilon$, ապա $g \in Hom(Q_\lambda, Q_\lambda)$ և

$$H_i = \left\{a \in Q_\lambda | \, g^i(a) = 0\right\}, \qquad i = 0, 1, \ldots, m :$$

Ապացուցենք, որ g-ի համար գոյություն ունի Ժորդանյան հենք: Նախ նկատենք, որ x^m բազմանդամը կլինի g-ի փոքրագույն բազմանդամ: Իրոք, $g^m(a) = 0$ ցանկացած $a \in Q_\lambda$ վեկտորի համար և եթե h_g-ն փոքրագույն բազմանդամ է g-ի համար, ապա x^m-ը կբաժանվի h_g-ի վրա, հետևաբար, $h_g = \mu x^t$, որտեղ $\mu \in P$, $\mu \neq 0$, իսկ $t \leqslant m$: Սակայն $t < m$ դեպքում՝ $H_t < H_m = Q_\lambda$ և, հետևաբար, h_g-ն չի լինի $g : Q_\lambda \to Q_\lambda$ գծային ձևափոխության բացասող բազմանդամ: Ուստի, $t = m$ և $h_g = \mu x^m$:

Համաձայն թեորեմ 17.59-ի, g-ի միակ սեփական արժեքը կլինի 0-ն:

Այժմ դիտարկենք $H_m = Q_\lambda \leqslant Q$ ենթատարածությունը: Դիցուք $h_1, \ldots, h_{\ell_1} \in H_m$ համակարգը հենք է H_{m-1}-ի համար, իսկ $h_1, \ldots, h_{\ell_1}, f_1, \ldots, f_{t_1}$ հաջորդականությունը հենք է H_m-ի համար: Հաջորդ քայլում, $h_1, \ldots, h_{\ell_1}$ հենքը փոխարինվում է H_{m-1}-ի մեկ այլ հենքով: Իրոք, H_{m-2}-ի ցանկացած $b_1, \ldots, b_{\ell_2}$ հենքի համար, $b_1, \ldots, b_{\ell_2}, g(f_1), \ldots, g\left(f_{t_1}\right) \in H_{m-1}$ հաջորդականությունը կլինի գծայնորեն անկախ, որը կարելի է շարունակել մինչև H_{m-1}-ի հենքի՝

$$b_1, \ldots, b_{\ell_2}, g(f_1), \ldots, g\left(f_{t_1}\right), f_{t_1+1}, \ldots, f_{t_2} :$$

Նման եղանակով կառուցելով հենքեր $H_{m-2}, H_{m-3}, \ldots, H_1$ ենթատարածությունների համար, ստանում ենք $H_m = Q_\lambda$ ենթատարածության հետևյալ հենքը՝

$$\begin{array}{l}
f_1, \ldots, f_{t_1}, \\
g(f_1), \ldots, g\left(f_{t_1}\right), f_{t_1+1}, \ldots, f_{t_2}, \\
\quad \ldots \quad \ldots \quad \ldots \quad \ldots \\
g^{m-1}(f_1), \ldots, g^{m-1}\left(f_{t_1}\right), g^{m-2}\left(f_{t_1+1}\right), \ldots, g^{m-2}\left(f_{t_2}\right), \ldots, f_{t_{m-1}+1}, \ldots, f_{t_m} :
\end{array}$$

Այս հենքը վերադասավորենք ըստ սյունակների և դիտարկենք ստացված սյունակներին համապատասխան գծային թաղանթները՝

$$\begin{array}{l}
G_1 = \langle f_1, g(f_1), \ldots, g^{m-1}(f_1)\rangle, \\
G_2 = \langle f_2, g(f_2), \ldots, g^{m-1}(f_2)\rangle, \\
\quad \ldots \quad \ldots \quad \ldots \quad \ldots
\end{array}$$

Վերջին սյունակներով ծնված գծային թաղանթները կլինեն 1-չափանի: Այսպիսով,

$$Q_\lambda = G_1 \oplus G_2 \oplus \cdots \oplus G_{t_m},$$

որտեղ բոլոր G_i ենթատարածությունները ակնհայտորեն g-ինվարիանտ են, իսկ G_i-ի նշված հենքում g-ի մատրիցը կլինի ժորդանյան վանդակ: Ըստ որում, ստացվող ժորդանյան վանդակները կլինեն $\lambda = 0$-ին համապատասխանող:

Քանի որ $g = g_\lambda - \lambda\varepsilon$, ապա կառուցված հենքի նկատմամբ $g_\lambda = g + \lambda\varepsilon$: $Q_\lambda \to Q_\lambda$ գծային ձևափոխության մատրիցը կլինի ժորդանյան մատրից: Հետևաբար, միավորելով բոլոր Q_λ ենթատարածություններում կառուցված հենքերը կստանանք ժորդանյան հենք սկզբնական $\varphi \in Hom(Q,Q)$ գծային ձևափոխության համար: □

Հետևություն 17.54 (ժորդան): *Վերջավոր չափանի կոմպլեքս գծային տարածության յուրաքանչյուր գծային ձևափոխության համար գոյություն ունի ժորդանյան հենք:* □

Հետևություն 17.55: *Կոմպլեքս թվերով յուրաքանչյուր քառակուսային մատրից նման է որևէ ժորդանյան մատրիցի:* □

$\varphi \in Hom(Q,Q)$ գծային ձևափոխությունը կոչվում է **նիլպոտենտ**, եթե գոյություն ունի այնպիսի n բնական թիվ, որ $\varphi^n = 0$: Այդպիսի n բնական թվերից փոքրագույնը կոչվում է φ նիլպոտենտ գծային ձևափոխության **նիլպոտենտության ցուցիչ**: Օրինակ, $deg(f) \leqslant n-1$ պայմանին բավարարող բոլոր բազմանդամների գծային տարածության ածանցման $\varphi(f) = f'$ գծային ձևափոխությունը նիլպոտենտ է:

Հիմնական թեորեմի ապացուցման ընթացքում, ըստ էության, ապացուցվել է նաև հետևյալ արդյունքը:

Հետևություն 17.56: *Վերջավոր չափանի գծային տարածության յուրաքանչյուր նիլպոտենտ գծային ձևափոխության համար գոյություն ունի ժորդանյան հենք:* □

$A \in P^{m\times m}$ մատրիցը կոչվում է նիլպոտենտ, եթե գոյություն ունի այնպիսի n բնական թիվ, որ $A^n = 0$: Այդպիսի n բնական թվերից փոքրագույնը կոչվում է φ նիլպոտենտ մատրիցի **նիլպոտենտության ցուցիչ**: Օրինակ, $G_m(0)$ ժորդանյան վանդակը նիլպոտենտ մատրից է, որովհետև $(G_m(0))^m = 0$:

Լեմմ 17.68: *Եթե A մատրիցը նիլպոտենտ է, ապա նրա միակ սեփական արժեքը 0-ն է:* □

***Հետևություն 17.57*:** *Յուրաքանչյուր նիլպոտենտ մատրից նման է որևէ ժորդանյան մատրիցի:* □

Լեմմ 17.69: *Եթե $\varphi \in Hom(Q, Q)$ գծային ձևափոխությունը նիլպոտենտ է՝ n նիլպոտենտության ցուցիչով և $\varphi^{n-1}(\xi) \neq 0$, $\xi \in Q$, ապա*

$$\xi, \varphi(\xi), \varphi^2(\xi), \ldots, \varphi^{n-1}(\xi)$$

հաջորդականությունը գծայնորեն անկախ է, իսկ դրանով ծնված ենթատարածությունը կլինի φ-ինվարիանտ: □

Վարժություններ և խնդիրներ

1. Գտնել $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ տեսքի մատրիցների L գծային տարածության որևէ հենք, որտեղ $a, b \in \mathbb{Z}_2$:

2. Գտնել $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ տեսքի մատրիցների H գծային տարածության որևէ հենք, որտեղ $a, b \in \mathbb{Z}_2$:

3. Ապացուցել, որ նախորդ երկու վարժություններում սահմանված L և H գծային տարածություններն իզոմորֆ են և կառուցել որևէ $\varphi : L \to H$ իզոմորֆիզմ:

4. 1 և 2 վարժությունները լուծել այն դեպքում, երբ $a, b \in \mathbb{R}$, այսինքն՝

$$L' = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \; a, b \in \mathbb{R} \right\} \leqslant \mathbb{R}^{2\times 2}$$

և

$$H' = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \middle| \; a, b \in \mathbb{R} \right\} \leqslant \mathbb{R}^{2\times 2}$$

ենթատարածությունների դեպքում: Ապացուցել, որ $a_0 + L' = a_1 + L'$, իսկ $a_0 + H' \neq a_1 + H'$, որտեղ

$$a_0 = \begin{pmatrix} 3 & 4 \\ 5 & -4 \end{pmatrix}, \qquad a_1 = \begin{pmatrix} 1 & 4 \\ 5 & 0 \end{pmatrix} :$$

5. Ապացուցել, որ եթե Q-ն 2-չափանի գծային տարածություն է, իսկ նրա $Q_1, Q_2 \leqslant Q$ 1-չափանի ենթատարածությունները միմյանցից տարբեր են, ապա $Q = Q_1 \oplus Q_2$:

6. Ապացուցել, որ եթե Q-ն 3-չափանի գծային տարածություն է, իսկ նրա $Q_1, Q_2 \leqslant Q$ 2-չափանի ենթատարածությունները միմյանցից տարբեր են, ապա $Q = Q_1 \cap Q_2$ ենթատարածությունը 1-չափանի է, իսկ $Q = Q_1 + Q_2$:

7. Ապացուցել, որ $\varphi : Q \to Q$ գծային ձևափոխության մատրիցի ռանգը և φ-ի ռանգը հավասար են:

8. Օգտվելով օրթոգոնալացման ընթացքից, կառուցել օրթոնորմալ հենք բազմանդամների $F_3 = \{f \in \mathbb{R}[x] | \, deg(f) \leqslant 2\}$ էվկլիդյան տարածության համար, որտեղ սկալյար արտադրյալը որոշվում է հետևյալ բանաձևով՝

$$(f, g) = \int_0^1 f(x) g(x) \, dx :$$

9. Գտնել Q իրական գծային տարածության $\varphi \in Hom(Q, Q)$ գծային ձևափոխության սեփական արժեքները և սեփական վեկտորները, եթե φ-ն Q-ի որևէ հենքում ունի հետևյալ մատրիցը՝

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} :$$

10. Օգտվելով Կոշի-Բունյակովսկու անհավասարությունից ստանալ

$$\left(\int_a^b f(x) g(x) \, dx \right)^2 \leqslant \int_a^b (f(x))^2 \, dx \cdot \int_a^b (g(x))^2 \, dx$$

անհավասարությունը, որտեղ f, g ֆունկցիաները $[a, b] \subseteq \mathbb{R}$ հատվածում անընդհատ ֆունկցիաներ են ($a < b$):

11. Եթե $A \in P^{n \times n}$ մատրիցը հակադարձելի է, այսինքն՝ $det(A) \neq 0$, իսկ նրա բնութագրիչ բազմանդամն է՝

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n,$$

ապա

$$A^{-1} = -\frac{1}{b_n}\left(A^{n-1} + b_1 A^{n-2} + \cdots + b_{n-2}A + b_{n-1}E\right) :$$

12. Գտնել զրոյական գծային ձևափոխության փոքրագույն բազմանդամը:

13. Գտնել միավոր (նույնական) գծային ձևափոխության փոքրագույն բազմանդամը:

14. Գտնել λ գործակցով նմանության փոքրագույն բազմանդամը:

15. Ապացուցել, որ $(x - \lambda)^m$ բազմանդամը հանդիսանում է $G_m(\lambda)$ Ժորդանյան վանդակի փոքրագույն բազմանդամ:

16. Եթե երկու Ժորդանյան մատրիցներ նման են, ապա այդ մատրիցները բաղկացած են նույն Ժորդանյան վանդակներից և կարող են տարբերվել միայն Ժորդանյան վանդակների դասավորությամբ:

Մաս Գ

Հանրահաշվական կառուցվածքներ

Գ լ ու խ 18

ԽՄԲԵՐ

18.1. Կիսախմբի, քվազիխմբի, խմբի և աբելյան խմբի գաղափարները

18.1.1. Հանրահաշվական գործողության և հանրահաշվի գաղափարները: Դիցուք $Q \neq \emptyset$, $Q^n = \underbrace{Q \times Q \times \cdots \times Q}$, $n \in N$: Ցանկացած $f : Q^n \to Q$ արտապատկերում (ֆունկցիա) կոչվում է հանրահաշվական **գործողություն** կամ համառոտ **գործողություն**՝ որոշված կամ սահմանված Q-ի վրա (մեջ), $n \geqslant 1$: Այդ դեպքում, n-ը կոչվում է f գործողության **տեղայնություն**, իսկ f-ը՝ n-տեղանի գործողություն: Ընդ որում, եթե $f : (x_1, \ldots, x_n) \to z$, ապա գրվում է $z = f(x_1, \ldots, x_n)$: $n = 2$ դեպքում f-ը կոչվում է **երկտեղ գործողություն**, իսկ $n = 1$ դեպքում հանգում ենք բազմության ձևափոխության գաղափարին: Հաճախ դիտարկվում են նաև զրո-տեղանի գործողություններ: Q բազմության վրա որոշված զրո-տեղանի (համառոտ՝ 0-տեղանի) գործողություն ասելով հասկացվում է այդ բազմության որևէ տարրի սևեռումը (ֆիքսումը):

$Q \neq \emptyset$ բազմությունն իր մեջ սահմանված գործողությունների Σ բազմության հետ մեկտեղ կոչվում է **հանրահաշիվ** և նշանակվում է՝ $(Q; \Sigma)$ կամ $Q(\Sigma)$: Եթե Σ բազմությունը վերջավոր է և $\Sigma = \{f_1, f_2, \ldots, f_m\}$, ապա $Q(\Sigma)$-ն նշանակվում է՝ $Q(f_1, f_2, \ldots, f_m)$: Q (համապատասխանաբար Σ) բազմության տարրերը կոչվում են $Q(\Sigma)$ **հանրահաշվի տարրեր** (գործողություններ), իսկ Q-ն կոչվում է նաև $Q(\Sigma)$ հանրահաշվի **հենքային բազմություն**: Հենքային բազմության հզորությունը (կարգը) կոչվում է հանրահաշվի հզորություն (կարգ): Հանրահաշիվը կոչվում է վերջավոր, եթե վերջավոր է նրա հենքային բազմությունը, և անվերջ՝ հակառակ դեպքում: Ընդ որում, եթե հենքային բազմության կարգը հավասար է n-ի, ապա վերջավոր հանրահաշիվը կոչվում է նաև n-տարրանի: Երկու $(Q; \Sigma)$ և $(Q'; \Sigma')$ հանրահաշիվներ կոչվում են **հավասար**, եթե $Q = Q'$ և $\Sigma = \Sigma'$: $Q(\Sigma)$ հանրահաշիվը հաճախ համառոտ նշանակվում է նաև Q-ով: *Օրինակ,* գծային (վեկտորական) տարածությունը հանրահաշիվ է, որի գործողությունների բազմությունը կազմված է մեկ $+$ երկտեղ գործողությունից և յուրաքանչյուր α սկալյարին (թվին) համապատասխանող $\alpha(x) = \alpha x$ 1-տեղանի գործողություններից:

Հանրահաշիվը կոչվում է **երկտեղ** (բինար), եթե երկտեղ են նրա բոլոր գործողությունները: *Օրինակ,* $\mathbb{R}(+, \cdot, -)$-ը, $\mathbb{N}(+, \cdot, \circ, *)$-ը, որտեղ $m \circ n = (m, n)$, $m * n = [m, n]$, երկտեղ հանրահաշիվներ են: Այսուհետ ուսումնասիրվող հանրահաշիվները հիմնականում կլինեն երկտեղ հանրահաշիվներ, որոնք բավարարում են լրացուցիչ աքսիոմների (պայմանների, նույնությունների): Այդ պատճառով, գործողություն ասելով այսուհետ կհասկացվի հենց երկտեղ գործողություն (տես նաև 1.4-ը), եթե չի նշվում հակառակը: Եթե f-ը փոխարինվում է $\circ$ կամ $+$ նշանով, ապա $f(x, y)$-ի փոխարեն գրվում է $x \circ y$ կամ` $x + y$: Մեկ գործողությամբ հանրահաշիվը սովորաբար նշանակվում է $Q(\circ)$-ով և կոչվում է **խմբակերպ**, իսկ երկու գործողությամբ հանրահաշիվը հաճախ նշանակվում է $Q(+, \cdot)$-ով և կոչվում է **երկխմբակերպ**:

Վերջավոր բազմության վրա սահմանվող (կամ արդեն սահմանված) գործողությունը հաճախ տրվում (կամ ներկայացվում) է թվաբանության մեջ գործածվող բազմապատկման աղյուսակների ձևով`

$$\begin{array}{c|cccc}
\circ & a_1 & a_2 & \cdots & a_n \\
\hline
a_1 & a_1 \circ a_1 & a_1 \circ a_2 & \cdots & a_1 \circ a_n \\
a_2 & a_2 \circ a_1 & a_2 \circ a_2 & \cdots & a_2 \circ a_n \\
\cdots & \cdots & \cdots & \cdots & \cdots \\
a_n & a_n \circ a_1 & a_n \circ a_2 & \cdots & a_n \circ a_n
\end{array} :$$

ժամանակակից հանրահաշվում գործողությունների տրման այս «բազմապատկման» աղյուսակները կոչվում են նաև Քելիի (A. Cayley) աղյուսակներ կամ երբեմն լատինական քառակուսիներ:

Քանի որ երկու A, B վերջավոր բազմությունների միջև գործող բոլոր $f : A \to B$ արտապատկերումների թիվը հավասար է $|B|^{|A|}$ (տես 0.3-ը), ապա n-տարրանի Q վերջավոր բազմության վրա որոշված բոլոր (երկտեղ) գործողությունների թիվը կլինի հավասար` $n^{n^2}$: Մասնավորապես, երկու տարրանի բազմության վրա կարելի է սահմանել ընդամենը $2^{2^2} = 16$, իսկ արդեն երեք տարրանի բազմության վրա` $3^{3^2} = 19683$ գործողություններ:

Դիցուք $\circ$ գործողությունը որոշված է Q բազմության վրա: $\circ$ գործողությունը կամ $Q(\circ)$ խմբակերպը կոչվում է **օժտված աջ** (ձախ) **միավորով**, եթե գոյություն ունի այնպիսի $e \in Q$ տարր, որ $a \circ e = a$

(համապատասխանաբար $e \circ a = a$) կամայական $a \in Q$ տարրի համար: $e \in Q$ տարրը, այդ դեպքում, կոչվում է $\circ$ գործողության կամ $Q(\circ)$ խմբակերպի **աջ** (ձախ) **միավոր**: Օրինակ, 0-ն $Q = \mathbb{Z}$ բազմության վրա որոշված հանման գործողության աջ միավորն է: Գործողության կամ խմբակերպի աջ (ձախ) միավորը, ընդհանուր դեպքում, միարժեքորեն չի որոշվում: Օրինակ, Q բազմության յուրաքանչյուր տարր կլինի նրա վրա որոշված $x \circ y = x$ (կամ $x \circ y = y$) գործողության աջ (համապատասխանաբար ձախ) միավորը:

$\circ$ գործողությունը կամ $Q(\circ)$ խմբակերպը կոչվում է (օժտված) **միավորով**, եթե գոյություն ունի այնպիսի $e \in Q$ տարր, որը միաժամանակ աջ և ձախ միավոր է: Այս դեպքում, e-ն կոչվում է $\circ$-ի **միավոր**: Եթե $\circ$ գործողությունը օժտված է որևէ e աջ միավորով և որևէ e' ձախ միավորով, ապա սահմանումներից բխում է, որ նրանք ակնհայտորեն կլինեն հավասար, որովհետև

$$e = e' \circ e = e',$$

և, հետևաբար, $\circ$ գործողությունը կլինի օժտված միավորով: Այստեղից նաև բխում է, որ եթե $\circ$ գործողությունը օժտված է միավորով, ապա այն որոշվում է միարժեքորեն:

Գործողության արտադրյալային գրելաձևի դեպքում միավորը (եթե այն գոյություն ունի) հաճախ նշանակվում է e-ով կամ երբեմն 1-ով, իսկ գործողության գումարային գրելաձևի դեպքում միավորը նշանակվում է 0-ով:

$\circ$ գործողությունը կոչվում է **տեղափոխական**, եթե այն բավարարում է տեղափոխական նույնությանը, այսինքն՝

$$x \circ y = y \circ x$$

ցանկացած $x, y \in Q$ տարրերի համար:

$\circ$ գործողությունը կոչվում է **զուգորդական**, եթե այն բավարարում է զուգորդական նույնությանը, այսինքն՝

$$x \circ (y \circ z) = (x \circ y) \circ z$$

ցանկացած $x, y, z \in Q$ տարրերի համար:

18.1.2. Կիսախմբի, խմբի, աբելյան խմբի, քվազիխմբի և լուպայի սահմանումները: $Q(\circ)$-ը կոչվում է **կիսախումբ**, եթե $\circ$ գործողությունը զուգորդական է: $Q(\circ)$ կիսախումբը կոչվում է.

ա) **միավորով (օժտված)** կամ **մոնոիդ**, եթե $\circ$ գործողությունն օժտված է միավորով;

բ) աջ (ձախ) միավորով (օժտված), եթե $\circ$ գործողությունն օժտված է աջ (ձախ) միավորով:

Եթե $Q(\circ)$-ը կիսախումբ է, ապա Q բազմությունը կոչվում է կիսախումբ $\circ$ գործողության նկատմամբ:

Օրինակներ: 1) $\mathbb{N}(+)$-ը և $\mathbb{N}(\cdot)$-ը կիսախմբեր են, ընդ որում $\mathbb{N}(\cdot)$-ը $e = 1$ միավորով (օժտված) կիսախումբ է (եթե $0 \in \mathbb{N}$, ապա $\mathbb{N}(+)$-ը ևս կլինի միավորով կիսախումբ): Բոլոր զույգ բնական (ամբողջ) թվերի բազմությունը կիսախումբ է՝ ամբողջ թվերի արտադրյալի նկատմամբ, որն արդեն չի օժտված միավորով:

2) X բազմության բոլոր $\alpha : X \to X$ ձևափոխությունների $\mathcal{F}_X$ բազմությունը միավորով օժտված կիսախումբ է՝ արտապատկերումների արտադրյալի նկատմամբ: Այս կիսախումբը կոչվում է X բազմության **սիմետրիկ կիսախումբ**:

3) X բազմության բոլոր ներդրող (ինյեկտիվ) ձևափոխությունների բազմությունը միավորով օժտված կիսախումբ է՝ արտապատկերումների արտադրյալի նկատմամբ:

4) X բազմության բոլոր վերադրող (սյուրեկտիվ) ձևափոխությունների բազմությունը միավորով օժտված կիսախումբ է՝ արտապատկերումների արտադրյալի նկատմամբ:

5) Կամայական U բազմության բոլոր ենթաբազմությունների դասը, որը նշանակվում է 2^U-ով, կլինի միավորով օժտված կիսախումբ՝ տեսաբազմային միավորման (հատման) նկատմամբ:

6) $\mathbb{N}(\circ)$-ը և $\mathbb{N}(*)$-ը կիսախմբեր են, որտեղ $m \circ n = (m, n)$-ը երկու բնական թվերի ամենամեծ ընդհանուր բաժանարարն է, իսկ $m * n = [m, n]$-ը երկու բնական թվերի ամենափոքր ընդհանուր բազմապատիկն է:

7) Իրական թվերով (տարրերով) n-րդ կարգի բոլոր մատրիցների $\mathbb{R}^{n\times n}$ բազմությունը միավորով օժտված կիսախումբ է՝ մատրիցների բազմապատկման նկատմամբ: (Նույնը վերաբերվում է նաև տրված P դաշտի վրա որոշված n-րդ կարգի բոլոր մատրիցների $P^{n\times n}$ բազմությանը:)

8) $\mathbb{Z}(-)$-ը կիսախումբ չէ, որովհետև հանման գործողությունը զուգորդական չէ:

$Q(\circ)$ կիսախումբը կոչվում է **տեղափոխական**, եթե $\circ$ գործողությունը տեղափոխական է: e միավորով օժտված $Q(\circ)$ կիսախմբի $a \in Q$ տարրը կոչվում է.

ա) **հակադարձելի աջից**, եթե գոյություն ունի այնպիսի $a' \in Q$ տարր, որ

$$a \circ a' = e;$$

բ) **հակադարձելի ձախից**, եթե գոյություն ունի այնպիսի $a'' \in Q$, տարր, որ

$$a'' \circ a = e;$$

գ) **հակադարձելի**, եթե գոյություն ունի այնպիսի $a^* \in Q$ տարր, որ

$$a \circ a^* = a^* \circ a = e :$$

Դժվար չէ նկատել, որ եթե e միավորով օժտված $Q(\circ)$ կիսախմբի $a \in Q$ տարրը հակադարձելի է աջից և ձախից, ապա a-ն կլինի հակադարձելի, որովհետև $a \circ a' = e$ և $a'' \circ a = e$ պայմաններից բխում է՝

$$a'' = a'' \circ e = a'' \circ (a \circ a') = (a'' \circ a) \circ a' = e \circ a' = a' :$$

Մասնավորապես, եթե e միավորով օժտված $Q(\circ)$ կիսախմբի a տարրը հակադարձելի է, ապա a^* տարրը որոշվում է միարժեքորեն, այն կոչվում է a-ի հակադարձ տարր և նշանակվում է a^{-1}-ով: Հետևաբար, եթե a-ն հակադարձելի է, ապա նրա հակադարձը ևս կլինի հակադարձելի ու հակադարձի միակության պարճառով՝ $\left(a^{-1}\right)^{-1} = a$:

Սահմանումից բխում է նաև, որ որպեսզի միավորով օժտված $Q(\circ)$ կիսախմբի $a, b \in Q$ տարրերը լինեն հակադարձելի անհրաժեշտ է և բավարար, որ $a \circ b \in Q$ և $b \circ a \in Q$ տարրերը լինեն հակադարձելի: Ընդ որում, այդ դեպքում՝

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1} :$$

Գործողության գումարային գրելաձևի դեպքում a^{-1}-ի փոխարեն գրվում է $-a$ և այն կոչվում է a-ի հակադիր (տարր): Մասնավորապես, նշված հավասարությունները կընդունեն հետևյալ տեսքը՝

$$-(-a) = a,$$
$$-(a + b) = (-b) + (-a) :$$

Միավորով օժտված $Q(\circ)$ կիսախումբը կոչվում է **խումբ**, եթե նրա յուրաքանչյուր տարր հակադարձելի է: Եթե $Q(\circ)$-ը խումբ է, ապա Q բազմությունը կոչվում է խումբ $\circ$ գործողության նկատմամբ, իսկ $\circ$ գործողությունը կոչվում է խմբային գործողություն՝ որոշված Q

բազմության վրա (մեջ): Այսպիսով, Q բազմությունը կոչվում է խումբ $\circ$ գործողության նկատմամբ, եթե տեղի ունեն հետևյալ պայմանները, որոնք կոչվում են խմբային աքսիոմներ.

1) եթե $x, y \in Q$, ապա $x \circ y \in Q$ (գործողության փակության պայման կամ գործողության գոյության պայման);

2) $x \circ (y \circ z) = (x \circ y) \circ z$ կամայական $x, y, z \in Q$ տարրերի համար (զուգորդականության պայման);

3) գոյություն ունի այնպիսի $e \in Q$ տարր, որ $e \circ x = x \circ e = x$ կամայական $x \in Q$ տարրի համար (միավորի գոյության պայման);

4) յուրաքանչյուր $x \in Q$ տարրի համար գոյություն ունի այնպիսի $x^{-1} \in Q$ տարր, որ $x \circ x^{-1} = x^{-1} \circ x = e$ (հակադարձների գոյության պայման):

Վերհանգման եղանակով հեշտությամբ ապացուցվում է, որ եթե $Q(\circ)$-ը խումբ է, ապա

$$(x_1 \circ x_2 \circ \cdots \circ x_m)^{-1} = x_m^{-1} \circ x_{m-1}^{-1} \circ \cdots \circ x_1^{-1},$$

որտեղ $x_1, \ldots, x_m \in Q$, $m \in \mathbb{N}$, $m \geqslant 2$:

Հետևյալ արդյունքից բխում է, որ խմբի սահմանման պայմանները (աքսիոմները) կարելի է էապես քչացնել:

Թեորեմ 18.1 (L. Dickson): *Եթե կիսախումբն օժտված է այնպիսի աջ (ձախ) միավորով, որի նկատմամբ կիսախմբի յուրաքանչյուր տարր հակադարձելի է աջից (ձախից), ապա այն խումբ է:*

Ապացուցում: Դիցուք e-ն $Q(\circ)$ կիսախմբի աջ միավորն է և դիցուք յուրաքանչյուր $a \in Q$ տարրի համար գոյություն ունի այնպիսի $a' \in Q$ տարր, որ $a \circ a' = e$: Պահանջվում է ապացուցել, որ $Q(\circ)$-ը խումբ է: Նախ ապացուցենք, որ $e \in Q$ աջ միավորը կլինի $Q(\circ)$-ի նաև ձախ միավորը, այսինքն՝ $e \circ a = a$ կամայական $a \in Q$ տարրի համար: Իրոք,

$$e \circ a \circ a' = e \circ e = e = a \circ a';$$

Այս հավասարության երկու մասերը աջից բազմապատկելով $(a')' = a''$-ով, կստանանք՝

$$e \circ a \circ a' \circ a'' = a \circ a' \circ a'',$$

$$e \circ a \circ e = a \circ e,$$

$$e \circ a = a :$$

Այժմ ապացուցենք, որ a-ի a' աջ հակադարձը նաև a-ի ձախ հակադարձն է.

$$a' \circ a \circ a' = a' \circ e = a',$$

$$a' \circ a \circ a' \circ a'' = a' \circ a'',$$

$$a' \circ a \circ e = e,$$

$$a' \circ a = e :$$

Համանման եղանակով պնդումն ապացուցվում է նաև ձախ միավորի և դրա նկատմամբ ձախ հակադարձների գոյության դեպքում: □

Օրինակներ: 1) X բազմության բոլոր $\alpha : X \to X$ բիեկտիվ (կամ փոխմիարժեք) ձևափոխությունների (տեղադրությունների) S_X բազմությունը խումբ է՝ արտապատկերումների արտադրյալի նկատմամբ: Այս խումբը կոչվում է X բազմության **սիմետրիկ խումբ**: Եթե X բազմությունը վերջավոր է, ապա ենթադրվում է $X = \{1, \ldots, n\}$, իսկ S_X-ը նշանակվում է S_n-ով և կոչվում է n**-րդ աստիճանի սիմետրիկ խումբ**: Հայտնի է, որ $|S_n| = n!$, իսկ S_n-ի տարրերը կոչվում են n-րդ աստիճանի տեղադրություններ:

2) Ինչպես հայտնի է, n-րդ աստիճանի բոլոր զույգ տեղադրությունների բազմությունը նշանակվում է $\mathbb{A}_n$-ով: $\mathbb{A}_n$-ը խումբ է արտապատկերումների արտադրյալի նկատմամբ, որովհետև երկու զույգ տեղադրությունների արտադրյալը զույգ տեղադրություն է, նույնական (միավոր) արտապատկերումը զույգ է և յուրաքանչյուր զույգ տեղադրության հակադարձը ևս զույգ տեղադրություն է: Այս խումբը կոչվում է n**-րդ աստիճանի նշանափոխ խումբ**:

3) Բոլոր n-տեղափոխությունների $\mathbb{P}_n$ բազմությունը խումբ է՝ n-տեղափոխությունների արտադրյալի նկատմամբ:

4) Բոլոր զույգ n-տեղափոխությունների $\mathbb{T}_n$ բազմությունը խումբ է՝ n-տեղափոխությունների արտադրյալի նկատմամբ:

5) Իրական թվերով (տարրերով) n-րդ կարգի բոլոր հակադարձելի մատրիցների բազմությունը խումբ է՝ մատրիցների բազմապատկման նկատմամբ: Այս խումբը նշանակվում է $GL_n(\mathbb{R})$-ով և կոչվում է **լրիվ գծային խումբ**: Իրական թվերով (տարրերով) n-րդ կարգի բոլոր 1 որոշիչով մատրիցների բազմությունը խումբ է՝ մատրիցների

բազմապատկման նկատմամբ: Այս խումբը նշանակվում է $SL_n(\mathbb{R})$-ով և կոչվում է **հատուկ գծային խումբ**: (Նույնը վերաբերվում է նաև տրված P դաշտի վրա որոշված n-րդ կարգի բոլոր հակադարձելի մատրիցների բազմությանը և n-րդ կարգի բոլոր 1 որոշիչով մատրիցների բազմությանը, որոնք, համապատասխանաբար, նշանակվում են $GL_n(P)$-ով և $SL_n(P)$-ով:)
6) Մեկ տարրանի խումբը կոչվում է **միավոր** կամ **զրոյական խումբ**:

$Q(\circ)$ խումբը կոչվում է **աբելյան** (N. Abel) կամ տեղափոխական (կոմուտատիվ), եթե $\circ$ գործողությունը տեղափոխական է: Հակառակ դեպքում, խումբը կոչվում է ոչ աբելյան: Հաճախ աբելյան խմբի գործողությունը նշանակվում է $+$ նշանով, միավորը՝ 0-ով, իսկ a-ի հակադարձը կոչվում է նրա հակադիր և նշանակվում է $-a$-ով:

Օրինակ, 2^U $(\ominus)$-ը, $\mathbb{Z}(+)$-ը, $\mathcal{O}_p(+)$-ը, $\mathbb{Z}_n(+)$-ը, $\mathbb{Q}(+)$-ը, $\mathbb{Q}^\star(\cdot)$-ը, $\mathbb{R}(+)$-ը, $\mathbb{R}_p(+)$-ը, $\mathbb{R}^\star(\cdot)$-ը, $\mathbb{C}(+)$-ը, $\mathbb{C}^\star(\cdot)$-ը, $\sqrt[n]{1}$-ը աբելյան խմբեր են (այստեղ $\mathbb{Q}^\star$-ը, $\mathbb{R}^\star$-ը, $\mathbb{C}^\star$-ը բոլոր ոչ զրոյական ռացիոնալ, իրական, կոմպլեքս թվերի բազմություններն են): Եթե p-ն պարզ թիվ է, ապա $\mathbb{Z}_p^*(\cdot)$-ը աբելյան խումբ է, որտեղ $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]\}$: S_X սիմետրիկ խումբը կլինի աբելյան խումբ այն և միայն այն դեպքում, երբ $|X| \leqslant 2$, իսկ $\mathbb{A}_n$ նշանափոխ խումբը կլինի աբելյան խումբ այն և միայն այն դեպքում, երբ $n \leqslant 3$ (բխում է նաև թեորեմ 18.13-ից):

Իրական թվերով (տարրերով) $n \times m$-չափանի բոլոր մատրիցների $\mathbb{R}^{n\times m}$ բազմությունը աբելյան խումբ է՝ մատրիցների գումարման նկատմամբ: (Նույնը վերաբերվում է նաև տրված P դաշտի վրա որոշված $n \times m$-չափանի բոլոր մատրիցների $P^{n\times m}$ բազմությանը:)

Թեորեմ 18.2 (Մյոբիուս): *Եթե $Q(+)$-ը աբելյան խումբ է, իսկ $\mu : \mathbb{N} \to \mathbb{Z}$ ֆունկցիան Մյոբիուսի ֆունկցիան է, ապա ցանկացած $f, g : \mathbb{N} \to Q$ ֆունկցիաների համար տեղի ունի թեորեմ 9.10-ի պնդումը, այսինքն՝*

$$f(n) = \sum_{n/d, d>0} g(d) \longleftrightarrow g(n) = \sum_{n/d, d>0} \mu(d) f\left(\frac{n}{d}\right),$$

որտեղ $a \in Q$ տարրի համար՝

$$\mu(d)a = \begin{cases} a, & \text{եթե } \mu(d) = 1, \\ 0, & \text{եթե } \mu(d) = 0, \\ -a, & \text{եթե } \mu(d) = -1 : \end{cases}$$

(Արտադրյալային տարբերակ). եթե $Q(\circ)$-ը աբելյան խումբ է, իսկ $\mu : \mathbb{N} \to \mathbb{Z}$ ֆունկցիան Մյոբիուսի ֆունկցիան է, ապա ցանկացած

$f, g : \mathbb{N} \to Q$ ֆունկցիաների համար տեղի ունի թեորեմ 9.10-ի պնդումը՝ հետևյալ իմաստով.

$$f(n) = \prod_{n/d, d>0} g(d) \longleftrightarrow g(n) = \prod_{n/d, d>0} f\left(\frac{n}{d}\right)^{\mu(d)},$$

որտեղ $a \in Q$ տարրի համար՝

$$a^{\mu(d)} = \begin{cases} a, & \text{եթե } \mu(d) = 1, \\ e, & \text{եթե } \mu(d) = 0, \\ a^{-1}, & \text{եթե } \mu(d) = -1 : \end{cases}$$

Ապացույց: Թեորեմ 9.10-ի ապացուցման կրկնությունն է: □

$Q(\circ)$-ը կոչվում է **քվազիխումբ**, եթե նրա կամայական $a, b \in Q$ տարրերի համար

$$a \circ x = b$$

և

$$y \circ a = b$$

հավասարումներից յուրաքանչյուրն ունի (օժտված է) Q-ին պատկանող միակ (միարժեքորեն որոշվող) լուծում, այսինքն՝ գոյություն ունեն միարժեքորեն որոշվող այնպիսի $c \in Q$ և $d \in Q$ տարրեր, որ

$$a \circ c = b$$

և

$$d \circ a = b :$$

Օրինակ, $\mathbb{Z}(-)$-ը, $\mathcal{O}_p(-)$-ը, $\mathbb{Q}(-)$-ը, $\mathbb{R}(-)$-ը, $\mathbb{C}(-)$-ը, $\mathbb{R}_p(-)$-ը, $\mathbb{Q}^{\star}(/)$-ը, $\mathbb{R}^{\star}(/)$-ը և $\mathbb{C}^{\star}(/)$-ը քվազիխմբեր են, որտեղ «$/$» գործողությունը բաժանումն է:

Եթե $Q(\circ)$-ը քվազիխումբ է, ապա $\circ$ գործողությունը կոչվում է քվազիխմբային գործողություն: $Q(\circ)$ քվազիխումբը կոչվում է **լուպա** (կամ միավորով քվազիխումբ), եթե $\circ$ գործողությունն օժտված է միավորով: $Q(\circ)$ խմբակերպը կոչվում է **կրճատումով** (բաժանումով) օժտված, եթե ցանկացած $a, b \in Q$ տարրերի համար $a \circ x = b$ և $y \circ a = b$ հավասարումներից յուրաքանչյուրն ունի ամենաշատը (ամենաքիչը) մեկ լուծում:

Հատկություն 18.1: *Քվազիխմբի մեջ կարելի է կատարել կրճատում, այսինքն՝ եթե $Q(\circ)$-ը քվազիխումբ է, ապա*

$$a \circ x_1 = a \circ x_2 \longrightarrow x_1 = x_2, \quad \text{(կրճատում ձախից)}$$

$$y_1 \circ a = y_2 \circ a \longrightarrow y_1 = y_2, \quad \text{(կրճատում աջից)}$$

որտեղ $a, x_1, x_2, y_1, y_2 \in Q$: Կրճատումով օժտված վերջավոր խմբակերպը քվազիխումբ է: Բաժանումով օժտված վերջավոր խմբակերպը քվազիխումբ է:

Ապացուցում: Նշանակելով $a \circ x_1 = a \circ x_2 = b$, ստանում ենք $a \circ x = b$ հավասարման $x = x_1$ և $x = x_2$ լուծումները, իսկ քվազիխմբի սահմանման համաձայն՝ $a \circ x = b$ հավասարումն օժտված է միայն մեկ լուծումով, հետևաբար՝ $x_1 = x_2$: Նույն դատողությունները կիրառելով $y \circ a = b$ հավասարման նկատմամբ, ստանում ենք աջից կրճատման հատկությունը: Հատկության երկրորդ և երրորդ մասերը համապատասխանաբար բխում են թեորեմ 0.4-ից և թեորեմ 0.5-ից: Իրոք, կրճատումով օժտված $Q(\circ)$ խմբակերպի դեպքում $\alpha_a(x) = a \circ x$ և $\beta_a(y) = y \circ a$ օրենքներով որոշվող $\alpha_a : Q \to Q$ և $\beta_a : Q \to Q$ ձևափոխությունները կլինեն ինյեկտիվ: Եվ քանի որ Q-ն վերջավոր է, ապա α_a և β_a ձևափոխությունները կլինեն նաև սյուրեկտիվ: Հետևաբար, $a \circ x = b$ և $y \circ a = b$ հավասարումներից յուրաքանչյուրը կունենա լուծում Q բազմությանը պատկանող (ցանկացած $a, b \in Q$ տարրերի համար): Իսկ բաժանումով օժտված $Q(\circ)$ խմբակերպի դեպքում α_a և β_a ձևափոխությունները կլինեն սյուրեկտիվ: Հետևաբար, վերջավոր Q բազմության դեպքում α_a և β_a ձևափոխությունները կլինեն նաև ինյեկտիվ: Այսպիսով, $a \circ x = b$ և $y \circ a = b$ հավասարումներից յուրաքանչյուրը կունենա միայն մեկ լուծում Q բազմությանը պատկանող: □

Ժխտօրինակներ: 1) Կրճատումով օժտված $\mathbb{N}(+)$ անվերջ խմբակերպը (կիսախումբը) քվազիխումբ չէ:
2) $\mathbb{N}(\circ)$ խմբակերպը, որտեղ $x \circ y = |x - y|$, $x, y \in \mathbb{N}$, կլինի բաժանումով օժտված անվերջ խմբակերպ, որը, սակայն, քվազիխումբ չէ:

18.1.3. Խմբի սահմանումը քվազիխմբի միջոցով: Պարզվում է, որ խումբը կարելի է սահմանել նաև որպես այնպիսի կիսախումբ, որը միաժամանակ քվազիխումբ է:

Թեորեմ 18.3: *Յուրաքանչյուր խումբ զուգորդական գործողությամբ քվազիխումբ է: Եվ հակառակը, զուգորդական գործողությամբ յուրաքանչյուր քվազիխումբ խումբ է, այսինքն՝ այն օժտված է միավորով և նրա յուրաքանչյուր տարր հակադարձելի է: Այսպիսով, որպեսզի խմբակերպը լինի խումբ անհրաժեշտ է և բավարար, որ այն լինի կիսախումբ և քվազիխումբ:*

Ապացույց: Նախ ապացուցենք, որ եթե $Q(\circ)$-ը խումբ է, ապա այն քվազիխումբ է: Իրոք, ցանկացած $a, b \in Q$ տարրերի համար $x = a^{-1} \circ b \in Q$ տարրը կլինի $a \circ x = b$ հավասարման համար լուծում, որովհետև

$$a \circ x = a \circ \left(a^{-1} \circ b\right) = \left(a \circ a^{-1}\right) \circ b = e \circ b = b;$$

Եվ այդ լուծումը միակն է, որովհետև եթե $x' \in Q$ տարրը $a \circ x = b$ հավասարման համար լուծում է, ապա

$$a \circ x' = b,$$

$$a^{-1} \circ (a \circ x') = a^{-1} \circ b,$$

$$\left(a^{-1} \circ a\right) \circ x' = a^{-1} \circ b,$$

$$e \circ x' = a^{-1} \circ b,$$

$$x' = a^{-1} \circ b:$$

Նույն կերպ համոզվում ենք, որ $Q(\circ)$ խմբում $y \circ a = b$ հավասարումն ունի լուծում, այն էլ միայն մեկը՝ $y = b \circ a^{-1}$:

Ապացուցենք թեորեմի երկրորդ պնդումը: Նախ ապացուցենք, որ $Q(\circ)$-ը օժտված է միավորով: Դիցուք $Q(\circ)$-ը զուգորդական գործողությամբ քվազիխումբ է, $a \in Q$: Քվազիխմբի սահմանման համաձայն $a \circ x = a$ հավասարումը կունենա $x = e_a \in Q$ լուծում: Ապացուցենք, որ e_a-ն $Q(\circ)$ քվազիխմբի աջ միավորն է, այսինքն՝ $b \circ e_a = b$ ցանկացած $b \in Q$ տարրի համար: Իրոք, քվազիխմբի սահմանման համաձայն b տարրը կարելի է ներկայացնել $b = y \circ a$ տեսքով, և հետևաբար՝

$$b \circ e_a = (y \circ a) \circ e_a = y \circ (a \circ e_a) = y \circ a = b:$$

Այնուհետև, $y \circ a = a$ հավասարման լուծումը նշանակելով $y = f_a$-ով, նույն եղանակով ստանում ենք, որ f_a-ն $Q(\circ)$ քվազիխմբի ձախ միավորն է, այսինքն՝ $f_a \circ b = b$ ցանկացած $b \in Q$ տարրի համար: Իրոք, ներկայացնելով b-ն $b = a \circ x$ տեսքով, կստանանք՝

$$f_a \circ b = f_a \circ (a \circ x) = (f_a \circ a) \circ x = a \circ x = b :$$

Սակայն $Q(\circ)$-ի $f_a = e_1$ ձախ միավորը և $e_a = e_2$ աջ միավորը համընկնում են (ինչպես նկատեցինք վերևում)՝

$$e_1 = e_1 \circ e_2 = e_2 :$$

Այժմ ապացուցենք, որ $e = e_1 = e_2 \in Q$ միավորով օժտված $Q(\circ)$ քվազիխմբի (լուպայի) յուրաքանչյուր $a \in Q$ տարր հակադարձելի է: Իրոք, քվազիխմբի սահմանման համաձայն $a \circ x = e$ և $y \circ a = e$ հավասարումներից յուրաքանչյուրն օժտված է Q-ին պատկանող լուծումով: Առաջին հավասարման լուծումը նշանակելով $x = a'$-ով, իսկ երկրորդինը՝ $y = a''$-ով, կունենանք՝

$$\begin{cases} a \circ a' = e, \\ a'' \circ a = e; \end{cases}$$

Սակայն, ինչպես տեսանք վերևում, կիսախմբի մեջ, այստեղից բխում է $a' = a''$ հավասարությունը:

Թեորեմի երկրորդ պնդումն ավելի հեշտ կարելի էր ստանալ հենվելով Դիքսոնի թեորեմի վրա (թեորեմ 18.1): □

Հետևություն 18.1 (E. Huntington): *Եթե $Q(\circ)$ կիսախմբի կամայական $a, b \in Q$ տարրերի համար*

$$a \circ x = b$$

և

$$y \circ a = b$$

հավասարումներից յուրաքանչյուրն օժտված է Q-ին պատկանող լուծումով, ապա $Q(\circ)$-ը խումբ է: Այսինքն՝ բաժանունով օժտված յուրաքանչյուր կիսախումբ խումբ է:

Ապացուցում: Բխում է թեորեմ 18.3-ի ապացուցումից: □

18.1.4. Աբելյան խմբի սահմանումը քվազիխմբի միջոցով: Աբելյան խմբի սահմանման մեջ եղած զուգորդական և տեղափոխական նույնությունները կարելի է միավորել մեկ նույնության մեջ:

Թեորեմ 18.4*: Որպեսզի $Q(\circ)$ քվազիխումբը լինի աբելյան խումբ անհրաժեշտ է և բավարար, որ*

$$(x \circ y) \circ z = x \circ (z \circ y) \tag{18.1}$$

կամայական $x, y, z \in Q$ տարրերի համար:

Ապացուցում: Անհրաժեշտությունն ակնհայտ է, որովհետև ցանկացած $Q(\circ)$ աբելյան խմբի մեջ տեղի ունի (18.1) հավասարությունը (նույնությունը)՝

$$(x \circ y) \circ z = x \circ (y \circ z) = x \circ (z \circ y) :$$

Բավարարություն: Դիցուք $Q(\circ)$ քվազիխմբում տեղի ունի (18.1) հավասարությունը և $a \in Q$: $a \circ x = a$ հավասարման լուծումը նշանակելով $x = e_a$-ով կունենանք ((18.1) հավասարության մեջ վերցնելով $y = e_a$)՝

$$(a \circ e_a) \circ c = a \circ (c \circ e_a),$$

$$a \circ c = a \circ (c \circ e_a)$$

և կատարելով կրճատում (համաձայն հատկության 18.1-ի), կստանանք՝

$$c = c \circ e_a$$

ցանկացած $c \in Q$ տարրի համար: Ուստի, (18.1) նույնությանը բավարարող $Q(\circ)$ քվազիխումբը օժտված է $e_a \in Q$ աջ միավորով: Այժմ նկատենք, որ e_a-ն $Q(\circ)$-ի նաև ձախ միավորն է: (18.1) նույնության մեջ վերցնելով $z = e_a$ կստանանք՝

$$(x \circ y) \circ e_a = x \circ (e_a \circ y),$$

$$x \circ y = x \circ (e_a \circ y),$$

$$y = e_a \circ y$$

ցանկացած $y \in Q$ տարրի համար: Որից հետո ապացուցվում է $\circ$ գործողության տեղափոխականությունը՝ (18.1) հավասարության մեջ վերցնելով $x = e_a$.

$$(e_a \circ y) \circ z = e_a \circ (z \circ y),$$

$$y \circ z = z \circ y,$$

իսկ ելնելով սրանից՝ նաև $\circ$ գործողության զուգորդականությունը.

$$(x \circ y) \circ z = x \circ (z \circ y) = x \circ (y \circ z) :$$

Այսպիսով, $Q(\circ)$ քվազիխմբի $\circ$ գործողությունը զուգորդական է և տեղափոխական, հետևաբար $Q(\circ)$-ը կլինի աբելյան խումբ (համաձայն թեորեմ 18.3-ի): $\square$

Նույնանման դատողություններով ապացուցվում են նաև հետևյալ երկու արդյունքները.

Թեորեմ 18.5: *Որպեսզի $Q(\circ)$ քվազիխումբը լինի աբելյան խումբ անհրաժեշտ է և բավարար, որ*

$$(x \circ y) \circ z = y \circ (x \circ z) \tag{18.2}$$

կամայական $x, y, z \in Q$ տարրերի համար: $\square$

Թեորեմ 18.6: *Որպեսզի $Q(\circ)$ քվազիխումբը լինի աբելյան խումբ անհրաժեշտ է և բավարար, որ*

$$(x \circ y) \circ z = y \circ (z \circ x) \tag{18.3}$$

կամայական $x, y, z \in Q$ տարրերի համար: $\square$

Հետևյալ արդյունքն ակնհայտ է:

Հատկություն 18.2: *Միավորով օժտված $Q(\circ)$ խմբակերպի համար հետևյալ պայմանները համարժեք են.*

1) $\circ$ գործողությունը զուգորդական է և տեղափոխական;

2) $Q(\circ)$-ը բավարարում է (18.1) նույնությանը;

3) $Q(\circ)$-ը բավարարում է (18.2) նույնությանը;

4) $Q(\circ)$-ը բավարարում է (18.3) նույնությանը: $\square$

18.1.5. Քվազիխմբի սահմանումը նույնություններով: Պարզվում է, որ քվազիխմբի գաղափարը համասարազոր է երեք գործողություններով օժտված այնպիսի հանրահաշվի գաղափարի, որը բավարարում է նաև չորս նույնությունների:

Թեորեմ 18.7: *Դիցուք A գործողությունը որոշված է Q բազմության վրա: Որպեսզի $Q(A)$ խմբակերպը լինի քվազիխումբ անհրաժեշտ է և բավարար, որ գոյություն ունենան նույն Q բազմության վրա որոշված այնպիսի B և C գործողություններ, որոնց համար տեղի ունեն հետևյալ չորս նույնությունները՝*

$$A(x, B(x, y)) = y,$$

$$B(x, A(x, y)) = y,$$

$$A(C(y, x), x) = y,$$

$$C(A(y, x), x) = y$$

(ցանկացած $x, y \in Q$ տարրերի համար):

Ապացուցում: Անհրաժեշտություն: Եթե $Q(A)$-ն քվազիխումբ է, ապա սահմանման համաձայն, կամայական $a, b \in Q$ տարրերի համար

$$A(a, x) = b,$$

$$A(y, a) = b$$

հավասարումները կունենան միարժեքորեն որոշվող $x \in Q$ և $y \in Q$ լուծումներ: Նշանակելով՝ $x = B(a, b)$ և $y = C(b, a)$, կստանանք Q բազմության վրա որոշված B և C գործողություններ, որոնք բավարարում են նշված չորս նույնություններին: Իրոք, առաջին և երրորդ նույնությունները բխում են B և C գործողությունների սահմանումներից: Ապացուցենք երկրորդ նույնությունը: Դիցուք $B(x, A(x, y)) = z$: Այդ դեպքում, կունենանք՝

$$A(x, B(x, A(x, y))) = A(x, z),$$

և համաձայն առաջին նույնության՝

$$A(x, y) = A(x, z),$$

որտեղից $y = z$ (համաձայն քվազիխմբի կրճատման հատկության): Այսպիսով, $B(x, A(x, y)) = y$:

Համանման դատողություններով ապացուցվում է նաև չորրորդ նույնությունը:

Բավարարություն: Եթե Q բազմության վրա որոշված A, B, C գործողությունները բավարարում են նշված չորս նույնություններին, ապա $Q(A)$-ն քվազիխումբ է: Իրոք, առաջին հավասարությունից բխում է, որ ցանկացած $a, b \in Q$ տարրերի համար $B(a, b)$-ն կլինի $A(a, x) = b$ հավասարման լուծումը: Դիցուք $A(a, x_1) = A(a, x_2) = b$: Այդ դեպքում,

$$B(a, A(a, x_1)) = B(a, A(a, x_2))$$

և երկրորդ նույնության համաձայն՝ $x_1 = x_2$:

Նման դատողություններով ապացուցվում է նաև $A(y, a) = b$ հավասարման լուծման գոյությունը և միակությունը: □

Եթե $Q(A)$-ն քվազիխումբ է, ապա նախորդ թեորեմի B և C գործողությունները որոշվում են միարժեքորեն և համապատասխանաբար կոչվում են A-ի **աջ և ձախ հակադարձներ** ու նշանակվում են՝ $B = A^{-1}$, $C =^{-1} A$:

Հատկություն 18.3: *Եթե $Q(A)$-ն քվազիխումբ է, ապա $Q\left(A^{-1}\right)$-ը և $Q\left(^{-1}A\right)$-ը ևս կլինեն քվազիխմբեր: Ըստ որում՝*

$$\left(A^{-1}\right)^{-1} = A, \qquad ^{-1}\left(^{-1}A\right) = A,$$

$$\left(^{-1}\left(A^{-1}\right)\right)^{-1} =^{-1}\left(\left(^{-1}A\right)^{-1}\right) = A^*,$$

որտեղ $A^*(x, y) = A(y, x)$: Հետևաբար, միմյանցից տարբեր կարող են լինել միայն հետևյալ հակադարձները՝

$$A^{-1}, \quad ^{-1}A, \quad ^{-1}\left(A^{-1}\right), \quad \left(^{-1}A\right)^{-1}, \quad \left(^{-1}\left(A^{-1}\right)\right)^{-1}:$$

Ապացուցում: Անմիջական ստուգման եղանակով: □

Եթե A քվազիխմբային գործողությունը նշանակվում է $\circ$-ով կամ կետով, ապա A^{-1} և ^{-1}A գործողությունները համապատասխանաբար նշանակվում են «$\backslash$»-ով և «$/$»-ով:

Q ոչ դատարկ բազմության վրա որոշված բոլոր երկտեղ գործողությունների դասը նշանակենք $\mathcal{F}_Q^2$-ով և այս բազմության վրա սահմանենք հետևյալ երկու գործողությունները՝

$$A \cdot B(x, y) = A(x, B(x, y)),$$

$$A \circ B(x, y) = A(B(x, y), y),$$

որտեղ $A, B \in \mathcal{F}_Q^2$, $x, y \in Q$: Հեշտությամբ ստուգվում են, որ $\mathcal{F}_Q^2(\cdot)$-ը և $\mathcal{F}_Q^2(\circ)$-ը միավորով կիսախմբեր են, ուր որպես միավորներ հանդես են գալիս հետևյալ δ_2^2 և δ_2^1 գործողությունները՝

$$\delta_2^1(x, y) = x,$$

$$\delta_2^2(x, y) = y,$$

որտեղ $x, y \in Q$: Այս երկու կիսախմբերը համապատասխանաբար կոչվում են երկտեղ գործողությունների առաջին և երկրորդ կիսախմբեր: Այժմ նախորդ թեորեմը (հայտանիշը) կարելի է վերաձևակերպել հետևյալ կերպ:

Թեորեմ 18.8: *Որպեսզի $Q(A)$ խմբակերպը լինի քվազիխումբ անհրաժեշտ է և բավարար, որ $A \in \mathcal{F}_Q^2$ գործողությունը լինի հակադարձելի $\mathcal{F}_Q^2(\cdot)$ և $\mathcal{F}_Q^2(\circ)$ միավորով օժտված կիսախմբերում: Ընդ որում, եթե $Q(A)$-ն քվազիխումբ է, ապա A^{-1}-ը կլինի A-ի հակադարձը $\mathcal{F}_Q^2(\cdot)$ կիսախմբում, իսկ ${}^{-1}A$-ը կլինի A-ի հակադարձը $\mathcal{F}_Q^2(\circ)$ կիսախմբում:* □

Վերջում նշենք, որ ի նկատի ունենալով թեորեմ 18.7-ը, երբեմն քվազիխումբը սահմանվում է նաև որպես երեք երկտեղ գործողություններով $Q(A, B, C)$ հանրահաշիվ, որի մեջ տեղի ունեն այդ թեորեմում նշված բոլոր չորս նույնությունները:

Կարելի է ապացուցել, որ 3 տարրանի Q բազմության վրա հնարավոր է կառուցել (սահմանել) ընդամենը 12 քվազիխմբեր, իսկ արդեն 4 տարրանի Q բազմության վրա՝ 576 քվազիխմբեր: Այս թիվը մեծ արագությամբ աճում է:

18.2. Ենթակիսախմբեր և ենթախմբեր

18.2.1. Ենթակիսախմբի և ենթախմբի գաղափարները: Սահմանենք ենթակիսախմբի և ենթախմբի գաղափարները կիսախմբի մեջ (համար): Դիցուք $Q(\circ)$-ը կիսախումբ է, իսկ $Q' \subseteq Q$, $Q' \neq \emptyset$: Կասենք, որ Q'-ը $Q(\circ)$ կիսախմբի **ենթակիսախումբն է** և կնշանակենք $Q' \lesssim Q$, եթե այն փակ է $\circ$ գործողության նկատմամբ, այսինքն՝ Q'-ը իր կամայական երկու a, b տարրերի հետ մեկտեղ պարունակում է նաև դրանց $a \circ b$ արտադրյալը՝

$$a, b \in Q' \longrightarrow a \circ b \in Q' :$$

Այդ դեպքում, Q բազմության վրա որոշված $\circ$ գործողությունը կարելի է դիտել նաև որպես գործողություն որոշված $Q' \subseteq Q$ ենթաբազմության վրա և $Q'(\circ)$-ը կլինի կիսախումբ, որովհետև զուգորդական նույնությունն այստեղ տեղի կունենա ինքնըստինքյան: Եթե $Q'(\circ)$ կիսախումբը նաև խումբ է, ապա Q'-ը կոչվում է $Q(\circ)$ կիսախմբի **ենթախումբ** և նշանակվում է $Q' \leqslant Q$: Օրինակ, $SL_n(\mathbb{R}) \leqslant GL_n(\mathbb{R})$, $\mathbb{A}_n \leqslant S_n$, $n\mathbb{Z} \leqslant \mathbb{Z}$, որտեղ $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$, $n \in \mathbb{N}$:

Այսպիսով, $Q(\circ)$ կիսախմբի ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը կկոչվի $Q(\circ)$ կիսախմբի ենթախումբ, եթե տեղի ունեն հետևյալ պայմանները.

ա) Q' -ը պարունակում է իր ցանկացած երկու a, b տարրերի $a \circ b$ արտադրյալը;

բ) գոյություն ունի այնպիսի $e \in Q'$ տարր, որ $e \circ a = a \circ e = a$ ցանկացած $a \in Q'$ տարրի համար (e-ն կոչվում է ենթախմբի միավոր);

գ) յուրաքանչյուր $a \in Q'$ տարրի համար գոյություն ունի այնպիսի $a' \in Q'$ տարր, որ $a \circ a' = a' \circ a = e$:

«$\lesssim$» և «$\leqslant$» հարաբերությունները բավարարում են մասնակի կարգի սահմանման բոլոր երեք (ռեֆլեքսիվության, հակահամաչափության և փոխանցականության) պայմաններին:

Ակնհայտ է, որ յուրաքանչյուր $Q(\circ)$ կիսախումբ ունի առնվազն մեկ ենթակիսախումբ, օրինակ $Q' = Q$: Մինչդեռ կիսախումբը կարող է չունենալ ենթախումբ: Օրինակ, բնական թվերի $\mathbb{N}(+)$ կիսախումբը, որտեղ $0 \notin \mathbb{N}$,այդպիսին է: Յուրաքանչյուր $Q(\circ)$ խումբ, $|Q| \geqslant 2$ դեպքում, ունի առնվազն երկու ենթախմբեր՝ $Q' = \{e\}$ և $Q'' = Q$, որտեղ e-ն խմբի միավորն է: Միևնույն կիսախմբի երկու տարբեր ենթախմբեր կարող են ունենալ տարբեր միավորներ: Օրինակ, $\mathbb{Z}(\cdot)$ կիսախմբի $Q' = \{0\}$ և $Q'' = \{1, -1\}$ ենթախմբերը այդպիսին են: Սակայն, եթե կիսախմբի երկու ենթախմբեր հատվում են (այսինքն՝ հատումը դատարկ չէ), ապա դրանց համար տեղի ունի հետևյալ պնդումը:

Լեմմ 18.1: *Եթե միևնույն կիսախմբի երկու ենթախմբեր հատվում են, ապա այդ ենթախմբերի միավորները համընկնում են:*

Ապացուցում: Դիցուք $Q(\circ)$-ը տրված կիսախումբն է, $Q_1 \leqslant Q$, $Q_2 \leqslant Q$, $Q_1 \cap Q_2 \neq \emptyset$, $a \in Q_1 \cap Q_2$, $e \in Q_1$ տարրը $Q_1(\circ)$ խմբի միավորն է, իսկ $f \in Q_2$ տարրը $Q_2(\circ)$ խմբի միավորն է: Նշանակելով a-ի հակադարձը $Q_1(\circ)$ խմբում a'-ով, իսկ $Q_2(\circ)$ խմբում՝ a''-ով, կունենանք՝

$$a \circ a' = a' \circ a = e, \;\; a \circ e = e \circ a = a,$$

$$a \circ a'' = a'' \circ a = f, \;\; a \circ f = f \circ a = a:$$

Հետևաբար,

$$e = a \circ a' = (f \circ a) \circ a' = f \circ (a \circ a') = f \circ e = (a'' \circ a) \circ e =$$

$$= a'' \circ (a \circ e) = a'' \circ a = f: \qquad \square$$

Սակայն գոյություն ունի (նույնիսկ միավորով) կիսախումբ, որն օժտված է միմյանցից տարբեր միավորներ ունեցող այնպիսի երկու ենթակիսախմբերով, որոնց հատումը դատարկ չէ: Օրինակ, $\mathbb{R} \times \mathbb{R}$-ը $(1, 1)$ միավորով կիսախումբ է, հետևյալ գործողության նկատմամբ՝

$$(x, y) \cdot (u, v) = (x \cdot u, y \cdot v),$$

որն օժտված է $(1, 0)$ և $(0, 1)$ միավորներով $\mathbb{R}^{\circ} = \{(x, 0) \mid x \in \mathbb{R}\}$ և $\mathbb{R}_{\circ} = \{(0, x) \mid x \in \mathbb{R}\}$ ենթակիսախմբերով, որոնց հատումը դատարկ չէ:

$Q(\circ)$ կիսախմբի $e \in Q$ տարրը կոչվում է **ինքնահամընկնող**, եթե $e \circ e = e$: Օրինակ, $\mathbb{Z}(\cdot)$ կիսախմբի 0 և 1 տարրերը ինքնահամընկնող են: Գոյություն ունեն կիսախմբեր, որոնց բոլոր տարրերը ինքնահամընկնող են (օրինակ, $Q(\circ)$-ը, որտեղ $x \circ y = y$), սակայն խմբի միակ ինքնահամընկնող տարրը խմբի միավորն է: Իրոք, եթե $Q(\circ)$-ը խումբ է, $e \in Q$ տարրը նրա միավորն է, իսկ $f \in Q$ և $f \circ f = f$, ապա $f \circ f = f \circ e$, որտեղից՝ $f = e$: Մասնավորապես, խմբի e միավորը կհամընկնի իր յուրաքանչյուր ենթախմբի f միավորի հետ և, հետևաբար, խմբի բոլոր ենթախմբերի հատումը դատարկ չէ: Եթե $Q = \mathbb{N}$, իսկ $x \circ y$ արտադրյալը սահմանենք որպես x, y բնական թվերի ամենամեծ ընդհանուր բաժանարար (ամենափոքր ընդհանուր բազմապատիկ), ապա $\mathbb{N}(\circ)$-ը կլինի կիսախումբ (հատկություն 2.6, հատկություն 4.2), որի յուրաքանչյուր տարր ինքնահամընկնող է: Հետևաբար, $\mathbb{N}(\circ)$-ը խումբ չէ:

Հատկություն 18.4*: Որպեսզի $Q(\circ)$ կիսախումբն ունենա ենթախումբ անհրաժեշտ է և բավարար, որ ունենա ինքնահամընկնող տարր:*

Ապացույց: Եթե $Q(\circ)$ կիսախումբն ունի ենթախումբ, ապա այդ խմբի e միավորը կլինի ինքնահամընկնող տարր: Եվ հակառակը, եթե $Q(\circ)$ կիսախմբի $e \in Q$ տարրն ինքնահամընկնող է, ապա $Q' = \{e\} \subseteq Q$ ենթաբազմությունը կլինի մեկ տարրանի ենթախումբ: $\square$

Թեորեմ 18.9: *Կիսախմբի երկու ենթակիսախմբերի հատումը ենթակիսախումբ է, եթե այն դատարկ չէ: Կիսախմբի երկու ենթախմբերի հատումը կլինի ենթախումբ, եթե այն դատարկ չէ: Նույն պնդումը տեղի ունի նաև կիսախմբի ցանկացած թվով ենթախմբերի (ենթակիսախմբերի) համար: Մասնավորապես, խմբի ցանկացած թվով ենթախմբերի հատումը կլինի ենթախումբ:* $Q(\circ)$ *կիսախմբի* H_i, $i \in \mathbb{N}$ *ենթախմբերի (ենթակիսախմբերի)* $\bigcup\limits_{i=1}^{\infty} H_i$ *միավորումը կլինի ենթախումբ (ենթակիսախումբ), եթե*

$$H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n \subseteq \cdots$$

Ապացուցում: Եթե $Q(\circ)$-ը տրված կիսախումբն է, $Q_1 \leqslant Q$, $Q_2 \leqslant Q$, $Q_1 \cap Q_2 \neq \emptyset$, $a \in Q_1 \cap Q_2$, $e \in Q_1$ տարրը $Q_1(\circ)$ խմբի միավորն է, իսկ $f \in Q_2$ տարրը $Q_2(\circ)$-ի միավորն է, ապա (համաձայն լեմմ 18.1)-ի՝ $e = f \in Q_1 \cap Q_2$: Այնուհետև, նշանակելով a-ի հակադարձը $Q_1(\circ)$ խմբում a'-ով, իսկ $Q_2(\circ)$ խմբում՝ a''-ով, կունենանք՝

$$a \circ a' = a' \circ a = e,$$

$$a \circ a'' = a'' \circ a = e\ :$$

Հետևաբար, $a' = a'' \in Q_1 \cap Q_2$: Մնացած պնդումներն ակնհայտ են: □

Որպես օրինակ դիտարկենք բոլոր կոմպլեքս թվերի $\mathbb{C}(\cdot)$ (արտադրյալային) կիսախումբը: Յուրաքանչյուր $n \in \mathbb{N}$ բնական թվի համար $\sqrt[n]{1} = \{\varepsilon_0 = 1, \varepsilon_1, \ldots, \varepsilon_{n-1}\} \subseteq \mathbb{C}$ ենթաբազմությունը, որտեղ

$$\varepsilon_k = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, \quad k = 0, 1, \ldots, n-1,$$

կազմում է $\mathbb{C}(\cdot)$ կիսախմբի n-րդ կարգի ենթախումբ՝ $\sqrt[n]{1} \leqslant \mathbb{C}$: Ակնհայտ է, որ $\sqrt[n]{1} \subseteq \sqrt[n^2]{1} \subseteq \cdots \subseteq \sqrt[n^k]{1} \subseteq \cdots$ և հետևաբար, $\bigcup\limits_{k=1}^{\infty} \sqrt[n^k]{1}$ տեսաբազմային միավորումը կլինի $\mathbb{C}(\cdot)$-ի ենթախումբ, որը սովորաբար նշանակվում է $\mathbb{C}_{n^\infty}$-ով կամ $\sqrt[n^\infty]{1}$-ով:

Սակայն ընդհանուր դեպքում, խմբի երկու ենթախմբերի տեսաբազմային միավորումը կարող է չլինել ենթախումբ: Օրինակ, S_3 սիմետրիկ խմբի երկու տարբեր երկրորդ կարգի ենթախմբերի տեսաբազմային միավորումը ենթախումբ չէ:

Որպեսզի $Q(\circ)$ խմբի ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը լինի ենթախումբ անհրաժեշտ է և բավարար, որ Q'-ը բավարարի հետևյալ երեք պայմաններին.

ա) Q'-ը պարունակի իր ցանկացած երկու տարրերի արտադրյալը,

բ) Q'-ը պարունակի $Q(\circ)$ խմբի e միավորը,

գ) Q'-ը իր յուրաքանչյուր տարրի հետ մեկտեղ պարունակի նաև դրա հակադարձը $Q(\circ)$ խմբում:

Հատկություն 18.5: *Որպեսզի $Q(\circ)$ խմբի ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը լինի ենթախումբ անհրաժեշտ է և բավարար, որ Q'-ը բավարարի հետևյալ պայմաններից որևէ մեկին.*

ե$_1$) $x, y \in Q' \longrightarrow x \circ y^{-1} \in Q'$,

ե$_2$) $x, y \in Q' \longrightarrow x^{-1} \circ y \in Q'$,

որտեղ a^{-1}-ը a-ի հակադարձն է $Q(\circ)$ խմբում:

Ապացուցում: ե$_1$): *Անհրաժեշտություն:* Եթե $Q' \leqslant Q$, ապա $e \in Q'$ և $a^{-1} \in Q'$, եթե $a \in Q'$, իսկ e-ն $Q(\circ)$ խմբի միավորն է: Հետևաբար, եթե $x, y \in Q'$, ապա $x, y^{-1} \in Q'$ և $x \circ y^{-1} \in Q'$:

Բավարարություն: Եթե տված ե$_1$) պայմանի մեջ վերցնենք $x = y$, ապա կունենանք $e \in Q'$, որտեղ e-ն $Q(\circ)$ խմբի միավորն է, իսկ $x = e$ դեպքում կունենանք $y^{-1} \in Q'$, որտեղ $y \in Q'$: Այնուհետև,

$$x, y \in Q' \longrightarrow x, y^{-1} \in Q' \longrightarrow x \circ \left(y^{-1}\right)^{-1} \in Q' \longrightarrow x \circ y \in Q' :$$

Այսպիսով, ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը կլինի խումբ $\circ$ գործողության նկատմամբ: $\square$

18.2.2. Միավորով կիսախմբի հակադարձելի տարրերի խումբը: Կիսախմբի մաքսիմալ ենթախումբ: Ներմուծենք կիսախմբի մաքսիմալ ենթախմբի գաղափարը հետևյալ կերպ: $Q(\circ)$ կիսախմբի $Q' \leqslant Q$ ենթախումբը կոչվում է **մաքսիմալ ենթախումբ** $Q(\circ)$ կիսախմբում, եթե Q'-ը հնարավոր չէ ընդգրկել իրենից տարբեր $Q(\circ)$-ի որևէ H ենթախմբում, այսինքն՝

$$Q' \subseteq H \leqslant Q \longrightarrow Q' = H :$$

Օրինակ, $\mathbb{Z}(\cdot)$ կիսախմբի $Q' = \{0\}$ ենթախումբը մաքսիմալ է, իսկ $Q' = \{1\}$ ենթախումբը ոչ, որովհետև վերջինս ընդգրկվում է $H = \{1, -1\}$ ենթախնբում: Հետևյալ արդյունքն ունի ավելի ընդհանուր բնույթ:

Թեորեմ 18.10: *e միավորով օժտված $Q(\circ)$ կիսախմբի բոլոր հակադարձելի տարրերի*

$$Q^* = \{a \in Q |\ \exists a' \in Q,\ a \circ a' = a' \circ a = e\}$$

բազմությունը $Q(\circ)$-ի ենթախումբ է: Ըստ որում, Q^*-ը պարունակում է իր հետ հատվող $Q(\circ)$-ի յուրաքանչյուր ենթախումբ: Մասնավորապես, Q^* ենթախումբը մաքսիմալ է $Q(\circ)$ կիսախմբում:

Ապացույց: $Q^* \neq \emptyset$, որովհետև $e \in Q^*$: $Q^* \lesssim Q$, որովհետև

$$a, b \in Q^* \longrightarrow a \circ b \in Q^*$$

և $(a \circ b)' = b' \circ a'$: Այնուհետև, $Q^* \leqslant Q$, որովհետև

$$a \in Q^* \longrightarrow a' \in Q^*,$$

որտեղ $(a')' = a$:

Դիցուք $G \leqslant Q$ և $G \cap Q^* \neq \emptyset$, $a \in G \cap Q^*$: Պահանջվում է ապացուցել $G \subseteq Q^*$ ներդրումը: Նախ, համաձայն լեմմ 18.1-ի, եթե $f \in G$ տարրը $G(\circ)$ խմբի միավորն է, ապա $f = e$ (սակայն այս դեպքում, $e = f$ հավասարությունը ստացվում է ավելի հեշտ՝

$$e = a \circ a' = (f \circ a) \circ a' = f \circ (a \circ a') = f \circ e = f)\ :$$

Դիցուք $x \in G$: Քանի որ $G(\circ)$-ը e միավորով խումբ է, ապա գոյություն ունի այնպիսի $x_1 \in G \subseteq Q$, որ

$$x \circ x_1 = x_1 \circ x = e,$$

հետևաբար, $x \in Q^*$: Մնում է ապացուցել Q^* ենթախմբի մաքսիմալությունը $Q(\circ)$ կիսախմբում: Եթե $Q^* \subseteq H \leqslant Q$, ապա $Q^* \cap H = Q^* \neq \emptyset$ և համաձայն նախորդ պնդման՝ $H \subseteq Q^*$: Այսպիսով՝ $Q^* = H$: □

18.2.3. Կիսախմբի ինքնահամընկնող տարրին համապատասխանող մաքսիմալ ենթախումբը: Դիցուք $Q(\circ)$ կիսախումբն օժտված է e ինքնահամընկնող տարրով, այսինքն՝ $e \circ e = e$: Այդ դեպքում,

$$Q_e = \{a \in Q |\ a \circ e = e \circ a = a\}$$

ենթաբազմությունը կլինի $Q(\circ)$-ի ենթակիսախումբ՝ օժտված e միավորով: Իրոք, նախ $Q_e \neq \emptyset$, որովհետև $e \in Q_e$: Եթե $a, b \in Q_e$, ապա

$$(a \circ b) \circ e = a \circ (b \circ e) = a \circ b,$$

$$e \circ (a \circ b) = (e \circ a) \circ b = a \circ b$$

և, հետևաբար, $a \circ b \in Q_e$: Այսպիսով, $Q_e \lesssim Q$ և օժտված է e միավորով: Մասնավորապես, որպես հետևություն նախորդ թեորեմից, հանգում ենք հետևյալ արդյունքին, որտեղ Q_e^*-ը $Q_e(\circ)$ միավորով օժտված կիսախմբի բոլոր հակադարձելի տարրերի բազմությունն է:

Հետևություն 18.2*: Եթե $Q(\circ)$-ը e ինքնահամընկնող տարրով օժտված կիսախումբ է, ապա $Q_e \lesssim Q$, իսկ $Q_e^* \leqslant Q_e$: Ըստ որում, Q_e^*-ը պարունակում է իր հետ հատվող $Q_e(\circ)$-ի յուրաքանչյուր ենթախումբ: Մասնավորապես, Q_e^* ենթախումբը մաքսիմալ է $Q_e(\circ)$ միավորով օժտված կիսախմբում:* □

Դեռ ավելին, տեղի ունի հետևյալ պնդումը:

Թեորեմ 18.11*: Եթե $Q(\circ)$-ը e ինքնահամընկնող տարրով օժտված կիսախումբ է, ապա $Q_e^* \leqslant Q$ ենթախումբը պարունակում է իր հետ հատվող $Q(\circ)$-ի յուրաքանչյուր ենթախումբ: Մասնավորապես, Q_e^* ենթախումբը մաքսիմալ է $Q(\circ)$ կիսախմբում: Ըստ որում, եթե $e_1 \neq e_2$, ապա $Q_{e_1}^* \cap Q_{e_2}^* = \emptyset$, որտեղ $e_1, e_2 \in Q$ տարրերը ինքնահամընկնող են:*

Ապացուցում: Դիցուք $G \leqslant Q$ և $G \cap Q_e^* \neq \emptyset$, $a \in G \cap Q_e^*$: Պահանջվում է ապացուցել $G \subseteq Q_e^*$ ներդրումը, որի համար, ինչպես և թեորեմ 18.10-ում, բավական է նկատել, որ $G(\circ)$ խմբի $f \in G$ միավորը, համաձայն լեմմ 18.1-ի, համընկնում է $e \in Q$ ինքնահամընկնող տարրի հետ, որովհետև e-ն $Q_e^*(\circ)$ խմբի միավորն է: Հետևաբար, $G \subseteq Q_e^*$: Այնուհետև, Q_e^* ենթախմբի մաքսիմալությունը $Q(\circ)$ կիսախմբում ապացուցվում է ճիշտ նույն կերպ, ինչպես Q^*-ի մաքսիմալությունը թեորեմ 18.10-ում:

Մնում է ապացուցել, որ $e_1, e_2 \in Q$ ինքնահամընկնող տարրերի համար՝

$$e_1 \neq e_2 \longrightarrow Q_{e_1}^* \cap Q_{e_2}^* = \emptyset :$$

Ենթադրելով հակառակը, ստանում ենք հակասություն: Իրոք, եթե $Q_{e_1}^* \cap Q_{e_2}^* \neq \emptyset$, ապա կունենանք $Q_{e_1}^* \subseteq Q_{e_2}^*$, այսինքն՝ $Q_{e_1}^* \leqslant Q_{e_2}^*$ և, հետևաբար, $Q_{e_1}^*(\circ)$ և $Q_{e_2}^*(\circ)$ ենթախմբերի e_1 և e_2 միավորները կլինեն հավասար՝

$e_1 = e_2$: Այս հավասարությունը բխում է նաև այն փաստից, որ միևնույն կիսախմբի երկու հատվող ենթախմբերի միավորները համընկնում են: Հակասություն: □

$Q_e^* \leqslant Q$ ենթախումբը կոչվում է $Q(\circ)$ կիսախմբի $e \in Q$ **ինքնահամընկնող տարրին համապատասխանող ենթախումբ**:

18.2.4. Կիսախմբի մաքսիմալ ենթախմբերի բնութագրումը: Ինչպես տեսանք $Q(\circ)$ կիսախմբի e ինքնահամընկնող տարրին համապատասխանող Q_e^* ենթախումբը մաքսիմալ է տրված կիսախմբում: Պարզվում է ճիշտ է նաև հակառակը, որ ցանկացած կիսախմբի յուրաքանչյուր մաքսիմալ ենթախումբ ունի այդ տեսքը, այսինքն՝ կիսախմբում ուրիշ մաքսիմալ ենթախմբեր գոյություն չունեն:

Թեորեմ 18.12: *Ցանկացած $Q(\circ)$ կիսախմբի յուրաքանչյուր $Q' \leqslant Q$ մաքսիմալ ենթախմբի համար գոյություն ունի միարժեքորեն որոշվող այնպիսի $e \in Q$ ինքնահամընկնող տարր, որ*

$$Q' = Q_e^* :$$

Ապացուցում : Իրոք, $Q'(\circ)$ խմբի $e \in Q'$ միավորը կլինի ինքնահամընկնող տարր $Q(\circ)$-ում, հետևաբար կարելի է դիտարկել $Q_e^* \leqslant Q$ ենթախումբը, որը հատվում է $Q' \leqslant Q$ ենթախմբի հետ, որովհետև $e \in Q' \cap Q_e^*$: Ուստի, ըստ նախորդ թեորեմի առաջին մասի, $Q' \subseteq Q_e^* \subseteq Q$ և քանի որ $Q' \leqslant Q$ ենթախումբը մաքսիմալ է $Q(\circ)$-ում, ապա $Q' = Q_e^*$: e ինքնահամընկնող տարրի միակությունն ակնհայտ է: □

18.2.5. Խմբի կենտրոն և նորմալացնող ենթախումբ (նորմալիզատոր): Դիցուք $Q(\circ)$-ը կամայական խումբ է: $Q(\circ)$ խմբի **կենտրոնը** նշանակվում է $Z(Q)$-ով և սահմանվում է հետևյալ կերպ՝

$$Z(Q) = \{a \in Q |\ a \circ x = x \circ a \ \text{ ցանկացած } x \in Q \text{ տարրի համար}\} :$$

Լեմմ 18.2: *Խմբի կենտրոնը ենթախումբ է, ավելի ճիշտ՝ $Z(Q) \leqslant Q$:*

Ապացուցում: Նախ $Z(Q) \neq \emptyset$, որովհետև $e \in Z(Q)$: Այնուհետև՝

$$a, b \in Z(Q) \longrightarrow a \circ b \in Z(Q)$$

և

$$a \in Z(Q) \longrightarrow a^{-1} \in Z(Q),$$

որովհետև՝

$$(a \circ b) \circ x = a \circ (b \circ x) = a \circ (x \circ b) = (a \circ x) \circ b = (x \circ a) \circ b = x \circ (a \circ b),$$

$$a \circ x = x \circ a \longrightarrow x = a^{-1} \circ x \circ a \longrightarrow x \circ a^{-1} = a^{-1} \circ x \; : \qquad \square$$

Ակնհայտ է, որ $Q(\circ)$ խումբը կլինի աբելյան այն և միայն այն դեպքում, երբ $Z(Q) = Q$: Մյուս ծայրահեղ դեպքում, երբ $Z(Q) = \{e\}$, $Q(\circ)$ խումբը կոչվում է **առանց կենտրոնի** կամ **կենտրոն չունեցող**:

Թեորեմ 18.13: *Եթե $n \geqslant 3$, ապա n-րդ աստիճանի S_n սիմետրիկ խումբն առանց կենտրոնի է, իսկ $n \geqslant 4$ դեպքում n-րդ աստիճանի $\mathbb{A}_n$ նշանափոխ խումբը ևս առանց կենտրոնի է:*

Ապացուցում: Եթե $\alpha \in S_n$, $\alpha \neq \varepsilon$, ապա գոյություն ունեն այնպիսի $i \neq j$ թվեր, որ $\alpha(i) = j$, $1 \leqslant i, j \leqslant n$: Քանի որ $n \geqslant 3$, ապա գոյություն ունի նաև այնպիսի $\beta \in S_n$ տեղադրություն, որ $\beta = (j, k)$, որտեղ $k \neq j$ և $k \neq i$: Ակնհայտ է, որ $\alpha \neq \beta$ և

$$(\alpha \cdot \beta)i = \beta(\alpha i) = \beta(j) = k,$$

$$(\beta \cdot \alpha)i = \alpha(\beta i) = \alpha(i) = j,$$

այսինքն՝ $\alpha \cdot \beta \neq \beta \cdot \alpha$ և, հետևաբար, $\alpha \notin Z(S_n)$:

Ապացուցենք թեորեմի երկրորդ մասը: Շնորհիվ $n \geqslant 4$ պայմանի, կամայական $\alpha \in \mathbb{A}_n$, $\alpha \neq \varepsilon$ տեղադրության հետ մեկտեղ, որտեղ $\alpha(i) = j$, $i \neq j$, կարելի է դիտարկել նաև հետևյալ $\gamma \in \mathbb{A}_n$ տեղադրությունը՝

$$\gamma = (j, k, s) = (j, k) \cdot (j, s),$$

որտեղ i, j, k, s թվերը զույգ առ զույգ միմյանցից տարբեր են: Այնուհետև,

$$(\alpha \cdot \gamma)i = \gamma(\alpha i) = \gamma(j) = k,$$

$$(\gamma \cdot \alpha)i = \alpha(\gamma i) = \alpha(i) = j\,;$$

Ուստի, $\alpha \cdot \gamma \neq \gamma \cdot \alpha$ և հետևաբար, $\alpha \notin Z(\mathbb{A}_n)$: $\square$

Եթե $Q(\circ)$-ը կամայական խումբ է, $a \in Q$, $H \leqslant Q$, իսկ $a^{-1}Ha = \left\{a^{-1} \circ x \circ a \middle|\, x \in H\right\}$ և

$$N_Q(H) = \left\{a \in Q \middle|\, a^{-1}Ha = H\right\},$$

ապա տեղի ունի հետևյալ պնդումը:

Լեմմ 18.3: *$a^{-1}Ha \leqslant Q$ և $N_Q(H) \leqslant Q$ ցանկացած $a \in Q$ տարրի և ցանկացած $H \leqslant Q$ ենթախմբի համար :*

Ապացույցում: Եթե $u, v \in a^{-1}Ha$, ապա $u = a^{-1} \circ x \circ a$, $v = a^{-1} \circ y \circ a$, որտեղ $x, y \in H$: Հետևաբար,

$$u \circ v = a^{-1} \circ x \circ a \circ a^{-1} \circ y \circ a = a^{-1} \circ (x \circ y) \circ a \in a^{-1}Ha,$$

որովհետև $x \circ y \in H$: Այնուհետև,

$$u^{-1} = \left(a^{-1} \circ x \circ a\right)^{-1} = a^{-1} \circ x^{-1} \circ \left(a^{-1}\right)^{-1} = a^{-1} \circ x^{-1} \circ a \in a^{-1}Ha,$$

որովհետև $x^{-1} \in H$:

$N_Q(H) \leqslant Q$ հատկությունը ստուգվում է համանման եղանակով: □

Վերջին դեպքում ավելի դյուրին է վարվել հետևյալ կերպ:

Եթե $Q(\cdot)$ կիսախմբի կամայական $X, Y \subseteq Q$ ենթաբազմությունների համար սահմանենք

$$X \cdot Y = \{x \cdot y \mid \ x \in X,\, y \in Y\},$$

ապա այս գործողությունը ևս կլինի զուգորդական, այսինքն՝

$$(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$$

ցանկացած $X, Y, Z \subseteq Q$ ենթաբազմությունների համար: Հետևաբար, ընհանրացված զուգորդական օրենքի (թեորեմ 1.3) համաձայն, ենթաբազմությունների $X_1 \cdot X_2 \cdots X_n$ արտադրյալը կախված չէ փակագծերի դասավորությունից: Մասնավորապես, $Q(\cdot)$ խմբում՝

$$a^{-1}Ha = \left\{a^{-1}\right\} \cdot H \cdot \{a\}$$

և, եթե $a^{-1}Ha = H$, $b^{-1}Hb = H$, ապա

$$(ab)^{-1}H(ab) = \left(b^{-1}a^{-1}\right)H(ab) = \left\{b^{-1}\right\} \cdot \left\{a^{-1}\right\} \cdot H \cdot \{a\} \cdot \{b\} =$$

$$= \left\{b^{-1}\right\} \cdot H \cdot \{b\} = H,$$

$$\left(a^{-1}\right)^{-1} Ha^{-1} = aHa^{-1} = \{a\} \cdot H \cdot \left\{a^{-1}\right\} = \{a\} \cdot \left\{a^{-1}\right\} \cdot H \cdot \{a\} \cdot \left\{a^{-1}\right\} = H :$$

$N_Q(H) \leqslant Q$ ենթախումբը կոչվում է H-ի **նորմալացնող ենթախումբ** (նորմալիզատոր) $Q(\cdot)$ խմբում: Ակնհայտ է, որ $H \leqslant N_Q(H)$:

18.2.6. Ըստ ենթախմբի համուղղված (կողմնորոշված) հենքեր: Դիցուք Q-ն կամայական ոչ զրոյական n-չափանի գծային տարածություն է՝ որոշված P դաշտի վրա, իսկ $H(\cdot)$-ը n-րդ կարգի հակադարձելի մատրիցների որևէ խումբ է, այսինքն՝ $H \leqslant GL_n(P)$: Եթե $e_1, \ldots, e_n$ հաջորդականությունը Q-ի հենք է, իսկ $A \in H$, $A = (a_{ij})$, ապա Q-ի տարրերի $e_1', \ldots, e_n'$ հաջորդականությունը, որտեղ

$$\begin{aligned} &e_1' = a_{11}e_1 + \cdots + a_{1n}e_n, \\ &\cdots\ \cdots\ \cdots \\ &e_n' = a_{n1}e_1 + \cdots + a_{nn}e_n, \end{aligned}$$

ևս կլինի Q-ի հենք: Մատրիցային տեսքով՝ $e' = A \bullet e$, որտեղ

$$e' = \begin{pmatrix} e_1' \\ \vdots \\ e_n' \end{pmatrix}, \quad e = \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}:$$

Q-ի երկու e և e' հենքեր կանվանենք H-համարժեք և կգրենք $e \underset{H}{\sim} e'$, եթե $e' = A \bullet e$, որտեղ $A \in H$:

Հատկություն 18.6: *Եթե $H \leqslant GL_n(P)$, ապա սահմանված «$\underset{H}{\sim}$» հարաբերությունը համարժեքության հարաբերություն է՝ որոշված ոչ զրոյական n-չափանի Q գծային տարածության բոլոր հենքերի բազմության վրա, այսինքն՝*

ա) $e \underset{H}{\sim} e$, Q-ի ցանկացած հենքի համար,

բ) $e \underset{H}{\sim} e' \longrightarrow e' \underset{H}{\sim} e$,

գ) $e \underset{H}{\sim} e',\ e' \underset{H}{\sim} e'' \longrightarrow e \underset{H}{\sim} e''$,:

Ապացուցում: $e \underset{H}{\sim} e$, որովհետև $e = E \cdot e$, որտեղ E-ն n-րդ կարգի միավոր մատրիցն է և $E \in H$: Եթե $e \underset{H}{\sim} e'$, ապա $e' = A \bullet e$, որտեղից $e = A^{-1} \bullet e$ և $A^{-1} \in H$: Հետևաբար, $e' \underset{H}{\sim} e$: Դիցուք $e \underset{H}{\sim} e'$ և $e' \underset{H}{\sim} e''$: Հետևաբար, գոյություն կունենան այնպիսի $A_1 \in H$ և $A_2 \in H$ մատրիցներ, որ $e' = A_1 \bullet e$ և $e'' = A_2 \bullet e'$: Կունենանք՝ $e'' = A_2 \bullet (A_1 \bullet e) = (A_2 \cdot A_1) \bullet e$, որտեղ $A_2 \cdot A_1 \in H$: Ուստի՝ $e \underset{H}{\sim} e''$: □

Այս համարժեքության հարաբերությունը կոչվում է H-համարժեքության հարաբերություն, որտեղ $H \leqslant GL_n(P)$: Ըստ որում, e

հենքի համապատասխան համարժեքության դասը կլինի՝

$$H(e) = \{A \bullet e \,|\, A \in H\}$$

հենքերի բազմությունը: Միևնույն $H(e)$ համարժեքության դասին պատկանող երկու հենքեր կոչվում են **համուղղված** կամ **կողմնորոշված** ըստ $H \leqslant GL_n(P)$ ենթախմբի: Հակառակ դեպքում, հենքերը կոչվում են **հակուղղված** ըստ $H \leqslant GL_n(P)$ ենթախմբի:

Արդյունքում ստանում ենք ոչ զրոյական վերջավոր չափանի գծային տարածության հենքերի դասակարգում՝ տրված խմբի օգնությամբ:

Օրինակ: Դիցուք $H \leqslant GL_n(P)$ ենթախումբը որոշվում է հետևյալ կերպ՝

$$H = \{A \in GL_n(P) \,|det(A) > 0\} \leqslant GL_n(P),$$

իսկ Q-ն ոչ զրոյական n-չափանի գծային տարածություն է: Ապացուցենք, որ այս H ենթախմբի դեպքում Q-ի բոլոր հենքերը բաժանվում են երկու համարժեքության դասերի ըստ H-համարժեքության հարաբերության: Դիցուք $H(e)$-ն այդ համարժեքության դասերից որևէ մեկն է, իսկ $e' \notin H(e)$, որտեղ e'-ը Q-ի որևէ հենք է: Դիտարկենք նաև $H(e')$ համարժեքության դասը և ապացուցենք, որ Q-ի ցանկացած e'' հենք ընկած է այդ երկու դասերից որևէ մեկում: Իրոք, եթե $e' \notin H(e)$, ապա

$$e' = B \bullet e,$$

որտեղ B-ն հակադարձելի մատրից է և $det(B) < 0$: Դիցուք՝

$$\begin{aligned} &e'' = C \bullet e, \\ &e'' = D \bullet e' = D \bullet (B \bullet e) = (DB) \bullet e : \end{aligned}$$

Այսպիսով, $C = DB$: Եթե $e'' \notin H(e)$, ապա $det(C) < 0$ և, քանի որ, $det(C) = det(D) \cdot det(B)$, ապա կունենանք՝ $det(D) > 0$: Հետևաբար, $e'' \in H(e')$:

18.3. Խմբերի և կիսախմբերի իզոմորֆիզմը: Քելիի թեորեմը և դրա հակադարձումը

Դիցուք $Q(\cdot)$-ը և $Q'(\circ)$-ը կիսախմբեր, քվազիխմբեր, խմբեր կամ խմբակերպեր են: Չի բացառվում, որ դրանցից միայն մեկը լինի կիսախումբ, քվազիխումբ, խումբ կամ խմբակերպ:

$\varphi : Q \to Q'$ արտապատկերումը կոչվում է **նմանածնություն** կամ **հոմոմորֆ արտապատկերում (հոմոմորֆություն, հոմոմորֆիզմ)**՝ $Q(\cdot)$-ից $Q'(\circ)$-ի մեջ, եթե տեղի ունի հետևյալ պայմանը.

$$\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)$$

ցանկացած $x, y \in Q$ տարրերի համար: Եթե այդ դեպքում φ արտապատկերումը փոխմիարժեք (բիեկտիվ) է, ապա φ-ն կոչվում է **նույնածնություն** կամ **իզոմորֆ արտապատկերում** (**իզոմորֆություն**, **իզոմորֆիզմ**): $Q(\cdot)$-ը և $Q'(\circ)$-ը կոչվում են **իզոմորֆ** կամ **նույնածն** և գրվում է $Q \simeq Q'$ կամ $Q \cong Q'$, եթե գոյություն ունի որևէ $\varphi : Q \to Q'$ իզոմորֆ արտապատկերում: Երբեմն գրվում է՝ $Q(\cdot) \simeq Q'(\circ)$ կամ $Q(\cdot) \cong Q'(\circ)$: Այս «$\simeq$» հարաբերությունը կոչվում է **նույնածնության** (իզոմորֆության) **հարաբերություն**:

$\varphi : Q \to Q'$ հոմոմորֆիզմը կոչվում է **ներդրող հոմոմորֆիզմ** կամ **մոնոմորֆիզմ**, եթե φ-ն նաև ներդրող (ինյեկտիվ) արտապատկերում է:

$\varphi : Q \to Q'$ հոմոմորֆիզմը կոչվում է **վերադրող հոմոմորֆիզմ** կամ **էպիմորֆիզմ**, եթե φ-ն նաև վերադրող (սյուրեկտիվ) արտապատկերում է:

Հետևյալ պնդումներն ակնհայտ են.

ա) Եթե $Q(\cdot) \simeq Q'(\circ)$ և $Q(\cdot)$-ը կիսախումբ է, ապա $Q'(\circ)$-ը ևս կլինի կիսախումբ;

բ) Եթե $Q(\cdot) \simeq Q'(\circ)$ և $Q(\cdot)$-ը քվազիխումբ է, ապա $Q'(\circ)$-ը ևս կլինի քվազիխումբ;

գ) Եթե $Q(\cdot) \simeq Q'(\circ)$ և $Q(\cdot)$-ը խումբ է, ապա $Q'(\circ)$-ը ևս կլինի խումբ:

Օրինակներ: 1) $S_n \simeq \mathbb{P}_n$ և $\mathbb{A}_n \simeq \mathbb{T}_n$, այսինքն՝ n-րդ աստիճանի բոլոր տեղադրությունների S_n սիմետրիկ խումբն իզոմորֆ է բոլոր n-տեղափոխությունների $\mathbb{P}_n$ խմբին և n-րդ աստիճանի բոլոր զույգ տեղադրությունների $\mathbb{A}_n$ նշանափոխ խումբն իզոմորֆ է բոլոր զույգ n-տեղափոխությունների $\mathbb{T}_n$ խմբին:

2) Երկտեղ գործողությունների վերոհիշյալ $\mathcal{F}_Q^2(\cdot)$ և $\mathcal{F}_Q^2(\circ)$ կիսախմբերն իզոմորֆ են, որովհետև $\varphi : A \to A^*$ արտապատկերումը, որտեղ

$A^*(x,y) = A(y,x)$, կլինի իզոմորֆ արտապատկերում $\mathcal{F}_Q^2(\cdot)$ կիսախմբից $\mathcal{F}_Q^2(\circ)$ կիսախմբի մեջ, քանի որ φ-ն փոխմիարժեք է և

$$(A \cdot B)^* = A^* \circ B^*$$

ցանկացած $A, B \in \mathcal{F}_Q^2$ տարրերի համար: Իրոք, $(A \cdot B)^*(x,y) = (A \cdot B)(y,x) = A(y, B(y,x)) = A^*(B^*(x,y), y) = (A^* \circ B^*)(x,y)$, որտեղ $x, y \in Q$: Այսպիսով, $\mathcal{F}_Q^2(\cdot) \simeq \mathcal{F}_Q^2(\circ)$:
3) $a^{x+y} = a^x \cdot a^y$ դպրոցական բանաձևը, որտեղ $a > 0$, $a \neq 1$, նշանակում է, որ $\varphi : x \to a^x$ արտապատկերումն իզոմորֆիզմ է բոլոր իրական թվերի գումարային խմբից բոլոր դրական իրական թվերի արտադրյալային խմբի մեջ՝ $\mathbb{R}(+) \simeq \mathbb{R}_+(\cdot)$:
4) $det(A \cdot B) = det(A) \cdot det(B)$ բանաձևը նշանակում է, որ $\varphi : A \to det(A)$ արտապատկերումն հոմոմորֆիզմ է բոլոր n-րդ կարգի մատրիցների արտադրյալային կիսախմբից բոլոր իրական թվերի արտադրյալային կիսախմբի մեջ (նույն բանաձևով որոշվում է նաև հոմոմորֆիզմ՝ բոլոր n-րդ կարգի հակադարձելի մատրիցների $GL_n(\mathbb{R})$ արտադրյալային խմբից բոլոր ոչ զրոյական իրական թվերի արտադրյալային խմբի մեջ): Այս հոմոմորֆիզմը նշանակվում է det-ով:

Լեմմ 18.4: *Իզոմորֆության սահմանված «$\simeq$» հարաբերությունը բավարարում է համարժեքության հարաբերության սահմանման երեք պայմաններին՝*

ա) $Q \simeq Q$,
բ) եթե $Q \simeq Q'$, ապա $Q' \simeq Q$,
գ) եթե $Q \simeq Q'$ և $Q' \simeq Q''$, ապա $Q \simeq Q''$:

Ապացուցում: Իրոք, ա) պայմանը բխում է այն փաստից, որ $\varepsilon_Q : Q \to Q$ նույնական արտապատկերումն իզոմորֆ արտապատկերում է: բ) պայմանը բխում է այն փաստից, որ եթե $\varphi : Q \to Q'$ արտապատկերումն իզոմորֆ արտապատկերում է, ապա այդպիսին է նաև $\varphi^{-1} : Q' \to Q$ փոխմիարժեք արտապատկերումը, որովհետև

$$\varphi(x \cdot y) = \varphi(x) \circ \varphi(y), \quad x, y \in Q,$$

պայմանից $x = \varphi^{-1}(x')$, $y = \varphi^{-1}(y')$ արժեքների դեպքում կունենանք՝

$$\varphi\left(\varphi^{-1}(x') \cdot \varphi^{-1}(y')\right) = \varphi\left(\varphi^{-1}(x')\right) \circ \varphi\left(\varphi^{-1}(y')\right),$$

$$\varphi\left(\varphi^{-1}(x') \cdot \varphi^{-1}(y')\right) = x' \circ y',$$

$$\varphi^{-1}(x') \cdot \varphi^{-1}(y') = \varphi^{-1}\left(x' \circ y'\right),$$

որտեղ $x', y' \in Q'$: գ) պայմանը բխում է այն փաստից, որ եթե $\varphi : Q \to Q'$ և $\varphi' : Q' \to Q''$ փոխմիարժեք արտապատկերումները իզոմորֆ արտապատկերումներ են, ապա այդպիսին կլինի նաև դրանց $\varphi \cdot \varphi' : Q \to Q''$ փոխմիարժեք արտադրյալը, որովհետև

$$(\varphi \cdot \varphi')(x \cdot y) = \varphi'\left(\varphi(x \cdot y)\right) = \varphi'\left(\varphi x \circ \varphi y\right) =$$

$$= \varphi'(\varphi x) * \varphi'(\varphi y) = (\varphi \cdot \varphi')x * (\varphi \cdot \varphi')y,$$

որտեղ $x, y \in Q$: $\square$

Կասենք, որ $Q(\cdot)$-ը **ներդրվում** է $Q'(\circ)$-ի մեջ և կգրենք $Q \underset{\to}{\subseteq} Q'$ կամ $Q(\cdot) \underset{\to}{\subseteq} Q'(\circ)$, եթե գոյություն ունի որևէ $\varphi : Q \to Q'$ մոնոմորֆիզմ, այսինքն՝ ներդրող (ինյեկտիվ) և հոմոմորֆ արտապատկերում: Այս դեպքում, եթե $Q(\cdot)$-ը կիսախումբ (խումբ, քվազիխումբ) է, ապա

$$\varphi(Q) = \{\varphi(x) \mid \ x \in Q\} \subseteq Q'$$

ենթաբազմությունը նույնպես կլինի կիսախումբ (խումբ, քվազիխումբ) $\circ$ գործողության նկատմամբ և $Q \simeq \varphi(Q)$:

Ակնհայտ է, որ յուրաքանչյուր $Q(\cdot)$ կիսախումբ ներդրվում է e միավորով օժտված $Q'(\circ)$ կիսախմբի մեջ, եթե ընդունենք $Q' = Q \cup \{e\}$, $e \notin Q$, և $x, y \in Q'$ տարրերի համար սահմանենք՝

$$x \circ y = \begin{cases} x \cdot y, & \text{եթե } x, y \in Q, \\ x, & \text{եթե } x \in Q',\ y = e, \\ y, & \text{եթե } y \in Q',\ x = e: \end{cases}$$

Այստեղ որպես $\varphi : Q \to Q'$ ներդրող և հոմոմորֆ արտապատկերում կարելի է վերցնել ε_Q նույնական արտապատկերումը:

Թեորեմ 18.14 (Քելի, 1854թ.): *Միավորով օժտված յուրաքանչյուր $Q(\cdot)$ կիսախումբ ներդրվում է Q բազմության $\mathcal{F}_Q$ սիմետրիկ կիսախմբում, այսինքն՝ միավորով օժտված յուրաքանչյուր $Q(\cdot)$ կիսախումբ իզոմորֆ է $\mathcal{F}_Q$ սիմետրիկ կիսախմբի որևէ ենթակիսախմբի: Յուրաքանչյուր $Q(\cdot)$ խումբ ներդրվում է Q բազմության S_Q սիմետրիկ խմբում, այսինքն՝ յուրաքանչյուր $Q(\cdot)$ խումբ իզոմորֆ է S_Q սիմետրիկ խմբի որևէ ենթախմբի:*

Ապացույց: Դիցուք $Q(\cdot)$-ը $e \in Q$ միավորով օժտված կիսախումբ է, $a \in Q$: Սահմանենք $R_a : Q \to Q$ արտապատկերումը (աջ տեղաշարժ) հետևյալ կերպ՝

$$R_a(x) = x \cdot a, \quad x \in Q :$$

Տեղի ունի

$$R_a \cdot R_b = R_{a \cdot b}$$

հավասարությունը՝ ցանկացած $a, b \in Q$ տարրերի համար: Իրոք, ցանկացած $x \in Q$ տարրի համար՝

$$(R_a \cdot R_b)\, x = R_b\, (R_a(x)) = R_b(x \cdot a) = (x \cdot a)b = x \cdot (a \cdot b) = R_{a \cdot b}(x) :$$

Հետևաբար, $\mathcal{R}_Q = \{R_a \,|\quad a \in Q\}$ բազմությունը կիսախումբ է արտապատկերումների արտադրյալի նկատմամբ, այսինքն՝ $\mathcal{R}_Q \lesssim \mathcal{F}_Q$: Այժմ ապացուցենք, որ $Q(\cdot)$-ը ներդրվում է $\mathcal{F}_Q$ սիմետրիկ կիսախմբում: Որոնելի $\varphi : Q \to \mathcal{F}_Q$ ներդրող և հոմոմորֆ արտապատկերումը կարելի է սահմանել հետևյալ կերպ՝

$$\varphi(a) = R_a,$$

քանի որ այն իրոք ներդրող է, այսինքն՝

$$\varphi(a) = \varphi(b) \longrightarrow a = b,$$

որովհետև

$$R_a = R_b \longrightarrow R_a(x) = R_b(x) \longrightarrow R_a(e) = R_b(e) \longrightarrow e \cdot a = e \cdot b \longrightarrow a = b,$$

և

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

որովհետև

$$R_{a \cdot b} = R_a \cdot R_b :$$

Այսպիսով $Q \simeq \mathcal{R}_Q$:

Խմբի դեպքում բավական է նկատել, որ սահմանված R_a արտապատկերումները տեղադրություններ են և, հետևաբար, ընկած են S_Q-ի մեջ, այսինքն՝ $\varphi : Q \to S_Q \subseteq \mathcal{F}_Q$, $\mathcal{R}_Q \leqslant S_Q$, եթե $Q(\cdot)$-ը խումբ է: Այսպիսով, $Q(\cdot) \underset{\to}{\subsetneq} \mathcal{F}_Q(\cdot)$, եթե $Q(\cdot)$-ը միավորով կիսախումբ է, իսկ $Q(\cdot) \underset{\to}{\subsetneq} S_Q(\cdot)$, եթե $Q(\cdot)$-ը խումբ է: $\square$

Հետևություն 18.3: *Յուրաքանչյուր կիսախումբ ներդրվում է որևէ սիմետրիկ կիսախմբում: Ավելի ճիշտ, յուրաքանչյուր $Q(\cdot)$ կիսախումբ ներդրվում է $\mathcal{F}_X$ սիմետրիկ կիսախմբում, որտեղ $X = Q \cup \{e\}$, $e \notin Q$, այսինքն՝ յուրաքանչյուր $Q(\cdot)$ կիսախումբ իզոմորֆ է $\mathcal{F}_X$ սիմետրիկ կիսախմբի որևէ ենթակիսախմբի:*

Ապացուցում: Յուրաքանչյուր $Q(\cdot)$ կիսախումբ ներդրվում է e միավորով օժտված $Q \cup \{e\}(\circ)$ կիսախմբի մեջ: Մնում է կիրառել ապացուցված թեորեմը և նկատել, որ ներդրման հատկությունը փոխանցական է, այսինքն՝ եթե $Q_1 \underset{\rightarrow}{\subseteq} Q_2$ և $Q_2 \underset{\rightarrow}{\subseteq} Q_3$, ապա $Q_1 \underset{\rightarrow}{\subseteq} Q_3$: □

Ակնհայտ է, որ եթե $Q(\cdot)$ խմբակերպի համար $R_a(x) = x \cdot a$, որտեղ $x, a \in Q$, և $\varphi : a \rightarrow R_a$ արտապատկերումը հոմոմորֆիզմ է $Q(\cdot)$ խմբակերպից $\mathcal{F}_Q$ սիմետրիկ կիսախմբի մեջ, ապա $Q(\cdot)$-ը կիսախումբ է: Մասնավորապես, եթե $Q(\cdot)$ քվազիխմբի համար $\varphi : a \rightarrow R_a$ արտապատկերումը հոմոմորֆիզմ է $Q(\cdot)$ քվազիխմբից S_Q սիմետրիկ խմբի մեջ, ապա $Q(\cdot)$-ը խումբ է: Հաջորդ արդյունքը տալիս է Քելիի թեորեմի հակադարձման մեկ այլ տարբերակ:

Թեորեմ 18.15 (Քելիի թեորեմի հակադարձումը): *Եթե միավորով օժտված $Q(\cdot)$ խմբակերպի $R_a : x \rightarrow x \cdot a$ արտապատկերումների (աջ տեղաշարժերի)*

$$\mathcal{R}_Q = \{R_a \mid a \in Q\}$$

բազմությունը կիսախումբ է՝ արտապատկերումների արտադրյալի նկատմամբ, ապա $Q(\cdot)$-ը միավորով կիսախումբ է: Մասնավորապես, եթե $Q(\cdot)$ լուպայի $R_a : x \rightarrow x \cdot a$ արտապատկերումների (աջ տեղաշարժերի)

$$\mathcal{R}_Q = \{R_a \mid a \in Q\}$$

բազմությունը կիսախումբ է՝ արտապատկերումների արտադրյալի նկատմամբ, ապա $Q(\cdot)$-ը խումբ է:

Ապացուցում: Դիցուք e-ն $Q(\cdot)$-ի միավորն է: Նախ նկատենք, որ

$$R_a(e) = R_b(e) \longrightarrow R_a = R_b :$$

Իրոք,

$$R_a(e) = R_b(e) \longrightarrow e \cdot a = e \cdot b \longrightarrow a = b \longrightarrow R_a = R_b :$$

Ցանկացած $a, b \in Q$ տարրերի համար՝

$$(R_a \cdot R_b)\, e = R_b\,(R_a(e)) = (e \cdot a) \cdot b = a \cdot b,$$

$$R_{a \cdot b}(e) = e \cdot (a \cdot b) = a \cdot b;$$

Քանի որ, ըստ թեորեմի պայմանի, $R_a \cdot R_b \in \mathcal{R}_Q$ ու $(R_a \cdot R_b)\, e = R_{a\cdot b}(e)$, ապա $R_a \cdot R_b = R_{a \cdot b}$, այսինքն՝ $(R_a \cdot R_b)\, x = (R_{a\cdot b})\, x$ ցանկացած $x \in Q$ տարրի համար: Այսպիսով,

$$R_b\,(R_a(x)) = (R_{a\cdot b})\, x,$$

$$(x \cdot a) \cdot b = x \cdot (a \cdot b)$$

և $Q(\cdot)$-ը կիսախումբ է: □

Հետևություն 18.4: Եթե $Q(\cdot)$ լուպայի $R_a : x \to x \cdot a$ արտապատկերումների (աջ տեղաշարժերի)

$$\mathcal{R}_Q = \{R_a \mid a \in Q\}$$

բազմությունը կիսախումբ է՝ արտապատկերումների արտադրյալի նկատմամբ, ապա $\mathcal{R}_Q$-ն խումբ է: □

Խմբի (կիսախմբի, քվազիխմբի) այն հատկությունը, որով օժտված է նաև այդ խմբին (կիսախմբին, քվազիխմբին) իզոմորֆ ցանկացած խումբ (կիսախումբ, քվազիխումբ), կոչվում է խմբի (կիսախմբի, քվազիխմբի) **հանրահաշվական հատկություն**, կամ **հանրահաշվական ինվարիանտ**: Օրինակ, խմբի (կիսախմբի, քվազիխմբի) կարգը (հզորությունը), նրա տեղափոխական հատկությունը հանրահաշվական ինվարիանտներ են: Ակնհայտ է, որ երկու իզոմորֆ խմբեր (կիսախմբեր, քվազիխմբեր) կունենան նույն հանրահաշվական հատկությունները:

Դիցուք տրված են Q_1, Q_1', Q_2, Q_2' խմբերը (կիսախմբերը, քվազիխմբերը): Երկու $f : Q_1 \to Q_2$ և $f' : Q_1' \to Q_2'$ արտապատկերումներ կոչվում են **հանրահաշվորեն համարժեք** և գրվում է $f \sim f'$, եթե գոյություն ունեն այնպիսի $\varphi : Q_1 \to Q_1'$ և $\psi : Q_2 \to Q_2'$ իզոմորֆիզմներ, որ տեղափոխական է հետևյալ դիագրամը՝

$$\begin{tikzcd} Q_1 \arrow[r, "f"] \arrow[d, "\varphi"'] & Q_2 \arrow[d, "\psi"] \\ Q_1' \arrow[r, "f'"'] & Q_2' \end{tikzcd} \quad ,$$

այսինքն՝ $f \cdot \psi = \varphi \cdot f'$, կամ $f' = \varphi^{-1} \cdot f \cdot \psi$:

Հեշտությամբ ստուգվում է, որ արտապատկերումների հանրահաշվորեն համարժեքությունը բավարարում է համարժեքության հարաբերության սահմանման բոլոր երեք պայմաններին (աքսիոմներին):

$f : Q_1 \to Q_2$ արտապատկերման որևէ հատկություն կոչվում է **հանրահաշվական**, եթե այդ հատկությամբ օժտված է նաև f-ին հանրահաշվորեն համարժեք ցանկացած արտապատկերում: Օրինակ, դժվար չէ ստուգել, որ արտապատկերման նմանաձևություն (հոմոմորֆիզմ) լինելու հատկությունը հանրահաշվական հատկություն է:

Այժմ խմբերի (կիսախմբերի, քվազիխմբերի) տեսությունը կարելի է բնութագրել որպես գիտություն, որն ուսումնասիրում է խմբերի (կիսախմբերի, քվազիխմբերի) և դրանց հոմոմորֆ արտապատկերումների հանրահաշվական հատկությունները:

18.4. Խմբի տարրի ամբողջ աստիճան և կարգ: Միածին ենթախմբեր և միածին խմբեր: Լագրանժի թեորեմը վերջավոր միածին խմբերում

18.4.1. Խմբի տարրի ամբողջ աստիճան և կարգ, միածին ենթախմբեր: Դիցուք $Q(\circ)$-ը կամայական խումբ է ($e \in Q$ միավորով), $a \in Q$, $n \in \mathbb{N}$, $n \neq 0$: Սահմանենք a տարրի ամբողջ աստիճանի գաղափարը հետևյալ կերպ՝

$$a^n = \underbrace{a \circ a \circ \cdots \circ a}_{n},$$

$$a^{\circ} = e,$$
$$a^{-n} = \underbrace{a^{-1} \circ a^{-1} \circ \cdots \circ a^{-1}}_{n} = \left(a^{-1}\right)^{n},$$

որտեղ արտադրյալները գրված են առանց փակագծերի՝ համաձայն թեորեմ 1.3-ի: Այսպիսով, սահմանված է խմբի a տարրի ամբողջ աստիճանի գաղափարը, այսինքն՝ a^m-ը, որտեղ $m \in \mathbb{Z}$:

Խմբային գործողության գումարային գրելաձևի ժամանակ a^m-ի փոխարեն գրվում է ma և կարդացվում է «a-ի m-պատիկ», որտեղ $m \in \mathbb{Z}$:

Լեմմ 18.5: *Կամայական $Q(\circ)$ խմբի մեջ՝*

$$\left(a^{m}\right)^{-1} = a^{-m}$$

և

$$\left(a^{-1}\right)^{m} = a^{-m}$$

ցանկացած $m \in \mathbb{Z}$ ամբողջ թվի և ցանկացած $a \in Q$ տարրի համար: Խմբային գործողության գումարային գրելաձևի դեպքում՝

$$-(ma) = (-m)a,$$
$$m(-a) = (-m)a:$$

Ապացուցում: Ապացույցը կատարենք երեք դեպքով՝ ամբողջ աստիճանի սահմանմանը համապատասխան.

Ա) $m > 0$ դեպքում՝

$$\left(a^{m}\right)^{-1} = (\underbrace{a \circ \cdots \circ a}_{m})^{-1} = \underbrace{a^{-1} \circ \cdots \circ a^{-1}}_{m} = a^{-m};$$

Բ) $m = 0$ դեպքում՝ $\left(a^{m}\right)^{-1} = a^{-m}$, որովհետև հավասարության աջ և ձախ մասերը հավասար են խմբի e միավորին;

Գ) $m < 0$ դեպքում, $m = -|m|$ և

$$\left(a^{m}\right)^{-1} = \left(a^{-|m|}\right)^{-1} = (\underbrace{a^{-1} \circ \cdots \circ a^{-1}}_{|m|})^{-1} = \underbrace{\left(a^{-1}\right)^{-1} \circ \cdots \circ \left(a^{-1}\right)^{-1}}_{|m|} =$$

$$= \underbrace{a \circ \cdots \circ a}_{|m|} = a^{|m|} = a^{-m};$$

Նույն դատողություններով ապացուցվում է երկրորդ հավասարությունը:
$\square$

Հատկություն 18.7: *Կամայական $Q(\circ)$ խմբի մեջ`*

$$a^m \circ a^n = a^{m+n}$$

ցանկացած $m, n \in \mathbb{Z}$ ամբողջ թվերի և ցանկացած $a \in Q$ տարրի համար: Խմբային գործողության գումարային գրելաձևի դեպքում`

$$ma + na = (m+n)a :$$

Ապացուցում: Եթե $m = 0$ կամ $n = 0$, ապա գրված հավասարությունն ակնհայտ է, իսկ $m \neq 0$ և $n \neq 0$ դեպքում հնարավոր են հետևյալ ենթադեպքերը.

ա) $m > 0$, $n > 0$;

բ) $m > 0$, $n < 0$;

գ) $m < 0$, $n > 0$;

դ) $m < 0$, $n < 0$:

ա) դեպքում պնդումն ակնհայտ է: Ապացուցենք այն բ) դեպքում.

$$a^m \circ a^n = a^m \circ a^{-|n|} = \underbrace{a \circ \cdots \circ a}_{m} \cdot \underbrace{a^{-1} \circ \cdots \circ a^{-1}}_{|n|} =$$

$$= \begin{cases} a^{m-|n|}, & \text{եթե } m > |n|, \\ e, & \text{եթե } m = |n|, \\ \left(a^{-1}\right)^{|n|-m}, & \text{եթե } |n| > m \end{cases} = a^{m+n} :$$

Նույն կերպ պնդումն ապացուցվում է նաև մնացած երկու դեպքերում:
$\square$

Հատկություն 18.8: *Կամայական $Q(\circ)$ խմբի մեջ`*

$$a^{m_1} \circ a^{m_2} \circ \cdots \circ a^{m_n} = a^{m_1+m_2+\cdots+m_n}$$

ցանկացած $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ ամբողջ թվերի և ցանկացած $a \in Q$ տարրի համար: Խմբային գործողության գումարային գրելաձևի դեպքում`

$$m_1 a + m_2 a + \cdots + m_n a = (m_1 + m_2 + \cdots + m_n)a :$$

Ապացույց: Վերիանգման եղանակով՝ ըստ $n \geqslant 2$ բնական թվի: $\square$

Հատկություն 18.9: *Կամայական $Q(\circ)$ խմբի մեջ՝*

$$(a^m)^n = a^{mn}$$

ցանկացած $m, n \in \mathbb{Z}$ ամբողջ թվերի և ցանկացած $a \in Q$ տարրի համար: Խմբային գործողության գումարային գրելաձևի դեպքում՝

$$n(ma) = (nm)a :$$

Ապացույց: 1) $n > 0$ դեպքում պնդումը բխում է նախորդ հատկությունից՝

$$(a^m)^n = \underbrace{a^m \circ a^m \circ \cdots \circ a^m}_{n} = a^{m+m+\cdots+m} = a^{mn} :$$

2) $n = 0$ դեպքում պնդումն ակնհայտ է, որովհետև հանգում է $e = e$ հավասարությանը:

3) $n < 0$ դեպքում, $n = -|n|$ և համաձայն լեմմ 18.5-ի՝

$$(a^m)^n = (a^m)^{-|n|} = \Big((a^m)^{-1}\Big)^{|n|} = \big(a^{-m}\big)^{|n|} = a^{-m\cdot|n|} = a^{-m(-n)} = a^{mn} :$$

$\square$

Հատկություն 18.10: *Որպեսզի $Q(\circ)$ խմբի վերջավոր ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը լինի ենթախումբ անհրաժեշտ է և բավարար, որ Q'-ը լինի ենթակիսախումբ, այսինքն՝ Q'-ը լինի փակ $\circ$ գործողության նկատմամբ՝*

$$x, y \in Q' \longrightarrow x \circ y \in Q' :$$

Ապացույց: Անհրաժեշտությունն ակնհայտ է:

Բավարարություն: Եթե Q'-ը բավարարում է նշված պայմանին, ապա այն կպարունակի նաև իր ցանկացած վերջավոր թվով տարրերի արտադրյալը՝

$$x_1, \ldots, x_n \in Q' \longrightarrow x_1 \circ \cdots \circ x_n = (x_1 \circ \cdots \circ x_{n-1}) \circ x_n \in Q' :$$

Մասնավորապես, եթե $x \in Q'$, ապա $x^n \in Q'$, $n \in \mathbb{N}$, և վերջավոր Q' ենթաբազմության տարրերի

$$x, x^2, \ldots, x^n, \ldots$$

անվերջ հաջորդականության մեջ կլինեն կրկնություններ, այսինքն՝

$$x^t = x^s, \quad t > s,$$

$$x^{t-s} = x^0 = e,$$

$$x^n = e, \quad n = t - s > 0,$$

և, հետևաբար, $e = x^n \in Q'$, $x^{-1} = x^{n-1} \in Q'$: Այսպիսով $Q'(\circ)$-ը խումբ է: □

Հատկություն 18.11: *$Q(\circ)$ խմբի կամայական $a \in Q$ տարրի համար,*

$$(a) = \{a^m |\, m \in \mathbb{Z}\}$$

ենթաբազմությունը կլինի ենթախումբ, որը կոչվում է $Q(\circ)$ խմբի a **տարրով ծնված միածին ենթախումբ**, *իսկ a տարրը կոչվում է միածին ենթախմբի* **ծնիչ** *կամ* **ծնորդ** *տարր:*

Ապացուցում: $(a) \subseteq Q$ ոչ դատարկ ենթաբազմությունը բավարարում է ենթախումբ լինելու պայմանին (հատկություն 18.5), որովհետև եթե $x, y \in (a)$, ապա $x = a^{m_1}$, $y = a^{m_2}$, $m_1, m_2 \in \mathbb{Z}$ և

$$x \circ y^{-1} = a^{m_1} \circ (a^{m_2})^{-1} = a^{m_1} \circ a^{-m_2} = a^{m_1+(-m_2)} = a^{m_1-m_2} \in (a) : \; \square$$

Հնարավոր են հետևյալ երկու դեպքերը.

I) $Q(\circ)$ խմբի $a \in Q$ տարրի բոլոր ամբողջ աստիճանները զույգ առ զույգ միմյանցից տարբեր են, այսինքն՝

$$m \neq n \longrightarrow a^m \neq a^n, \quad m, n \in \mathbb{Z};$$

Այս դեպքում, a տարրը կոչվում է **անվերջ կարգ ունեցող** կամ **անվերջ կարգանի** և գրվում է $|a| = \infty$: Այնուհետև, այս դեպքում, (a) միածին ենթախումբը կլինի անվերջ խումբ և $(a) = (b) \leftrightarrow b = a$ կամ $b = a^{-1}$, որտեղ $b \in Q$: Իրոք, եթե $H = (a)$, ապա ակնհայտ է, որ $H = (a^{-1})$: Եվ հակառակը, եթե $H = (a) = (b)$, ապա $a = b^m$ և $b = a^n$, հետևաբար $a = (a^n)^m = a^{nm}$, որտեղից $nm = 1$ և $n = \pm 1$, այսինքն՝ $b = a^{\pm 1}$:

II) Գոյություն ունեն այնպիսի $m \neq n$ ամբողջ թվեր, որ $a^m = a^n$: Դիցուք $m > n$: Հետևաբար,

$$a^m \circ a^{-n} = a^n \circ a^{-n},$$

$$a^{m-n} = a^0,$$

$$a^q = e,$$

որտեղ $q \in \mathbb{Z}$, $q > 0$: Այս դեպքում $Q(\circ)$ խմբի $a \in Q$ տարրը կոչվում է **վերջավոր կարգ ունեցող** կամ **վերջավոր կարգանի**, իսկ այն ամենափոքր ամբողջ և դրական q թիվը, որի համար $a^q = e$, կոչվում է a **տարրի** (վերջավոր) **կարգ** և նշանակվում է՝ $q = |a|$ կամ $q = o(a)$ (order բառից):

Այսպիսով, n ամբողջ և դրական թիվը կոչվում է $Q(\circ)$ խմբի a տարրի կարգ, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա) $a^n = e$,

բ) $a^m = e, m > 0, m \in \mathbb{Z} \longrightarrow m \geqslant n$:

Օրինակ, $\mathbb{Z}(+)$ խմբի յուրաքանչյուր ոչ զրոյական տարր կլինի անվերջ կարգանի: Խմբի միավորի կարգը հավասար է 1-ի՝ $|e| = 1$: Եվ հակառակը, եթե խմբի մեջ $|a| = 1$, ապա $a^1 = e$, այսինքն՝ $a = e$: Վերջավոր խմբի կամայական տարր կլինի վերջավոր կարգանի:

Խումբը կոչվում է **պարբերական**, եթե նրա յուրաքանչյուր տարր ունի վերջավոր կարգ: Դիցուք p-ն պարզ թիվ է; Պարբերական խումբը կոչվում է p**-խումբ**, եթե նրա յուրաքանչյուր տարրի կարգ հավասար է p-ի որևէ աստիճանի:

Խումբը կոչվում է **առանց ոլորման**, եթե նրա միավորից տարբեր յուրաքանչյուր տարր անվերջ կարգանի է:

$Q(\circ)$ խումբը կոչվում է **միածին (կամ ցիկլային) խումբ**, եթե այն համընկնում է իր միածին ենթախմբերից որևէ մեկի հետ, այսինքն՝ գոյություն ունի այնպիսի $a \in Q$ տարր, որ $Q = (a)$: Այդ դեպքում, $a \in Q$ տարրը կոչվում է $Q(\circ)$ **միածին խմբի ծնիչ** կամ **ծնորդ** տարր: Քանի որ $(a) \subseteq Q$, ապա այստեղ պահանջվում է հակառակ ներդրումը՝ $Q \subseteq (a)$, այսինքն՝ Q բազմության յուրաքանչյուր $z \in Q$ տարր ունի $z = a^m$, $m \in \mathbb{Z}$, ներկայացումը:

Խումբը կոչվում է **քվազիմիածին** (կամ քվազիցիկլային), եթե այն միածին չէ, սակայն նրա իրենից տարբեր յուրաքանչյուր ենթախումբ միածին է:

Օրինակ, $\mathbb{Z}(+)$, $n\mathbb{Z}(+)$, $\mathbb{Z}_n(+)$, կոմպլեքս թվերի $\sqrt[n]{1}\,(\cdot)$ խմբերը միածին խմբեր են, որովհետև $\mathbb{Z} = (1)$, $n\mathbb{Z} = (n)$, $\mathbb{Z}_n = ([1])$ և $\sqrt[n]{1} = (\varepsilon_1)$, որտեղ $\varepsilon_1 = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$: Հետևաբար, յուրաքանչյուր n բնական թվի համար գոյություն ունի n-րդ կարգի միածին խումբ, որտեղ ծնիչ տարրի կարգը հավասար է n-ի:

Ակնհայտ է, որ միածին խմբերն աբելյան են, որովհետև եթե $x, y \in Q = (a)$, ապա $x = a^{m_1}$, $y = a^{m_2}$ և $x \circ y = a^{m_1} \circ a^{m_2} = a^{m_1+m_2} = a^{m_2+m_1} = a^{m_2} \circ a^{m_1} = y \circ x$: Սակայն հակառակը ճիշտ չէ, որովհետև գոյություն ունի չորս տարրանի աբելյան խումբ, որը միածին չէ: Ակնհայտ է նաև, որ միածին խումբը վերջավոր է կամ հաշվելի:

Հատկություն 18.12: *Եթե $Q(\circ)$ խմբի a տարրն ունի վերջավոր կարգ՝ $|a| = n$, ապա $a^0 = e, a, a^2, \ldots, a^{n-1}$ հաջորդականության տարրերը զույգ առ զույգ միմյանցից տարբեր են և*

$$(a) = \left\{e, a, a^2, \ldots, a^{n-1}\right\};$$

Մասնավորապես, տարրի կարգը հավասար է իրենով ծնված միածին ենթախմբի կարգին և $x^n = e$ կամայական $x \in (a)$ տարրի համար, եթե $|a| = n$:

Ապացուցում: Եթե $a^i = a^j$, որտեղ $0 \leqslant i < j < n$, ապա $0 < j - i < n$ և $a^{j-i} = e$, որը հակասում է տրված $|a| = n$ պայմանին:

Միածին ենթախմբի սահմանումից բխում է $\left\{e, a, a^2, \ldots, a^{n-1}\right\} \subseteq (a)$ ներդրումը: Ապացուցենք հակառակ ներդրումը՝ $(a) \subseteq \left\{e, a, a^2, \ldots, a^{n-1}\right\}$:

Եթե $x \in (a)$, ապա $x = a^m$, $m \in \mathbb{Z}$: Թեորեմ 1.1-ի համաձայն՝ $m = nq + r$, որտեղ $0 \leqslant r < n$: Հետևաբար,

$$x = a^m = a^{nq+r} = a^{nq} \circ a^r = (a^n)^q \circ a^r = e^q \circ a^r = e \circ a^r =$$

$$= a^r \in \left\{e, a, a^2, \ldots, a^{n-1}\right\}:$$

Ի վերջո, տեղի ունի $x^n = e$ հավասարությունը՝ կամայական $x = a^i$ տարրի համար, որովհետև

$$x^n = \left(a^i\right)^n = a^{in} = (a^n)^i = e^i = e: \qquad \square$$

18.4.2. Խմբի տարրի կարգի հիմնական հատկությունները: Հետևյալ արդյունքը հանդիսանում է լեմմ 9.1-ի և հատկություն 15.14-ի ընդհանրացումը:

Հատկություն 18.13: *Եթե $Q(\circ)$ խմբի մեջ՝ $a^m = e$, $m \in \mathbb{Z}$, ապա m-ը բաժանվում է a-ի կարգի վրա՝ $m/\,|a|$:*

Ապացուցում: Դիցուք $|a| = n$ և $m = nq + r$, որտեղ $0 \leqslant r < n$: Եթե $r \neq 0$, ապա $0 < r < n$, $r = m - nq$ և

$$a^r = a^{m-nq} = a^m \circ a^{-nq} = e \circ (a^n)^{-q} = e \circ e = e,$$

որը հակասում է $|a| = n$ պայմանին: Հետևաբար, $r = 0$ և $m = nq$: □

Հետևյալ արդյունքը հանդիսանում է հատկություն 15.15-ի ընդհանրացումը:

Հատկություն 18.14*: Եթե $Q(\circ)$ խմբի մեջ $|a| = n$, ապա*

$$\left|a^k\right| = \frac{n}{(n,k)}, \quad k \in \mathbb{Z} :$$

Ապացուցում: Ստուգենք տարրի կարգի սահմանման երկու պայմանները.

ա) $\left(a^k\right)^{\frac{n}{(n,k)}} = (a^n)^{\frac{k}{(n,k)}} = e$;

բ) Եթե $\left(a^k\right)^m = e$, $m > 0$, $m \in \mathbb{Z}$, ապա $a^{km} = e$ և համաձայն նախորդ հատկության՝ $km = nq$, $q \in \mathbb{Z}$: Եթե $d = (n,k)$, ապա $\left(\frac{n}{d}, \frac{k}{d}\right) = 1$ (հատկություն 3.1) և $\frac{k}{d}m = \frac{n}{d}q$ հավասարությունից, համաձայն հատկություն 3.4-ի, կունենանք $m / \frac{n}{d}$ պայմանը, որտեղից էլ բխում է $m \geqslant \frac{n}{d} = \frac{n}{(n,k)}$ անհավասարությունը: □

Հետևություն 18.5: *Եթե $Q(\circ)$ խմբի մեջ՝ $|a| = n$, ապա $|a^k| = n \longleftrightarrow (n,k) = 1$: Մասնավորապես, n-րդ կարգի վերջավոր միածին խմբի բոլոր ծնիչ տարրերի թիվը հավասար է $\varphi(n)$-ի, որտեղ φ-ն էյլերի ֆունկցիան է:* □

Հետևյալ արդյունքը հանդիսանում է թեորեմ 15.4-ի ընդհանրացումը:

Թեորեմ 18.16*: Եթե $Q(\circ)$ խմբի $a, b \in Q$ տարրերի (վերջավոր) կարգերը փոխադարձաբար պարզ են և $a \circ b = b \circ a$, ապա*

$$|a \circ b| = |a| \cdot |b| ,$$

$$(a \circ b) = (a) \circ (b)$$

և

$$X_{a \circ b} = X_a \circ X_b ,$$

որտեղ X_c-ն (c) վերջավոր միածին ենթախմբի բոլոր ծնիչ տարրերի բազմությունն է:

*Մասնավորապես, $\varphi(k \cdot t) = \varphi(k) \cdot \varphi(t)$, **եթե** $(k,t) = 1$ (նորից ստանում ենք Էյլերի φ ֆունկցիայի արտադրյալային հատկությունը):*

Ապացուցում: Նշանակենք՝ $|a| = k$, $|b| = t$ և ապացուցենք $|a \circ b| = k \cdot t$ հավասարությունը՝ ելնելով տարրի կարգի սահմանումից: Համաձայն $a \circ b = b \circ a$ պայմանի, կունենանք՝

ա) $(a \circ b)^{kt} = \underbrace{(a \circ b) \circ (a \circ b) \circ \cdots \circ (a \circ b)}_{kt} = \underbrace{a \circ \cdots \circ a}_{kt} \circ \underbrace{b \circ \cdots \circ b}_{kt} =$
$= a^{kt} \circ b^{kt} = \left(a^k\right)^t \circ \left(b^t\right)^k = e \circ e = e$:

Որպեսզի ստուգենք տարրի կարգի սահմանման

բ) $(a \circ b)^m = e$, $m > 0$, $m \in \mathbb{Z} \longrightarrow m \geqslant k \cdot t$
պայմանը, նախ ապացուցենք

$$(a) \cap (b) = \{e\}$$

հավասարությունը:

Եթե $c \in (a) \cap (b)$, ապա $c \in (a)$, $c \in (b)$ և $c = a^i$, $c = b^j$, որտեղ $i, j \in \mathbb{Z}$: Հետևաբար,

$$c^k = \left(a^i\right)^k = a^{ik} = \left(a^k\right)^i = e^i = e,$$

$$c^t = \left(b^j\right)^t = b^{jt} = \left(b^t\right)^j = e^j = e :$$

Այստեղից, համաձայն հատկություն 18.13-ի՝ $k/\,|c|$ և $t/\,|c|$: Բայց քանի որ $(k,t) = 1$, ապա $|c| = 1$ և $c = e$:

Ստուգենք բ) պայմանը: Քանի որ $a \circ b = b \circ a$, ապա $(a \circ b)^m = a^m \circ b^m$ և $(a \circ b)^m = e \to a^m \circ b^m = e \to a^m = b^{-m} \in (a) \cap (b) = \{e\} \to a^m = e$, $b^{-m} = e = b^m$, որտեղից, հատկություն 18.13-ի համաձայն, $m/\,k$ և $m/\,t$, այսինքն՝ m-ը k և t բնական թվերի ընդհանուր բազմապատիկն է: Ուստի (հետևություն 4.3), $m/\,[k,\ t]$, որտեղ $[k,t] = k \cdot t$ (հետևություն 4.4), և $m \geqslant k \cdot t$:

Այնուհետև, քանի որ $|(a)| = |a| = k$ և $|(b)| = |b| = t$, ապա $|(a) \circ (b)| \leqslant k \cdot t$, որտեղ

$$(a) \circ (b) = \{x \circ y \mid x \in (a),\, y \in (b)\} :$$

Սակայն՝ $|(a \circ b)| = |a \circ b| = |a| \cdot |b| = k \cdot t$ և $(a \circ b) \subseteq (a) \circ (b)$, քանի որ $a \circ b = b \circ a$: Հետևաբար, $(a \circ b) = (a) \circ (b)$: Եթե X_a-ով նշանակենք

(a) միածին ենթախմբի բոլոր ծնիչ տարրերի բազմությունը, այսինքն՝ $X_a = \{x \in (a) \mid \ (x) = (a)\} = \{x \in (a) \mid \ |x| = k\}$, ապա տեղի կունենա նաև հետևյալ հավասարությունը՝

$$X_a \circ X_b = X_{a \circ b} \ ,$$

որտեղ $|X_a \circ X_b| = |X_a \times X_b|$: Իրոք, նախ նկատենք, որ $X_a \circ X_b \subseteq X_{a \circ b}$, որովհետև, եթե $u \in X_a$ և $v \in X_b$, ապա $u \circ v \in X_a \circ X_b \subseteq (a) \circ (b) = (a \circ b)$, $|u| = k$, $|v| = t$, $u \circ v = v \circ u$ և, հետևաբար, $|u \circ v| = |u| \cdot |v| = k \cdot t$, այսինքն՝ $(u \circ v) = (a \circ b)$ և $u \circ v \in X_{a \circ b}$:

Ապացուցենք հակառակ ներդրումը՝ $X_{a \circ b} \subseteq X_a \circ X_b$: Եթե $w \in X_{a \circ b} \subseteq (a \circ b) = (a) \circ (b)$, ապա $w = x \circ y$, որտեղ $x \in (a)$ և $y \in (b)$: Բավական է այժմ ապացուցել, որ $|x| = k$ և $|y| = t$: Ենթադրելով հակառակը, կստանանք հակասություն: Իրոք, $|x| = k' \leqslant k$, $|y| = t' \leqslant t$ ու

$$w^{k't'} = (x \circ y)^{k't'} = x^{k't'} \circ y^{k't'} = \left(x^{k'}\right)^{t'} \circ \left(y^{t'}\right)^{k'} = e \ :$$

Այժմ, եթե $k' \leqslant k$ և $t' \leqslant t$ անհավասարություններից գոնե մեկը լինի խիստ, ապա ստացված $w^{k't'} = e$ հավասարությունը կհակասի $|w| = k \cdot t$ պայմանին:

Մնում է նկատել, որ $\psi : (u, v) \to u \circ v$ համապատասխանությունը փոխմիարժեք (բիեկտիվ) արտապատկերում է՝ $X_a \times X_b \to X_a \circ X_b$, այսինքն՝ $|X_a \circ X_b| = |X_a \times X_b|$: Հետևաբար, $|X_{a \circ b}| = |X_a \circ X_b| = |X_a| \cdot |X_b|$ և, օգտվելով նախորդ հետևությունից, ստանում ենք $\varphi(k \cdot t) = \varphi(k) \cdot \varphi(t)$ հավասարությունը: □

Հետևություն 18.6*: Եթե $Q(\circ)$ խմբի $a, b \in Q$ տարրերն ունեն վերջավոր կարգեր, $a \circ b = b \circ a$ և*

$$(a) \cap (b) = \{e\},$$

ապա $a \circ b$ արտադրյալի կարգը հավասար է a և b տարրերի կարգերի ամենափոքր ընդհանուր բազմապատիկին՝

$$|a \circ b| = [|a|, |b|] \ : \qquad \square$$

Սակայն այս բանաձևը առանց միածին ենթախմբերի հատմանը վերաբերող պայմանի, ընդհանուր դեպքում տեղի չունի (նույնիսկ աբելյան խմբերում): Օրինակ, 10-րդ կարգի $Q = (a)$ միածին խմբում՝

$|a| = |a^3| = |a^7| = |a^9| = 10$ (հետևություն 18.5), սակայն (հատկություն 18.14)՝

$$\left|a \circ a^3\right| = \left|a^4\right| = \frac{10}{(10,4)} = \frac{10}{2} = 5 \neq [10,10] :$$

Այս տեսակետից հետաքրքրական է հետևյալ արդյունքը, որն ունի նաև օգտակար կիրառություններ:

Հատկություն 18.15: *$Q(\circ)$ աբելյան խմբի վերջավոր կարգեր ունեցող ցանկացած $a, b \in Q$ տարրերի համար գոյություն ունի վերջավոր կարգ ունեցող այնպիսի $c \in Q$ տարր, որ $|c| = [|a|, |b|]$:*

Ապացուցում: Դիցուք $|a| = k$ և $|b| = t$: Եթե $(k,t) = 1$, ապա $c = a \circ b$ (համաձայն թեորեմ 18.16-ի): Ընդհանուր դեպքում, օգտվում ենք հետևություն 6.3-ից, որի համաձայն գոյություն ունեն k, t բնական թվերի այնպիսի

$$k = m_0 \cdot m_1,$$

և

$$t = n_0 \cdot n_1$$

վերլուծություններ, որ $(m_0, n_0) = 1$, իսկ $[k,t] = m_0 \cdot n_0$: Որոշենք a^{m_1} և b^{n_1} տարրերի կարգերը՝ համաձայն հատկություն 18.14-ի.

$$|a^{m_1}| = \frac{k}{(k, m_1)} = \frac{k}{m_1} = m_0,$$

$$|b^{n_1}| = \frac{t}{(t, n_1)} = \frac{t}{n_1} = n_0 :$$

Այսպիսով, աբելյան խմբի a^{m_1} և b^{n_1} տարրերի կարգերը փոխադարձաբար պարզ են և համաձայն թեորեմ 18.16-ի՝

$$|a^{m_1} \circ b^{n_1}| = |a^{m_1}| \cdot |b^{n_1}| = m_0 \cdot n_0 = [k,t] : \qquad \square$$

18.4.3. Միածին խմբեր: Լագրանժի թեորեմը միածին խմբերում: Նախ նկարագրենք միածին խմբերն իզոմորֆիզմի ճշտությամբ:

Լեմմ 18.6: *Միևնույն կարգի (հզորության) ցանկացած երկու միածին խմբեր իզոմորֆ են: Հետևաբար, յուրաքանչյուր անվերջ միածին խումբ իզոմորֆ է $\mathbb{Z}(+)$ միածին խմբին, իսկ n-րդ կարգի յուրաքանչյուր վերջավոր միածին խումբ իզոմորֆ է $\mathbb{Z}_n(+)$ միածին խմբին:*

Ապացուցում: Եթե $Q = (a)$, $Q' = (b)$ և $|Q| = |Q'|$, ապա հնարավոր է երկու դեպք: 1) $|Q| = |Q'| = n \geqslant 1$: Այս դեպքում`

$$Q = \left\{e, a, \ldots, a^{n-1}\right\},$$

$$Q' = \left\{e', b, \ldots, b^{n-1}\right\}$$

և $\varphi : a^i \to b^i$, $i = 0, 1, \ldots, n-1$, արտապատկերումը կլինի որոնելի իզոմորֆիզմը: 2) $|Q| = |Q'| = \infty$: Այս դեպքում`

$$Q = \left\{a^i \,|i \in \mathbb{Z}\right\}, \quad \text{որտեղ } a^i \neq a^j, \text{ եթե } i \neq j,$$

$$Q' = \left\{b^i \,|i \in \mathbb{Z}\right\}, \quad \text{որտեղ } b^i \neq b^j, \text{ եթե } i \neq j,$$

և $\varphi : a^i \to b^i$, $i \in \mathbb{Z}$, արտապատկերումը կլինի իզոմորֆիզմ: □

Օրինակ, $\sqrt[n]{1} \simeq \mathbb{Z}_n$, $n\mathbb{Z} \simeq \mathbb{Z}$ ցանկացած n բնական թվի համար: Հետևաբար, $n\mathbb{Z} \simeq m\mathbb{Z}$ ցանկացած n, m բնական թվերի համար:

Այժմ ներմուծենք խմբի մաքսիմալ ենթախմբի գաղափարը: Դիցուք $Q(\circ)$-ը կամայական խումբ է: $H \leqslant Q$ ենթախումբը կոչվում է **մաքսիմալ** $Q(\circ)$ **խմբում**, եթե $H \neq Q$ և H-ը հնարավոր չէ ընդգրկել իրենից և Q-ից տարբեր որևէ ենթախմբում, այսինքն`

$$H \leqslant H' \leqslant Q \longrightarrow H' = H \text{ կամ } H' = Q:$$

Ակնհայտ է, որ առնվազն երկու տարրանի ցանկացած վերջավոր խումբ օժտված է որևէ մաքսիմալ ենթախմբով: Իրոք, եթե այդպիսի $Q(\circ)$ խմբի $H = \{e\}$ ենթախումբը մաքսիմալ չէ, ապա գոյություն կունենա այնպիսի $Q' \leqslant Q$ ենթախումբ, որ $H \neq Q' \neq Q$: Եթե Q' ենթախումբը մաքսիմալ չէ $Q(\circ)$ խմբում, ապա գոյություն կունենա այնպիսի $Q'' \leqslant Q$ ենթախումբ, որ $Q' \leqslant Q''$ և $Q' \neq Q'' \neq Q$: Եվ այսպես շարունակ . . . : Քանի որ սկզբնական $Q(\circ)$ խումբը վերջավոր է, ապա այս դատողությունները վերջավոր թվով քայլերից հետո կընդհատվեն և արդյունքում կստանանք $Q(\circ)$ վերջավոր խմբի որևէ մաքսիմալ ենթախումբ: Սակայն, ընդհանուր դեպքում, խմբի մաքսիմալ ենթախումբը միարժեքորեն չի որոշվում: Օրինակ, 4-րդ կարգի ոչ միածին խումբն ունի 3 հատ երկրորդ կարգի մաքսիմալ ենթախմբեր, իսկ 6-րդ կարգի $\mathbb{Z}_6(+)$ միածին խումբն օժտված է 2-րդ և 3-րդ կարգի մաքսիմալ ենթախմբերով: Նույնը վերաբերվում է նաև S_3 սիմետրիկ խմբին: Մինչդեռ $\mathbb{Z}_2(+)$, $\mathbb{Z}_3(+)$, $\mathbb{Z}_4(+)$, $\mathbb{Z}_5(+)$, $\mathbb{Z}_7(+)$, $\mathbb{Z}_8(+)$, $\mathbb{Z}_9(+)$ միածին խմբերն օժտված են միակ մաքսիմալ ենթախմբերով:

Թեորեմ 18.17: *Միածին խմբի կամայական ենթախումբ ևս միածին խումբ է:*

Ապացույց: Դիցուք $Q(\circ)$-ը միածին խումբ է ծնված a տարրով՝ $Q = (a)$ և դիցուք $H \leqslant Q$: Պահանջվում է ապացուցել, որ գոյություն ունի այնպիսի $b \in H$ տարր, որ $H = (b)$: Հնարավոր են հետևյալ երկու դեպքերը:

ա) $H = \{e\} = (e)$ և $b = e$:

բ) $H \neq \{e\}$: Այս դեպքում, գոյություն կունենա այնպիսի $z \in H$ տարր, որ $z \neq e$: Հետևաբար, $z = a^k$, $k \neq 0$: Այստեղ կարող ենք նաև ենթադրել, որ $k > 0$, որովհետև, հակառակ դեպքում, կդիտարկեինք $z^{-1} = a^{-k} \in H$ տարրը, որտեղ $-k > 0$: Նշանակենք k_0-ով այն ամենափոքր ամբողջ և դրական թիվը, որի համար $a^{k_0} \in H$ և ապացուցենք, որ $b = a^{k_0}$, այսինքն՝ $H = \left(a^{k_0}\right)$:

Քանի որ $a^{k_0} \in H$, ապա $\left(a^{k_0}\right) \subseteq H$: Ստուգենք $H \subseteq \left(a^{k_0}\right)$ ներդրումը: Եթե $z \in H \leqslant Q = (a)$, ապա $z = a^m$, որտեղ $m \in \mathbb{Z}$, $m = k_0 q + r$, $0 \leqslant r < k_0$: եթե այստեղ $r \neq 0$, ապա $0 < r < k_0$, $r = m - k_0 q$ և

$$a^r = a^{m-k_0 q} = a^m \circ \left(a^{k_0}\right)^{-q} \in H\,,$$

որը հակասում է k_0-ի ընտրությանը: Հետևաբար, $r = 0$, $m = k_0 q$ և

$$z = a^m = a^{k_0 q} = \left(a^{k_0}\right)^q \in \left(a^{k_0}\right) : \qquad \square$$

Օրինակ, $\mathbb{Z}(+)$, $n\mathbb{Z}(+)$, $\mathbb{Z}_n(+)$ և $\sqrt[n]{1}(\cdot)$ խմբերի բոլոր ենթախմբերը կլինեն միածին խմբեր:

Թեորեմ 18.18 (Լագրանժ): *1) Վերջավոր միածին խմբի կարգը բաժանվում է իր յուրաքանչյուր ենթախմբի կարգի վրա: Վերջավոր խմբի կարգը բաժանվում է իր յուրաքանչյուր միածին ենթախմբի կարգի վրա:*

2) Եվ հակառակը, եթե վերջավոր միածին խմբի կարգը բաժանվում է որևէ m բնական թվի վրա, ապա այդ խմբի մեջ գոյություն ունի m կարգի ենթախումբ:

3) Վերջավոր միածին խմբի ենթախումբն իր կարգով որոշվում է միարժեքորեն:

4) Եթե վերջավոր միածին խմբի կարգը հավասար է p^k-ի, որտեղ p-ն պարզ թիվ է, ապա այն օժտված է միակ մաքսիմալ ենթախմբով, որի կարգը հավասար է p^{k-1}-ի, $k \geqslant 1$:

Ապացուցում: 1) Դիցուք $Q = (a)$, $|Q| = n$ և $H \leqslant Q$: Պահանջվում է ապացուցել, որ $^n/_{|H|}$: Հատկություն 18.12-ի համաձայն՝ $|a| = n$ և $a^n = e$: Հնարավոր են հետևյալ երկու դեպքերը.

ա) $H = \{e\}$, $|H| = 1$ և $^n/_{|H|}$;

բ) $H \neq \{e\}$ և, ըստ նախորդ թեորեմի, $H \leqslant Q$ ենթախումբը կլինի միածին խումբ, որի համար որպես ծնիչ տարր կարելի է ընտրել $b = a^{k_0} \in H$ տարրը, որտեղ k_0-ն այն ամենափոքր ամբողջ և դրական թիվն է, որի համար $a^{k_0} \in H$: Նախ ապացուցենք, որ n-ը բաժանվում է k_0-ի վրա: Դիցուք $n = k_0 q + r$, $0 \leqslant r < k_0$: Եթե այստեղ $r \neq 0$, ապա $0 < r < k_0$, $r = n - k_0 q$ և

$$a^r = a^{n-k_0q} = a^n \circ \left(a^{k_0}\right)^{-q} = e \circ \left(a^{k_0}\right)^{-q} = \left(a^{k_0}\right)^{-q} \in H,$$

որը հակասում է k_0-ի ընտրությանը: Հետևաբար, $r = 0$ և $n = k_0 q$: Այնուհետև, հատկություն 18.14-ի համաձայն,

$$|H| = \left|a^{k_0}\right| = \frac{n}{(n, k_0)} = \frac{n}{k_0} = q :$$

1) պնդման առաջին մասն ապացուցված է:

Այստեղ նկատենք նաև, որ բ) դեպքում՝

$$H = (b) = \left(a^{k_0}\right) = \left(a^{\frac{n}{q}}\right),$$

որտեղ $n = |Q|$, իսկ $q = |H|$: Ըստ որում, այս բանաձևը ճիշտ է նաև ա) դեպքում, երբ $|H| = 1$: Այսպիսով, եթե $Q(\circ)$-ը n-րդ կարգի վերջավոր միածին խումբ է՝ ծնված $a \in Q$ տարրով, իսկ $H \leqslant Q$ ենթախմբի կարգը հավասար է q-ի, ապա H միածին խումբը որոշվում է հետևյալ կերպ՝

$$H = \left(a^{\frac{n}{q}}\right) :$$

Ուստի, ապացուցված է նաև թեորեմի 3) պնդումը:

Այժմ ապացուցենք 1) պնդման երկրորդ մասը: Դիցուք $Q(\circ)$-ը կամայական վերջավոր խումբ է, $|Q| = n$, իսկ նրա $H \leqslant Q$ ենթախումբը միածին ենթախումբ է՝ $H = (a)$ և $|H| = |a| = k$: Հետևաբար,

$$H = \left\{e, a, a^2, \ldots, a^{k-1}\right\} :$$

Եթե $x_1 \in Q$ և $x_1 \notin H$, ապա $H \cap x_1 H = \emptyset$, որտեղ

$$x_1 H = \left\{x_1, x_1 \circ a, x_1 \circ a^2, \ldots, x_1 \circ a^{k-1}\right\} :$$

Ակնհայտ է, որ $|x_1H| = |H| = k$: Եթե գոյություն ունի այնպիսի $x_2 \in Q$ տարր, որ $x_2 \notin H \cup x_1H$, ապա H և x_1H բազմություններից յուրաքանչյուրը չի հատվի

$$x_2H = \left\{x_2, x_2 \circ a, x_2 \circ a^2, \ldots, x_2 \circ a^{k-1}\right\}$$

բազմության հետ: Քանի որ Q-ն վերջավոր է, ապա վերջավոր թվով այդպիսի քայլերից հետո կունենանք՝

$$Q = H \cup x_1H \cup x_2H \cup \cdots \cup x_{s-1}H,$$

որտեղ H, x_1H, x_2H, ..., $x_{s-1}H$ բազմությունները զույգ առ զույգ չեն հատվում և դրանցից յուրաքանչյուրի կարգը հավասար է k-ի: Հետևաբար՝

$$n = |Q| = |H| + |x_1H| + |x_2H| + \cdots + |x_{s-1}H| = \underbrace{k + k + k + \cdots + k}_{s} = k \cdot s\,,$$

այսինքն՝ վերջավոր $Q(\circ)$ խմբի n կարգը բաժանվում է իր յուրաքանչյուր միածին ենթախմբի k կարգի վրա:

Ապացուցենք 2)-ը: Դիցուք $Q = (a)$, $|Q| = n = m \cdot t$ և $H = (a^t)$: Կունենանք՝

$$|H| = \left|a^t\right| = \frac{n}{(n,t)} = \frac{n}{t} = m\,:$$

Ապացուցենք 4)-ը: Դիցուք $|Q| = n = p^k$, որտեղ p-ն պարզ թիվ է: Քանի որ p^k-ի բոլոր բնական բաժանարարներն են $1, p, p^2, \ldots, p^{k-1}, p^k$ թվերը, ապա, ըստ 2) և 3) պնդումների, գոյություն կունենա միարժեքորեն որոշվող այնպիսի $H_i \leqslant Q$ ենթախումբ, որ $|H_i| = p^i$, որտեղ $i = 0, 1, \ldots, k$: Ըստ որում, 1) պնդման շնորհիվ, նշված ենթախմբերով սպառվում են $Q(\circ)$ խմբի բոլոր ենթախմբերը և

$$\{e\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{k-1} \leqslant H_k = Q\,:$$

Այսպիսով, $H_{k-1} \leqslant Q$ ենթախումբը կլինի $Q(\circ)$ խմբի միակ մաքսիմալ ենթախումբը, որն իր հերթին նաև պարունակում է $Q(\circ)$ խմբի Q-ից տարբեր բոլոր ենթախմբերը: $\square$

Թեորեմ 18.19: *Կոմպլեքս թվերի* $\mathbb{C}_{p^\infty}(\cdot)$ *խումբը, որտեղ* $\mathbb{C}_{p^\infty} = \bigcup\limits_{k=1}^{\infty} \sqrt[p^k]{1}$, *միածին չէ, սակայն նրա յուրաքանչյուր* $H \leqslant \mathbb{C}_{p^\infty}$ *ենթախումբ, որտեղ*

$\{1\} \neq H \neq \mathbb{C}_{p^\infty}$, *կլինի վերջավոր միածին խումբ և* $H = \sqrt[p^k]{1}$ *որևէ* $k \in \mathbb{N}$ *բնական թվի համար (*p*-ն պարզ թիվ է): Հետևաբար,* $\mathbb{C}_{p^\infty}(\cdot)$ *խումբը քվազիմիածին է:*

Ապացուցում: Եթե $g \in \mathbb{C}_{p^\infty} = \bigcup_{k=1}^{\infty} \mathbb{C}_{p^k}$, որտեղ $\mathbb{C}_{p^k} = \sqrt[p^k]{1}$ և $g \neq e$, ապա գոյություն կունենա այնպիսի $k \in \mathbb{N}$, որ $g \in \mathbb{C}_{p^k} \setminus \mathbb{C}_{p^{k-1}}$, որտեղ $\mathbb{C}_1 = \{1\}$: Այնուհետև, $(g) \subseteq \mathbb{C}_{p^k}$ և $\mathbb{C}_{p^\infty} \neq (g)$: Հետևաբար, $\mathbb{C}_{p^\infty}(\cdot)$ խումբը միածին չէ: Ըստ նախորդ թեորեմի, $\mathbb{C}_{p^{k-1}} \leqslant \mathbb{C}_{p^k}$ ենթախումբը կլինի $\mathbb{C}_{p^k}(\cdot)$ միածին խմբի (միակ) մաքսիմալ ենթախումբը և պարունակում է $\mathbb{C}_{p^k}$ խմբի $\mathbb{C}_{p^k}$-ից տարբեր բոլոր ենթախմբերը, իսկ $(g) \leqslant \mathbb{C}_{p^k}$ ենթախմբի համար ունենք՝ $(g) \nsubseteq \mathbb{C}_{p^{k-1}}$, քանի որ $g \notin \mathbb{C}_{p^{k-1}}$: Հետևաբար, $(g) = \mathbb{C}_{p^k}$: Այժմ կարելի է ապացուցել, որ $\mathbb{C}_{p^\infty}(\cdot)$ խումբը չունի իրենից տարբեր որևէ անվերջ ենթախումբ: Դիցուք $H \leqslant \mathbb{C}_{p^\infty}$ ենթախումբը անվերջ է: Այդ դեպքում, անվերջ թվով $g_i \in H$, $i \in \mathbb{N}$, տարրերի համապատասխան գոյություն կունենան անվերջ թվով այնպիսի k_i բնական թվեր, որ $g_i \in \mathbb{C}_{p^{k_i}} \setminus \mathbb{C}_{p^{k_i - 1}}$: Հետևաբար, $(g_i) = \mathbb{C}_{p^{k_i}}$ ու

$$H \supseteq \bigcup_{g_i \in H} (g_i) = \bigcup_{i=1}^{\infty} \mathbb{C}_{p^{k_i}} = \bigcup_{k=1}^{\infty} \mathbb{C}_{p^k} = \mathbb{C}_{p^\infty}$$

և $H = \mathbb{C}_{p^\infty}$:

Իսկ եթե $H \leqslant \mathbb{C}_{p^\infty}$ ենթախումբը վերջավոր է, ապա գոյություն կունենա այնպիսի $l \in \mathbb{N}$ բնական թիվ, որ $H \subseteq \mathbb{C}_{p^l}$ և նախորդ թեորեմի համաձայն՝ $H = \mathbb{C}_{p^k}$, որտեղ $k \leqslant l$: □

18.4.4. Վերջավոր խմբի միածին լինելու բավարար պայմաններ: Հետաքրքրական է նաև միածին խմբերի նկարագրության հետևյալ եղանակը, որն ունի նաև օգտակար կիրառություններ:

Թեորեմ 18.20*: Եթե* n*-րդ կարգի* $Q(\circ)$ *վերջավոր խմբում,* n*-ի յուրաքանչյուր* d *բնական բաժանարարի համար գոյություն ունի ամենաշատը մեկ հատ (այսինքն՝ կամ գոյություն չունի կամ գոյություն ունի ճիշտ* 1 *հատ)* d*-րդ կարգի* $H \leqslant Q$ *միածին ենթախումբ, ապա* $Q(\circ)$ *խումբը միածին է: Մասնավորապես, եթե վերջավոր խմբի կարգը հավասար է պարզ թվի, ապա այն միածին է:*

Ապացուցում: Նախ Q բազմության վրա սահմանենք հետևյալ համարժեքության հարաբերությունը.

$$a \sim b \longleftrightarrow (a) = (b):$$

Այստեղ՝ $[a] = \{x \in Q |\ x \sim a\}$ համարժեքության դասը կազմված է $(a) \leqslant Q$ միածին ենթախմբի բոլոր ծնիչ տարրերից: Եթե $|(a)| = d$, ապա համաձայն հետևություն 18.5-ի, $|[a]| = \varphi(d)$, որտեղ φ-ն էյլերի ֆունկցիան է: Դիցուք «$\sim$» համարժեքության զույգ առ զույգ միմյանց հետ չհատվող բոլոր համարժեքության դասերն են՝ $[a_1], [a_2], \ldots, [a_k]$: Հետևաբար (լեմմ 0.2)՝

$$Q = [a_1] \cup [a_2] \cup \cdots \cup [a_k],$$

$$|Q| = |[a_1]| + |[a_2]| + \cdots + |[a_k]|,$$

$$n = \varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_k),$$

որտեղ $|(a_i)| = d_i$ և, համաձայն թեորեմ 18.18-ի, n / d_i, $i = 1, 2, \ldots, k$: Եթե $d_1, d_2, \ldots, d_k$ բնական թվերով չսպառվեն n-ի բոլոր բնական բաժանարարները, ապա օգտվելով թեորեմ 9.7-ից, հանգում ենք հակասության՝

$$n = \varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_k) < \sum_{n/d, d>0} \varphi(d) = n:$$

Ուստի, $d_1, d_2, \ldots, d_k$ բնական թվերով սպառվում են n-ի բոլոր բնական բաժանարարները; Մասնավորապես, գոյություն կունենա այնպիսի $i \in \{1, \ldots, k\}$ համար, որ $d_i = n$, այսինքն՝ $|(a_i)| = n$ և հետևաբար, $(a_i) = Q$, այսինքն՝ $Q(\circ)$ խումբը միածին է:

Թեորեմի երկրորդ մասը բխում է այն փաստից, որ պարզ թիվն ունի ընդամենը երկու բնական բաժանարարներ՝ 1-ը և ինքը, որոնց համար թեորեմի պայմանն ակնհայտորեն տեղի ունի: □

Թեորեմ 18.21*: Եթե n-րդ կարգի $Q(\circ)$ վերջավոր խմբում, n-ի ցանկացած d բնական բաժանարարի համար $x^d = e$ հավասարման լուծումների քանակը չի գերազանցում d-ն, ապա $Q(\circ)$ խումբը միածին է:*

Ապացուցում: Եթե $Q(\circ)$ խմբում գոյություն ունենային d կարգի երկու միմյանցից տարբեր $H_1 \leqslant Q$ և $H_2 \leqslant Q$ միածին ենթախմբեր, ապա

$|H_1 \cup H_2| > d$: Հետևաբար, կամայական $a \in H_1 \cup H_2$ տարրի համար՝ $a \in H_1$ կամ $a \in H_2$; Երկու դեպքում էլ՝ $a^d = e$ (հատկություն 18.12), այսինքն՝ $x^d = e$ հավասարումն օժտված կլիներ d-ից շատ թվով լուծումներով: Հակասություն:

Մնում է օգտվել թեորեմ 18.20-ից:[18] □

18.5. Ձախ և աջ հարակից դասեր: Ենթախմբի նշիչ: Լագրանժի և Ֆերմայի թեորեմները վերջավոր խմբերում: Ինվարիանտ ենթախմբեր, քանորդ-խմբեր: Կոշիի թեորեմը վերջավոր աբելյան խմբերում

18.5.1. Տարրի ձախ և աջ հարակից դասեր ըստ ենթախմբի: Ենթախմբի ձախ և աջ նշիչների հավասարությունը: Լագրանժի և Ֆերմայի թեորեմները վերջավոր խմբերում: Դիցուք $Q(\circ)$-ը կամայական խումբ է, $H \leqslant Q$ և $a \in Q$: a տարրի ձախ և աջ **հարակից դասերը** ըստ $H \leqslant Q$ ենթախմբի համապատասխանաբար նշանակվում են aH-ով ու Ha-ով և սահմանվում են հետևյալ կերպ (Է. Գալուա, 1830 թ.)՝

$$aH = \{a \circ h|\ h \in H\},$$

$$Ha = \{h \circ a|\ h \in H\}:$$

aH (կամ Ha) հարակից դասի համար $a \in Q$ տարրը կոչվում է այդ դասի **ներկայացուցիչ**:

Օրինակ, $eH = H = He$, $hH = H = Hh$, $(a \circ h)H = aH$, $H(h \circ a) = Ha$ ցանկացած $h \in H$, $a \in Q$ տարրերի համար: Եթե $t \in aH$, ապա $tH = aH$, իսկ եթե $t \in Ha$, ապա $Ht = Ha$: Հետևաբար, միևնույն հարակից դասը կարող է ունենալ տարբեր ներկայացուցիչներ:

Հատկություն 18.16 (Հարակից դասերի հավասարության հայտանիշը):
1) $aH = bH \longleftrightarrow a^{-1} \circ b \in H$,
2) $Ha = Hb \longleftrightarrow a \circ b^{-1} \in H$,
որտեղ $a, b \in Q$, $H \leqslant Q$:

Ապացուցում: 1) Քանի որ $e \in H$, $a = a \circ e$, ապա $a \in aH$: Այնուհետև,

$$b \in bH = aH \longrightarrow b \in aH \longrightarrow b = a \circ h, \quad h \in H \longrightarrow a^{-1} \circ b = h \in H:$$

[18] Աբելյան խմբերի դեպքում, նույն արդյունքին կարելի է նաև հասնել օգտվելով հատկություն 18.16-ից:

Եվ հակառակը, եթե $a^{-1} \circ b \in H \leqslant Q$, ապա $a^{-1} \circ b = h \in H$, $b = a \circ h$, $a = b \circ h^{-1}$: Այս ներկայացումներից բխում են $aH \subseteq bH$ և $bH \subseteq aH$ ներդրումները: Իրոք,

$$x \in aH \longrightarrow x = a \circ h_1, \quad h_1 \in H \longrightarrow x = \left(b \circ h^{-1}\right) \circ h_1 = b \circ \left(h^{-1} \circ h_1\right) \in bH,$$

$$y \in bH \longrightarrow y = b \circ h_2, \quad h_2 \in H \longrightarrow y = (a \circ h) \circ h_2 = a \circ (h \circ h_2) \in aH :$$

2) հայտանիշն ապացուցվում է նույն եղանակով:

Հատկություն 18.17*: Եթե երկու ձախ (աջ) հարակից դասեր հատվում են, ապա դրանք համընկնում են, այսինքն՝*

$$aH \cap bH \neq \emptyset \longrightarrow aH = bH,$$

$$(Ha \cap Hb \neq \emptyset \longrightarrow Ha = Hb) :$$

Ապացույց: Եթե $aH \cap bH \neq \emptyset$, ապա գոյություն ունի $c \in aH \cap bH$: Այնուհետև,

$$c \in aH \cap bH \to c \in aH, \;\; c \in bH \to c = a \circ h_1, \;\; c = b \circ h_2, \;\; h_1, h_2 \in H \to$$

$$a \cdot h_1 = b \circ h_2 \to a^{-1} \circ b = h_1 \circ h_2^{-1} \in H;$$

Մնում է օգտվել նախորդ հատկությունից:

(Երկրորդ հատկությունն ապացուցվում է նույն եղանակով:) □

Հատկություն 18.18*:Երկու ձախ (աջ) հարակից դասեր կամ չեն հատվում կամ համընկնում են:*

Ապացույց: Բխում է նախորդ հատկությունից: □

Հատկություն 18.19*: $Q(\circ)$ խմբի յուրաքանչյուր տարր պատկանում է միարժեքորեն որոշվող որևէ ձախ (աջ) հարակից դասի՝ ըստ տված $H \leqslant Q$ ենթախմբի, այսինքն՝*

$$Q/_{H_l} = \{aH |\, a \in Q\}$$

և

$$Q/_{H_r} = \{Ha |\, a \in Q\}$$

բազմություններից յուրաքանչյուրը կազմում է Q բազմության տրոհում:

Ապացույց: Q բազմության յուրաքանչյուր $a \in Q$ տարրի համար՝ $a \in aH$ (և $a \in Ha$), որտեղ aH (և Ha) հարակից դասը որոշվում է միարժեքորեն՝ համաձայն հատկություն 18.17-ի: $\square$

$Q/_{H_l}$ բազմության հզորությունը (կարգը) կոչվում է $H \leqslant Q$ ենթախմբի **ձախ նշիչ** $Q(\circ)$ խմբում, իսկ $Q/_{H_r}$ բազմության հզորությունը (կարգը)՝ $H \leqslant Q$ ենթախմբի **աջ նշիչ** $Q(\circ)$ խմբում:

Լեմմ 18.7: *Ըստ $H \leqslant Q$ ենթախմբի բոլոր ձախ և աջ հարակից դասերն ունեն նույն հզորությունը (նույն քանակի տարրեր), այսինքն՝*

$$|aH| = |Ha| = |H|$$

ցանկացած $a \in Q$ տարրի համար:

Ապացույց: Սահմանելով $\mu_1 : H \to aH$ և $\mu_2 : H \to Ha$ արտապատկերումները հետևյալ կերպ՝

$$\mu_1(h) = a \circ h,$$

$$\mu_2(h) = h \circ a,$$

ստանում ենք բիեկտիվ (փոխմիարժեք) արտապատկերումներ: $\square$

Լեմմ 18.8: *Ցանկացած $Q(\circ)$ խմբում նրա յուրաքանչյուր $H \leqslant Q$ ենթախմբի ձախ և աջ նշիչները հավասար են՝ $\left|Q/_{H_l}\right| = \left|Q/_{H_r}\right|$, այդ պատճառով դրանցից յուրաքանչյուրը կոչվում է H ենթախմբի նշիչ տրված $Q(\circ)$ խմբում և սովորաբար նշանակվում է $(Q : H)$-ով կամ $|Q : H|$-ով:*

Ապացույց: Դիցուք $Q(\circ)$-ը կամայական խումբ է, իսկ $H \leqslant Q$: Սահմանելով $\mu : Q/_{H_r} \to Q/_{H_l}$ արտապատկերումը հետևյալ կերպ՝

$$\mu(Ha) = a^{-1}H, \quad a \in Q,$$

ստանում ենք բիեկտիվ արտապատկերում: Իրոք, μ արտապատկերումը սյուրեկտիվ է և ինյեկտիվ, որովհետև համաձայն հատկություն 18.16-ի, կունենանք՝

$$\mu(Ha) = \mu(Hb) \to a^{-1}H = b^{-1}H \to \left(a^{-1}\right)^{-1} \circ b^{-1} \in H \to$$

$$a \circ b^{-1} \in H \to Ha = Hb: \qquad \square$$

Թեորեմ 18.22 (Լագրանժ): *Վերջավոր խմբի կարգը հավասար է իր յուրաքանչյուր ենթախմբի կարգի և նրա նշիչի արտադրյալին: Մասնավորապես, վերջավոր խմբի կարգը բաժանվում է իր յուրաքանչյուր ենթախմբի կարգի և նշիչի վրա:*

Ապացուցում: Դիցուք $Q(\circ)$-ը վերջավոր խումբ է, $|Q| = n$, $H \leqslant Q$, $|H| = k$, $\left|{}^{Q}/_{H_l}\right| = t = \left|{}^{Q}/_{H_r}\right|$: Համաձայն հատկություն 18.19-ի՝

$$Q = H \cup a_1H \cup \cdots \cup a_{t-1}H,$$

որտեղ նշված ձախ հարակից դասերը զույգ առ զույգ չեն հատվում:

Օգտվելով լեմմ 18.7-ից, կունենանք՝

$$n = |Q| = |H| + |a_1H| + \cdots + |a_{t-1}H| = k \cdot t : \qquad \square$$

Հետևություն 18.7*: Վերջավոր խմբի կարգը բաժանվում է իր յուրաքանչյուր տարրի կարգի վրա:*

Ապացուցում: Տարրի կարգը հավասար է իրենով ծնված միածին ենթախմբի կարգին (հատկություն 18.12), իսկ ըստ թեորեմ 18.22-ի վերջավոր խմբի կարգը բաժանվում է իր յուրաքանչյուր ենթախմբի կարգի վրա: $\square$

Ձևակերպենք նաև հետևյալ արդյունքը՝ որպես հետևություն Լանգանժի ապացուցված թեորեմից, որի առաջին մասը հայտնի է թեորեմ 18.20-ից, իսկ երկրորդ մասը՝ հետևություն 18.5-ից:

Հետևություն 18.8*: Եթե վերջավոր խմբի կարգը հավասար է պարզ թվի, ապա այն միածին է և ծնվում է միավորից տարբեր իր յուրաքանչյուր տարրով:*

Ապացուցում: Դիցուք $Q(\circ)$-ը վերջավոր խումբ է և դիցուք $|Q| = p$: Քանի որ $p \geqslant 2$, ապա գոյություն ունի $a \in Q$, $a \neq e$: Տեղի ունի $Q = (a)$ հավասարությունը: Իրոք, եթե $Q \neq (a)$, ապա p պարզ թիվը, համաձայն թեորեմ 18.22-ի, կբաժանվի $m = |(a)| \neq 1, p$ բնական թվի վրա: Հակասություն: $\square$

Հետևյալ արդյունքը հանդիսանում է Պ. Ֆերմայի փոքր թեորեմի (հետևություն 9.1) ընդհանրացումը:

Հետևություն 18.9 (Պ. Ֆերմա): *n-րդ կարգի վերջավոր խմբի յուրաքանչյուր x տարրի համար՝ $x^n = e$:*

Ապացուցում: Դիցուք $|x| = k$: Հետևություն 18.7-ի համաձայն $n = k \cdot q$, $q \in \mathbb{N}$, և, հետևաբար,

$$x^n = x^{kq} = \left(x^k\right)^q = e^q = e :$$ □

Սակայն, ընդհանուր դեպքում, վերջավոր խմբի n կարգը $x^n = e$ նույնությանը բավարարող ամենափոքր բնական թիվը չէ: Օրինակ, 4-րդ կարգի ոչ միածին աբելյան խմբում տեղի ունի նաև $x^2 = e$ նույնությունը:

18.5.2. 12**-րդ կարգի** $\mathbb{A}_4$ **նշանափոխ խումբը չունի** 6**-րդ կարգի ենթախումբ:** Տեղի ունի հետևյալ արդյունքը:

Թեորեմ 18.23: *Եթե* $Q(\circ)$ *խմբում* $H \leqslant Q$ *ենթախմբի նշիչը հավասար է* 2*-ի, ապա* ${Q}/{H_\mathrm{l}} = {Q}/{H_\mathrm{r}}$ *և* $x^2 \in H$ *ցանկացած* $x \in Q$ *տարրի համար: Մասնավորապես,* 12*-րդ կարգի* $\mathbb{A}_4$ *նշանափոխ խմբում գոյություն չունի* 6*-րդ կարգի ենթախումբ:*

Ապացուցում: Եթե $\left|{Q}/{H_l}\right| = \left|{Q}/{H_r}\right| = 2$, ապա համաձայն հատկություն 18.19-ի՝

$${Q}/{H_l} = \{H,\ Q \setminus H\} = {Q}/{H_r} :$$

Այնուհետև, եթե $x \in H$, ապա $x^2 \in H \leqslant Q$: Դիցուք $x \notin H$, այսինքն՝ $x \in Q \setminus H = aH$, որտեղ $a \notin H$, հետևաբար՝ $x = a \circ h_1$, $h_1 \in H$: Եթե այս դեպքում՝ $x^2 \notin H$, ապա $x^2 \in Q \setminus H = aH$, այսինքն՝ $x^2 = a \circ h_2$, $h_2 \in H$: Ուստի,

$$x = x^{-1} \circ x^2 = h_1^{-1} \circ a^{-1} \circ a \circ h_2 = h_1^{-1} \circ h_2 \in H :$$

Հակասություն:

Այժմ ապացուցենք, որ զույգ տեղադրությունների $\mathbb{A}_4$ նշանափոխ խմբում գոյություն չունի այնպիսի $H \leqslant \mathbb{A}_4$ ենթախումբ, որ $|H| = 6$: Ենթադրենք հակառակը, որ այդպիսի $H \leqslant \mathbb{A}_4$ ենթախումբ գոյություն ունի: Ըստ թեորեմ 18.22-ի, այդպիսի H ենթախմբի նշիչը $\mathbb{A}_4$ խմբում կլինի հավասար՝ $\dfrac{|\mathbb{A}_4|}{|H|} = \dfrac{12}{6} = 2$: Հետևաբար, $x^2 \in H$ ցանկացած $x \in \mathbb{A}_4$ տարրի համար: Քանի որ, յուրաքանչյուր $\alpha = (i,j,k) = (i,j)(i,k) \in \mathbb{A}_4$, որտեղ զույգ առ զույգ միմյանցից տարբեր i, j, k թվերը պատկանում են $\{1,2,3,4\}$ բազմությանը և $\alpha^3 = \varepsilon$, ապա $\alpha = \varepsilon \cdot \alpha = \alpha^3 \cdot \alpha = \alpha^4 = \left(\alpha^2\right)^2 \in H$: Այսպիսով, 6 կարգ ունեցող H ենթախումբը կպարունակի հետևյալ 8 տեղադրությունները՝

$(1,2,3)$, $(1,4,2)$,
$(1,3,2)$, $(1,4,3)$,
$(1,2,4)$, $(2,3,4)$,
$(1,3,4)$, $(2,4,3)$:
Հակասություն: $\square$

Այսպիսով, թեորեմ 18.22-ի հակադարձումը տեղի չունի, այսինքն՝ եթե $Q(\circ)$ վերջավոր խմբի կարգը բաժանվում է m բնական թվի վրա, ապա այստեղից դեռևս չի բխում, որ $Q(\circ)$ խումբն օժտված է m կարգի $H \leqslant Q$ ենթախմբով:

18.5.3. Ինվարիանտ (կայուն) ենթախմբեր կամ նորմալ բաժանարարներ : Ինչպես տեսանք (լեմմ 18.8)՝ $\left|{}^{Q}/_{H_l}\right| = \left|{}^{Q}/_{H_r}\right|$ ցանկացած $Q(\circ)$ խմբի և նրա ցանկացած $H \leqslant Q$ ենթախմբի համար: Սակայն, ընդհանուր դեպքում, ${}^{Q}/_{H_l} \neq {}^{Q}/_{H_r}$ (օրինակ, եթե $Q = S_3$, իսկ $H = \{\varepsilon, (1,2)\}$):

$Q(\circ)$ խմբի $H \leqslant Q$ ենթախումբը կոչվում է **ինվարիանտ (կայուն)** $Q(\circ)$ **խմբում** և նշանակվում է $H \trianglelefteq Q$, եթե ${}^{Q}/_{H_l} = {}^{Q}/_{H_r}$: Այս դեպքում, ${}^{Q}/_{H_l} = {}^{Q}/_{H_r}$ բազմությունը կնշանակվի ${}^{Q}/_{H}$-ով: Ինվարիանտ ենթախմբերը կոչվում են նաև **նորմալ բաժանարարներ** կամ **նորմալ ենթախմբեր**:

Օրինակներ: 1) Կամայական $Q(\circ)$ խմբի $H = \{e\}$ ենթախմբի համար՝

$${}^{Q}/_{H_l} = \{xH |\, x \in Q\} = \{\{x\} |\, x \in Q\} = {}^{Q}/_{H_r} :$$

2) Կամայական $Q(\circ)$ խմբի $H = Q$ ենթախմբի համար՝

$${}^{Q}/_{H_l} = \{xH |\, x \in Q\} = \{Q\} = {}^{Q}/_{H_r} :$$

3) $Q = S_n$ խմբի մեջ նրա $H = \mathbb{A}_n$ ենթախմբի նշիչը հավասար է՝ $\dfrac{|S_n|}{|\mathbb{A}_n|} = \dfrac{n!}{\frac{n!}{2}} = 2$ և, հետևաբար (թեորեմ 18.23), $\mathbb{A}_n \trianglelefteq S_n$:

4) Կամայական $Q(\circ)$ խմբի և նրա կամայական $H \leqslant Q$ ենթախմբի համար՝ $H \trianglelefteq N_Q(H)$, որովհետև $xH = Hx$, եթե $x \in N_Q(H)$:

5) Կամայական $Q(\circ)$ խմբում $H = Z(Q)$ ենթախումբը ինվարիանտ է՝ $Z(Q) \trianglelefteq Q$: Դեռ ավելին, եթե $H \leqslant Z(Q)$, ապա $H \trianglelefteq Q$, որովհետև $xH = Hx$, եթե $x \in Q$, $H \leqslant Z(Q)$:

6) Կամայական $Q(\circ)$ աբելյան խմբի կամայական $H \leqslant Q$ ենթախումբ ինվարիանտ է՝ $H \trianglelefteq Q$:

Հատկություն 18.20 (ենթախմբի ինվարիանտության առաջին հայտանիշը): *Որպեսզի $Q(\circ)$ խմբի $H \leqslant Q$ ենթախումբը լինի ինվարիանտ $Q(\circ)$ խմբում անհրաժեշտ է և բավարար, որ $xH = Hx$ ցանկացած $x \in Q$ տարրի համար: Հետևաբար, եթե $H \trianglelefteq G \leqslant Q$, ապա $G \subseteq N_Q(H)$, այսինքն՝ $N_Q(H)$-ը H-ը պարունակող Q-ի այն ամենամեծ ենթախումբն է, որի մեջ ինվարիանտ է $H \leqslant Q$ ենթախումբը:*

Ապացուցում: Բավարարությունն ակնհայտ է, ապացուցենք *անհրաժեշտությունը*: Եթե $Q/_{H_l} = Q/_{H_r}$, ապա յուրաքանչյուր $xH \in Q/_{H_l}$ տարրի համար գոյություն կունենա այնպիսի $Hy \in Q/_{H_r}$, որ $xH = Hy$: Քանի որ $x \in xH = Hy$, ապա $x \in Hy \cap Hx$ և հետևաբար (հատկություն 18.18)՝ $Hy = Hx$: Ուստի $xH = Hx$ ցանկացած $x \in Q$ տարրի համար: Պնդման երկրորդ մասն ակնհայտ է: □

Թեորեմ 18.24 (ենթախմբի ինվարիանտության երկրորդ հայտանիշը): *Որպեսզի $Q(\circ)$ խմբի $H \leqslant Q$ ենթախումբը լինի ինվարիանտ $Q(\circ)$ խմբում անհրաժեշտ է և բավարար, որ $x \circ h \circ x^{-1} \in H$ ցանկացած $x \in Q$ և ցանկացած $h \in Q$ տարրերի համար:*

Ապացուցում: Անհրաժեշտություն: Եթե $H \trianglelefteq Q$, ապա համաձայն նախորդ հատկության, $xH = Hx$ ցանկացած $x \in Q$ տարրի համար: Հետևաբար, ցանկացած $h \in H$ տարրի համար գոյություն կունենա այնպիսի $h' \in H$ տարր, որ $x \circ h = h' \circ x$, այսինքն՝ $x \circ h \circ x^{-1} = h' \in H$:

Բավարարություն: Եթե $x \circ h \circ x^{-1} \in H$, ապա նշանակելով $x \circ h \circ x^{-1} = h_1 \in H$, ստանում ենք $x \circ h = h_1 \circ x$, այսինքն՝ $xH \subseteq Hx$: Այստեղ x-ը փոխարինելով x^{-1}-ով, կունենանք $x^{-1}H \subseteq Hx^{-1}$, այսինքն՝ ցանկացած $h \in H$ տարրի համար գոյություն կունենա այնպիսի $h_2 \in H$ տարր, որ $x^{-1} \circ h = h_2 \circ x^{-1}$, որտեղից՝ $h \circ x = x \circ h_2$ և, հետևաբար, $Hx \subseteq xH$: Այսպիսով, $xH = Hx$ ցանկացած $x \in Q$ տարրի համար և մնում է օգտվել նախորդ հայտանիշից: □

Հետևություն 18.10*: Միևնույն $Q(\circ)$ խմբի ցանկացած թվով ինվարիանտ ենթախմբերի հատումը նորից ինվարիանտ ենթախումբ է $Q(\circ)$ խմբում:* □

Օրինակ, $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$:

$Q(\circ)$ խումբը կոչվում է **պարզ**, եթե այն չունի ուրիշ ինվարիանտ ենթախմբեր, բացի $H_1 = \{e\}$ և $H_2 = Q$ ինվարիանտ ենթախմբերից:

Կարելի է ապացուցել, որ զույգ տեղադրությունների $\mathbb{A}_n$ նշանափոխ խումբը պարզ է, եթե $n \geqslant 5$ (է. Գալուա):

18.5.4. Քանորդ-խմբեր կամ ֆակտոր-խմբեր: Կոշիի թեորեմը: Դիցուք $Q(\cdot)$-ը կամայական խումբ է: $S(Q)$-ով նշանակենք Q-ի բոլոր ոչ դատարկ ենթաբազմությունների բազմությունը և $S(Q)$-ի մեջ սահմանենք հետևյալ գործողությունը՝

$$X \cdot Y = \{x \cdot y |\, x \in X, y \in Y\} \in S(Q),$$

որտեղ $X, Y \in S(Q)$: Օրինակ, եթե $a \in Q$, $X = \{a\}$, $H \leqslant Q$, $Y = H$, ապա $X \cdot Y = aH$, $Y \cdot X = Ha$: Ակնհայտ է, որ սահմանված գործողությունը զուգորդական է, այսինքն՝ տեղի ունի

$$(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$$

տեսա-բազմային հավասարությունը՝ ցանկացած $X, Y, Z \in S(Q)$ տարրերի համար, որովհետև խմբային գործողությունն է զուգորդական: Ուստի, $S(Q)$ բազմությունը կլինի կիսախումբ՝ սահմանված գործողության նկատմամբ, որը կոչվում է Q խմբի ոչ դատարկ **ենթաբազմությունների կիսախումբ**: $S(Q)(\cdot)$ կիսախումբն օժտված է $\bar{e} = \{e\}$ միավորով, որովհետև

$$\{e\} \cdot X = X \cdot \{e\} = X$$

ցանկացած $X \in S(Q)$ տարրի համար: Միավորով օժտված $S(Q)$ կիսախմբի բոլոր հակադարձելի տարրերի ենթախումբը նկարագրվում է հեշտությամբ՝

$$S(Q)^* = \{\{x\} |\, x \in Q\}\,,$$

և իզոմորֆ է սկզբնական $Q(\cdot)$ խմբին: Սակայն $S(Q)$ կիսախմբի կամայական ինքնահամընկնող տարրին համապատասխանող ենթախմբի նկարագրությունը կախված է ինչպես սկզբնական խմբից, այնպես էլ ինքնահամընկնող տարրից:

Եթե $H \leqslant Q$ և $X = Y = H$, ապա $X \cdot Y = H \cdot H = H$, այսինքն՝ $H \leqslant Q$ ենթախումբը ինքնահամընկնող տարր է՝ $S(Q)$ կիսախմբի համար: Սակայն, ընդհանուր դեպքում, երկու ենթախմբերի արտադրյալը ենթախումբ չէ: Օրինակ, եթե $Q = S_3$, $H = \{\varepsilon, (1,2)\}$, $K = \{\varepsilon, (1,3)\}$, ապա $H \cdot K = \{\varepsilon, (1,2), (1,3), (1,2,3)\}$ արտադրյալը չի լինի S_3 խմբի ենթախումբ (ինչը կիակասեր Լագրանժի թեորեմին (թեորեմ 18.22), որովհետև 6-ը չի բաժանվում 4-ի):

Հատկություն 18.21: *Որպեսզի $Q(\cdot)$ խմբի $H \leqslant Q$ և $K \leqslant Q$ ենթախմբերի $H \cdot K$ արտադրյալը լինի $Q(\cdot)$ խմբի ենթախումբ անհրաժեշտ է և բավարար, որ $H \cdot K = K \cdot H$: Մասնավորապես, եթե H և K ենթախմբերից գոնե մեկը ինվարիանտ է $Q(\cdot)$ խմբում, ապա $H \cdot K \leqslant Q$, իսկ եթե $H \trianglelefteq Q$ և $K \trianglelefteq Q$, ապա $H \cdot K \trianglelefteq Q$:*

Ապացուցում: Դիցուք $H \cdot K \leqslant Q$: Քանի որ $K \subseteq H \cdot K$ և $H \subseteq H \cdot K$, ապա $K \cdot H \subseteq H \cdot K$, այսինքն՝ ցանկացած $k \in K$ և ցանկացած $h \in H$ տարրերի համար գոյություն ունեն այնպիսի $h' \in H$ և $k' \in K$ տարրեր, որ

$$k \cdot h = h' \cdot k',$$

$$(k \cdot h)^{-1} = (h' \cdot k')^{-1},$$

$$h^{-1} \cdot k^{-1} = (k')^{-1} \cdot (h')^{-1}$$

և $H \cdot K \subseteq K \cdot H$: Հետևաբար, $H \cdot K = K \cdot H$:

Եվ հակառակը, եթե $H \cdot K = K \cdot H$, ապա $H \cdot K \leqslant Q$, այսինքն՝ $x \cdot y^{-1} \in H \cdot K$, որտեղ $x, y \in H \cdot K$: Իրոք, եթե $x = h_1 \cdot k_1$, $y = h_2 \cdot k_2$, ապա

$$x \cdot y^{-1} = h_1 \cdot k_1 \cdot k_2^{-1} \cdot h_2^{-1} = h_1 \cdot k_3 \cdot h_2^{-1} = h_1 \cdot h_3 \cdot k_4 = h_4 \cdot k_4 \in H \cdot K,$$

որտեղ $k_3 = k_1 \cdot k_2^{-1}$, $k_3 h_2^{-1} = h_3 \cdot k_4$ (համաձայն $K \cdot H = H \cdot K$ պայմանի) և $h_1 \cdot h_3 = h_4 \in H$:

Ապացուցենք հատկության երկրորդ մասը: Եթե, օրինակ, $H \trianglelefteq Q$, ապա համաձայն հատկություն 18.20-ի՝ $Hx = xH$ ցանկացած $x \in Q$ տարրի համար, մասնավորապես՝ $Hk = kH$ ցանկացած $k \in K$ տարրի համար և $H \cdot K = K \cdot H$: Հետևաբար, $H \cdot K \leqslant Q$: Իսկ, եթե $H \trianglelefteq Q$ և $K \trianglelefteq Q$, ապա ցանկացած $x \in Q$ տարրի համար դիտարկելով $\{x\}, H, K \in S(Q)$ երեք տարրերի արտադրյալը $S(Q)$ կիսախմբում, կունենանք՝

$$x(H \cdot K) = (xH) \cdot K = (Hx) \cdot K = H \cdot (xK) = H \cdot (Kx) = (H \cdot K)x$$

և, համաձայն հատկություն 18.20-ի, $H \cdot K \trianglelefteq Q$: □

Անցնենք քանորդ-խմբի կառուցմանը (O. Hölder, 1889):

Թեորեմ 18.25: *Եթե $Q(\cdot)$-ը կամայական խումբ է, իսկ $H \trianglelefteq Q$, ապա*

$$Q/_H = \{xH |\, x \in Q\} \subseteq S(Q)$$

ենթաբազմությունը կլինի $S(Q)$ կիսախմբի ենթախումբ, որը կոչվում է տրված $Q(\cdot)$ խմբի **քանորդ-խումբ** *կամ* **ֆակտոր-խումբ**` *ըստ $H \trianglelefteq Q$ ինվարիանտ ենթախմբի:*

$Q/_H \leqslant S(Q)$ *ենթախմբի գործողությունը, միավորը և տարրերի հակադարձները համապատասխանաբար որոշվում են հետևյալ կերպ՝*

$$xH \cdot yH = (x \cdot y)H,$$

$$eH = H,$$

$$(xH)^{-1} = \left(x^{-1}\right) H,$$

որտեղ $x, y \in Q$: Ըստ որում, $Q/_H$ քանորդ-խումբը համընկնում է $S(Q)$ կիսախմբի $H \in S(Q)$ ինքնահամընկնող տարրին համապատասխանող $S(Q)^*_H$ ենթախմբի հետ (սահմանման համար՝ տես 18.2.3 ենթավերնագիրը):

Ապացուցում: $Q/_H \subseteq S(Q)$ ենթաբազմության համար ստուգենք խմբային աքսիոմները.

ա) $xH \cdot yH \in Q/_H$, որտեղ $xH, yH \in Q/_H$: Իրոք,

$$xH \cdot yH = \{x\} \cdot H \cdot \{y\} \cdot H = \{x\} \cdot Hy \cdot H = \{x\} \cdot yH \cdot H =$$

$$= \{x\} \cdot \{y\} \cdot H \cdot H = \{x \cdot y\} \cdot H = (x \cdot y)H,$$

որովհետև $Hy = yH$ և $H \cdot H = H$:

բ) գործողության զուգորդականությունը նկատվեց վերևում:

գ) $[e] = eH = H$ հարակից դասը կլինի $Q/_H(\cdot)$ կիսախմբի միավորը, որովհետև՝

$$eH \cdot xH = (e \cdot x)H = xH,$$

$$xH \cdot eH = (x \cdot e)H = xH:$$

դ) $Q/_H(\cdot)$ կիսախմբի յուրաքանչյուր xH տարրի հակադարձը կլինի $\left(x^{-1}\right) H \in Q/_H$ տարրը, որովհետև

$$xH \cdot x^{-1}H = \left(x \cdot x^{-1}\right) H = eH,$$

$$x^{-1}H \cdot xH = \left(x^{-1} \cdot x\right) H = eH,$$

այսինքն՝ $(xH)^{-1} = x^{-1}H$:

Այժմ ապացուցենք, որ $S(Q)$ կիսախմբի $H \in S(Q)$ ինքնահամընկնող տարրին համապատասխանող $S(Q)^*_H$ ենթախումբը համընկնում է ${}^{Q}/_{H}$ քանորդ-խմբի հետ: Իրոք, ըստ սահմանման $S(Q)^*_H$ ենթախումբը կազմված է $S(Q)$ կիսախմբի բոլոր այն $X \in S(Q)$ տարրերից, որոնց համար՝ $X \cdot H = H \cdot X = X$ և գոյություն ունի այնպիսի $Y \in S(Q)$ տարր, որ $X \cdot Y = Y \cdot X = H$, $Y \cdot H = H \cdot Y = Y$: Հետևաբար, ակնհայտ է, որ ${}^{Q}/_{H} \subseteq S(Q)^*_H$: Մնում է ապացուցել հակառակ ներդրումը:

Եթե $X \in S(Q)^*_H$ և $x \in X$, ապա $X \cdot H = X$ պայմանից բխում է, որ $xH \subseteq X$, իսկ $X \cdot Y = H$ պայմանից հետևում է $xY \subseteq H$ ներդրումը: Եթե $y \in Y$, ապա վերջինից կունենանք $x \cdot y = h \in H$ և հետևաբար՝ $x^{-1} = y \cdot h^{-1} \in Y \cdot H = Y$, այսինքն՝ $x^{-1} \in Y$: Դիցուք $t \in X$: Այդ դեպքում՝ $x^{-1} \cdot t \in Y \cdot X = H$ և $t \in xH$, այսինքն՝ $X \subseteq xH$: Այսպիսով, $X = xH$ և $X \in {}^{Q}/_{H}$: □

Օրինակներ: 1) ${}^{\mathbb{C}}/_{\mathbb{R}}$ քանորդ-խումբը կազմված է իրական առանցքին զուգահեռ ուղիղներից;

2) ${}^{\mathbb{C}^*}/_{\mathbb{R}^*}$ քանորդ-խումբը կազմված է կոորդինատների սկզբնակետից ելնող ճառագայթներից;

3) ${}^{\mathbb{C}^*}/_{S^1}$ քանորդ-խումբը, որտեղ $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$, կազմված է համակենտրոն շրջանագծերից, որոնց կենտրոնը կոորդինատների սկզբնակետն է;

4) ${}^{GL_n(\mathbb{R})}/_{SL_n(\mathbb{R})}$ քանորդ-խումբը կազմված է նույն որոշիչն ունեցող մատրիցներից:

***Հետևություն 18.11**: Եթե $Q(\cdot)$-ը կամայական խումբ է, $H \trianglelefteq Q$, ապա ${}^{Q}/_{H}(\cdot)$ քանորդ-խմբում՝*

$$x_1H \cdot x_2H \cdots x_nH = (x_1 \cdot x_2 \cdots x_n)H,$$

$$(xH)^m = (x^m)\,H$$

ցանկացած $m \in \mathbb{Z}$ ամբողջ և ցանկացած $n \in \mathbb{N}$ բնական թվերի համար:

Ապացուցում: Առաջին հավասարությունն ապացուցվում է վերհանգման եղանակով՝ ըստ n-ի, իսկ երկրորդ հավասարության ապացուցման համար դիտարկենք հետևյալ երեք դեպքերը:

ա) $m > 0$: Այս դեպքում՝

$$(xH)^m = \underbrace{xH \cdot xH \cdots xH}_{m} = (\underbrace{x \cdot x \cdots x}_{m})H = (x^m)\,H;$$

բ) $m = 0$: Այս դեպքում, ապացուցվող հավասարության աջ և ձախ մասերը հավասար են $Q/_H$ քանորդ-խմբի միավորին:

գ) $m < 0$: Այս դեպքում, $m = -|m|$ և

$$(xH)^m = (xH)^{-|m|} = \left((xH)^{-1}\right)^{|m|} =$$

$$= \left(x^{-1}H\right)^{|m|} = \left(x^{-1}\right)^{|m|} H = \left(x^{-|m|}\right) H = (x^m)\, H : \qquad \square$$

Հատկություն 18.22: *Եթե $Q(\cdot)$ խումբն աբելյան է, ապա նրա բոլոր $Q/_H$ քանորդ-խմբերը ևս կլինեն աբելյան խմբեր:*

Ապացուցում: Եթե $Q(\cdot)$ խումբը աբելյան է և $H \leqslant Q$, ապա $H \trianglelefteq Q$ և

$$xH \cdot yH = (x \cdot y)H = (y \cdot x)H = yH \cdot xH,$$

որտեղ $x, y \in Q$: $\square$

Հատկություն 18.23: *Եթե $Q(\cdot)$ խումբը միածին է, ապա նրա բոլոր $Q/_H$ քանորդ-խմբերը ևս կլինեն միածին:*

Ապացուցում: Եթե $Q(\cdot)$ խումբը միածին է՝ $Q = (a)$ և $H \leqslant Q$, ապա $H \trianglelefteq Q$, որովհետև $Q(\cdot)$ խումբն աբելյան է: Ապացուցենք $Q/_H = (aH)$ հավասարությունը: Եթե $x \in Q$, $x = a^m$, ապա հետևություն 18.11-ի համաձայն՝ $xH = (a^m)\, H = (aH)^m$, $m \in \mathbb{Z}$: $\square$

Հատկություն 18.24: *Եթե $Q(\cdot)$ խմբի քանորդ-խումբը ըստ իր $Z(Q)$ կենտրոնի միածին է, ապա $Q(\cdot)$ խումբն աբելյան է:*

Ապացուցում: Դիցուք $H = Z(Q)$ և $Q/_H = (aH)$, $a \in Q$: Ապացուցենք $x \cdot y = y \cdot x$ հավասարությունը՝ ցանկացած $x, y \in Q$ տարրերի համար: Քանի որ $xH, yH \in Q/_H = (aH)$, ապա $xH = (aH)^i = \left(a^i\right) H$, $yH = (aH)^j = \left(a^j\right) H$, որտեղ $i, j \in \mathbb{Z}$: Հետևաբար, $x = a^i \cdot h_1$, $y = a^j \cdot h_2$, որտեղ $h_1, h_2 \in H = Z(Q)$, $a^i \cdot a^j = a^j \cdot a^i$ և

$$x \cdot y = a^i \cdot h_1 \cdot a^j \cdot h_2 = a^j \cdot h_2 \cdot a^i \cdot h_1 = y \cdot x : \qquad \square$$

Հետևություն 18.12: *Եթե $Q(\cdot)$ խմբի քանորդ-խումբը ըստ իր $H \leqslant Z(Q)$ ինվարիանտ ենթախմբի միածին է, ապա $Q(\cdot)$ խումբն աբելյան է:* $\square$

Հետևություն 18.13: Եթե $Q(\cdot)$ խումբն աբելյան չէ, ապա նրա քանորդ-խումբը ըստ իր $H \leqslant Z(Q)$ ինվարիանտ ենթախմբի չի կարող լինել միածին: □

Թեորեմ 18.26 (Կոշի): *Եթե p պարզ թիվը հանդիսանում է վերջավոր աբելյան խմբի կարգի բաժանարար, ապա այդ աբելյան խմբում գոյություն ունի p կարգի որևէ տարր (հետևաբար և p կարգի որևէ ենթախումբ):*

Ապացուցում: Դիցուք $Q(\cdot)$-ը վերջավոր աբելյան խումբ է՝ $|Q| = n \geqslant 2$: Թեորեմն ապացուցենք վերիանգման եղանակով՝ ըստ n բնական թվի: $n = 2$ դեպքում թեորեմն ակնհայտ է, որովհետև $p = 2$ պարզ թիվը միակ պարզ թիվն է, որի վրա բաժանվում է $n = 2$-ը, իսկ երկրորդ կարգի $Q(\cdot)$ խմբի միավորից տարբեր տարրի կարգը հավասար է 2-ի:

Ենթադրենք n-ից փոքր կարգ ունեցող բոլոր աբելյան խմբերի համար թեորեմի պնդումը ճիշտ և ապացուցենք այն n-րդ կարգի կամայական $Q(\cdot)$ աբելյան խմբի համար: Դիցուք $a \in Q$, $a \neq e$, $|a| = k > 1$ և դիցուք $H = (a)$: Հետևաբար, $|H| = k$ և $H \trianglelefteq Q$ քանի որ $Q(\cdot)$ խումբն աբելյան է:

Հնարավոր են հետևյալ երկու դեպքերը.

ա) k-ն բաժանվում է նույն p պարզ թվի վրա՝ $k = p \cdot t$: Նշանակելով՝ $b = a^t$, կունենանք՝ $|b| = p$:

բ) k-ն չի բաժանվում p-ի վրա: Սակայն, ըստ Լագրանժի թեորեմի (թեորեմ 18.22)՝ $n = k \cdot s$, որտեղ $\left|{}^{Q}\!/_{H}\right| = s < n$ (որովհետև $k > 1$) և s-ը կբաժանվի p-ի վրա (հատկություն 6.3): Համաձայն վերիանգման ենթադրության, գոյություն կունենա $bH \in {}^{Q}\!/_{H}$ այնպիսին, որ $|bH| = p$: Դիցուք $|b| = m$, $b \in Q$: Հետևաբար, $(bH)^m = (b^m)\,H = eH = H$ և ${}^{Q}\!/_{H}$ քանորդ-խմբում կարող ենք կիրառել հատկություն 18.13-ը: Ուստի, ${}^{m}\!/_{p}$ և $m = p \cdot l$, $l \in \mathbb{N}$: Նշանակելով՝ $c = b^l \in Q$, կունենանք՝ $|c| = \left|b^l\right| = p$: □

Հետևություն 18.14: Վերջավոր աբելյան p-խմբի կարգը հավասար է p^k-ի, որտեղ $k \in \mathbb{N}$:

Ապացուցում: Ըստ սահմանման, p-խմբի յուրաքանչյուր տարրի կարգը հավասար է p-ի որևէ աստիճանի: Հետևաբար, վերջավոր աբելյան p-խմբի n կարգը, համաձայն հետևության 18.7-ի, կբաժանվի p-ի վրա: Մնում է ապացուցել, որ n-ը չի բաժանվում p-ից տարբեր որևէ պարզ թվի վրա և այնուհետև օգտվել թվաբանության հիմնական թեորեմից:

Իրոք, եթե n-ը բաժանվեր որևէ $q \neq p$ պարզ թվի վրա, ապա թեորեմ 18.26-ի համաձայն, դիտարկվող խմբում գոյություն կունենար այնպիսի c տարր, որ $|c| = q$: Սակայն, մյուս կողմից, ըստ p-խմբի սահմանման՝ $|c| = p^t$, $t \geqslant 1$: Այսպիսով, $q = p^t$: Հակասություն: □

Հետևություն 18.15*: $p \cdot q$ կարգի յուրաքանչյուր աբելյան խումբ միածին է, եթե $p \neq q$ բնական թվերը պարզ են:*

Ապացուցում: Համաձայն թեորեմ 18.26-ի տրված $p \cdot q$ կարգի $Q(\cdot)$ աբելյան խումբը կունենա p կարգի որևէ $a \in Q$ տարր և q կարգի որևէ $b \in Q$ տարր, որտեղ $(p, q) = 1$: Հետևաբար, համաձայն թեորեմ 18.16-ի $|a \cdot b| = |a| \cdot |b| = p \cdot q$ և $Q = (a \cdot b)$: □

Ինչպես նշել ենք, եթե խումբն աբելյան է, ապա նրա գործողությունը սովորաբար նշանակվում է $+$ նշանով, միավորը՝ 0-ով, a^{-1}-ը՝ $-a$-ով, իսկ aH հարակից դասը՝ $a + H$-ով: Հետևաբար, այս դեպքում, Q/H քանորդ-խմբի գործողությունը, միավորը և տարրերի հակադարձները (հակադիրները) համապատասխանաբար կորոշվեն հետևյալ կերպ՝

$$(x + H) + (y + H) = (x + y) + H,$$

$$0 + H = H,$$

$$-(a + H) = (-a) + H :$$

18.6. Խմբային հոմոմորֆիզմներ, խմբային հոմոմորֆիզմի միջուկ և պատկեր: Քելիի ընդհանրացված թեորեմը: Հոմոմորֆիզմների և իզոմորֆիզմների թեորեմները խմբերում

Դիցուք $Q(\cdot)$-ը և $Q'(\circ)$-ը կամայական խմբեր են: Ինչպես գիտենք, $\varphi : Q \to Q'$ արտապատկերումը կոչվում է **հոմոմորֆություն**, **հոմոմորֆիզմ**, **նմանածնություն** կամ **հոմոմորֆ արտապատկերում**՝ $Q(\cdot)$ խմբից $Q'(\circ)$ խմբի մեջ, եթե տեղի ունի հետևյալ պայմանը.

$$\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)$$

ցանկացած $x, y \in Q$ տարրերի համար: Այս դեպքում ասում են նաև, որ φ արտապատկերումը **համաձայնեցված է** դիտարկվող խմբերի խմբային գործողությունների հետ: Խմբերի միջև գործող հոմոմորֆիզմը հաճախ կոչվում է նաև խմբային հոմոմորֆիզմ: Դժվար չէ ստուգել, որ երկու (հետևաբար և վերջավոր թվով) խմբային հոմոմորֆիզմների արտադրյալը նորից խմբային հոմոմորֆիզմ է, եթե այն գոյություն ունի: Իրոք, եթե $\varphi : Q \to Q'$ և $\varphi' : Q' \to Q''$ արտապատկերումները խմբային հոմոմորֆիզմներ են, ապա այդպիսին կլինի նաև $\varphi \cdot \varphi' : Q \to Q''$ արտադրյալը, որովհետև

$$(\varphi{\cdot}\varphi')(x{\cdot}y) = \varphi'(\varphi(x{\cdot}y)) = \varphi'(\varphi x{\circ}\varphi y) = \varphi'(\varphi x){*}\varphi'(\varphi y) = (\varphi{\cdot}\varphi')x{*}(\varphi{\cdot}\varphi')y$$

ցանկացած $x, y \in Q$ տարրերի համար:

$\varphi : Q \to Q'$ խմբային հոմոմորֆիզմը կոչվում է **ներդրող հոմոմորֆիզմ** կամ **խմբային մոնոմորֆիզմ**, եթե φ արտապատկերումը նաև ներդրող (ինյեկտիվ) արտապատկերում է, այսինքն՝

$$\varphi(x) = \varphi(y) \longrightarrow x = y,$$

որտեղ $x, y \in Q$: Երկու (հետևաբար և վերջավոր թվով) խմբային մոնոմորֆիզմների արտադրյալը նորից խմբային մոնոմորֆիզմ է, եթե այն գոյություն ունի:

$\varphi : Q \to Q'$ խմբային հոմոմորֆիզմը կոչվում է **վերադրող հոմոմորֆիզմ** կամ **խմբային էպիմորֆիզմ**, եթե φ արտապատկերումը նաև վերադրող (սյուրեկտիվ) արտապատկերում է, այսինքն՝ յուրաքանչյուր $y \in Q'$ տարրի համար գոյություն ունի այնպիսի $x \in Q$ տարր, որ $\varphi(x) = y$: Երկու (հետևաբար և վերջավոր թվով) խմբային էպիմորֆիզմների արտադրյալը նորից խմբային էպիմորֆիզմ է, եթե այն գոյություն ունի:

$\varphi : Q \to Q'$ խմբային հոմոմորֆիզմը կոչվում է **խմբային իզոմորֆիզմ**, **իզոմորֆություն**, **նույնաձևություն** կամ **իզոմորֆ արտապատկերում** (տես նաև 18.3-ը), եթե φ արտապատկերումը նաև փոխմիարժեք (բիեկտիվ) արտապատկերում է, այսինքն՝ այն միաժամանակ ներդրող և վերադրող է:

Օրինակներ: 1) Հայտնի

$$\int\limits_0^1 (f(x) + g(x))\, dx = \int\limits_0^1 f(x)\, dx + \int\limits_0^1 g(x)\, dx$$

բանաձևը նշանակում է, որ $\varphi : f \to \int\limits_0^1 f(x)\, dx$ արտապատկերումը

խմբային հոմոմորֆիզմ է՝ իրական թվերի $[0,1]$ հատվածի վրա որոշված բոլոր անընդհատ (կամ ինտեգրելի) իրական ֆունկցիաների գումարային խմբից բոլոր իրական թվերի $\mathbb{R}(+)$ գումարային խմբի մեջ:
2) $sgn(\alpha \cdot \beta) = sgn(\alpha) \cdot sgn(\beta)$ բանաձևը նշանակում է, որ $\varphi : \alpha \to sgn(\alpha)$ արտապատկերումը հոմոմորֆիզմ է բոլոր n-րդ աստիճանի տեղադրությունների S_n սիմետրիկ խմբից երկու տարրանի $H = \{1, -1\}$ արտադրյալային խմբի մեջ: Այս հոմոմորֆիզմը նշանակվում է sgn-ով կամ $(sgn)_n$-ով:

Եթե $Q(\cdot)$-ը կամայական խումբ է, իսկ $H \trianglelefteq Q$, ապա $\pi(x) = xH$, $x \in Q$,բանաձևով (արտապատկերումով) որոշվում է խմբային հոմոմորֆիզմ՝ $Q(\cdot)$ խմբից Q/H քանորդ-խմբի մեջ, որը կոչվում է **բնական** (կամ քանորդ-) հոմոմորֆիզմ: $\pi : Q \to Q/H$ բնական հոմոմորֆիզմը անհրաժեշտության դեպքում նշանակվում է նաև π_H-ով: Ակնհայտ է, որ բնական հոմոմորֆիզմը վերադրող հոմոմորֆիզմ (էպիմորֆիզմ) է: Քիչ հետո կհամոզվենք, որ վերադրող հոմոմորֆիզմները, ըստ էության, սպառվում են բնական հոմոմորֆիզմներով (տե՛ս հոմոմորֆիզմների առաջին թեորեմը):

Լեմմ 18.9: *Եթե $Q(\cdot)$-ը և $Q'(\circ)$-ը կամայական խմբեր են՝ e և e' միավորներով, ապա յուրաքանչյուր $\varphi : Q \to Q'$ խմբային հոմոմորֆիզմ բավարարում է հետևյալ պայմաններին.*

1) $\varphi(e) = e'$*;*

2) $\varphi(x^{-1}) = (\varphi(x))^{-1}$ *ցանկացած* $x \in Q$ *տարրի համար;*

3) $\varphi(x_1 \cdot x_2 \cdots x_n) = \varphi(x_1) \circ \varphi(x_2) \circ \cdots \circ \varphi(x_n)$ *ցանկացած* $n \in \mathbb{N}$ *և ցանկացած* $x_1, x_2, \ldots, x_n \in Q$ *տարրերի համար: Այնուհետև,*

$$\varphi(x^m) = (\varphi x)^m$$

ցանկացած $x \in Q$ *և ցանկացած* $m \in \mathbb{Z}$ *տարրերի համար;*

4) Եթե $H \leqslant Q$*, ապա*

$$\varphi(H) = \{\varphi(h) \mid h \in H\} \leqslant Q';$$

$\varphi(H)$*-ը կոչվում է* H*-ի հոմոմորֆ պատկեր, կամ ավելի ճիշտ* H*-ի* φ*-հոմոմորֆ պատկեր:*

5) *Եթե* $H \leqslant Q$ *ենթախումբն աբելյան է, ապա* $\varphi(H) \leqslant Q'$ *ենթախումբը ևս կլինի աբելյան;*

6) *Եթե* $H \leqslant Q$ *ենթախումբը միածին է, ապա* $\varphi(H) \leqslant Q'$ *ենթախումբը ևս կլինի միածին;*

7) *Եթե* $H \trianglelefteq Q$, *ապա* $\varphi(H) \trianglelefteq \varphi(Q)$;

8) *Եթե* $H' \leqslant Q'$, *ապա*

$$\varphi^{-1}(H') = \{h \in Q \mid \varphi(h) \in H'\} \leqslant Q;$$

9) *Եթե* $H' \trianglelefteq Q'$, *ապա* $\varphi^{-1}(H') \trianglelefteq Q$:

Ապացուցում: 1) Եթե $x \cdot e = e \cdot x = x$, ապա

$$\varphi x \cdot \varphi e = \varphi e \cdot \varphi x = \varphi x :$$

2) Եթե $x \cdot x^{-1} = x^{-1} \cdot x = e$, ապա

$$\varphi x \cdot \varphi\left(x^{-1}\right) = \varphi\left(x^{-1}\right) \cdot \varphi(x) = \varphi e = e' :$$

3) Առաջին հավասարությունը հաստատվում է վերհանգման եղանակով: Այդ դեպքում, որպես հետևանք, երկրորդ հավասարությունը կլինի ճիշտ կամայական $m \in \mathbb{N}$ բնական թվի դեպքում: Դիցուք $m \in \mathbb{Z}$ և $m < 0$: Հետևաբար, $m = -|m|$ և

$$\varphi\left(x^m\right) = \varphi\left(x^{-|m|}\right) = \varphi\left(\left(x^{|m|}\right)^{-1}\right) = \left(\varphi\left(x^{|m|}\right)\right)^{-1} =$$

$$= \left((\varphi x)^{|m|}\right)^{-1} = (\varphi x)^{-|m|} = (\varphi x)^m :$$

4) Եթե $x_1 = \varphi(h_1)$, $x_2 = \varphi(h_2)$, $h_1, h_2 \in H \leqslant Q$, ապա $h_1 \cdot h_2^{-1} \in H$ և

$$x_1 \circ x_2^{-1} = \varphi(h_1) \circ (\varphi(h_2))^{-1} = \varphi(h_1) \circ \varphi\left(h_2^{-1}\right) = \varphi\left(h_1 \cdot h_2^{-1}\right) \in \varphi(H) :$$

5) Ակնհայտ է:

6) Եթե $H \leqslant Q$ ենթախումբը միածին է և $H = (a)$, $a \in Q$, ապա $\varphi(H) = (\varphi a)$: Իրոք, կամայական $x' \in \varphi(H)$ տարրի համար կունենանք $x' = \varphi(h)$, $h \in H$, որտեղ $h = a^m$, $m \in \mathbb{Z}$: Հետևաբար, համաձայն 3) հատկության՝
$$x' = \varphi(a^m) = (\varphi a)^m :$$

7) Եթե $h' \in \varphi(H)$, $x' \in \varphi(Q)$, ապա $h' = \varphi(h)$, $x' = \varphi(x)$, որտեղ $h \in H$ և $x \in Q$: Հետևաբար, $x \cdot h \cdot x^{-1} \in H \trianglelefteq Q$ և
$$x' \circ h' \circ (x')^{-1} = \varphi(x) \circ \varphi(h) \circ (\varphi x)^{-1} = \varphi(x) \circ \varphi(h) \circ \varphi\left(x^{-1}\right) =$$
$$= \varphi(x \cdot h \cdot x^{-1}) \in \varphi(H) :$$

8) Եթե $x_1 \in \varphi^{-1}(H')$ և $x_2 \in \varphi^{-1}(H')$, ապա $\varphi(x_1) \in H'$ և $\varphi(x_2) \in H'$: Հետևաբար, $\varphi\left(x_2^{-1}\right) = (\varphi x_2)^{-1} \in H'$ և
$$\varphi\left(x_1 \cdot x_2^{-1}\right) = \varphi(x_1) \circ \varphi\left(x_2^{-1}\right) \in H',$$
այսինքն՝ $x_1 \cdot x_2^{-1} \in \varphi^{-1}(H')$:

9) Եթե $h \in \varphi^{-1}(H')$ և $x \in Q$, ապա $\varphi(h) \in H'$, $\varphi x \in Q'$ և
$$\varphi\left(x \cdot h \cdot x^{-1}\right) = \varphi(x)\circ\varphi(h)\circ\varphi\left(x^{-1}\right) = \varphi(x)\circ\varphi(h)\circ(\varphi x)^{-1} \in H' \trianglelefteq Q',$$
այսինքն՝ $x \cdot h \cdot x^{-1} \in \varphi^{-1}(H')$:

□

$\varphi : Q \to Q'$ խմբային հոմոմորֆիզմի **միջուկը** և **պատկերը** նշանակվում են $Ker(\varphi)$-ով և $Im(\varphi)$-ով ու սահմանվում են հետևյալ կերպ՝
$$Ker(\varphi) = \{x \in Q \mid \varphi x = e'\},$$
$$Im(\varphi) = \{\varphi x \mid x \in Q\} = \varphi(Q) :$$

$\varphi(Q)$-ն կոչվում է նաև Q խմբի **հոմոմորֆ պատկեր**:

$Ker(\varphi)$-ի և $Im(\varphi)$-ի սերտ կապը, որ հաստատվել է գծային արտապատկերումների դեպքում, մնում է ուժի մեջ նաև այստեղ:

Օրինակներ: 1) $\varphi(x) = x^n$ բանաձևով որոշվող $\varphi : \mathbb{C}^* \to \mathbb{C}^*$ արտապատկերումը խմբային հոմոմորֆիզմ է՝ $\mathbb{C}^*(\cdot)$ խմբից իր մեջ, որի համար $Ker(\varphi) = \sqrt[n]{1}$, իսկ $Im(\varphi) = \mathbb{C}^*$;

2) $Ker(det) = SL_n(\mathbb{R})$, իսկ $Im(det) = \mathbb{R}^*$;

3) $Ker\left((sgn)_n\right) = \mathbb{A}_n$, իսկ $Im\left((sgn)_n\right) = \{1, -1\}$, եթե $n \geqslant 2$:

Լեմմ 18.10: *1) $\varphi : Q \to Q'$ խմբային հոմոմորֆիզմի միջուկը $Q(\cdot)$ խմբի ինվարիանտ ենթախումբ է՝ $Ker(\varphi) \trianglelefteq Q$: 2) Եվ հակառակը, $Q(\cdot)$ խմբի կամայական $H \trianglelefteq Q$ ինվարիանտ ենթախումբ հանդիսանում է $\pi_H : Q \to Q/H$ բնական հոմոմորֆիզմի միջուկ՝ $Ker(\pi_H) = H$: Այսպիսով, $H \leqslant Q$ ենթախումբը կլինի $Q(\cdot)$ խմբի ինվարիանտ ենթախումբ այն և միայն այն դեպքում, երբ գոյություն ունի այնպիսի $Q'(\circ)$ խումբ և այնպիսի $\varphi : Q \to Q'$ խմբային հոմոմորֆիզմ, որ $H = Ker(\varphi)$, այսինքն՝ երբ H-ը հանդիսանում է որևէ հոմոմորֆիզմի միջուկ:*

Ապացուցում: 1) $x \in Q$, $h \in Ker(\varphi) \to \varphi\left(xhx^{-1}\right) = \varphi x \varphi h \varphi(x^{-1}) = \varphi x \cdot e' \cdot (\varphi x)^{-1} = e' \to xhx^{-1} \in Ker(\varphi)$: Մնում է ստուգել $Ker(\varphi) \leqslant Q$ հատկությունը:

2) $x \in Ker(\pi_H) \leftrightarrow \pi_H(x) = H \leftrightarrow xH = H \leftrightarrow x \in H$: □

Եթե $\varphi(a) = a'$, ապա

$$\varphi^{-1}(a') = \{x \in Q \mid \varphi x = a'\} = aKer(\varphi) :$$

$\varphi : Q \to Q'$ հոմոմորֆիզմը կլինի ներդրող հոմոմորֆիզմ այն և միայն այն դեպքում, երբ $Ker(\varphi) = \{e\}$:

Թեորեմ 18.27 (Քելիի ընդհանրացված թեորեմը): *Եթե $Q(\cdot)$-ը խումբ է, $H \leqslant Q$, իսկ $X = Q/H_r$, ապա գոյություն ունի այնպիսի $\varphi : Q \to S_X$ խմբային հոմոմորֆիզմ, որի միջուկը ընկած է H-ում և պարունակում է $Q(\cdot)$-ի բոլոր այն ինվարիանտ ենթախմբերը, որոնք ընկած են H-ում: ($H = \{e\}$ դեպքում այս թեորեմը համընկնում է Քելիի թեորեմի հետ:)*

Ապացուցում: Յուրաքանչյուր $a \in Q$ տարրի համար սահմանենք $\tau_a : X \to X$ արտապատկերումը, որտեղ $X = Q/H_r$, հետևյալ կերպ՝

$$\tau_a(Hx) = H(xa), \quad x \in Q :$$

Ակնհայտ է, որ τ_a-ն վերադրող (սյուրեկտիվ) է: Ապացուցենք նրա ներդրող (ինյեկտիվ) լինելը.

$$\tau_a(Hx) = \tau_a(Hy) \to H(xa) =$$

$$= H(ya) \to (xa)(ya)^{-1} \in H \to xy^{-1} \in H \to Hx = Hy :$$

Այսպիսով, τ_a-ն փոխմիարժեք (բիեկտիվ) է, այսինքն՝ $\tau_a \in S_X$ ցանկացած $a \in Q$ տարրի համար: Ապացուցենք նաև

$$\tau_a \cdot \tau_b = \tau_{a \cdot b}$$

հավասարությունը՝ ցանկացած $a, b \in Q$ տարրերի համար: Իրոք,

$$(\tau_a \cdot \tau_b)\, Hx = \tau_b\,(\tau_a(Hx)) = \tau_b\,(H(xa)) = H((x{\cdot}a)b) = H(x{\cdot}(a{\cdot}b)) = \tau_{a\cdot b}(Hx) :$$

Հետևաբար, սահմանելով $\varphi : a \to \tau_a$ արտապատկերումը կունենանք $\varphi : Q \to S_X$ խմբային հոմոմորֆիզմը: Մնում է նկատել, որ կառուցված φ հոմոմորֆիզմը բավարարում է թեորեմի երկու պնդումներին: Նախ ապացուցենք, որ $Ker(\varphi) \subseteq H$.

$$a \in Ker(\varphi) \to \varphi(a) = \varepsilon_X \to \tau_a = \varepsilon_X \to$$

$$\tau_a(Hx) = Hx \to \tau_a(H) = H \to Ha = H \to a \in H :$$

Դիցուք $H' \trianglelefteq Q$ և $H' \subseteq H$: Ապացուցենք, որ $H' \subseteq Ker(\varphi)$: Քանի որ $xH' = H'x$, $x \in Q$, ապա կամայական $a \in H'$ և կամայական $x \in Q$ տարրերի համար գոյություն կունենա այնպիսի $a^* \in H' \subseteq H$ տարր, որ $xa = a^*x$: Ուստի

$$\tau_a(Hx) = H(xa) = H(a^*x) = Hx$$

և $\varphi(a) = \varepsilon_X$, այսինքն՝ $a \in Ker(\varphi)$, որտեղ ε_X-ը $X = Q/H_r$ բազմության նույնական արտապատկերումն է: □

Հետևյալ արդյունքը հաճախ կոչվում է հոմոմորֆիզմների թեորեմ (C. Jordan, 1870), ուր հաստատվում է խմբային հոմոմորֆիզմի միջուկի, պատկերի, խմբային հոմոմորֆիզմի, ինվարիանտ ենթախմբի, բնական հոմոմորֆիզմի և քանորդ-խմբի հասկացությունների հավասարազոր լինելը:

Թեորեմ 18.28 (խմբային հոմոմորֆիզմների առաջին թեորեմը)*: Եթե* $\varphi : Q \to Q'$ *արտապատկերումը կամայական խմբային էպիմորֆիզմ է* $Q(\cdot)$ *և* $Q'(\circ)$ *խմբերի միջև, իսկ* $Ker(\varphi) = H$, *ապա* $Q' \simeq Q/H$*: Ավելի ճշգրիտ, գոյություն ունի միարժեքորեն որոշվող այնպիսի* $\mu : Q' \to Q/H$ *խմբային իզոմորֆիզմ, որ տեղափոխական է արտապատկերումների հետևյալ եռանկյունը՝*

$$\begin{tikzcd}
Q \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & Q' \arrow[d, "\mu"] \\
 & Q/H
\end{tikzcd} ,$$

այսինքն՝ $\pi = \varphi \cdot \mu$, *որտեղ* π*-ն բնական հոմոմորֆիզմն է:*

Ապացուցում: Թեորեմի ապացուցումը հանգում է որոնելի μ արտապատկերման կառուցմանը: Քանի որ $\varphi : Q \to Q'$ արտապատկերումը վերադրող է, ապա կամայական $x' \in Q'$ տարրի համար գոյություն կունենա այնպիսի $x \in Q$ տարր, որ $\varphi(x) = x'$: Սահմանենք՝

$$\mu(x') = xH, \quad \text{որտեղ } \varphi(x) = x' :$$

Նախ նկատենք, որ μ-ն իրոք արտապատկերում է, այսինքն՝ որ $\mu(x')$-ը կախված չէ $\varphi(x) = x'$ հավասարությանը բավարարող x-ի ընտրությունից: Դիցուք նաև $\varphi(y) = x'$, $y \in Q$: Հետևաբար,

$$\begin{aligned} &\varphi(x) = \varphi(y), \\ &e' = (\varphi x)^{-1} \circ \varphi(y) = \varphi(x^{-1}) \circ \varphi(y) = \varphi(x^{-1} \cdot y), \end{aligned}$$

այսինքն՝ $x^{-1} \cdot y \in Ker(\varphi) = H$ և $xH = yH$ (համաձայն երկու ձախ հարակից դասերի հավասարության հայտանիշի):

Ակնհայտ է, որ μ արտապատկերումը վերադրող (սյուրեկտիվ) է: Ապացուցենք, որ այն նաև ներդրող (ինյեկտիվ) է՝

$$\mu(x') = \mu(y') \longrightarrow x' = y' :$$

Դիցուք $x' = \varphi(x)$, $y' = \varphi(y)$, $x, y \in Q$: Կունենանք՝

$$\mu(x') = \mu(y') \to xH = yH \to x^{-1} \cdot y \in H = Ker(\varphi) \to \varphi(x^{-1} \cdot y) = e' \to$$

$$\to \varphi(x^{-1}) \circ \varphi(y) = e' \to (\varphi x)^{-1} \circ \varphi(y) = e' \to \varphi y = \varphi x \to x' = y' :$$

Ապացուցենք, որ μ-ն հոմոմորֆիզմ է: Քանի որ $x' \circ y' = \varphi(x) \circ \varphi(y) = \varphi(x \cdot y)$, ապա

$$\mu(x' \circ y') = (x \cdot y)H = xH \cdot yH = \mu(x') \cdot \mu(y') :$$

Այսպիսով, μ-ն իզոմորֆիզմ է: Ի վերջո նկատենք, որ արտապատկերումների պատկերված եռանկյունը տեղափոխական է՝

$$\mu(x') = xH, \varphi x = x' \to \mu(\varphi x) = xH \to (\varphi \cdot \mu)x = \pi(x) \to \varphi \cdot \mu = \pi,$$

որտեղից էլ բխում է μ-ի միակությունը.

$$\varphi \cdot \mu = \pi, \; \varphi \cdot \mu' = \pi \longrightarrow \varphi \cdot \mu = \varphi \cdot \mu' \longrightarrow (\varphi \cdot \mu)x = (\varphi \cdot \mu')x$$

$$\longrightarrow \mu(\varphi x) = \mu'(\varphi x) \longrightarrow \mu(x') = \mu'(x')$$

ցանկացած $x' \in Q'$ տարրի համար: □

***Հետևություն 18.16**: Եթե $\varphi : Q \to Q'$ արտապատկերումը կամայական խմբային հոմոմորֆիզմ է $Q(\cdot)$ և $Q'(\circ)$ խմբերի միջև, իսկ $Ker(\varphi) = H$, ապա $\varphi(Q) \simeq Q/H$: Ավելի ճշգրիտ, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\mu : \varphi(Q) \to Q/H$ խմբային իզոմորֆիզմ, որ տեղափոխական է արտապատկերումների հետևյալ եռանկյունը՝*

$$\begin{tikzcd} Q \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & \varphi(Q) \arrow[d, "\mu"] \\ & Q/H \end{tikzcd} ,$$

այսինքն՝ $\pi = \varphi \cdot \mu$: Մասնավորապես, եթե $Q(\cdot)$ խումբը վերջավոր է, ապա $|Q| = |Im(\varphi)| \cdot |Ker(\varphi)|$: □

Օրինակ: Որոշենք (բնութագրենք) $\mathbb{R}/\mathbb{Z}$ քանորդ-խումբը: S^1-ով նշանակենք 1 շառավղով շրջանագծի վրա գտնվող բոլոր կոմպլեքս թվերի արտադրյալային խումբը և $f(x) = e^{2\pi ix} = \cos 2\pi x + i \sin 2\pi x$ օրենքով սահմանենք $f : \mathbb{R} \to S^1$ խմբային էպիմորֆիզմը, որի միջուկը՝ $Ker(f) = \mathbb{Z}$: Հետևաբար, խմբային հոմոմորֆիզմների առաջին թեորեմի համաձայն՝ $\mathbb{R}/\mathbb{Z} \simeq S^1$:

Թեորեմ 18.29 (խմբային հոմոմորֆիզմների երկրորդ թեորեմը): *Կամայական $\varphi_1 : Q \to Q'$ և $\varphi_2 : Q \to Q''$ խմբային էպիմորֆիզմների համար, որտեղ $Ker(\varphi_1) \subseteq Ker(\varphi_2)$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\varphi_3 : Q' \to Q''$ խմբային էպիմորֆիզմ, որ $\varphi_1 \cdot \varphi_3 = \varphi_2$, այսինքն՝ տեղափոխական է հոմոմորֆիզմների հետևյալ եռանկյունը.*

$$\begin{tikzcd} Q \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & Q' \arrow[d, "\varphi_3"] \\ & Q'' \end{tikzcd} :$$

Ըստ որում, φ_3-ը կլինի իզոմորֆիզմ այն և միայն այն դեպքում, երբ $Ker(\varphi_1) = Ker(\varphi_2)$*:*

Ապացուցում: Քանի որ $\varphi_1 : Q \to Q'$ արտապատկերումը վերադրող (սյուրեկտիվ) է, ապա յուրաքանչյուր $y \in Q'$ տարրի համար գոյություն ունի այնպիսի $x \in Q$ տարր, որ $\varphi_1(x) = y$: Սահմանենք՝ $\varphi_3(y) = \varphi_2(x)$: Նախ համոզվենք, որ $\varphi_3(y)$-ը կախված չէ $\varphi_1(x) = y$ պայմանին բավարարող x-ի ընտրությունից: Իրոք, եթե նաև $\varphi_1(x') = y$, ապա $\varphi_1(x) = \varphi_1(x')$ և $(\varphi_1(x))^{-1} \cdot \varphi_1(x') = \varphi_1\left(x^{-1}\right) \cdot \varphi_1(x') = \varphi_1\left(x^{-1} \cdot x'\right) = e'$, այսինքն՝ $x^{-1} \cdot x' \in Ker(\varphi_1) \subseteq Ker(\varphi_2)$: Հետևաբար, $x^{-1} \cdot x' \in Ker(\varphi_2)$, այսինքն՝ $\varphi_2\left(x^{-1} \cdot x'\right) = e''$ ($e' \in Q'$ և $e'' \in Q''$ տարրերը Q' և Q'' խմբերի միավորներն են) և $\varphi_2(x) = \varphi_2(x')$: Այնուհետև, φ_3-ի վերադրող լինելն ակնհայտ է, որովհետև, եթե $z \in Q''$ և $z = \varphi_2(x)$, $x \in Q$, ապա նշանակելով $\varphi_1(x) = y$, կունենանք՝ $\varphi_3(y) = z$, որտեղ $y \in Q'$: Այժմ ապացուցենք, որ φ_3-ը բավարարում է հոմոմորֆության պայմանին՝

$$\varphi_3(y_1 \cdot y_2) = \varphi_3(y_1) \cdot \varphi_3(y_2),$$

որտեղ $y_1, y_2 \in Q'$: Դիցուք $y_1 = \varphi_1(x_1)$ և $y_2 = \varphi_1(x_2)$: Այդ դեպքում՝ $y_1 \cdot y_2 = \varphi_1(x_1) \cdot \varphi_1(x_2) = \varphi_1(x_1 \cdot x_2)$ և, հետևաբար,

$$\varphi_3(y_1 \cdot y_2) = \varphi_2(x_1 \cdot x_2) = \varphi_2(x_1) \cdot \varphi_2(x_2) = \varphi_3(y_1) \cdot \varphi_3(y_2) :$$

Ի վերջո, քանի որ՝ $\varphi_3(y) = \varphi_2(x)$, որտեղ $y = \varphi_1(x)$, ապա $\varphi_3(\varphi_1(x)) = \varphi_2(x)$, այսինքն՝ $(\varphi_1 \cdot \varphi_3)x = \varphi_2(x)$ ցանկացած $x \in Q$ տարրի համար և $\varphi_1 \cdot \varphi_3 = \varphi_2$, որտեղից էլ բխում է φ_3-ի միակությունը.

$$\varphi_1 \cdot \varphi_3 = \varphi_2,\ \varphi_1 \cdot \varphi_3' = \varphi_2 \longrightarrow \varphi_1 \cdot \varphi_3 = \varphi_1 \cdot \varphi_3' \longrightarrow (\varphi_1 \cdot \varphi_3)x = (\varphi_1 \cdot \varphi_3')x$$

$$\longrightarrow \varphi_3(\varphi_1 x) = \varphi_3'(\varphi_1 x) \longrightarrow \varphi_3(y) = \varphi_3'(y)$$

ցանկացած $y \in Q'$ տարրի համար:

Մնում է ստանալ φ_3-ի փոխմիարժեքության (բիեկտիվության) պայմանը: Դիցուք $Ker(\varphi_1) = Ker(\varphi_2)$: Այդ դեպքում,

$$\varphi_3(y_1) = \varphi_3(y_2),\ y_1 = \varphi_1(x_1),\ y_2 = \varphi_1(x_2) \longrightarrow \varphi_2(x_1) = \varphi_2(x_2) \longrightarrow$$

$$\varphi_2\left(x_1^{-1} \cdot x_2\right) = e'' \longrightarrow \varphi_1\left(x_1^{-1} \cdot x_2\right) = e' \longrightarrow \varphi_1(x_1) = \varphi_1(x_2) \longrightarrow y_1 = y_2,$$

հետևաբար, φ_3-ը նաև ներդրող (ինյեկտիվ) է, այսինքն՝ φ_3-ը փոխմիարժեք (բիեկտիվ) է: Եվ հակառակը, եթե φ_3-ը նաև ներդրող է, ապա

$$x \in Ker(\varphi_2) \longrightarrow \varphi_2(x) = e'' = \varphi_2(e) \longrightarrow \varphi_3\left(\varphi_1(x)\right) = \varphi_3\left(\varphi_1(e)\right) \longrightarrow$$

$$\varphi_1(x) = \varphi_1(e) = e' \longrightarrow x \in Ker(\varphi_1),$$

այսինքն՝ $Ker(\varphi_2) \subseteq Ker(\varphi_1)$ և $Ker(\varphi_1) = Ker(\varphi_2)$: □

Նկատենք նաև, որ խմբային հոմոմորֆիզմների առաջին թեորեմը բխում է խմբային հոմոմորֆիզմների երկրորդ թեորեմից:

Թեորեմ 18.30 (խմբային իզոմորֆիզմների առաջին թեորեմը)*: Եթե $Q(\cdot)$-ը կամայական խումբ է, $K \leqslant Q$, իսկ $H \trianglelefteq Q$, ապա $H \cdot K \leqslant Q$, $H \trianglelefteq H \cdot K$, $H \cap K \trianglelefteq K$ և*

$$K/H \cap K \simeq H \cdot K/H :$$

Ապացույց: Թեորեմի ապացույցը ի վերջո հանգում է խմբային հոմոմորֆիզմների առաջին թեորեմին: Քանի որ $H \trianglelefteq Q$, ապա $H \cdot K = K \cdot H \leqslant Q$ (հատկություն 18.21) և H-ը կլինի ինվարիանտ իրեն պարունակող Q-ի ցանկացած ենթախմբում: Մասնավորապես, $H \trianglelefteq H \cdot K$: Ապացուցենք $H \cap K \trianglelefteq K$ հատկությունը (չնայած այն կստացվի նաև ինքնըստինքյան՝ որպես հոմորֆիզմի միջուկ): Եթե $h \in H \cap K$, իսկ $x \in K$, ապա $xhx^{-1} \in H \trianglelefteq Q$, $xhx^{-1} \in K$ և, հետևաբար, $xhx^{-1} \in H \cap K$, այսինքն՝ $H \cap K \trianglelefteq K$:

Եթե $x \in H \cdot K = K \cdot H$, ապա $x = k \cdot h$, $k \in K$, $h \in H$: Հետևաբար,

$$xH = (k \cdot h)H = kH, \quad k \in K :$$

Այժմ կառուցենք $f : K \to H \cdot K/H$ արտապատկերումը հետևյալ կերպ՝ $f(k) = kH$, $k \in K$: Քանի որ ցանկացած $x \in H \cdot K$ տարրի համար $xH = kH$, $k \in K$, ապա f արտապատկերումը վերադրող է: Ակնհայտ է նաև, որ f-ը հոմոմորֆ արտապատկերում է՝

$$f(k_1 \cdot k_2) = (k_1 \cdot k_2)H = k_1 H \cdot k_2 H = f(k_1) \cdot f(k_2) :$$

Այսպիսով, f հոմոմորֆիզմը խմբային էպիմորֆիզմ է և համաձայն խմբային հոմոմորֆիզմների առաջին թեորեմի՝

$$H \cdot K/H \simeq K/Ker(f) :$$

Մնում է որոշել (հաշվել) $Ker(f)$ միջուկը.

$$k \in Ker(f) \leftrightarrow k \in K,\ f(k) = e' \leftrightarrow k \in K,\ kH = H \leftrightarrow$$

$$\leftrightarrow k \in K,\ k \in H \leftrightarrow k \in K \cap H,$$

այսինքն՝ $Ker(f) = K \cap H$: □

Թեորեմ 18.31 (խմբային իզոմորֆիզմների երկրորդ թեորեմը)*: Եթե $Q(\cdot)$-ը կամայական խումբ է, $H, K \trianglelefteq Q$ և $K \subseteq H$, ապա $K \trianglelefteq H$, $H/K \trianglelefteq Q/K$ և*

$$Q/K \Big/ H/K \simeq Q/H :$$

Ապացուցում: Ակնհայտ է, որ $K \trianglelefteq H$: Սահմանենք հետևյալ $f : Q/K \to Q/H$ արտապատկերումը՝ $f(xK) = xH$, $x \in Q$: Նախ համոզվենք, որ այս համապատասխանեցումն արտապատկերում է, այսինքն՝ եթե $xK = x'K$, ապա $xH = x'H$: Իրոք,

$$xK = x'K \to x^{-1} \cdot x' \in K \subseteq H \to x^{-1} \cdot x' \in H \to xH = x'H :$$

Ակնհայտ է, որ f արտապատկերումը վերադրող է, ապացուցենք դրա հոմոմորֆ լինելը.

$$f(xK \cdot yK) = f((x \cdot y)K) = (x \cdot y)H = xH \cdot yH = f(xK) \cdot f(yK) :$$

Ուստի, կառուցված է $f : Q/K \to Q/H$ խմբային էպիմորֆիզմը և կարելի է կիրառել խմբային հոմոմորֆիզմների առաջին թեորեմը՝ $Q/H \simeq Q/K \Big/ Ker(f)$: Մնում է որոշել $Ker(f)$ միջուկը.

$$xK \in Ker(f) \leftrightarrow f(xK) = H \leftrightarrow xH = H \leftrightarrow x \in H \trianglerighteq K \leftrightarrow xK \in H/K,$$

այսինքն՝ $Ker(f) = H/K \trianglelefteq Q/K$ և

$$Q/H \simeq Q/K \Big/ H/K :$$ □

18.7. Խմբերի ավտոմորֆիզմներ և ներքին ավտոմորֆիզմներ

Խմբի իզոմորֆիզմն իր մեջ կոչվում է այդ **խմբի ավտոմորֆիզմ** կամ **ինքնաձևություն**, այսինքն՝ $\varphi : Q \to Q$ տեսքի իզոմորֆիզմը կոչվում է $Q(\cdot)$ խմբի ավտոմորֆիզմ կամ ինքնաձևություն: $Q(\cdot)$ խմբի բոլոր ավտոմորֆիզմների բազմությունը նշանակվում է $Aut\,Q$-ով:

Լեմմ 18.11: *1) $Aut\,Q$ բազմությունը խումբ է՝ արտապատկերումների արտադրյալի նկատմամբ, ավելի ճիշտ՝ $Aut\,Q \leqslant S_Q$: 2) Եթե $Q \simeq Q'$, ապա $Aut\,Q \simeq Aut\,Q'$:*

Ապացույց: 1) $Aut\,Q$-ի համար հեշտությամբ ստուգվում են խմբի աքսիոմները: 2) Եթե $\varphi : Q \to Q'$ արտապատկերումը, տրված իզոմորֆիզմն է, ապա որոնելի $\mu : Aut\,Q \to Aut\,Q'$ իզոմորֆիզմը որոշվում է հետևյալ բանաձևով՝ $\mu(\alpha) = \varphi^{-1} \cdot \alpha \cdot \varphi : Q' \to Q'$, որտեղ $\alpha \in Aut\,Q$: □

Դիցուք $Q(\cdot)$-ը կամայական խումբ է, իսկ $a \in Q$: Սահմանենք $\alpha_a : Q \to Q$ արտապատկերումը հետևյալ կերպ՝

$$\alpha_a(x) = a^{-1} \cdot x \cdot a, \quad x \in Q :$$

Հեշտությամբ ստուգվում է, որ $\alpha_a \in Aut\,Q$ ցանկացած $a \in Q$ տարրի համար, այսինքն՝ α_a-ն փոխմիարժեք (բիեկտիվ) է և

$$\alpha_a(x \cdot y) = a^{-1}(xy)a = \left(a^{-1}xa\right)\left(a^{-1}ya\right) = \alpha_a(x) \cdot \alpha_a(y) :$$

Այս α_a ավտոմորֆիզմը կոչվում է $Q(\cdot)$ խմբի **ներքին ավտոմորֆիզմ**՝ ծնված $a \in Q$ տարրով: $Q(\cdot)$ խմբի բոլոր ներքին ավտոմորֆիզմների բազմությունն ընդունված է նշանակել $Int\,Q$-ով՝

$$Int\,Q = \{\alpha_a \mid a \in Q\} :$$

Թեորեմ 18.32: *$Int\,Q$ բազմությունը խումբ է արտապատկերումների արտադրյալի նկատմամբ, այսինքն՝ $Int\,Q \leqslant Aut\,Q$: Ավելի ճիշտ՝ $Int\,Q \trianglelefteq Aut\,Q$ և*

$$Int\,Q \simeq Q/Z(Q) :$$

Մասնավորապես, $Int\,S_n \simeq S_n$, եթե $n \geqslant 3$, և $Int\,\mathbb{A}_n \simeq \mathbb{A}_n$, եթե $n \geqslant 4$:

Ապացուցում: Նախ նկատենք, որ $\alpha_e = \varepsilon \in Int\,Q$ և ցանկացած $a, b \in Q$ տարրերի համար՝

$$\alpha_a \cdot \alpha_b = \alpha_{a\cdot b} \in Int\,Q :$$

Հետևաբար, $b = a^{-1}$ դեպքում կունենանք՝ $(\alpha_a)^{-1} = \alpha_{a^{-1}} \in Int\,Q$:

Հեշտությամբ ստուգվում է նաև հետևյալ հավասարությունը՝

$$\varphi \cdot \alpha_a \cdot \varphi^{-1} = \alpha_{\varphi^{-1}(a)} \in Int\,Q$$

ցանկացած $\varphi \in Aut\,Q$ և ցանկացած $a \in Q$ տարրերի համար: Այնուհետև, $\psi : a \to \alpha_a$ համապատասխանությունը կլինի վերադրող հոմոմորֆիզմ՝ $Q(\cdot)$ խմբից $Int\,Q$ խմբի մեջ (վրա), որի միջուկը՝ $Ker(\psi) = Z(Q)$, որովհետև

$$a \in Ker(\psi) \longleftrightarrow \alpha_a = \varepsilon \longleftrightarrow a \cdot x = x \cdot a, \quad \forall x \in Q \longleftrightarrow a \in Z(Q) :$$

Մնում է կիրառել խմբային հոմոմորֆիզմների առաջին թեորեմը:

Վերջին երկու իզոմորֆությունները ստանալու համար բավական է վերհիշել

$$Z(S_n) = \{\varepsilon\}, \quad \text{եթե } n \geqslant 3,$$

և

$$Z(\mathbb{A}_n) = \{\varepsilon\}, \quad \text{եթե } n \geqslant 4,$$

բանաձևերը: □

Հետաքրքրական է, որ $Aut\,S_3 \simeq S_3$, որովհետև $Aut\,S_3 = Int\,S_3$:

Օրինակներ: 1) Անվերջ միածին խումբն օժտված է ընդամենը երկու ավտոմորֆիզմներով՝ ա) $\alpha(x) = x$, բ) $\alpha(x) = x^{-1}$: Այսպիսով, որպեսզի $\alpha : Q \to Q$ արտապատկերումը լինի $Q(\cdot)$ անվերջ միածին խմբի ավտոմորֆիզմ անհրաժեշտ է և բավարար, որ

$$\alpha(x) = x, \qquad \forall x \in Q,$$

կամ

$$\alpha(x) = x^{-1}, \qquad \forall x \in Q :$$

Բավարարությունն ակնհայտ է, ապացուցենք անհրաժեշտությունը: Քանի, որ $Q(\cdot)$ անվերջ միածին խումբն օժտված է ընդամենը երկու ծնիչ տարրերով, որովհետև $Q = (a) = (b) \longleftrightarrow b = a^{\pm 1}$ և $Q = \alpha(Q) = (\alpha a)$, ապա հնարավոր են հետևյալ երկու դեպքերը:

Ա) Եթե $\alpha a = a$, ապա յուրաքանչյուր $x \in Q$ տարրի համար կունենանք՝ $x = a^i$, $i \in \mathbb{Z}$ և $\alpha(x) = \alpha(a^i) = (\alpha a)^i = a^i = x$:
Բ) Եթե $\alpha a = a^{-1}$, ապա յուրաքանչյուր $x \in Q$ տարրի համար կունենանք՝ $x = a^i$, $i \in \mathbb{Z}$ և $\alpha(x) = \alpha(a^i) = (\alpha a)^i = (a^{-1})^i = a^{-i} = (a^i)^{-1} = x^{-1}$:

2) Եթե $Q = (a)$ միածին խմբի կարգը հավասար է n-ի, այսինքն՝ $|a| = n$, ապա այն կլինի օժտված ընդամենը $\varphi(n)$ հատ ավտոմորֆիզմներով, որտեղ φ-ն էյլերի ֆունկցիան է: Իրոք, եթե $\alpha(x) = x^m$, որտեղ $1 \leqslant m \leqslant n$ և $(m, n) = 1$, ապա $\alpha : Q \to Q$ արտապատկերումը կլինի Q խմբի ավտոմորֆիզմ, որովհետև

$$\alpha(x \cdot y) = (x \cdot y)^m = x^m \cdot y^m = \alpha(x) \cdot \alpha(y)$$

և α-ն փոխմիարժեք (բիեկտիվ) է: Նախ ապացուցենք α-ի վերադրող (սյուրեկտիվ) լինելը: Քանի որ $mu + nv = 1$, որտեղ $u, v \in \mathbb{Z}$, ապա յուրաքանչյուր $b \in Q = (a)$ տարրի համար կունենանք՝

$$b = a^t = a^{t \cdot 1} = a^{t(mu+nv)} = a^{tmu} \cdot a^{tnv} = \left(a^{tu}\right)^m \cdot (a^n)^{tv} =$$

$$= \left(a^{tu}\right)^m \cdot e = x^m = \alpha(x),$$

որտեղ $x = a^{tu} \in Q$: Այժմ ապացուցենք α-ի ներդրող (ինյեկտիվ) լինելը: Դիցուք $\alpha(x) = \alpha(y)$, որտեղ $x, y \in Q = \{e, a, \ldots, a^{n-1}\}$, $x = a^i$, $y = a^j$, $0 \leqslant i, j \leqslant n-1$, $|i - j| < n$: Հետևաբար,

$$x^m = y^m \longrightarrow \left(a^i\right)^m = \left(a^j\right)^m \longrightarrow a^{im - jm} =$$

$$= e \longrightarrow m(i-j) \Big/ n \longrightarrow i - j \Big/ n \longrightarrow |i-j| \Big/ n \longrightarrow i - j =$$

$$= 0 \longrightarrow i = j \longrightarrow x = y \ :$$

Եվ հակառակը, եթե $\alpha : Q \to Q$ արտապատկերումը $Q = (a)$ միածին խմբի ավտոմորֆիզմ է, ապա α-ն Q միածին խմբի a ծնիչ տարրը արտապատկերում է ծնիչ տարրի վրա, այսինքն՝ այնպիսի $a^m \in Q$ տարրի վրա, որտեղ $(n, m) = 1$, $1 \leqslant m \leqslant n$: Հետևաբար,

$$\alpha(x) = \alpha\left(a^i\right) = (\alpha a)^i = (a^m)^i = a^{mi} = \left(a^i\right)^m = x^m, \ x \in Q :$$

Այսպիսով, հանգում ենք հետևյալ արդյունքին:

Հատկություն 18.25: *Որպեսզի $\alpha : Q \to Q$ արտապատկերումը լինի վերջավոր n-րդ կարգի Q միածին խմբի ավտոմորֆիզմ անհրաժեշտ է և բավարար, որ ցանկացած $x \in Q$ տարրի համար՝*

$$\alpha(x) = x^m,$$

որտեղ $1 \leqslant m \leqslant n$, $(m,n) = 1$: Հետևաբար, n-րդ կարգի միածին խմբի ավտոմորֆիզմների թիվը հավասար է $\varphi(n)$-ի, որտեղ φ-ն էյլերի ֆունկցիան է: □

Խումբը կոչվում է **կատարյալ**, եթե այն չի օժտված կենտրոնով, իսկ բոլոր ավտոմորֆիզմները ներքին են: Կարելի է ապացուցել, որ S_n սիմետրիկ խումբը կլինի կատարյալ, եթե $n = 3$, $n = 4$, $n = 5$, կամ $n > 6$:

Թեորեմ 18.33: *Կենտրոն չունեցող խմբի բոլոր ավտոմորֆիզմների խումբը ևս կենտրոն չունեցող խումբ է:*

Ապացուցում: Պահանջվում է ապացուցել, որ եթե $Z(Q) = \{e\}$, ապա $Z(Aut\,Q) = \{\varepsilon\}$: Ենթադրենք հակառակը, որ տրված $Q(\cdot)$ խմբի համար՝ $Z(Aut\,Q) \neq \{\varepsilon\}$, որտեղ ε-ը Q բազմության նույնական արտապատկերումն է: Հետևաբար, գոյություն կունենա այնպիսի $\varphi \in Z(Aut\,Q)$ ավտոմորֆիզմ, որ $\varphi \neq \varepsilon$, այսինքն՝ գոյություն կունենա այնպիսի $a \in Q$ տարր, որ $\varphi(a) \neq a$: Քանի որ՝ $\varphi \cdot \alpha_a = \alpha_a \cdot \varphi$, ապա

$$(\varphi \cdot \alpha_a)\, x = (\alpha_a \cdot \varphi)\, x,$$

$$\alpha_a(\varphi x) = \varphi(\alpha_a(x)),$$

$$a^{-1} \cdot \varphi x \cdot a = \varphi\left(a^{-1} \cdot x \cdot a\right) = (\varphi a)^{-1} \cdot \varphi x \cdot \varphi a :$$

Նշանակելով $\varphi(x) = u$, կունենանք՝

$$\varphi(a) \cdot a^{-1} \cdot u = u \cdot \varphi(a) \cdot a^{-1}$$

և $\varphi(a) \cdot a^{-1} \in Z(Q) = \{e\}$, որովհետև $u = \varphi x$ տարրը Q բազմության կամայական տարր է: Հետևաբար՝ $\varphi(a) \cdot a^{-1} = e$ և $\varphi a = a$: Հակասություն: □

18.8. Խմբերի ուղիղ և կիսաուղիղ արտադրյալներ

18.8.1. Խմբերի ուղիղ արտադրյալը: Դիցուք H-ը և K-ն կամայական երկու խմբեր են, որոնց գործողությունները պարզության համար կնշանակենք միևնույն $\cdot$ նշանով: Դիտարկենք H և K բազմությունների դեկարտյան արտադրյալը՝

$$H \times K = \{(h, k)|\; h \in H, k \in K\} :$$

Այս բազմությունն իր մեջ սահմանվող հետևյալ $\cdot$ գործողության նկատմամբ վերածվում է խմբի՝

$$(h, k) \cdot (h', k') = (h \cdot h', k \cdot k'),$$

որտեղ

$$(h, k)^{-1} = \big(h^{-1}, k^{-1}\big) :$$

Եթե e-ն H խմբի միավորն է, իսկ e'-ը K խմբի միավորը, ապա (e, e') զույգը կլինի $H \times K$ խմբի միավորը:

Կառուցված $H \times K$ խումբը կոչվում է H և K **խմբերի ուղիղ արտադրյալ**: Եթե H և K խմբերի գործողությունները նշանակված են $+$ նշանով, ապա $H \times K$ ուղիղ արտադրյալը կոչվում է նաև **ուղիղ գումար** և հաճախ նշանակվում է $H \oplus K$ ձևով:

Օրինակներ: 1) $\mathbb{Z}_2 \times \mathbb{Z}_3 \simeq \mathbb{Z}_6$;

2) $\mathbb{Z}_2 \times \mathbb{Z}_2$ խումբը իզոմորֆ է չորս տարրանի ոչ միածին խմբին:

Լեմմ 18.12: *1)* $H \times K \simeq K \times H$; $(H \times K) \times G \simeq H \times (K \times G)$; *2) Եթե* e-*ն* H *խմբի միավորն է, իսկ* e'-*ը* K *խմբի միավորը, ապա* $H \times \{e'\} \simeq H$, $\{e\} \times K \simeq K$; *3) Եթե* $H \simeq H'$ *և* $K \simeq K'$, *ապա* $H \times K \simeq H' \times K'$; *4)* $H \times K$ *խումբը կլինի աբելյան այն և միայն այն դեպքում, երբ* H *և* K *խմբերն աբելյան են:*

Ապացուցում: 1) Որոնելի իզոմորֆիզմները կառուցվում են հետևյալ կերպ՝

$$\varphi : (h, k) \longrightarrow (k, h), \quad h \in H,\; k \in K\,,$$

$$\psi : ((h, k), g) \longrightarrow (h, (k, g)), \quad h \in H,\; k \in K, g \in G :$$

2) Որոնելի իզոմորֆիզմների սահմանումներն ակնհայտ են:

3) Եթե գոյություն ունեն $\varphi_1 : H \to H'$ և $\varphi_2 : K \to K'$ իզոմորֆիզմները, ապա որոնելի $\varphi : H \times K \to H' \times K'$ իզոմորֆիզմը կառուցվում է հետևյալ կերպ՝

$$\varphi : (h, k) \longrightarrow (\varphi_1(h), \varphi_2(k)), \quad h \in H,\ k \in K :$$

4) Ապացույցն ակնհայտ է: $\square$

Հատկություն 18.26:*Դիցուք H-ը և K-ն կամայական երկու խմբեր են, $H_1 \trianglelefteq H$ և $K_1 \trianglelefteq K$: Այդ դեպքում՝ $H_1 \times K_1 \trianglelefteq H \times K$ և*

$$H \times K \Big/ H_1 \times K_1 \simeq H/H_1 \times K/K_1 :$$

Մասնավորապես, $H \times K \Big/ H \times \{e'\} \simeq K$, $H \times K \Big/ \{e\} \times K \simeq H$:

Ապացուցում: Դիտարկենք $\pi : H \to H/H_1$ և $\pi : K \to K/K_1$ բնական հոմոմորֆիզմները և սահմանենք $f : H \times K \to H/H_1 \times K/K_1$ արտապատկերումը հետևյալ կերպ՝

$$f : (h, k) \longrightarrow (\pi(h), \pi(k)) = (hH_1, kK_1)\,,$$

որտեղ $h \in H$, $k \in K$: Արդյունքում f-ը կլինի վերադրող հոմոմորֆիզմ (էպիմորֆիզմ), որի միջուկը՝ $Ker(f) = H_1 \times K_1$: Մնում է կիրառել խմբային հոմոմորֆիզմների առաջին թեորեմը: $\square$

Հատկություն 18.27:*Խմբերի $H \times K$ ուղիղ արտադրյալը պարունակում է այնպիսի $H' \simeq H$ և $K' \simeq K$ ինվարիանտ ենթախմբեր, որ $H' \cap K' = \{(e, e')\}$, իսկ $H \times K = H' \cdot K'$:*

Ապացուցում: H' և K' ինվարիանտ ենթախմբերը ընտրվում են հետևյալ կերպ՝

$$H' = \{(h, e') |\ h \in H\} \subseteq H \times K,$$

$$K' = \{(e, k) |\ k \in K\} \subseteq H \times K :$$

Նշված երկու պնդումներն, այդ դեպքում, ստուգվում են անմիջապես: $\square$

Տեղի ունի նաև հակառակ պնդումը՝ հետևյալ իմաստով.

Թեորեմ 18.34: *Եթե G խումբն օժտված է այնպիսի H և K ինվարիանտ ենթախմբերով, որ $H \cap K = \{e\}$ և $G = H \cdot K$, ապա $G \simeq H \times K$, այսինքն՝ G խումբն իզոմորֆ է H և K խմբերի ուղիղ արտադրյալին: Այս դեպքում, G խումբը կոչվում է վերլուծելի H և K խմբերի միջոցով:*

Ապացուցում: Միանգամից կառուցենք $f : H \times K \to G$ արտապատկերումը հետևյալ կերպ՝

$$f : (x,y) \to x \cdot y, \quad x \in H,\ y \in K;$$

ա) f արտապատկերումը ներդրող (ինյեկտիվ) է, որովհետև

$$f\left((x,y)\right) = f\left((x',y')\right) \longrightarrow x{\cdot}y = x'{\cdot}y' \longrightarrow (x')^{-1}{\cdot}x = y'{\cdot}y^{-1} \in H{\cap}K = \{e\}$$

$$\longrightarrow (x')^{-1} \cdot x = e,\ y' \cdot y^{-1} = e \longrightarrow x = x',\ y = y' \longrightarrow (x,y) = (x',y') :$$

բ) $G = H{\cdot}K$ հավասարությունից բխում է, որ f արտապատկերումը վերադրող (սյուրեկտիվ) է:

գ) Մնում է ապացուցել

$$f(u \cdot v) = f(u) \cdot f(v)$$

հավասարությունը: Իրոք, եթե $u = (x,y)$, $v = (x',y')$, ապա $u \cdot v = (x \cdot x', y{\cdot}y')$, $f(u) = x{\cdot}y$, $f(v) = x'{\cdot}y'$, $f(u){\cdot}f(v) = xy{\cdot}x'y'$, $f(u{\cdot}v) = xx'{\cdot}yy'$: Բավական է այժմ ապացուցել, որ ցանկացած $s \in H$ և ցանկացած $t \in K$ տարրերի համար՝ $s \cdot t = t \cdot s$: Իրոք, քանի որ $H \trianglelefteq G$ և $K \trianglelefteq G$, ապա

$$s\left(ts^{-1}t^{-1}\right) = \left(sts^{-1}\right)t^{-1} \in H \cap K = \{e\}$$

և, հետևաբար,

$$sts^{-1}t^{-1} = e,$$

$$s \cdot t = t \cdot s : \qquad \square$$

Հետևություն 18.17: *Դիցուք G-ն կամայական խումբ է իր կամայական $H, K \leqslant G$ ենթախմբերով: Որպեսզի $f : (x,y) \to x \cdot y$, $x \in H$, $y \in G$ օրենքով որոշվող $f : H \times K \to G$ արտապատկերումը.*

1) *լինի ներդրող (ինյեկտիվ) անհրաժեշտ է և բավարար, որ $H \cap K = \{e\}$;*

2) *լինի վերադրող (սյուրեկտիվ) անհրաժեշտ է և բավարար, որ $G = H \cdot K$;*

3) *բավարարի $f(u \cdot v) = f(u) \cdot f(v)$ հավասարությանը (ցանկացած $u, v \in H \times K$ տարրերի համար) անհրաժեշտ է և բավարար, որ $x \cdot y = y \cdot x$ ցանկացած $x \in H$ և ցանկացած $y \in K$ տարրերի համար:*

□

Օրինակ, եթե $(m,n) = 1$, ապա $\mathbb{Z}_{m\cdot n} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, կամ եթե $\mathfrak{A} = (a)$ վերջավոր միածին խմբի կարգը հավասար է $m\cdot n$-ի, ապա $\mathfrak{A} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, որտեղ $(m,n) = 1$: Իրոք, $|\mathfrak{A}| = |a| = m \cdot n$: Նշանակելով $H = (a^n) \trianglelefteq \mathfrak{A}$ և $K = (a^m) \trianglelefteq \mathfrak{A}$ կունենանք՝ $|H| = m$, $|K| = n$, $H \cap K = \{e\}$ և քանի որ $nx + my = 1$, ապա յուրաքանչյուր $z \in \mathfrak{A} = (a)$ տարրի համար կարող ենք գրել՝

$$z = a^t = a^{t(nx+my)} = a^{tnx} \cdot a^{tmy} = (a^n)^{xt} \cdot (a^m)^{yt} \in H \cdot K\,,$$

այսինքն՝ $\mathfrak{A} = H \cdot K$: Մնում է օգտվել թեորեմ 18.34-ից (և լեմմ 18.12-ից):

Եթե $(m,n) = d > 1$, ապա $\frac{m\cdot n}{d} < m \cdot n$ և $\mathbb{Z}_m \times \mathbb{Z}_n$ խմբի կամայական (a,b) տարրի համար (հետևություն 18.9)՝

$$\underbrace{(a,b) + (a,b) + \cdots + (a,b)}_{\frac{mn}{d}} = \Big(\frac{n}{d}(ma), \frac{m}{d}(nb)\Big) = (0,0) :$$

Ուստի, $\mathbb{Z}_m \times \mathbb{Z}_n$ խումբը միածին լինել չի կարող և, հետևաբար, չի կարող լինել իզոմորֆ $\mathbb{Z}_{m\cdot n}(+)$ միածին խմբին: Այսպիսով,

$$\mathbb{Z}_{m\cdot n} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \longleftrightarrow (m,n) = 1 \ :$$

Այլ կերպ ասած տեղի ունի հետևյալ պնդումը.

Հատկություն 18.28: *Երկու H, K վերջավոր միածին խմբերի $H \times K$ ուղիղ արտադրյալը կլինի միածին խումբ այն և միայն այն դեպքում, երբ դրանց $|H|$ և $|K|$ կարգերը փոխադարձաբար պարզ են:* □

Ոչ զրոյական Q խումբը ($|Q| > 1$) կոչվում է **տարալուծելի** (ըստ ուղիղ արտադրյալի), եթե գոյություն ունեն այնպիսի ոչ զրոյական H և K խմբեր, որ $Q \simeq H \times K$: Հակառակ դեպքում ոչ զրոյական Q խումբը կոչվում է **ոչ տարալուծելի** կամ կասենք, որ այն **տարալուծելի չէ**: Օրինակ, S_3 խումբը տարալուծելի չէ:

Թեորեմ 18.35: *Անվերջ միածին խումբը տարալուծելի չէ: Ոչ զրոյական վերջավոր միածին խումբը տարալուծելի չէ այն և միայն այն դեպքում, երբ նրա կարգը հավասար է պարզ թվի աստիճանի:*

Ապացուցում: $\mathbb{Z}(+)$ անվերջ միածին խումբը տարալուծելի չէ, որովհետև եթե $H \leqslant \mathbb{Z}$, $K \leqslant \mathbb{Z}$, ապա $H = (m)$, $K = (n)$ և $m \cdot n \in H \cap K$: Հետևաբար, եթե $|H| > 1$ և $|K| > 1$, ապա $m \neq 0$, $n \neq 0$, $m \cdot n \neq 0$ և $|H \cap K| > 1$, որը հակասում է հատկություն 18.27-ին:

Եթե Q վերջավոր միածին խմբի կարգը հավասար է p^n, ապա նրա բոլոր ենթախմբերն են՝

$$\{e\} = H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{n-1} \leqslant H_n = Q,$$

որտեղ $|H_i| = p^i$, $0 \leqslant i \leqslant n$ (թեորեմ 18.18): Հետևաբար, այս դեպքում ևս խումբը չի կարող լինել տարալուծելի: Իսկ, եթե վերջավոր $\mathfrak{A} = (a)$ միածին խմբի կարգը՝ $|\mathfrak{A}| = p_1^{k_1} \cdot p_2^{k_2} \cdots p_s^{k_s}$, $s \geqslant 2$, ապա նշանակելով $n = p_1^{k_1}$, $m = p_2^{k_2} \cdots p_s^{k_s}$, կունենանք՝ $(m, n) = 1$: Հետևաբար, $\mathfrak{A} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$: □

Հետևություն 18.18: *Երկու անվերջ միածին խմբերի ուղիղ արտադրյալը միածին խումբ չէ:* □

Եթե p-ն պարզ թիվ է, իսկ $\mathfrak{A}$-ն վերջավոր միածին խումբ է, որի կարգը հավասար է p^n, $n \geqslant 1$, ապա $\mathfrak{A}$-ն կոչվում է նաև **նախնական** միածին խումբ ըստ p պարզ թվի կամ p պարզ թվի նկատմամբ: Հետևաբար, միևնույն p պարզ թվի նկատմամբ նախնական միածին խմբերի ուղիղ արտադրյալը չի կարող լինել միածին խումբ: Երկու տարբեր պարզ թվերի նկատմամբ նախնական միածին խմբերի ուղիղ արտադրյալը միածին խումբ է, որովհետև

$$\mathbb{Z}_{p^n \cdot q^n} \simeq \mathbb{Z}_{p^n} \times \mathbb{Z}_{q^n},$$

քանի որ $(p^n, q^n) = 1$, եթե $p \neq q$ բնական թվերը պարզ են:

Վերջավոր թվով $H_1, H_2, \ldots, H_n$ խմբերի ուղիղ արտադրյալը սահմանվում է հետևյալ կերպ: Դիտարկում ենք $H_1 \times H_2 \times \cdots \times H_n$ դեկարտյան արտադրյալը, որը կազմում է խումբ հետևյալ գործողության նկատմամբ՝

$$(x_1, x_2, \ldots, x_n) \cdot (x'_1, x'_2, \ldots, x'_n) = (x_1 \cdot x'_1, x_2 \cdot x'_2, \ldots, x_n \cdot x'_n):$$

Կառուցված $H_1 \times H_2 \times \cdots \times H_n$ խումբը կոչվում է $H_1, H_2, \ldots, H_n$ խմբերի ուղիղ արտադրյալ:

Եթե $H_1, H_2, \ldots, H_n$ խմբերն աբելյան են և խմբային գործողությունները նշանակված են $+$ նշանով, ապա դրանց ուղիղ արտադրյալը հաճախ կոչվում է ուղիղ գումար:

Հեշտությամբ նկատվում է, որ խմբերի $H_1 \times H_2 \times \cdots \times H_n$ ուղիղ արտադրյալը օժտված է հետևյալ հատկություններով՝

1) Եթե

$$H_i' = \{(e_1, \ldots, e_{i-1}, x_i, e_{i+1}, \ldots, e_n) \mid x_i \in H_i\},$$

որտեղ e_i-ն H_i խմբի միավորն է, ապա $H_i' \simeq H_i$ և $H_i' \trianglelefteq H_1 \times H_2 \times \cdots \times H_n$, որտեղ $i = 1, 2, \ldots, n$;

2) $H_1 \times H_2 \times \cdots \times H_n = H_1' \cdot H_2' \cdots H_n'$;

3) $H_i' \cap H_1' \cdot H_2' \cdots H_{i-1}' \cdot H_{i+1}' \cdots H_n' = \{e\}$, որտեղ $e = (e_1, \ldots, e_n)$, $i = 1, 2, \ldots, n$:

Ճիշտ է նաև հակառակ պնդումը՝ հետևյալ իմաստով.

Թեորեմ 18.36: *Եթե e միավորով G խումբն օժտված է այնպիսի $H_1, H_2, \ldots, H_n$ ինվարիանտ ենթախմբերով, որ յուրաքանչյուր $i = 1, 2, \ldots, n$ ճշիչի համար՝ $H_i \cap H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n = \{e\}$ և $G = H_1 \cdot H_2 \cdots H_n$, ապա $G \simeq H_1 \times H_2 \times \cdots \times H_n$:*

Ապացուցում: Տրված $H_i \cap H_1 \cdot H_2 \cdots H_{i-1} \cdot H_{i+1} \cdots H_n = \{e\}$ պայմանից բխում է, որ $H_i \cap H_j = \{e\}$, եթե $i \neq j$: Հետևաբար, $x \cdot y = y \cdot x$ ցանկացած $x \in H_i$ և ցանկացած $y \in H_j$ տարրերի համար, որտեղ $i \neq j$: Համապատասխանեցնելով յուրաքանչյուր $(x_1, x_2, \ldots, x_n) \in H_1 \times H_2 \times \cdots \times H_n$ տարրին $x_1 \cdot x_2 \cdots x_n \in G$ արտադրյալը, ստանում ենք պահանջվող իզոմորֆիզմը: □

Հատկություն 18.29: *Եթե $H_1 \trianglelefteq K_1$, $H_2 \trianglelefteq K_2$, ..., $H_n \trianglelefteq K_n$, ապա $H_1 \times H_2 \times \cdots \times H_n \trianglelefteq K_1 \times K_2 \times \cdots \times K_n$ և*

$$K_1 \times K_2 \times \cdots \times K_n \Big/ H_1 \times H_2 \times \cdots \times H_n \simeq \left(K_1 \big/ H_1\right) \times \cdots \times \left(K_n \big/ H_n\right):$$

Ապացուցում: Դիտարկենք $\pi : K_i \to K_i \big/ H_i$ բնական հոմոմորֆիզմը և սահմանենք

$$f : K_1 \times K_2 \times \cdots \times K_n \longrightarrow \left(K_1 \big/ H_1\right) \times \cdots \times \left(K_n \big/ H_n\right)$$

արտապատկերումը՝ հետևյալ կերպ.

$$f : (k_1, \ldots, k_n) \longrightarrow (\pi(k_1), \ldots, \pi(k_n)) = (k_1 H_1, \ldots, k_n H_n),$$

որտեղ $k_i \in K_i$: Արդյունքում, f-ը կլինի վերադրող խմբային հոմոմորֆիզմ (էպիմորֆիզմ), որի միջուկը՝ $Ker(f) = H_1 \times \cdots \times H_n$: Մնում է կիրառել խմբային հոմոմորֆիզմների առաջին թեորեմը: □

Թեորեմ 18.37 (վերջավոր աբելյան խմբերի հիմնական թեորեմը): *Յուրաքանչյուր վերջավոր աբելյան խումբ կամ միածին խումբ է, կամ իզոմորֆ է վերջավոր թվով վերջավոր միածին խմբերի ուղիղ գումարին: Ավելի ճիշտ, միավորից տարբեր յուրաքանչյուր վերջավոր աբելյան խումբ կամ նախնական միածին խումբ է կամ իզոմորֆ է վերջավոր թվով նախնական միածին խմբերի ուղիղ արտադրյալին:* □

18.8.2. Խմբերի կիսաուղիղ արտադրյալը: Անցնենք խմբերի կիսաուղիղ արտադրյալի սահմանմանը: Դիցուք H-ը և K-ն կամայական երկու խմբեր են, իսկ $\varphi : K \to Aut\, H$ արտապատկերումը կամայական խմբային հոմոմորֆիզմ է: φ-ի օգնությամբ բազմությունների $H \times K$ դեկարտյան արտադրյալի վրա սահմանենք հետևյալ գործողությունը`

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot \varphi(k_1)(h_2), k_1 \cdot k_2) :$$

Անմիջական ստուգման եղանակով համոզվում ենք, որ $H \times K$ բազմությունը սահմանված գործողության նկատմամբ վերածվում է խմբի` (e, e') միավորով և

$$(h, k)^{-1} = \left(\varphi\left(k^{-1}\right)\left(h^{-1}\right), k^{-1}\right)$$

հակադարձներով: Ստացված խումբը նշանակվում է $H \underset{\varphi}{\rtimes} K$ ձևով և կոչվում է H և K **խմբերի կիսաուղիղ արտադրյալ**` ըստ $\varphi$ հոմոմորֆիզմի: Մասնավորապես, եթե ցանկացած $k \in K$ տարրի համար` $\varphi(k) = \varepsilon$, ապա խմբերի կիսաուղիղ արտադրյալը հանգում է խմբերի ուղիղի արտադրյալին: Տարբեր հոմոմորֆիզմներին համապատասխանում են տարբեր կիսաուղիղ արտադրյալներ:

G խումբը կանվանենք H և K խմբերի կիսաուղիղ արտադրյալ և կգրենք $G = H \rtimes K$, եթե գոյություն ունի այնպիսի $\varphi : K \to Aut\, H$ խմբային հոմոմորֆիզմ, որ $G = H \underset{\varphi}{\rtimes} K$:

Հատկություն 18.30: *Եթե G խումբը հանդիսանում է H և K խմբերի կիսաուղիղ արտադրյալ, ապա գոյություն կունենան այնպիսի $H' \trianglelefteq G$ ինվարիանտ ենթախումբ և $K' \leqslant G$ ենթախումբ, որ $H' \cap K' = \{(e, e')\}$ և $G = H' \cdot K'$:*

Ապացույցում: Ըստ սահմանման, գոյություն ունի այնպիսի $\varphi : K \to Aut\, H$ խմբային հոմոմորֆիզմ, որ $G = H \underset{\varphi}{\rtimes} K$: Որոնելի H' և K'

ենթախմբերը ընտրվում են հետևյալ կերպ՝

$$H' = \{(h, e') \mid h \in H\},$$

$$K' = \{(e, k) \mid k \in K\}:$$

Ստուգենք $H' \trianglelefteq G$ հատկությունը: Եթե $x \in G$, $x = (h, k)$ և $h^* = (h', e') \in H'$, ապա

$$xh^*x^{-1} = (h, k)(h', e)(h, k)^{-1} =$$

$$= (h, k)(h', e)\left(\varphi\left(k^{-1}\right)\left(h^{-1}\right), k^{-1}\right) = (h_2, e') \in H':$$

Ակնհայտ է, որ $K' \leqslant G$ և $G = H' \cdot K'$, որովհետև

$$(h, e') \cdot (e, k) = (h \cdot \varphi(e')(e), e' \cdot k) = (h \cdot \varepsilon(e), k) = (h \cdot e, k) = (h, k): \quad \square$$

Տեղի ունի նաև հակառակ պնդումը՝ հետևյալ իմաստով.

Թեորեմ 18.38: *Եթե G խումբն օժտված է այնպիսի $H \trianglelefteq G$ ինվարիանտ ենթախմբով և $K \leqslant G$ ենթախմբով, որ $H \cap K = \{e\}$ և $G = H \cdot K$, ապա գոյություն ունի այնպիսի $\varphi : K \to Aut\, H$ խմբային հոմոմորֆիզմ, որ $G \simeq H \underset{\varphi}{\rtimes} K$: Բացի այդ՝ $G/H \simeq K$:*

Ապացուցում: Յուրաքանչյուր $k \in K$ տարրի համար սահմանենք $\alpha_k : H \to H$ ավտոմորֆիզմը հետևյալ կերպ՝ $\alpha_k(h) = khk^{-1} \in H \trianglelefteq G$, իսկ $\varphi : K \to Aut\, H$ հոմոմորֆիզմը սահմանենք $\varphi(k) = \alpha_k \in Aut\, H$, $k \in K$, բանաձևով: Այնուհետև կազմենք $H \underset{\varphi}{\rtimes} K$ կիսաուղիղ արտադրյալը և նկատենք $G \simeq H \underset{\varphi}{\rtimes} K$ իզոմորֆությունը: Որպես պահանջվող իզոմորֆիզմ այստեղ կարելի է վերցնել $\psi : (h, k) \to h \cdot k$ արտապատկերումը, որի վերադրող լինելը բխում է $G = H \cdot K$ հավասարությունից, իսկ ներդրող լինելը՝ $H \cap K = \{e\}$ հավասարությունից:

Ստուգենք հոմոմորֆության պայմանը.

$$\psi\left((h_1, k_1) \cdot (h_2, k_2)\right) = \psi\left((h_1 \cdot \varphi\left(k_1\right)\left(h_2\right), k_1 \cdot k_2)\right) =$$

$$= \psi\left(\left(h_1 k_1 h_2 k_1^{-1}, k_1 k_2\right)\right) = h_1 k_1 h_2 k_1^{-1} k_1 k_2 = h_1 k_1 h_2 k_2 =$$

$$= \psi\left((h_1, k_1)\right) \cdot \psi\left((h_2, k_2)\right):$$

Ապացուցենք $G/H \simeq K$ իզոմորֆությունը՝ օգտվելով խմբային իզոմորֆիզմների առաջին թեորեմից.

$$G/H = {H \cdot K}\Big/H \simeq K\Big/H \cap K = K/(e) \simeq K : \qquad \square$$

Օրինակներ: 1) $S_3 \simeq A_3 \leftthreetimes ((1,2))$, մինչդեռ S_3 սիմետրիկ խումբը տարալուծելի չէ ըստ խմբերի ուղիղ արտադրյալի, որովհետև այդ դեպքում այն կլիներ աբելյան: Հետևաբար, S_3 սիմետրիկ խմբում գոյություն չունի երկրորդ կարգի ինվարիանտ ենթախումբ:

2) Ընդհանուր դեպքում՝ $S_n \simeq A_n \leftthreetimes (\alpha)$, որտեղ $\alpha = (1,2)$:

3) $S_4 \simeq V_4 \leftthreetimes S_3$, որտեղ V_4-ը $x^2 = e$ նույնությանը բավարարող չորրորդ կարգի խումբն է (որը կոչվում է նաև Քլեյնի չորրորդային խումբ):

Թեորեմ 18.39: *Եթե $H \simeq H'$, $K \simeq K'$ և $\varphi : K \to Aut\,H$ արտապատկերումը կամայական խմբային հոմոմորֆիզմ է, ապա $H \underset{\varphi}{\leftthreetimes} K \simeq H' \underset{\psi}{\leftthreetimes} K'$, որտեղ $\psi : K' \to Aut\,H'$ խմբային հոմոմորֆիզմը որոշվում է հետևյալ կերպ՝*

$$\psi = \gamma^{-1} \cdot \varphi \cdot \mu, \quad \mu(\alpha) = \beta^{-1} \cdot \alpha \cdot \beta,$$

իսկ $\beta : H \to H'$, $\gamma : K \to K'$ արտապատկերումները տրված իզոմորֆիզմներն են, $\alpha \in Aut\,H$: Այլ կերպ ասած, ψ արտապատկերումը որոշվում է այնպես, որ տեղափոխական լինի հոմոմորֆիզմների հետևյալ դիագրամը՝

$$\begin{tikzcd}
K \arrow[r, "\varphi"] \arrow[d, "\gamma"'] & Aut\,H \arrow[d, "\mu"] \\
K' \arrow[r, "\psi"'] & Aut\,H'
\end{tikzcd}$$

այսինքն՝ $\gamma \cdot \psi = \varphi \cdot \mu$:

Ապացուցում: Որոնելի $\delta : H \underset{\varphi}{\rightthreetimes} K \to H' \underset{\psi}{\rightthreetimes} K'$ արտապատկերումը սահմանենք հետևյալ կերպ՝

$$\delta : (h, k) \longrightarrow (\beta(h), \gamma(k)) ,$$

որի փոխմիարժեք (բիեկտիվ) լինելն ակնհայտ է: Մնում է ստուգել δ-ի հոմոմորֆությունը: Իրոք,

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1 \cdot \varphi(k_1)(h_2), k_1 \cdot k_2) ,$$

$$\delta\left((h_1, k_1)\right) \cdot \delta\left((h_2, k_2)\right) =$$

$$= (\beta(h_1), \gamma(k_1)) \cdot (\beta(h_2), \gamma(k_2)) = (\beta(h_1) \cdot \psi(\gamma(k_1))(\beta(h_2)), \gamma(k_1)\gamma(k_2)) =$$

$$= (\beta(h_1) \cdot (\varphi \cdot \delta)(k_1)(\beta(h_2)), \gamma(k_1)\gamma(k_2)) =$$

$$= (\beta(h_1) \cdot \delta(\varphi(k_1))(\beta(h_2)), \gamma(k_1)\gamma(k_2)) =$$

$$= \left(\beta(h_1) \cdot \left(\beta^{-1} \cdot \varphi(k_1) \cdot \beta\right)(\beta(h_2)), \gamma(k_1)\gamma(k_2)\right) =$$

$$= (\beta(h_1) \cdot \beta(\varphi(k_1)(h_2)), \gamma(k_1)\gamma(k_2)) =$$

$$= \delta\left((h_1 \cdot \varphi(k_1)(h_2), k_1 \cdot k_2)\right) = \delta\left((h_1, k_1) \cdot (h_2, k_2)\right) :$$ □

18.9. Խմբի ազդեցությունը բազմության վրա: Ուղեծիր, կայունացնող ենթախումբ և դասերի հավասարում: Բեռնսայդի և Ֆրոբենյուսի լեմմը

Դիցուք $Q(\cdot)$-ը կամայական խումբ է՝ $e \in Q$ միավորով, իսկ X-ը կամայական ոչ դատարկ բազմություն է:

Եթե $f : X \times Q \to X$ արտապատկերման դեպքում $f : (x, a) \to y$, ապա գրվում է $y = f(x, a)$ կամ $y = x \circ a$, երբ f-ի փոխարեն օգտագործվում է $\circ$ նշանակումը (նշանը): $(\circ) : X \times Q \to X$ արտապատկերումը կոչվում է $Q(\cdot)$ **խմբի** (աջ) **ազդեցություն** X **բազմության վրա,** եթե տեղի ունեն հետևյալ երկու պայմանները.

ա) $x \circ (a \cdot b) = (x \circ a) \circ b$,

բ) $x \circ e = x$

ցանկացած $x \in X$ և ցանկացած $a, b \in Q$ տարրերի համար: Կասենք, որ $Q(\cdot)$ խումբն ազդում է $X \neq \emptyset$ բազմության վրա, եթե գոյություն ունի կամ տրված է $Q(\cdot)$ խմբի որևէ ազդեցություն X բազմության վրա: Եթե

$G(\cdot)$ խումբն ազդում է X բազմության վրա, ապա X-ը կոչվում է G-բազմություն:

Օրինակներ: 1) Եթե կամայական $Q(\cdot)$ խմբին համապատասխան ընտրենք $X = Q$ և սահմանենք $x \circ a = x \cdot a$, ապա կստանանք $Q(\cdot)$ խմբի ազդեցության օրինակ իր (Q բազմության) վրա:

2) Եթե $Q(\cdot)$-ը կամայական խումբ է, $H \leqslant Q$, իսկ $X = Q/H_r$ և սահմանենք $Hx \circ a = H(x \cdot a)$, ապա կստանանք $Q(\cdot)$ խմբի ազդեցության օրինակ $X = Q/H_r$ բազմության վրա: Իրոք,

ա) $Hx \circ (a \cdot b) = H(x \cdot (a \cdot b)) = H((x \cdot a) \cdot b) = H(x \cdot a) \circ b = (Hx \circ a) \circ b$,

բ) $Hx \circ e = H(x \cdot e) = Hx$:

3) Եթե կամայական $Q(\cdot)$ խմբին համապատասխան ընտրենք $X = Q$ և սահմանենք $x \circ a = a^{-1}xa$, ապա կստանանք ազդեցության օրինակ, որը կոչվում է $Q(\cdot)$ խմբի ազդեցություն իր վրա՝ համալուծներով: Իրոք,

ա) $x \circ (a \cdot b) = (ab)^{-1}x(ab) = b^{-1}a^{-1}xab = b^{-1}(x \circ a)b = (x \circ a) \circ b$,

բ) $x \circ e = e^{-1}xe = x$:

4) Կամայական $Q(\cdot)$ խմբի բոլոր ենթախմբերի բազմությունը նշանակենք $Sub(Q)$-ով՝

$$Sub(Q) = \{H \subseteq Q \mid H \leqslant Q\} :$$

Եթե ընտրենք $X = Sub(Q)$ և սահմանենք

$$H \circ a = a^{-1}Ha = \left\{a^{-1}ha \mid h \in H\right\} \leqslant Q,$$

ապա կստանանք $Q(\cdot)$ խմբի ազդեցության օրինակ իր բոլոր ենթախմբերի բազմության վրա, որովհետև.

ա) $H \circ (a \cdot b) = (ab)^{-1}H(ab) = b^{-1}a^{-1}Hab = b^{-1}(H \circ a)b = (H \circ a) \circ b$,

բ) $H \circ e = e^{-1}He = H$:

5) Եթե $Q(\cdot)$ խմբի ազդեցությունը $X \neq \emptyset$ բազմության վրա տրված է $x \circ a$ օրենքով, ապա ցանկացած $Y \subseteq X$ (ոչ դատարկ) ենթաբազմության համար սահմանելով

$$Y \circ a = \{y \circ a \mid y \in Y\} \subseteq X,$$

կստանանք $Q(\cdot)$ խմբի նոր ազդեցության օրինակ X-ի բոլոր (ոչ դատարկ) ենթաբազմությունների բազմության վրա:

6) Եթե $Q(\cdot)$ խմբի ազդեցությունը $X \neq \emptyset$ բազմության վրա տրված է $x \circ a$ օրենքով, ապա այս ազդեցությունը մակածում է $Q(\cdot)$ խմբի նոր ազդեցություն $X^{(n)} = \underbrace{X \times \cdots \times X}_{n}$ բազմության վրա, հետևյալ կերպ.

$$(x_1, \ldots, x_n) \circ a = (x_1 \circ a, \ldots, x_n \circ a) \in X^{(n)} :$$

Հետևյալ արդյունքից բխում է, որ խմբի ազդեցության գաղափարը բնութագրվում է նաև խմբային հոմոմորֆիզմի օգնությամբ:

Թեորեմ 18.40*: $Q(\cdot)$ խմբի յուրաքանչյուր ազդեցություն X բազմության վրա մակածում է այդ խմբի հոմոմորֆիզմ S_X սիմետրիկ խմբի մեջ: Եվ հակառակը, $Q(\cdot)$ խմբի յուրաքանչյուր հոմոմորֆիզմ S_X սիմետրիկ խմբի մեջ մակածում է այդ խմբի ազդեցություն X բազմության վրա:*

Ապացույց: Դիցուք տրված է $Q(\cdot)$ խմբի $(\circ)$ ազդեցությունը X-ի վրա: Սահմանենք $R_a : X \to X$ արտապատկերումը (աջ տեղաշարժը) հետևյալ կերպ՝

$$R_a(x) = x \circ a, \quad x \in X,\ a \in Q :$$

Նկատենք, որ R_a-ն փոխմիարժեք (բիեկտիվ) է, որովհետև՝

$$R_a(x) = R_a(y) \longrightarrow x \circ a = y \circ a \longrightarrow (x \circ a) \circ a^{-1} = (y \circ a) \circ a^{-1} \longrightarrow$$

$$\longrightarrow x \circ (a \cdot a^{-1}) = y \circ \left(a \cdot a^{-1}\right) \longrightarrow x \circ e = y \circ e \longrightarrow x = y$$

և կամայական $y \in X$ տարրին համապատասխան ընտրելով $x = y \circ a^{-1}$ կունենանք՝

$$R_a(x) = x \circ a = \left(y \circ a^{-1}\right) \circ a = y \circ \left(a^{-1} \cdot a\right) = y \circ e = y :$$

Այսպիսով, $R_a \in S_X$ ցանկացած $a \in Q$ տարրի համար: Այնուհետև՝

$$R_{a \cdot b} = R_a \cdot R_b$$

ցանկացած $a, b \in Q$ տարրերի համար, որովհետև՝

$$R_{a \cdot b}(x) = x \circ (a \cdot b) = (x \circ a) \circ b = R_a(x) \circ b = R_b\left(R_a(x)\right) = \left(R_a \cdot R_b\right) x :$$

Սահմանելով $\varphi : Q \to S_X$ արտապատկերումը՝ $\varphi(a) = R_a$ օրենքով, նկատենք, որ այն հոմոմորֆ արտապատկերում է.

$$\varphi(a \cdot b) = R_{a \cdot b} = R_a \cdot R_b = \varphi(a) \cdot \varphi(b) :$$

Եվ հակառակը, $Q(\cdot)$ խմբի յուրաքանչյուր $\varphi : Q \to S_X$ հոմոմորֆիզմի համար սահմանելով՝ $x \circ a = \varphi(a)(x) \in X$, որտեղ $a \in Q$, $x \in X$, ստանում ենք $Q(\cdot)$ խմբի ազդեցություն X բազմության վրա, որովհետև.

ա) $x \circ (a \cdot b) = \varphi(a \cdot b)(x) = (\varphi(a) \cdot \varphi(b))\, x = \varphi(b)\,(\varphi(a)x) = \varphi(b)(x \circ a) = (x \circ a) \circ b$,

բ) $x \circ e = \varphi(e)(x) = \varepsilon(x) = x$:

□

Դիցուք $Q(\cdot)$ խումբն ազդում է $X \neq \emptyset$ բազմության վրա, $x \in X$: Ներմուծենք տարրի ուղեծրի գաղափարը հետևյալ կերպ.

$$\mathcal{O}(x) = \{x \circ a \,|\, a \in Q\} \subseteq X$$

ենթաբազմությունը կոչվում է x **տարրի ուղեծիր**: Ակնհայտ է, որ $x \in \mathcal{O}(x)$: Պարզվում է, որ բոլոր ուղեծրերի բազմությունը կազմում է X բազմության տրոհում: Հիմնավորման համար ներմուծենք հետևյալ համարժեքության հարաբերությունը՝

$$x \sim y \longleftrightarrow y = x \circ a \quad \text{որևէ} \;\; a \in Q \;\; \text{տարրի համար},$$

որի համարժեքության դասերը համընկնում են ուղեծրերի հետ: Նախ համոզվենք, որ սահմանված հարաբերությունը բավարարում է համարժեքության սահմանման բոլոր երեք պայմաններին.

1. $x \sim x$, քանի որ $x = x \circ e$;
2. $x \sim y \to y \sim x$, քանի որ $y = x \circ a \to x = y \circ a^{-1}$;
3. $x \sim y$, $y \sim z \to x \sim z$, քանի որ $z = y \circ b = (x \circ a) \circ b = x \circ (a \cdot b)$:

Մնում է նկատել, որ

$$y \in [x] \longleftrightarrow y \sim x \longleftrightarrow x \sim y \longleftrightarrow y = x \circ a \longleftrightarrow y \in \mathcal{O}(x),$$

այսինքն՝ $[x] = \mathcal{O}(x)$ ցանկացած $x \in X$ տարրի համար:

Լեմմ 18.13: *Եթե $X \neq \emptyset$ բազմության վրա ազդող $Q(\cdot)$ խումբը վերջավոր է, ապա ցանկացած $x \in X$ տարրի ուղեծիր կլինի վերջավոր, որի կարգը հանդիսանում է $Q(\cdot)$ խմբի կարգի բաժանարար:*

Այս պնդման ապացուցման համար նախ ներմուծենք մեկ ուրիշ ենթաբազմություն ևս: $x \in X$ **տարրի կայունացնող ենթաբազմությունը** (ստաբիլիզատոր) նշանակվում է $St(x)$-ով և սահմանվում է հետևյալ կերպ՝

$$St(x) = \{a \in Q \mid x \circ a = x\} \subseteq Q :$$

Ակնհայտ է, որ $St(x) \neq \emptyset$, քանի որ $e \in St(x)$:

Լեմմ 18.14: *Կամայական $x \in X$ տարրի համար՝ $St(x) \leqslant Q$:*

Ապացուցում: Ստուգենք ենթախումբ լինելու պայմանները.

$$a, b \in St(x) \longrightarrow x \circ (a \cdot b) = (x \circ a) \circ b = x \circ b = x \longrightarrow a \cdot b \in St(x),$$

$$a \in St(x) \longrightarrow x \circ a = x \longrightarrow (x \circ a) \circ a^{-1} = x \circ a^{-1} \longrightarrow x \circ \big(a \cdot a^{-1}\big) = x \circ a^{-1}$$
$$\longrightarrow x \circ e = x \circ a^{-1} \longrightarrow x \circ a^{-1} = x \longrightarrow a^{-1} \in St(x) : \qquad \square$$

$St(x)$ ենթախումբը կոչվում է x-ի **կայունացնող (կամ իզոտրոպության) ենթախումբ**:

Լեմմ 18.15: *Կամայական $x \in X$ տարրի ուղեծրի հզորությունը (կարգը) հավասար է նույն տարրի կայունացնող ենթախմբի ինդեքսին $Q(\cdot)$ խմբում՝*

$$|\mathcal{O}(x)| = (Q : St(x)) :$$

Մասնավորապես, եթե $Q(\cdot)$ խումբը վերջավոր է, ապա $|\mathcal{O}(x)| = \dfrac{|Q|}{|St(x)|}$:

Ապացուցում: Պահանջվում է կառուցել $\mu : \mathcal{O}(x) \to Q/St(x)_r$ փոխմիարժեք (բիեկտիվ) արտապատկերում: Նշանակենք $H = St(x)$ և սահմանենք $\mu(x \circ a) = Ha$, որտեղ $a \in Q$: Նախ նկատենք, որ այս հավասարությունով իրոք որոշվում է արտապատկերում.

$$x \circ a = x \circ b \longrightarrow x = (x \circ b) \circ a^{-1} = x \circ \big(b \cdot a^{-1}\big) \longrightarrow b \cdot a^{-1} \in H \longrightarrow Hb = Ha :$$

Ակնհայտ է, որ μ արտապատկերումը վերադրող (սյուրեկտիվ) է: Ապացուցենք, որ այն նաև ներդրող (ինյեկտիվ) է.

$$\mu(x \circ a) = \mu(x \circ b) \longrightarrow Ha = Hb \longrightarrow a \cdot b^{-1} \in H = St(x) \longrightarrow$$

$$x \circ \left(a \cdot b^{-1}\right) = x \longrightarrow x \circ a = x \circ b : \qquad \square$$

Օգտվելով նաև Լագրանժի թեորեմից, այստեղից որպես հետևանք ստանում ենք լեմմ 18.13-ի ապացուցումը:

Քանի որ X բազմությունը տրոհվում է իր տարրերի ուղեծրերով, ապա վերջավոր X բազմության դեպքում կարելի է գրել, որ X բազմության կարգը հավասար է զույգ առ զույգ միմյանց հետ չհատվող բոլոր ուղեծրերի կարգերի գումարին՝

$$|X| = \sum_{x_i} |\mathcal{O}(x_i)| :$$

Այս հավասարությունը կոչվում է **դասերի հավասարում**, որը հաճախ գրվում է նաև հետևյալ կերպ՝

$$|X| = \sum_{x_i} (Q : St(x_i)) :$$

Դասերի հավասարման մեջ երբեմն առանձնացվում են բոլոր այն ուղեծրերը, որոնցից յուրաքանչյուրի կարգը հավասար է 1-ի՝ $\mathcal{O}(x_i) = \{x_i\}$: Եթե m-ով նշանակենք մեկ տարրանի բոլոր ուղեծրերի քանակը, ապա դասերի հավասարումը կընդունի հետևյալ տեսքը՝

$$|X| = m + \sum_{\mathcal{O}(x_i) \neq \{x_i\}} |\mathcal{O}(x_i)| :$$

Նկատենք, որ

$$\mathcal{O}(x) = \{x\} \longleftrightarrow x \circ a = x, \quad \forall a \in Q :$$

Այս դեպքում $x \in X$ տարրը կոչվում է դիտարկվող **ազդեցության անշարժ կետ** (տարր): Նշանակենք նաև՝

$$Fix(a) = \{x \in X \mid x \circ a = x\} :$$

Թեորեմ 18.41 (Բեռնսայդի և Ֆրոբենյուսի լեմմը) : *Եթե $Q(\cdot)$ վերջավոր խումբը ազդում է վերջավոր $X \neq \emptyset$ բազմության վրա, իսկ N-ը X բազմության տարրերի ուղեծրերի թիվն է, ապա*

$$N = \frac{1}{|Q|} \cdot \sum_{a \in Q} |Fix(a)| :$$

Ապացուցում: $X \times Q$ բազմության մեջ դիտարկենք բոլոր այն (x,a) զույգերի բազմությունը, որոնց համար $x \circ a = x$: Դիցուք բոլոր այդպիսի զույգերի թիվը հավասար է r-ի: Հետևաբար, մի կողմից՝

$$r = \sum_{a \in Q} |Fix(a)|,$$

իսկ մյուս կողմից՝

$$r = \sum_{x \in X} |St(x)| = \sum_{x \in X} \frac{|Q|}{|\mathcal{O}(x)|} = |Q| \cdot \sum_{x \in X} \frac{1}{|\mathcal{O}(x)|} :$$

Ուստի՝

$$|Q| \cdot \sum \frac{1}{|\mathcal{O}(x)|} = \sum_{a \in Q} |Fix(a)| :$$

Սակայն, եթե $y \in \mathcal{O}(x)$, ապա $\mathcal{O}(y) = \mathcal{O}(x)$ և $|\mathcal{O}(x)| = n$ դեպքում կունենանք՝

$$\sum_{y \in \mathcal{O}(x)} \frac{1}{|\mathcal{O}(y)|} = \underbrace{\frac{1}{n} + \cdots + \frac{1}{n}}_{n} = 1,$$

և պատկերացնելով X-ը տրոհված ըստ N թվով ուղեծրերի, կստանանք՝

$$\sum_{x \in X} \frac{1}{|\mathcal{O}(x)|} = \underbrace{1 + \cdots + 1}_{N} = N :$$

Այսպիսով՝

$$|Q| \cdot N = \sum_{a \in Q} |Fix(a)|$$

և, հետևաբար,

$$N = \frac{1}{|Q|} \cdot \sum_{a \in Q} |Fix(a)|\,, \qquad \square$$

Դիցուք $G(\cdot)$-ը կամայական խումբ է, իսկ X-ը և Y-ը G-բազմություններ են: $f : X \to Y$ արտապատկերումը կոչվում է **էքվիվարիանտ** (G-էքվիվարիանտ) կամ G-**արտապատկերում** (համապատասխան ազդեցությունների միջև), եթե

$$f(x \circ a) = f(x) \circ a$$

ցանկացած $x \in X$ և ցանկացած $a \in G$ տարրերի համար, այսինքն՝ f արտապատկերումը տեղափոխելի է $G(\cdot)$ խմբի տրված ազդեցությունների հետ: Եթե $f : X \to Y$ էքվիվարիանտ արտապատկերումը նաև փոխմիարժեք (բիեկտիվ) է, ապա այն կոչվում է **էքվիիզոմորֆիզմ** կամ համառոտ՝ **էքվիմորֆիզմ**: Նույնական արտապատկերումը էքվիմորֆիզմ է: Երկու էքվիվարիանտ արտապատկերումների արտադրյալը էքվիվարիանտ արտապատկերում է: Երկու X, Y G-բազմություններ կոչվում են **էքվիմորֆ** և գրվում է $X \simeq Y$ կամ $X \cong Y$, եթե դրանց միջև գոյություն ունի որևէ էքվիմորֆիզմ:

Էքվիմորֆության «$\simeq$» հարաբերությունը բավարարում է համարժեքության հարաբերության սահմանման բոլոր երեք պայմաններին:

$G(\cdot)$ խմբի ազդեցությունը X բազմության վրա կոչվում է **տրանզիտիվ**, եթե կամայական $x, y \in X$ տարրերի համար գոյություն ունի այնպիսի $a \in G$ տարր, որ $x \circ a = y$ (այլ կերպ ասած X բազմության բոլոր կետերը համարժեք են դիտարկվող ազդեցության իմաստով):

$G(\cdot)$ խմբի ազդեցությունը X բազմության վրա կոչվում է **ճշգրիտ** կամ **էֆեկտիվ**, եթե $\varphi(a) = R_a$, $a \in G$, օրենքով որոշվող $\varphi : G \to S_X$ հոմոմորֆիզմը ներդրող է, այսինքն՝ $Ker(\varphi) = \{e\}$: Հակառակ դեպքում, խմբի ազդեցությունը կոչվում է **ոչ ճշգրիտ** կամ **ոչ էֆեկտիվ**:

18.10. Կոշիի թեորեմը կամայական վերջավոր խմբի համար: Վերջավոր p-խմբի կենտրոնը

Թեորեմ 18.42 (Կոշի) : *Եթե p պարզ թիվը հանդիսանում է վերջավոր խմբի կարգի բաժանարար, ապա այդ խմբում գոյություն ունի p կարգի որևէ տարր (հետևաբար և p կարգի որևէ ենթախումբ):*

Ապացուցում: Դիցուք վերջավոր $Q(\cdot)$ խմբի կարգը՝ $|Q| = n$ և $n = p \cdot m$, $m \geqslant 1$: Թեորեմն ապացուցենք վերհանգման եղանակով՝ ըստ m-ի: $m = 1$ դեպքում թեորեմի պնդումն ակնհայտ է: Դիցուք m-ից փոքր բնական թվերի համար թեորեմը ճիշտ է, ապացուցենք այն m-ի համար: Հնարավոր են հետևյալ երկու դեպքերը.

ա) $Q = Z(Q)$, այսինքն՝ $Q(\cdot)$ խումբն աբելյան է: Այս դեպքում թեորեմն արդեն ապացուցված է (թեորեմ 18.26):

բ) $Q \neq Z(Q)$, այսինքն՝ $Z(Q) < Q$ և գոյություն կունենա այնպիսի $x_i \in Q$, որ $x_i \notin Z(Q)$: Այս դեպքի համար դիտարկենք $Q(\cdot)$

խմբի ազդեցությունն իր վրա՝ համալուծներով, այսինքն՝ $X = Q$, իսկ ազդեցությունը որոշվում է $x \circ a = a^{-1}xa$ օրենքով: Այս ազդեցության համար գրենք դասերի հավասարումը՝

$$|Q| = \sum_{x_i} |\mathcal{O}(x_i)| = |Z(Q)| + \sum_{\mathcal{O}(x_i) \neq \{x_i\}} |\mathcal{O}(x_i)|$$

հաշվի առնելով, որ

$$\mathcal{O}(x_i) = \{x_i\} \longleftrightarrow x_i \circ a = x_i \ \forall a \in Q \longleftrightarrow a^{-1}x_i a = x_i, \ \forall a \in Q$$

$$\longleftrightarrow x_i a = a x_i, \ \forall a \in Q \longleftrightarrow x_i \in Z(Q),$$

այսինքն՝ մեկ տարրանի ուղեծրերի m թիվը կլինի հավասար $Z(Q)$ կենտրոնի կարգին:

Քանի որ $(Q : St(x_i)) = |\mathcal{O}(x_i)| > 1$. ապա $St(x_i) \neq Q$, այսինքն՝ $St(x_i) < Q$: Հետևաբար, $|St(x_i)| < |Q| = p \cdot m$: Հնարավոր են հետևյալ երկու ենթադեպքերը.

ա’) $St(x_i)$ ենթախմբերից գոնե մեկի կարգը բաժանվում է p-ի վրա, այսինքն՝ $|St(x_i)| = p \cdot m' < p \cdot m$ և $m' < m$: Այս դեպքում պնդումը կլինի ճիշտ՝ համաձայն վերհանգման ենթադրության:

բ’) $St(x_i)$ ենթախմբերից ոչ մեկի կարգը չի բաժանվում p-ի վրա: Բայց քանի որ ըստ Լագրանժի թեորեմի՝

$$|Q| = |St(x_i)| \cdot (Q : St(x_i))\,,$$

ապա այս դեպքում յուրաքանչյուր $(Q : St(x_i))$ արտադրիչ կբաժանվի p-ի վրա: Հետևաբար, դասերի հավասարման մեջ $|Z(Q)|$ գումարելին ևս կբաժանվի p-ի վրա և $Z(Q) < Q$ ենթախմբի համար պնդումը կլինի ճիշտ, որովհետև այն աբելյան խումբ է (կամ համաձայն վերհանգման ենթադրության): □

Ակնհայտ է, որ p^n կարգ ունեցող ցանկացած վերջավոր խումբ p-խումբ է (p-ն պարզ թիվ է): Ճիշտ է նաև հակառակը:

Հետևություն 18.19*: Վերջավոր p-խմբի կարգը հավասար է p^k-ի, որտեղ $k \in \mathbb{N}$:*

Ապացուցում: Բխում է նախորդ թեորեմից: □

Թեորեմ 18.43*: Միավորից տարբեր վերջավոր p-խումբն ունի կենտրոն, այսինքն՝ $Z(Q) \neq \{e\}$, որտեղ $Q(\cdot)$-ը միավորից տարբեր ցանկացած վերջավոր p-խումբ է :*

Ապացույց: Դիցուք $|Q| = p^k$, $k \geqslant 1$: Հնարավոր են հետևյալ երկու դեպքերը.

ա) $Q = Z(Q)$, այս դեպքում պնդումն ակնհայտ է, որովհետև $Q \neq \{e\}$:

բ) $Q \neq Z(Q)$, այսինքն՝ $Z(Q) < Q$ և գոյություն կունենա այնպիսի $x_i \in Q$, որ $x_i \notin Z(Q)$: Այս դեպքի համար դիտարկենք $Q(\cdot)$ խմբի ազդեցությունն իր վրա՝ համալուծներով և այդ ազդեցության համար նորից գրենք դասերի հավասարումը՝

$$|Q| = |Z(Q)| + \sum_{\mathcal{O}(x_i) \neq \{x_i\}} |\mathcal{O}(x_i)| :$$

Ինչպես գիտենք, յուրաքանչյուր $|\mathcal{O}(x_i)|$ գումարելի հանդիսանում է $Q(\cdot)$ խմբի կարգի բաժանարար, այսինքն՝ $|\mathcal{O}(x_i)| = p^{k_i}$, որտեղ $k_i \geqslant 1$: Հետևաբար, $|Z(Q)|$-ն ևս կբաժանվի p-ի վրա, այսինքն՝ $Z(Q)$-ն առնվազն p-տարրանի է: Ուստի $Z(Q) \neq \{e\}$: □

Թեորեմ 18.44: *Եթե վերջավոր p-խմբի կարգը հավասար է p^2, ապա այդպիսի խումբն աբելյան է: Ավելի ճշգրիտ, այդպիսի $Q(\cdot)$ խումբը կամ միածին է (և հետևաբար իզոմորֆ է $\mathbb{Z}_{p^2}(+)$ խմբին) կամ իզոմորֆ է p-րդ կարգի երկու միածին խմբերի ուղիղ արտադրյալին՝ $Q \simeq \mathbb{Z}_p \times \mathbb{Z}_p$: (Սակայն ցանկացած p պարզ թվի համար գոյություն ունի p^3 կարգի ոչ աբելյան խումբ:)*

Ապացույց: Դիտարկենք $Q(\cdot)$ խմբի $Z(Q)$ կենտրոնը: Քանի որ $Z(Q) \trianglelefteq Q$ և $|Q| = p^2$, ապա համաձայն Լագրանժի թեորեմի, $|Z(Q)|$-ն կարող է ընդունել 1, p, p^2 արժեքներից որևէ մեկը: Ըստ նախորդ թեորեմի՝ $|Z(Q)| \neq 1$: Մնում է ապացուցել, որ $|Z(Q)| \neq p$: Ենթադրելով հակառակը, կունենանք՝

$$|Q/Z(Q)| = \frac{|Q|}{|Z(Q)|} = \frac{p^2}{p} = p :$$

Հետևաբար, $Q/Z(Q)$ քանորդ-խումբը կլինի միածին խումբ (թեորեմ 18.20, հետևություն 18.8), այդ դեպքում $Q(\cdot)$ խումբը կլինի աբելյան, հատկություն 18.24, այսինքն՝ $|Z(Q)| = |Q| = p^2$: Հակասություն:

Այժմ ապացուցենք թեորեմի երկրորդ մասը: Դիցուք $Q(\cdot)$ խումբը միածին չէ և $a \in Q$, $a \neq e$: Դիտարկենք $H = (a) \leqslant Q$ ենթախումբը: Ըստ Լագրանժի թեորեմի՝ $|H| = p$, քանի որ $H \neq \{e\}$ և $H \neq Q$: Քանի որ

$Q \setminus H \neq \emptyset$, ապա գոյություն կունենա $b \in Q \setminus H$: Քննարկենք $K = (b) \leqslant Q$ միածին ենթախումբը: Ակնհայտ է, որ $|K| = p$, $H \cap K = \{e\}$, $H \trianglelefteq Q$, $K \trianglelefteq Q$: Նկատենք նաև, որ

$$H \cdot K = \{h \cdot k \mid h \in H, k \in K\} = Q,$$

որովհետև

$$h \cdot k = h' \cdot k' \longrightarrow (h')^{-1} \cdot h = k' \cdot k^{-1} \in H \cap K = \{e\} \longrightarrow$$

$$(h')^{-1} \cdot h = e,\ k' \cdot k = e \longrightarrow h = h',\ k = k'\ ,$$

և, հետևաբար, $|H \cdot K| = |H| \cdot |K| = p \cdot p = p^2 = |Q|$:

Այսպիսով (թեորեմ 18.34), $Q \simeq H \times K \simeq \mathbb{Z}_p \times \mathbb{Z}_p$, քանի որ $H \simeq \mathbb{Z}_p$ և $K \simeq \mathbb{Z}_p$ (լեմմ 18.12):

(Եթե $p = 2$, ապա $p^3 = 8$ կարգի ոչ աբելյան խմբի օրինակ կարող է ծառայել քվատերնիոնների խումբը, այսինքն՝ 2-րդ կարգի

$$\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \pm\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ \pm\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \pm\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

մատրիցների արտադրյալային խումբը ($i^2 = -1$), իսկ $p \neq 2$ դեպքում p^3 կարգի ոչ աբելյան խմբի օրինակ է 3-րդ կարգի

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad a, b, c \in \mathbb{Z}_p,$$

մատրիցների արտադրյալային խումբը: Եվ, օրինակ,

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

ու կառուցված խմբում տեղի ունի նաև $x^p = e$ նույնությունը, որտեղ p-ն կենտ պարզ թիվ է:) $\square$

18.11. Սիլովի թեորեմները (P.L.M. Sylow, 1832–1918)

Դիցուք p-ն պարզ թիվ է: $Q(\cdot)$ խմբի $H \leqslant Q$ ենթախումբը կոչվում է p**-ենթախումբ**, եթե այն p-խումբ է: Մասնավորապես, վերջավոր p-ենթախմբի կարգը կլինի հավասար p^k, $k \in \mathbb{N}$:

$Q(\cdot)$ խմբի $H \leqslant Q$ ենթախումբը կոչվում է p**-սիլովյան** կամ սիլովյան p-ենթախումբ $Q(\cdot)$ խմբում, եթե այն բավարարում է հետևյալ երկու պայմաններին.

ա) H-ը p-ենթախումբ է;

բ) H p-ենթախումբը հնարավոր չէ ընդգրկել իրենից տարբեր $Q(\cdot)$-ի մեկ այլ p-ենթախմբի մեջ:

$Q(\cdot)$ խմբի $H \leqslant Q$ ենթախումբը կոչվում է **սիլովյան**, եթե այն p-սիլովյան է որևէ p պարզ թվի դեպքում:

Ակնհայտ է, որ վերջավոր խմբում յուրաքանչյուր p-ենթախումբ (օրինակ, $H = (e)$) աստիճանական ընդլայնման միջոցով կարելի է հասնել մինչև p-սիլովյան ենթախմբի: Հետևաբար, վերջավոր խմբերում p-սիլովյան ենթախմբերի գոյությունն ակնհայտ է: Մնում է նրանց նկարագրության հարցը (ավելի ճիշտ նրանց կարգի, իզոմորֆության և քանակի հարցերը):

Դիցուք վերջավոր $Q(\cdot)$ խմբի կարգը՝ $|Q| = p^n \cdot t$, որտեղ $(p,t) = 1$, այսինքն՝ t-ն չի բաժանվում է p-ի վրա և հետևաբար p^n-ը p-ի այն ամենամեծ աստիճանն է, որի վրա բաժանվում է $|Q|$-ն: Այդ դեպքում, Լագրանժի թեորեմից բխում է, որ $|H| = p^n$ կարգ ունեցող ցանկացած $H \leqslant Q$ ենթախումբ կլինի p-սիլովյան (եթե այն գոյություն ունի):

Հետևյալ արդյունքը հետաքրքրական է նաև Լագրանժի թեորեմի հակադարձման տեսանկյունից:

Թեորեմ 18.45 (Սիլովի առաջին թեորեմը, 1872 թ.) : *Եթե p-ն պարզ թիվ է և $Q(\cdot)$ վերջավոր խմբի կարգը բաժանվում է p^n-ի վրա, ապա գոյություն ունի այնպիսի $H \leqslant Q$ ենթախումբ, որ $|H| = p^n$: Մասնավորապես, եթե $|Q| = p^n \cdot t$, որտեղ $(p,t) = 1$, ապա $Q(\cdot)$ խմբում գոյություն կունենա p^n կարգի p-սիլովյան ենթախումբ:*

Ապացույց: Կարելի ենթադրել, որ $n \geqslant 1$: Թեորեմն ապացուցենք վերհանգման եղանակով՝ ըստ n-ի: $n = 1$ դեպքում պնդումը ճիշտ է համաձայն Կոշիի թեորեմի (թեորեմ 18.42): Դիցուք n-ից փոքր բնական թվերի համար թեորեմը ճիշտ է, ապացուցենք այն n-ի համար:

Եթե $Q(\cdot)$ վերջավոր խմբի կարգը բաժանվում է p^n-ի վրա, ապա այն կբաժանվի նաև p^{n-1}-ի վրա, հետևաբար գոյություն կունենա այնպիսի

$H \leqslant Q$ ենթախումբ, որ $|H| = p^{n-1}$: Քանի, որ $|Q| = |H| \cdot (Q : H)$, ապա $(Q : H)$ նշիչը կբաժանվի p-ի վրա:

Դիտարկենք H ենթախմբի հետևյալ ազդեցությունը $X = Q/H_r$ բազմության վրա՝

$$Hx \circ h = H(x \cdot h), \quad h \in H, \; x \in Q,$$

և գրենք դասերի հավասարումն այս ազդեցության համար՝

$$|X| = \sum_{x_i} |\mathcal{O}(x_i)| = m + \sum_{\mathcal{O}(x_i) \neq \{x_i\}} |\mathcal{O}(x_i)| :$$

Այս հավասարության ձախ մասը բաժանվում է p-ի վրա, որովհետև $|X| = |Q/H_r| = (Q : H)$: Քանի որ $|\mathcal{O}(x_i)| = p^{k_i}$, ապա

$$\sum_{\mathcal{O}(x_i) \neq \{x_i\}} |\mathcal{O}(x_i)| = p^{k_1} + p^{k_2} + \cdots + p^{k_s}$$

գումարը նույնպես կբաժանվի p-ի վրա, որովհետև $k_i \geqslant 1$: Հետևաբար, m-ը նույնպես կբաժանվի p-ի վրա: Նկարագրենք դիտարկվող վերջավոր H ենթախմբի ազդեցության անշարժ կետերի բազմությունը.

$$Hx \circ h = Hx, \; \forall h \in H \longleftrightarrow H(x \cdot h) = Hx, \; \forall h \in H \longleftrightarrow$$

$$\longleftrightarrow xHx^{-1} = H \longleftrightarrow x \in N_Q(H) \longleftrightarrow Hx \in N_Q(H)/H :$$

Այսպիսով, $|N_Q(H)/H| = m$, որը բաժանվում է p-ի վրա և այժմ կարելի է կիրառել Կոշիի թեորեմը $N_Q(H)/H$ քանորդ-խմբի համար: Գոյություն կունենա այնպիսի $Hb \in N_Q(H)/H$ տարր, որ $|Hb| = p$, $b \in N_Q(H)$: Ներմուծենք $K = (Hb) \leqslant N_Q(H)/H$ միածին ենթախումբը և ընտրենք

$$H' = \pi^{-1}(K) = \{x \in N_Q(H) \,|\, \pi(x) \in K\} \leqslant N_Q(H)$$

ենթախումբը, որտեղ

$$\pi : N_Q(H) \longrightarrow N_Q(H)/H$$

արտապատկերումը բնական հոմոմորֆիզմն է: Խմբային հոմոմորֆիզմների առաջին թեորեմից կունենանք՝ $K \simeq H'/H$ և, հետևաբար, $|H'| = |H| \cdot |K| = p^{n-1} \cdot p = p^n$: $\square$

Հետևություն 18.20: *Եթե $Q(\cdot)$ վերջավոր խմբի կարգը բաժանվում է p^n-ի վրա և $i < n$, ապա p^i կարգ ունեցող ցանկացած $H \leqslant Q$ ենթախումբ կարելի է ընդգրկել այնպիսի $H' \leqslant Q$ ենթախմբում, որ $|H'| = p^{i+1}$ և $H \trianglelefteq H'$: Մասնավորապես, եթե $|Q| = p^n \cdot t$, որտեղ $(p,t) = 1$, ապա $Q(\cdot)$ խմբի յուրաքանչյուր p-սիլովյան ենթախումբ կլինի p^n կարգի:*

Ապացուցում: Նախորդ թեորեմի ապացուցման մեջ`

$$H \leqslant H' \leqslant N_Q(H), \quad \text{որտեղ} \ \ H \trianglelefteq N_Q(H) :$$

Հետևաբար, $H \trianglelefteq H'$: □

Հետևություն 18.21: *Եթե $Q(\cdot)$ վերջավոր խմբի կարգը բաժանվում է p^n-ի վրա, ապա այդ խմբի մեջ գոյություն կունենա ենթախմբերի այնպիսի հաջորդականություն`*

$$\{e\} = H_0 < H_1 < \cdots < H_{n-1} < H_n,$$

որտեղ $|H_i| = p^i$, $H_i \trianglelefteq H_{i+1}$ և հետևաբար $|H_{i+1}/H_i| = p$, այսինքն` H_{i+1}/H_i քանորդ-խումբը միածին է բոլոր $i = 0, 1, \ldots, n-1$ արժեքների դեպքում: □

Հետևություն 18.22: *Եթե $Q(\cdot)$ վերջավոր խմբի կարգը` $|Q| = p^n$, ապա նրա բոլոր մաքսիմալ ենթախմբերը կունենան նույն p^{n-1} կարգը և բոլորն էլ կլինեն ինվարիանտ $Q(\cdot)$ խմբում: (Դեռ ավելին, յուրաքանչյուր $k < n$ բնական թվի համար գոյություն ունի p^k կարգի $H \trianglelefteq Q$ ինվարիանտ ենթախումբ:)* □

Ինչպես տեսանք, եթե $Q(\cdot)$ վերջավոր խմբի կարգը` $|Q| = p^n \cdot t$, որտեղ $(p,t) = 1$, ապա այս խմբի բոլոր p-սիլովյան ենթախմբերը կլինեն բոլոր այն $H \leqslant Q$ ենթախմբերը, որոնց կարգը հավասար է p^n: Ըստ որում, եթե $H \leqslant Q$ ենթախումբը p-սիլովյան է, ապա այդպիսին կլինի նաև $xHx^{-1} \leqslant Q$ ենթախումբը $(x \in Q)$, որովհետև

$$|xHx^{-1}| = |H| = p^n :$$

Հաջորդ արդյունքից բխում է, որ ուրիշ p-սիլովյան ենթախմբեր գոյություն չունեն: Երկու $H, H' \in Q$ ենթախմբեր կոչվում են համալուծ $Q(\cdot)$ խմբում, եթե գոյություն ունի այնպիսի $x \in Q$ տարր, որ $H' = x^{-1}Hx$:

Թեորեմ 18.46 (Սիլովի երկրորդ թեորեմը) ։ *Եթե $Q(\cdot)$ վերջավոր խմբի կարգը՝ $|Q| = p^n \cdot t$, որտեղ $(p,t) = 1$, ապա կամայական $H' \leqslant Q$ p-ենթախմբի և կամայական $H \leqslant Q$ p-սիլովյան ենթախմբի համար գոյություն ունի այնպիսի $a \in Q$ տարր, որ*

$$H' \subseteq a^{-1}Ha :$$

Մասնավորապես, $Q(\cdot)$ խմբի ցանկացած երկու p-սիլովյան ենթախմբեր համալուծ են $Q(\cdot)$-ում և, հետևաբար, իզոմորֆ են (ու ունեն նույն կարգը[19])։

Ապացուցում: Դիտարկենք $H' \leqslant Q$ ենթախմբի հետևյալ ազդեցությունը $X = Q/H_r$ բազմության վրա.

$$Ha \circ h' = H(ah'),$$

որտեղ $a \in Q$, $h' \in H'$: Գրենք դասերի հավասարումն այս ազդեցության համար՝

$$|X| = \sum_{x_i} |\mathcal{O}(x_i)| = p^{k_1} + p^{k_2} + \cdots + p^{k_s} :$$

Մյուս կողմից՝ $|X| = \dfrac{|Q|}{|H|} = \dfrac{p^n \cdot t}{p^n} = t$, որտեղ t-ն չի բաժանվում p-ի վրա: Հետևաբար,

$$t = p^{k_1} + p^{k_2} + \cdots + p^{k_s}$$

հավասարության մեջ որևէ $k_i = 0$, այսինքն՝ $\mathcal{O}(x_i) = \{x_i\}$: Այսպիսով H' ենթախմբի դիտարկվող ազդեցությունը օժտված է որևէ $x_i \in X$ անշարժ կետով: Դիցուք $x_i = Ha$, $a \in Q$: Այդ դեպքում՝

$$Ha \circ h' = Ha,\ \forall h' \in H' \longrightarrow H(ah') = Ha,\ \forall h' \in H' \longrightarrow$$

$$ah' = ha,\ \forall h' \in H \longrightarrow aH' \subseteq Ha \longrightarrow H' \subseteq a^{-1}Ha :$$

Մասնավորապես, եթե $H' \leqslant Q$ ենթախումբը ևս p-սիլովյան է, ապա $H' = a^{-1}Ha \leqslant Q$, քանի որ $a^{-1}Ha$ ենթախումբը p-ենթախումբ է: $\square$

Հետևություն 18.23: *Վերջավոր $Q(\cdot)$ խմբի $H \leqslant Q$ p-սիլովյան ենթախումբը կլինի միակ p-սիլովյան ենթախումբն այն և միայն այն դեպքում, երբ $H \trianglelefteq Q$:* $\square$

[19]ինչը հայտնի է նաև Սիլովի առաջին թեորեմի հետևանքից:

Թեորեմ 18.47 (Սիլովի երրորդ թեորեմը) : *Դիցուք $Q(\cdot)$ վերջավոր խմբի կարգը՝ $|Q| = p^n \cdot t$, որտեղ $(p, t) = 1$ և դիցուք H-ը $Q(\cdot)$-ի որևէ p-սիլովյան ենթախումբ է: Այդ դեպքում $Q(\cdot)$ խմբի բոլոր p-սիլովյան ենթախմբերի քանակը կլինի հավասար $(Q : N_Q(H))$ նշիչին, որը բաղդատելի է 1-ի հետ ըստ p պարզ թվի՝*

$$(Q : N_Q(H)) \equiv 1 (mod\, p) :$$

Ապացուցում: Դիցուք $Syl_p(Q)$-ն $Q(\cdot)$ խմբի բոլոր p-սիլովյան ենթախմբերի բազմությունն է: Դիտարկենք $Q(\cdot)$ խմբի ազդեցությունն իր բոլոր ենթախմբերի

$$X = \{H' \subseteq Q \mid H' \leqslant Q\}$$

բազմության վրա՝ համալուծներով.

$$H' \circ a = a^{-1} H' a,$$

որտեղ $H' \in X$, $a \in Q$: Որոշենք $\mathcal{O}(x)$ ուղեծիրը $x = H \leqslant Q$ դեպքում, հաշվի առնելով Սիլովի երկրորդ թեորեմը.

$$\mathcal{O}(x) = \mathcal{O}(H) = \{H \circ a \mid a \in Q\} = \{a^{-1} H a \mid a \in Q\} = Syl_p(Q) :$$

Այնուհետև, հաշվենք $St(x)$-ը՝ նորից $x = H$ դեպքում.

$$St(x) = St(H) = \{a \in Q \mid H \circ a = H\} = \{a \in Q \mid a^{-1} H a = H\} = N_Q(H) :$$

Հետևաբար,

$$|Syl_p(Q)| = |\mathcal{O}(H)| = (Q : St(H)) = (Q : N_Q(H)) :$$

Թեորեմի առաջին մասն ապացուցված է, մնում է ապացուցել նրա երկրորդ մասը:

Քննարկենք $H \leqslant Q$ p-սիլովյան ենթախմբի ազդեցությունը

$$X' = Syl_p(Q) \subseteq X$$

բազմության վրա՝ համալուծներով.

$$G \circ h = h^{-1} G h \in X',$$

որտեղ $G \in X'$, $h \in H$: Այս ազդեցության համար գրենք դասերի հավասարումը՝

$$|X'| = \sum_{x_i} |\mathcal{O}(x_i)| = m + \sum_{\mathcal{O}(x_i)\neq\{x_i\}} |\mathcal{O}(x_i)|,$$

որտեղ m-ը քննարկվող ազդեցության անշարժ կետերի թիվն է: Այս հավասարման ձախ մասը $Q(\cdot)$ խմբի բոլոր p-սիլովյան ենթախմբերի քանակն է, $\sum\limits_{\mathcal{O}(x_i)\neq\{x_i\}} |\mathcal{O}(x_i)|$ գումարի յուրաքանչյուր գումարելի հանդիսանում է ազդող H խմբի կարգի բաժանարար՝ $|\mathcal{O}(x_i)| = p^i$, $i \geqslant 1$: Հետևաբար, $\sum\limits_{\mathcal{O}(x_i)\neq\{x_i\}} |\mathcal{O}(x_i)|$ գումարը կբաժանվի p-ի վրա: Մնում է ապացուցել, որ $m = 1$:

Նախ նկատենք, որ H-ը անշարժ կետ է, որովհետև

$$H \circ h = h^{-1}Hh = H, \quad \forall h \in H:$$

Այժմ ապացուցենք, որ այս ազդեցությունը բացի H-ից ուրիշ անշարժ կետ չունի: Իրոք, դիցուք $G \in X'$ տարրը անշարժ կետ է, այսինքն՝ $G \circ h = G$, $\forall h \in H$: Հետևաբար, $h^{-1}Gh = G$, $\forall h \in H$ և $H \subseteq N_Q(G)$: Մյուս կողմից, ինչպես գիտենք, $G \trianglelefteq N_Q(G)$: Քանի որ $H, G \leqslant Q$ ենթախմբերը p-սիլովյան են $Q(\cdot)$ խմբում, ապա նրանք կլինեն p-սիլովյան նաև իրենց պարունակող $N_Q(G) \leqslant Q$ ենթախմբում: Ուստի, համաձայն Սիլովի երկրորդ թեորեմի, H և G p-սիլովյան ենթախմբերը կլինեն համալուծ $N_Q(G)$ խմբում, այսինքն՝ գոյություն կունենա այնպիսի $a \in N_Q(G)$ տարր, որ

$$H = a^{-1}Ga = G,$$

քանի որ $G \trianglelefteq N_Q(G)$: □

18.12. Խմբի ծնիչների բազմություն: Խմբի ածանցյալ

18.12.1. Ծնիչների բազմություն: Դիցուք $Q(\cdot)$-ը կամայական խումբ է, իսկ X-ը Q բազմության կամայական ոչ դատարկ ենթաբազմություն է՝ $X \subseteq Q$, $X \neq \emptyset$: Կասենք, որ $Q(\cdot)$ **խումբը ծնվում է** X **ենթաբազմությամբ** կամ X ենթաբազմությունը ծնում է $Q(\cdot)$ խումբը և կգրենք $Q = (X)$, եթե գոյություն չունի $Q(\cdot)$ խմբի այնպիսի $H \leqslant Q$ ենթախումբ, որ $H \neq Q$ և $X \subseteq H$ (այսինքն՝ $Q(\cdot)$ խումբը X-ը պարունակող իր ամենափոքր ենթախումբն է): Այս դեպքում, X ենթաբազմությունը կոչվում է տրված խմբի **ծնիչների** (կամ ծնորդների) **բազմություն**, իսկ նրա տարրերը՝ խմբի ծնիչներ (ծնորդներ) կամ ծնիչ (ծնորդ) տարրեր:

Օրինակ, յուրաքանչյուր $Q(\cdot)$ խումբ օժտված է որևէ ծնիչների բազմությամբ՝ $X = Q$ կամ $X = Q\backslash\{e\}$: $Q = (a)$ միածին խումբը օժտված է մեկ տարրանի $X = \{a\}$ ծնիչների բազմությամբ: Եվ հակառակը, եթե խումբը օժտված է մեկ տարրանի $X = \{a\}$ ծնիչների բազմությամբ, ապա այն կլինի միածին խումբ՝ $Q = (a)$:

Թեորեմ 18.48: *Որպեսզի $Q(\cdot)$ խումբը ծնվի իր ոչ դատարկ $X \subseteq Q$ ենթաբազմությամբ անհրաժեշտ է և բավարար, որ*

$$Q = \{a_1^{\varepsilon_1} \cdot a_2^{\varepsilon_2} \cdots a_n^{\varepsilon_n} \mid \ a_1, a_2, \ldots, a_n \in X, \ \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n = \pm 1, \ n = 1, 2, \ldots\} :$$

Ապացուցում: Եթե հավասարության աջ մասը նշանակենք G-ով, ապա դժվար չէ նկատել, որ $X \subseteq G \leqslant Q$: Ուստի, եթե $Q = (X)$, ապա $Q = G$: Մնում է ապացուցել հակառակը:

Դիցուք $Q = G$: Այդ դեպքում, $X \subseteq Q$: Դիցուք $H \leqslant Q$ ենթախումբն այնպիսին է, որ $X \subseteq H$: Այդ դեպքում, $G \subseteq H$ և քանի որ $G = Q$, ապա $H = Q$: Այսպիսով, գոյություն չունի այնպիսի $H \leqslant Q$ ենթախումբ, որ $H \neq Q$ և $X \subseteq H$, այսինքն՝ $Q = (X)$: □

Օրինակներ: 1) Քանի որ յուրաքանչյուր n-րդ աստիճանի տեղադրություն դիրքափոխությունների արտադրյալ է (թեորեմ 13.1), ապա S_n սիմետրիկ խումբը ծնվում է իր կազմի մեջ եղած բոլոր դիրքափոխությունների բազմությամբ:

2) Հաշվի առնելով

$$(i, j) = (1, i)(1, j)(1, i)$$

հավասարությունը, կարելի է ասել, որ S_n սիմետրիկ խումբը ծնվում է նաև $(1, 2), (1, 3), \ldots, (1, n)$ դիրքափոխությունների բազմությամբ: Մյուս կողմից, քանի որ

$$(1, k) = (1, 2)(2, 3) \cdots (k-1, k)(k-1, k-2) \cdots (3, 2)(2, 1),$$

ապա S_n սիմետրիկ խումբը ծնվում է նաև $(1, 2), (2, 3), \ldots, (n-1, n)$ տեսքի տեղադրությունների բազմությամբ, ինչը բխում է նաև թեորեմ 13.1-ից:

3) Ուշագրավ է նաև այն հանգամանքը, որ S_n սիմետրիկ խմբի համար կարելի է ընտրել ծնիչների այնպիսի X բազմություն, որ $|X| \leqslant 2$:

Իրոք, $n \leqslant 2$ դեպքում S_n խումբը միածին է, իսկ $n \geqslant 3$ դեպքում S_n խումբը կծնվի հետևյալ երկու տեղադրությունների բազմությամբ՝

$$\alpha = (1,2) \quad \text{և} \quad \beta = (1,2,\ldots,n) = (1,2)(1,3)\cdots(1,n),$$

որովհետև

$$\begin{aligned}
&\beta^{-1}\alpha\beta = (2,3),\\
&\beta^{-2}\alpha\beta^{2} = (3,4),\\
&\ \vdots\\
&\beta^{-(n-2)}\alpha\beta^{(n-2)} = (n-1,n),
\end{aligned}$$

իսկ $(1,2),(2,3),\ldots,(n-1,n)$ տեղադրությունների (տարրական դիրքափոխությունների) բազմությամբ, ինչպես գիտենք, ծնվում է S_n խումբը:

4) Զույգ տեղադրությունների $\mathbb{A}_n$ նշանափոխ խումբը $n \leqslant 3$ դեպքում կլինի միածին խումբ, իսկ $n > 3$ դեպքում այն ծնվում է իր կազմի մեջ եղած բոլոր (i,j,k) տեսքի շրջուն տեղադրությունների բազմությամբ: Իրոք, ինչպես հայտնի է (թեորեմ 13.1), զույգ տեղադրությունը վերածվում է զույգ թվով դիրքափոխությունների արտադրյալի և

$$(i,j)(i,k) = (i,j,k),$$

$$(i,j)(k,l) = (i,l,j)(j,k,l):$$

5) Ցանկացած $n > 1$ բնական թվի համար n-րդ կարգի բոլոր մատրիցների գումարային խումբը ծնվում է իր կազմի մեջ եղած բոլոր այն n-րդ կարգի մատրիցների բազմությամբ, որոնց որոծիչը հավասար է 1-ի (H. Bass):

Հատկություն 18.31: *Եթե $Q(\cdot)$ խումբը ծնվում է որևէ $X \subseteq Q$ ենթաբազմությամբ և $\varphi : Q \to Q'$, $\psi : Q \to Q'$ խմբային հոմոմորֆիզմները համընկնում են $X \subseteq Q$ ենթաբազմության վրա, ապա նրանք կհամընկնեն ամենուրեք, այսինքն՝ ամբողջ Q բազմության վրա:*

Ապացուցում: Կամայական $z \in Q = (X)$ տարրի համար հաշվենք $\varphi z \in Q'$ և $\psi z \in Q'$ տարրերը՝ օգտվելով թեորեմ 18.48-ից: Ենթադրելով $z = x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$, որտեղ $x_1, x_2, \ldots, x_n \in X$, իսկ $\varepsilon_i = \pm 1$, $i = 1,2,\ldots,n$, կունենանք՝

$$\varphi z = \varphi\left(x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}\right) = \varphi\left(x_1^{\varepsilon_1}\right) \cdot \varphi\left(x_2^{\varepsilon_2}\right) \cdots \varphi\left(x_n^{\varepsilon_n}\right) =$$

$$= (\varphi x_1)^{\varepsilon_1} \cdot (\varphi x_2)^{\varepsilon_2} \cdots (\varphi x_n)^{\varepsilon_n} = (\psi x_1)^{\varepsilon_1} \cdot (\psi x_2)^{\varepsilon_2} \cdots (\psi x_n)^{\varepsilon_n} =$$
$$= \psi\left(x_1^{\varepsilon_1}\right) \cdot \psi\left(x_2^{\varepsilon_2}\right) \cdots \psi\left(x_n^{\varepsilon_n}\right) = \psi\left(x_1^{\varepsilon_1} \cdot x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}\right) = \psi z : \qquad \square$$

Կասենք, որ $Q(\cdot)$ խումբը օժտված է **վերջավոր** (թվով) **ծնիչներով** կամ ծնիչների վերջավոր բազմությամբ, եթե գոյություն ունի այնպիսի վերջավոր $X \subseteq Q$ ենթաբազմություն, որ $Q = (X)$: Ընդ որում, եթե $X = \{a_1, \ldots, a_n\}$, ապա գրվում է նաև $Q = (a_1, \ldots, a_n)$: Ծնիչների վերջավոր բազմությամբ օժտված խումբը կոչվում է նաև **վերջավոր-ծնված** խումբ:

Հատկություն 18.32*: Վերջավոր ծնիչներով օժտված խմբի յուրաքանչյուր հոմոմորֆ պատկեր ևս վերջավոր ծնիչներով օժտված խումբ է: Ավելի ճիշտ, եթե $Q = (a_1, \ldots, a_n)$, ապա $\varphi Q = (\varphi a_1, \ldots, \varphi a_n)$ կամայական $\varphi : Q \to Q'$ խմբային հոմոմորֆիզմի համար:*

Ապացուցում: Անմիջական ստուգման եղանակով (օգտվելով թեորեմ 18.48-ից): $\square$

Ակնհայտ է, որ տրված $Q(\cdot)$ խմբի և տրված ոչ դատարկ $X \subseteq Q$ ենթաբազմության համար միշտ գոյություն ունի այնպիսի $Q' \leqslant Q$ ենթախումբ, որը ծնվում է X-ով՝ $Q' = (X)$: Այդ $Q' \leqslant Q$ ենթախումբը հավասար է $Q(\cdot)$ խմբի բոլոր այն ենթախմբերի հատմանը, որոնք պարունակում են X-ը՝

$$Q' = \bigcap_{X \subseteq H \leqslant Q} H :$$

Տրված $Q(\cdot)$ խմբի $X \subseteq Q$ ծնիչների բազմությունը կոչվում է **մինիմալ** կամ **չբերվող**, եթե նրա որևէ իրենից տարբեր ենթաբազմությամբ չի ծնվում $Q(\cdot)$ խումբը: Օրինակ, միածին խմբի մեկ տարրանի ծնիչների բազմությունը մինիմալ է: $\mathbb{Z}(+)$ խմբի հետևյալ երկու տարրանի ծնիչների բազմությունները ևս մինիմալ են՝

$$\mathbb{Z} = (2, 3) = (3, 4) = \cdots :$$

$n \geqslant 3$ դեպքում S_n սիմետրիկ խմբի երկու տարրանի ծնիչների բազմությունը մինիմալ է, որովհետև այդ դեպքում S_n սիմետրիկ խումբը միածին չէ, այն նույնիսկ աբելյան չէ:

Ակնհայտ է նաև, որ ծնիչների վերջավոր բազմությամբ օժտված յուրաքանչյուր խումբ օժտված է նաև ծնիչների մինիմալ բազմությամբ: Սակայն գոյություն ունեն անվերջ խմբեր, որոնք չեն օժտված ծնիչների մինիմալ բազմությամբ:

Օրինակ: Բոլոր ռացիոնալ թվերի գումարային խումբը չի օժտված ծնիչների մինիմալ բազմությամբ: Հետևաբար, այդ խումբը չի օժտված նաև ծնիչների վերջավոր բազմությամբ:

Իրոք, դիցուք X-ը դիտարկվող $\mathbb{Q}(+)$ խմբի համար ծնիչների կամայական բազմություն է և $a \in X$: Սահմանենք $H = (X')$ ենթախումբը, որտեղ $X' = X \backslash \{a\}$: Քանի որ $\mathbb{Q}(+)$ խումբը ակնհայտորեն միածին չէ, ապա $X' \neq \emptyset$: Կամայական $b \in X'$ տարրի համար գոյություն ունեն այնպիսի $m, k \in \mathbb{Z}$ ամբողջ թվեր, որ

$$ka = mb \in H$$

(եթե $a = \dfrac{r}{t}$, $b = \dfrac{p}{q}$, ապա $k = pt$, $m = rq$): Մյուս կողմից, օգտվելով թեորեմ 18.48-ից, $\dfrac{1}{k}a \in \mathbb{Q} = (X)$ տարրի համար կունենանք հետևյալ վերլուծությունը՝

$$\frac{1}{k}a = sa + h,$$

որտեղ $s \in \mathbb{Z}$, իսկ $h \in H$: Հետևաբար,

$$a = s(ka) + kh \in H$$

և $H = \mathbb{Q}$:

Ինչպես երևում է $\mathbb{Z}(+)$ խմբի օրինակից , ծնիչների վերջավոր բազմությամբ օժտված խմբի երկու տարբեր մինիմալ ծնիչների բազմություններ կարող են պարունակել տարբեր քանակի տարրեր: Մինչդեռ, եթե խումբը չի օժտված ծնիչների վերջավոր բազմությամբ, ապա ճշմարիտ է հետևյալ արդյունքը:

Թեորեմ 18.49: *Եթե խումբն օժտված է ծնիչների անվերջ X մինիմալ բազմությամբ, ապա նրա ծնիչների յուրաքանչյուր Y մինիմալ բազմություն ևս անվերջ է և $|X| = |Y|$:*

Ապացուցում: Քանի որ $Q = (X)$ և $Q = (Y)$, ապա համաձայն թեորեն 18.48-ի, ցանկացած $y \in Y$ տարր կարելի է ներկայացնել հետևյալ տեսքով՝

$$y = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}, \quad x_1, \ldots, x_n \in X:$$

Նշանակելով՝ $W_y = \{x_1, \ldots, x_n\}$ և $W = \bigcup_{y \in Y} W_y$, կունենանք՝ $Q = (W)$, որտեղ $W \subseteq X$: Հետևաբար, շնորհիվ X-ի մինիմալության՝

$W = X$: Եթե $Y \subseteq Q$ ենթաբազմությունը լիներ վերջավոր, ապա W ենթաբազմությունը ևս կլիներ վերջավոր և շնորհիվ $W = X$ հավասարության վերջավոր կլիներ նաև X ենթաբազմությունը, որը հնարավոր չէ: Ուստի ծնիչների Y մինիմալ բազմությունը անվերջ է և $|Y| \geqslant |W| = |X|$: Սիմետրիկ դատողություններից ստացվում է նաև $|Y| \leqslant |X|$ առնչությունը: Այժմ, համաձայն Կանտոր-Շրյոդեր-Բեռնշտայնի թեորեմի, կունենանք $|X| = |Y|$ հավասարությունը:

□

Առանց ապացուցման նշենք հետևյալ արդյունքը.

Թեորեմ 18.50 (վերջավոր-ծնված աբելյան խմբերի հիմնական թեորեմը): *Վերջավոր ծնիչների բազմությամբ օժտված յուրաքանչյուր աբելյան խումբ կամ միածին խումբ է կամ հանդիսանում է վերջավոր թվով միածին խմբերի ուղիղ գումար (արտադրյալ):*

□

18.12.2. Խմբի ածանցյալ: Ակնհայտ է, որ $Q(\cdot)$ խմբի a և b տարրերը կլինեն տեղափոխելի (այսինքն $a \cdot b = b \cdot a$) այն և միայն այն դեպքում, երբ $a^{-1}b^{-1}ab = e$: Այս հավասարության ձախ մասը կոչվում է a և b տարրերի **տեղափոխիչ** (կոմուտատոր) և նշանակվում է $[a, b]$-ով: $Q(\cdot)$ **խմբի ածանցյալ** կամ **տեղափոխիչ** (կոմուտատոր) է կոչվում նրա այն ենթախումբը, որը ծնվում է նրա բոլոր տեղափոխիչների բազմությամբ և նշանակվում է $Q^{(1)}$-ով կամ Q'-ով՝

$$Q^{(1)} = ([a, b] \mid \ a, b \in Q) :$$

Օրինակներ: 1) Խումբը կլինի աբելյան այն և միայն այն դեպքում, երբ նրա ածանցյալը զրոյական (ենթախումբ) է:

2) $S'_n = \mathbb{A}_n$, եթե $n \geqslant 3$: Իրոք, յուրաքանչյուր $\alpha, \beta \in S_n$ տեղադրությունների համար՝

$$[\alpha, \beta] = \alpha^{-1}\beta^{-1}\alpha\beta$$

տեղափոխիչը ակնհայտորեն զույգ տեղադրություն է և հետևաբար $S'_n \subseteq \mathbb{A}_n$: Հակառակ ներդրումը՝ $\mathbb{A}_n \subseteq S'_n$ ապացուցելու համար նկատենք, որ

$$(i, j)^{-1}(i, k)^{-1}(i, j)(i, k) = (i, j, k)(i, j, k) = (i, k, j)$$

և վերհիշենք այն փաստը, որ զույգ տեղադրությունների $\mathbb{A}_n$ նշանափոխ խումբը ծնվում է իր կազմի մեջ եղած (i, j, k) տեսքի բոլոր տեղադրությունների բազմությամբ, եթե $n \geqslant 3$:

Նկատենք, որ $S_n' \trianglelefteq S_n$ և S_n/S_n' քանորդ-խումբը, լինելով երկրորդ կարգի միածին խումբ, աբելյան է: Այս երկու փաստերը ճիշտ են բոլոր դեպքերում:

Թեորեմ 18.51*: Խմբի ածանցյալը ինվարիանտ ենթախումբ է և համպատասխան քանորդ-խումբը աբելյան է: Խմբի ածանցյալը ընկած է բոլոր այն ինվարիանտ ենթախմբերի մեջ, որոնց նկատմամբ տրված խմբի քանորդ-խմբերն աբելյան են: Ինվարիանտ ենթախմբի ածանցյալը նորից ինվարիանտ ենթախումբ է: $Q(\cdot)$ խմբի ածանցյալը պարունակող ցանկացած $H \leqslant Q$ ենթախումբ ինվարիանտ է $Q(\cdot)$ խմբում:*

Ապացուցում: Հետևյալ հավասարություններից՝

$$[a,b]^{-1} = \left(a^{-1}b^{-1}ab\right)^{-1} = b^{-1}a^{-1}ba = [b,a],$$

$$x^{-1}[a,b]x = x^{-1}a^{-1}b^{-1}abx = x^{-1}a^{-1}x \cdot x^{-1}b^{-1}x \cdot x^{-1}ax \cdot x^{-1}bx = \\ = \left[x^{-1}ax, x^{-1}bx\right]$$

բխում է, որ եթե $z \in Q^{(1)}$ և $z = [a_1, b_1] \cdots [a_n, b_n]$, ապա

$$x^{-1}zx = \left[x^{-1}a_1x, x^{-1}b_1x\right] \cdots \left[x^{-1}a_nx, x^{-1}b_nx\right] \in Q^{(1)} :$$

Հետևաբար, խմբի ածանցյալը ինվարիանտ ենթախումբ է՝ $Q^{(1)} \trianglelefteq Q$: Մյուս կողմից, ցանկացած $a, b \in Q$ տարրերի համար՝

$$aQ^{(1)} \cdot bQ^{(1)} = (a \cdot b)Q^{(1)} = (ba[a,b])Q^{(1)} = (b \cdot a)Q^{(1)} = bQ^{(1)} \cdot aQ^{(1)},$$

քանի որ $[a,b] \in Q^{(1)}$: Մնում է ապացուցել թեորեմի երկրորդ մասը: Եթե $H \trianglelefteq Q$ և Q/H քանորդ-խումբն աբելյան է, ապա

$$H = [aH, bH] = a^{-1}H \cdot b^{-1}H \cdot aH \cdot bH = \left(a^{-1}b^{-1}ab\right)H = [a,b]H,$$

ուստի $[a,b] \in H$ կամայական $a, b \in Q$ տարրերի համար: Հետևաբար $Q^{(1)} \subseteq H$:

Վերը նշված հավասարություններից հետևում է նաև, որ եթե $G \trianglelefteq Q$, ապա $G^{(1)} \trianglelefteq Q$, իսկ եթե $Q^{(1)} \leqslant H \leqslant Q$ և $x \in Q$, $h \in H$, ապա

$$xh^{-1}x^{-1} = \left(xhx^{-1}h^{-1}\right)h = \left[x^{-1}, h^{-1}\right]h \in Q^{(1)}H = H : \qquad \square$$

Հաշվելով $Q^{(1)}$ ածանցյալի $Q^{(2)} = \left(Q^{(1)}\right)^{(1)}$ ածանցյալը, ստանում ենք տրված $Q(\cdot)$ խմբի երկրորդ կարգի ածանցյալը: Շարունակելով այս ընթացքը, կարելի է ստանալ տրված $Q(\cdot)$ խմբի ավելի բարձր կարգի ածանցյալները՝

$$Q \trianglerighteq Q^{(1)} \trianglerighteq Q^{(2)} \trianglerighteq \cdots,$$

որտեղ $Q^{(i+1)} = \left(Q^{(i)}\right)^{(1)}$:

Այս հաջորդականությունը կոչվում է տրված $Q(\cdot)$ **խմբի ածանցյալների շարք**: $Q(\cdot)$ խումբը կոչվում է **լուծելի**, եթե գոյություն ունի այնպիսի $n \geqslant 1$ բնական թիվ, որ $Q^{(n)} = (e)$:

Եթե $Q(\cdot)$ խումբը լուծելի է, ապա այն ամենափոքր n բնական թիվը, որի համար $Q^{(n)} = (e)$, կոչվում է տրված խմբի **լուծելիության ցուցիչ**:

Օրինակներ: 1) S_n սիմետրիկ խմբի ածանցյալների շարքն է՝

$$S_4 \trianglerighteq A_4 \trianglerighteq V \trianglerighteq (e),$$

որտեղ V-ն չորրորդ կարգի ոչ միածին աբելյան խումբն է:

2) Եթե $Q(\cdot)$ խումբը պարզ է, ապա $Q^{(1)} = (e)$ կամ $Q^{(1)} = Q$, որովհետև պարզ խումբը չի օժտված այլ ինվարիանտ ենթախմբերով: Մասնավորապես, ոչ աբելյան պարզ խմբի ածանցյալը հավասար է իրեն: Հետևաբար $\mathbb{A}_n^{(1)} = \mathbb{A}_n$, եթե $n \geqslant 5$: Այսպիսով, որպեսզի $\mathbb{A}_n$ նշանափոխ խումբը լինի լուծելի անհրաժեշտ է և բավարար, որ $n \leqslant 4$:

3) Որպեսզի տեղադրությունների S_n սիմետրիկ խումբը լինի լուծելի անհրաժեշտ է և բավարար, որ $n \leqslant 4$: Իրոք, $n = 1, 2, 3, 4$ դեպքերում

$$S_n^{(1)} = \mathbb{A}_n,$$

իսկ այս դեպքերում $\mathbb{A}_n$ նշանափոխ խումբը լուծելի է, հետևաբար, նշված դեպքերում, կլինի լուծելի նաև S_n-ը: Սակայն $n \geqslant 5$ դեպքում S_n սիմետրիկ խումբը լուծելի չէ, քանի որ, այդ դեպքում, այդպիսին է $\mathbb{A}_n$ նշանափոխ խումբը, որովհետև

$$\mathbb{A}_n = \mathbb{A}_n^{(1)} = \mathbb{A}_n^{(2)} = \cdots :$$

Գալուայի տեսության մեջ S_5 սիմետրիկ խմբի լուծելի չլինելուց բխեցվում է, օրինակ, $x^5 - x - 1 = 0$ հավասարման լուծելի չլինելը արմատանշանների օգնությամբ: Իսկ $n \leqslant 4$ աստիճանի հանրահաշվական հավասարումների արմատանշանների օգնությամբ լուծելի լինելու փաստի իրական պատճառն է S_4 սիմետրիկ խմբի և նրա բոլոր ենթախմբերի լուծելի լինելը:

18.13. Դիսկրետ լոգարիթմներ

Դիցուք $Q(\circ)$-ը կամայական խումբ է, $a \in Q$, իսկ e-ն խմբի միավորն է: Ինչպես գիտենք, այն ամենափոքր ամբողջ և դրական n թիվը, որի համար $a^n = e$, կոչվում է a-ի կարգ և նշանակվում է՝ $n = |a|$:

Եթե $Q(\circ)$-ը կամայական խումբ է, $a, b \in Q$, իսկ $|a| = n$, ապա l բնական թիվը կոչվում է b-ի **դիսկրետ լոգարիթմ ըստ** a **հիմքի** և նշանակվում է՝ $l = d\log_a b$, եթե

$$a^l = b, \quad 0 \leqslant l < n:$$

Ակնհայտ է, որ $a, b \in Q$ տարրերով $l = d\log_a b$ դիսկրետ լոգարիթմը որոշվում է միարժեքորեն:

Օրինակ, $d\log_a a = 1$, եթե $a \neq e$, և $d\log_a e = 0$ ցանկացած վերջավոր կարգ ունեցող $a \in Q$ տարրի համար:

Դպրոցական դասընթացից հայտնի լոգարիթմների տարրական հատկությունները տարածվում են նաև դիսկրետ լոգարիթմների վրա՝

1. $d\log_a b_1 = d\log_a b_2 \longleftrightarrow b_1 = b_2$,
2. $a^{d\log_a b} = b$,
3. $d\log_a(b_1 \cdot b_2) = d\log_a b_1 + d\log_a b_2$, եթե $d\log_a b_1 + d\log_a b_2 < |a|$,
4. $d\log_a \left(b_1 \cdot b_2^{-1}\right) = d\log_a b_1 - d\log_a b_2$, եթե $0 \leqslant d\log_a b_1 - d\log_a b_2$,
5. $d\log_a \left(b_1^{-1} \cdot b_2\right) = d\log_a b_2 - d\log_a b_1$, եթե $0 \leqslant d\log_a b_2 - d\log_a b_1$,
6. $d\log_a (b^m) = m \cdot d\log_a b$, $m \in \mathbb{N}$, եթե $m \cdot d\log_a b < |a|$
7. $a^{d\log_c b} = b^{d\log_c a}$, եթե $d\log_c b \cdot d\log_c a < |c|$,
8. $d\log_a b \cdot d\log_c a = d\log_c b$, եթե $d\log_a b \cdot d\log_c a < |c|$:

Կիրառությունների տեսանկյունից, վերջավոր խմբերում դիսկրետ լոգարիթմների հաշվելու խնդիրը համարվում է խմբերի տեսության կարևորագույն խնդիրներից մեկը: Պահանջվում է, որ հաշվելու համապատասխան ալգորիթմները ունենան հնարավորին չափ քիչ թվով քայլեր: Այս տեսակետից հետաքրքրական են հետևյալ արդյունքները:

Թեորեմ 18.52 (Ա. Օ. Գելֆոնդ, 1962թ.): *Եթե $Q(\circ)$-ը վերջավոր խումբ է, $a, b \in Q$, $|a| = n$ և $l = d\log_a b$, ապա l թիվը կարելի է գտնել $Q(\circ)$ խմբի մեջ կատարելով ամենաշատը $2(\sqrt{n} + \log_2 n) - 1$ հատ բազմապատկման գործողություններ:*

Թեորեմ 18.53 (Վ. Ի. Նեչաև, 1965թ.): *Եթե $Q(\circ)$-ը վերջավոր խումբ է, $a, b \in Q$, $|a| = n = n_1 \cdot n_2$, $1 < n_1 < n$, $1 < n_2 < n$ և $l = d\log_a b$, ապա l թիվը կարելի է գտնել $Q(\circ)$ խմբի մեջ կատարելով ամենաշատը $2(\sqrt{n_1} + \sqrt{n_2}) + 6\log_2 n + \log_2 n_1 - 1$ հատ բազմապատկման գործողություններ:*

18.14. Կիսախմբային հոմոմորֆիզմներ, կիսախմբային հոմոմորֆիզմի միջուկ և կոնգրուենցիա, քանորդ-կիսախումբ: Կիսախմբային հոմոմորֆիզմների թեորեմները

Դիցուք $Q(\cdot)$-ը և $Q'(\circ)$-ը կամայական կիսախմբեր են: $\varphi : Q \to Q'$ արտապատկերումը կոչվում է **հոմոմորֆիզմ**, **հոմոմորֆություն**, **նմանաձևություն** կամ **հոմոմորֆ արտապատկերում** $Q(\cdot)$ կիսախմբից $Q'(\circ)$ կիսախմբի մեջ, եթե տեղի ունի հետևյալ պայմանը.

$$\varphi(x \cdot y) = \varphi(x) \circ \varphi(y)$$

ցանկացած $x, y \in Q$ տարրերի համար: Այս դեպքում ասում են նաև, որ φ արտապատկերումը **համաձայնեցված է** դիտարկվող կիսախմբերի կիսախմբային գործողությունների հետ: Կիսախմբերի միջև գործող հոմոմորֆիզմը հաճախ կոչվում է նաև **կիսախմբային հոմոմորֆիզմ**:

Եթե $\varphi : Q \to Q'$ արտապատկերումը կիսախմբային հոմոմորֆիզմ է, ապա

$$\varphi(Q) = \{\varphi(x) | x \in Q\} \subseteq Q'$$

ոչ դատարկ ենթաբազմությունը կլինի $Q'(\circ)$ կիսախմբի ենթակիսախումբ, այսինքն՝ $\varphi(Q)$-ն կպարունակի իր ցանկացած երկու տարրերի արտադրյալը:

Դժվար չէ ստուգել, որ երկու (հետևաբար և վերջավոր թվով) կիսախմբային հոմոմորֆիզմների արտադրյալը նորից կիսախմբային հոմոմորֆիզմ է, եթե այն գոյություն ունի:

$\varphi : Q \to Q'$ կիսախմբային հոմոմորֆիզմը կոչվում է **ներդրող հոմոմորֆիզմ** կամ **կիսախմբային մոնոմորֆիզմ**, եթե φ

արտապատկերումը նաև ներդրող (ինյեկտիվ) արտապատկերում է: Երկու (հետևաբար և վերջավոր թվով) կիսախմբային մոնոմորֆիզմների արտադրյալը նորից կիսախմբային մոնոմորֆիզմ է, եթե այն գոյություն ունի:

$\varphi : Q \to Q'$ կիսախմբային հոմոմորֆիզմը կոչվում է **վերադրող հոմոմորֆիզմ** կամ **կիսախմբային էպմորֆիզմ**, եթե φ արտապատկերումը նաև վերադրող (սյուրեկտիվ) արտապատկերում է: Երկու (հետևաբար և վերջավոր թվով) կիսախմբային էպմորֆիզմների արտադրյալը նորից կիսախմբային էպիմորֆիզմ է, եթե այն գոյություն ունի:

$\varphi : Q \to Q'$ կիսախմբային հոմոմորֆիզմը կոչվում է **կիսախմբային իզոմորֆիզմ**, **իզոմորֆություն**, **նույնաձևություն** կամ **իզոմորֆ արտապատկերում**, եթե φ արտապատկերումը նաև փոխմիարժեք (բիեկտիվ) արտապատկերում է: Երկու (հետևաբար և վերջավոր թվով) կիսախմբային իզոմորֆիզմների արտադրյալը նորից կիսախմբային իզոմորֆիզմ է, եթե այն գոյություն ունի: Երկու $Q(\cdot)$ և $Q'(\circ)$ կիսախմբեր կոչվում են **իզոմորֆ** կամ **նույնաձև** և գրվում է $Q \simeq Q'$ կամ $Q \cong Q'$, եթե գոյություն ունի որևէ $\varphi : Q \to Q'$ կիսախմբային իզոմորֆիզմ:

Լեմմ 18.16: *Իզոմորֆության սահմանված «$\simeq$» հարաբերությունը բավարարում է համարժեքության հարաբերության սահմանման բոլոր երեք պայմաններին:* □

Դիցուք $Q(\cdot)$-ը կամայական կիսախումբ է: Q բազմության վրա որոշված «$\sim$» համարժեքությունը կոչվում է $Q(\cdot)$ կիսախմբի կորգրուենցիա, եթե տեղի ունի հետևյալ պայմանը.

$$x \sim y, u \sim v \longrightarrow x \cdot u \sim y \cdot v,$$

որտեղ $x, y, u, v \in Q$:

Միևնույն կիսախմբի ցանկացած թվով կոնգրուենցիաների հատումը նորից կոնգրուենցիա է:

Վերհիշենք $\varphi : Q \to Q'$ արտապատկերման $Ker(\varphi) \subseteq Q \times Q$ միջուկի սահմանումը՝

$$(x, y) \in Ker(\varphi) \longleftrightarrow \varphi(x) = \varphi(y), \quad x, y \in Q,$$

որն ակնհայտորեն համարժեքություն է՝ որոշված Q բազմության վրա:

Լեմմ 18.17: *Եթե $\varphi : Q \to Q'$ արտապատկերումը կիսախմբային հոմոմորֆիզմ է՝ $Q(\cdot)$ կիսախմբից $Q'(\circ)$ կիսախմբի մեջ, ապա նրա $Ker(\varphi)$ միջուկը կլինի $Q(\cdot)$ կիսախմբի կոնգրուենցիա:*

Ապացուցում: Իրոք, եթե նշանակենք $Ker(\varphi) = (\sim)$ և ենթադրենք՝ $x \sim y$, $u \sim v$, ապա $\varphi(x) = \varphi(y)$ և $\varphi(u) = \varphi(v)$: Հետևաբար,

$$\varphi(x \cdot u) = \varphi(x) \cdot \varphi(u) = \varphi(y) \cdot \varphi(v) = \varphi(y \cdot v),$$

որտեղից՝ $x \cdot u \sim y \cdot v$: □

Եթե Q բազմության վրա որոշված «$\sim$» համարժեքությունը $Q(\cdot)$ կիսախմբի կոնգրուենցիա է, ապա

$$Q/\sim = \{[a] | a \in Q\}$$

քանորդ-բազմության վրա (մեջ) կարելի է սահմանել բազմապատկման հետևյալ գործողությունը՝

$$[a] \cdot [b] = [a \cdot b],$$

որտեղ $a, b \in Q$: Կոնգրուենցիայի սահմանումից բխում է, որ այս գործողության արդյունքը կախված չէ համարժեքության դասերում ներկայացուցիչների ընտրությունից: Իրոք, եթե $[x] = [y]$ և $[u] = [v]$, ապա կունենանք՝ $x \sim y$ և $u \sim v$. Հետևաբար, ըստ կոնգրուենցիայի սահմանման, կստանանք՝ $x \cdot u \sim y \cdot v$, ուստի $[x \cdot u] = [y \cdot v]$: Սահմանված գործողության զուգորդականությունն ակնհայտ է՝

$$([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$$

ցանկացած $[x], [y], [z] \in Q/\sim$ տարրերի համար:

Այսպիսով, հանգում ենք մեկ գործողությամբ $Q/\sim(\cdot)$ հանրահաշվի, որը կիսախումբ է: Այս կիսախումբը կոչվում է սկզբնական $Q(\cdot)$ **կիսախմբի քանորդ-կիսախումբ** կամ $Q(\cdot)$ **կիսախմբի ֆակտոր-կիսախումբ** ըստ տրված «$\sim$» կոնգրուենցիայի:

$\pi(x) = [x]$ օրենքով որոշվող $\pi : Q \to Q/\sim$ արտապատկերումը կլինի կիսախմբային էպիմորֆիզմ, որովհետև այն սյուրեկտիվ է և

$$\pi(x \cdot y) = [x \cdot y] = [x] \cdot [y] = \pi(x) \cdot \pi(y)$$

ցանկացած $x, y \in Q$ տարրերի համար:

Այս π հոմոմորֆիզմը (էպիմորֆիզմը) կոչվում է **կիսախմբային բնական հոմոմորֆիզմ** (էպիմորֆիզմ) և երբեմն նշանակվում է $\pi_\sim$-ով: Ստուգենք $Ker(\pi_\sim) = (\sim)$ հավասարությունը.

$$(x, y) \in Ker(\pi_\sim) \longleftrightarrow \pi_\sim(x) = \pi_\sim(y) \longleftrightarrow [x] = [y] \longleftrightarrow x \sim y :$$

Այսպիսով, $Q(\cdot)$ կիսախմբի ցանկացած «$\sim$» կոնգրուենցիա հանդիսանում է $\pi_\sim : Q \to Q/_\sim$ կիսախմբային բնական հոմոմորֆիզմի միջուկ: Հանգում ենք հետևյալ արդյունքին. որպեսզի Q բազմության վրա որոշված «$\sim$» համարժեքությունը լինի $Q(\cdot)$ կիսախմբի կոնգրուենցիա անհրաժեշտ է և բավարար, որ գոյություն ունենա այնպիսի $Q'(\circ)$ կիսախումբ և այնպիսի $\varphi : Q \to Q'$ կիսախմբային հոմոմորֆիզմ, որ $Ker(\varphi) = (\sim)$, այսինքն՝ երբ «$\sim$»-ը հանդիսանում է որևէ կիսախմբային հոմոմորֆիզմի միջուկ:

Թեորեմ 18.54 (կիսախմբային հոմոմորֆիզմների առաջին թեորեմը): *Դիցուք $Q(\cdot)$-ը և $Q'(\circ)$-ը ցանկացած կիսախմբեր են: Եթե $\varphi : Q \to Q'$ արտապատկերումը կամայական կիսախմբային էպիմորֆիզմ է, որտեղ $Ker(\varphi) = (\sim)$, ապա $Q' \simeq Q/_\sim$: Ավելի ճշգրիտ, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\mu : Q' \to Q/_\sim$ կիսախմբային իզոմորֆիզմ, որ $\pi = \varphi \cdot \mu$, այսինքն՝ տեղափոխական է կիսախմբային հոմոմորֆիզմների հետևյալ եռանկյունը (դիագրամը).*

$$\begin{tikzcd} Q \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & Q' \arrow[d, "\mu"] \\ & Q/\sim \quad : \end{tikzcd}$$

Ապացուցում: Քանի որ $\varphi : Q \to Q'$ արտապատկերումը սյուրեկտիվ (վերադրող) է, ապա յուրաքանչյուր $z \in Q'$ տարրի համար գոյություն ունի այնպիսի $x \in Q$ տարր, որ $\varphi(x) = z$: Սահմանում ենք $\mu(z) = [x]$, որտեղ $\varphi(x) = z$: Նախ նկատում ենք, որ μ-ն իրոք արտապատկերում է, այսինքն՝ $\mu(z)$-ը կախված չէ $\varphi(x) = z$ պայմանին բավարարող x-ի ընտրությունից: Այնուհետև, ապացուցվում է μ-ի բիեկտիվությունը և հոմոմորֆությունը, իսկ վերջում՝ $\pi = \varphi \cdot \mu$ հավասարությունը և μ -ի միակությունը: $\square$

Թեորեմ 18.55 (կիսախմբային հոմոմորֆիզմների երկրորդ թեորեմը): *Ցանկացած $Q(\cdot)$, $Q'(\circ)$ և $Q''(*)$ կիսախմբերի կամայական $\varphi_1 : Q \to Q'$ և $\varphi_2 : Q \to Q''$ կիսախմբային էպիմորֆիզմների համար, որտեղ $Ker(\varphi_1) \subseteq Ker(\varphi_2)$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\varphi_3 : Q' \to Q''$ էպիմորֆիզմ, որ $\varphi_1 \cdot \varphi_3 = \varphi_2$, այսինքն՝ տեղափոխական է կիսախմբային հոմոմորֆիզմների հետևյալ եռանկյունը (դիագրամը).*

$$\begin{tikzcd} Q \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & Q' \arrow[d, "\varphi_3"] \\ & Q'' \end{tikzcd} \quad :$$

Ըստ որում, φ_3-ը կլինի կիսախմբային իզոմորֆիզմ այն և միայն այն դեպքում, երբ $Ker(\varphi_1) = Ker(\varphi_2)$:

Ապացուցում: Տես թեորեմ 0.9-ի ապացուցումը: □

Եթե $Q(\cdot)$-ը կիսախումբ է, ապա $A \subseteq Q$ և $B \subseteq Q$ ոչ դատարկ ենթաբազմությունների համար սահմանում ենք՝

$$A \cdot B = \{a \cdot b | a \in A, b \in B\} :$$

Q բազմության ոչ դատարկ $I \subseteq Q$ ենթաբազմությունը կոչվում է $Q(\cdot)$ **կիսախմբի իդեալ** և նշանակվում է $I \trianglelefteq Q$, եթե $I \cdot Q \subseteq I$ և $Q \cdot I \subseteq I$: Միևնույն կիսախմբի ցանկացած թվով իդեալների հատումը կլինի իդեալ, եթե այդ հատումը դատարկ չէ:

Կիսախմբերում կոնգրուենցիաների կառուցման տարածված եղանակներից մեկը հետևյալն է.

Դիցուք $Q(\cdot)$-ը կիսախումբ է, իսկ $I \trianglelefteq Q$: Սահմանենք $\rho \subseteq Q \times Q$ հարաբերությունը հետևյալ կերպ՝

$$(x, y) \in \rho \longleftrightarrow x, y \in I \quad \text{կամ} \quad x = y,$$

որտեղ $x, y \in Q$: Ակնհայտ է, որ ρ-ն համարժեքություն է:

Հեշտությամբ ապացուցվում է, որ սահմանված ρ համարժեքությունը նաև $Q(\cdot)$ կիսախմբի կոնգրուենցիա է: Համապատասխան $Q/_{\rho}$ քանորդ-կիսախումբը նշանակվում է նաև $Q/_{I}$-ով և կոչվում է Ռիսի քանորդ-կիսախումբ ըստ I իդեալի (D. Rees):

Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ

1. Ապացուցել, որ 2 կարգի ցանկացած քվազիխումբ խումբ է:

2. Ապացուցել, որ գոյություն ունի 3 կարգի քվազիխումբ, որը խումբ չէ:

3. Ապացուցել, որ 2 կարգի կիսախումբն իզոմորֆ է հետևյալ հինգ կիսախմբերից որևէ մեկին՝

   1) $Q = \{a, b\}$, $x \cdot y = y$;
   2) $Q = \{a, b\}$, $x \cdot y = x$;
   3) $Q = \{a, b\}$, $x \cdot y = a$;
   4) $Q = \{a, b\}$, $a^2 = a$, $b^2 = b$, $a \cdot b = b \cdot a = a$ (զրոյով կիսախումբ);
   5) $Q = \{a, b\}$, $a^2 = a$, $a \cdot b = b \cdot a = b$, $b^2 = a$ (խումբ):

4. Ապացուցել, որ 4 կարգի ցանկացած խումբ կամ միածին է կամ իզոմորֆ է հետևյալ գործողությամբ չորս-տարրանի աբելյան (բայց ոչ միածին) խմբին՝

$$\begin{array}{c|cccc} \cdot & e & a & b & c \\ \hline e & e & a & b & c \\ a & a & e & c & b \\ b & b & c & e & a \\ c & c & b & a & e \end{array} :$$

5. Որոշել $[17] \in \mathbb{Z}_{82}$ տարրի կարգը՝ օգտվելով հատկություն 18.14-ից ($[17] = 17[1]$):

6. Որոշել

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 1 & 4 & 6 & 7 & 8 & 5 \end{pmatrix} \in S_8$$

   տեղադրության կարգը՝ օգտվելով թեորեմ 18.16-ից ($\alpha = (1,2,3) \cdot (5,6,7,8)$) և դրանով ծնված միածին ենթախումբը:

7. Որոշել

ա) $\mathbb{Z}_2(+)$, $\mathbb{Z}_3(+)$, $\mathbb{Z}_4(+)$, $\mathbb{Z}_5(+)$, $\mathbb{Z}_6(+)$, $\mathbb{Z}_7(+)$ և $\mathbb{Z}_{87}(+)$ միածին խմբերի բոլոր ենթախմբերը և ծնիչ տարրերը:

բ) $\sqrt{1}$, $\sqrt[3]{1}$, $\sqrt[4]{1}$, $\sqrt[5]{1}$, $\sqrt[6]{1}$, $\sqrt[7]{1}$ և $\sqrt[87]{1}$ միածին խմբերի բոլոր ենթախմբերը և ծնիչ տարրերը:

8. Ապացուցել, որ $\mathbb{Z}_2^*(\cdot)$, $\mathbb{Z}_3^*(\cdot)$, $\mathbb{Z}_5^*(\cdot)$, $\mathbb{Z}_7^*(\cdot)$, $\mathbb{Z}_{11}^*(\cdot)$, $\mathbb{Z}_{13}^*(\cdot)$ խմբերը միածին են, որտեղ $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{[0]\}$: Որոշել այս միածին խմբերի բոլոր ծնիչ տարրերը:

9. Ապացուցել, որ $n \leqslant 7$ դեպքում $\mathbb{Z}_n(\cdot)$ կիսախմբի բոլոր հակադարձելի տարրերի խումբը միածին է:

10. Ապացուցել, որ $\mathbb{Z}_8(\cdot)$ կիսախմբի բոլոր հակադարձելի տարրերի խումբը միածին չէ և իզոմորֆ է 4 կարգի ոչ միածին խմբին:

11. Ապացուցել, որ $\mathbb{Z}_9(\cdot)$ կիսախմբի բոլոր հակադարձելի տարրերի խումբը միածին է և իզոմորֆ է 6 կարգի $\sqrt[6]{1}$ միածին խմբին:

12. Ապացուցել, որ $\mathbb{Z}_{10}(\cdot)$ կիսախմբի բոլոր հակադարձելի տարրերի խումբը միածին է և իզոմորֆ է 4 կարգի $\sqrt[4]{1}$ միածին խմբին:

13. Որոշել $\mathbb{Z}_{12}(\cdot)$ կիսախմբի $[4]$ և $[9]$ ինքնահամընկնող տարրերին համապատասխանող ենթախմբերը:

14. Ապացուցել, որ եթե e միավորով օժտված $Q(\circ)$ կիսախմբի յուրաքանչյուր $x \in Q$ տարրի համար՝ $x^2 = e$, ապա $Q(\circ)$-ը աբելյան խումբ է: Ցանկացած $p > 2$ պարզ թվի համար գոյություն ունի $x^p = e$ նույնությանը բավարարող ոչ աբելյան խումբ:

15. Գտնել խմբից տարբեր այնպիսի կիսախմբի օրինակ, որն օժտված է այնպիսի աջ (ձախ) միավորով, որի նկատմամբ կիսախմբի յուրաքանչյուր տարր հակադարձելի է ձախից (աջից):

16. Ապացուցել, որ եթե կիսախումբն օժտված է աջ (ձախ) միավորով, ապա բոլոր աջ (ձախ) միավորների բազմությունը կազմում է ենթակիսախումբ:

17. Եթե $Q(\circ)$ կիսախումբն օժտված է ձախ կրճատման հատկությամբ՝

$$a \circ x = a \circ y \longrightarrow x = y, \quad a, x, y \in Q,$$

և $e \in Q$ տարրն ինքնահամընկնող է, ապա e-ն կլինի $Q(\circ)$ կիսախմբի ձախ միավորը:

18. Ապացուցել, որ 8-րդ կարգի ոչ աբելյան խմբում գոյություն ունի 4-րդ կարգի տարր:

19. Ապացուցել, որ 6-րդ կարգի ոչ աբելյան խմբում գոյություն ունի 3-րդ կարգի տարր:

20. Ապացուցել, որ $1, 2, 3, 4$ կարգի յուրաքանչյուր լուպա խումբ է:

21. Կառուցել 5-րդ կարգի այնպիսի լուպայի օրինակ, որը խումբ չէ և որի մեջ գոյություն ունի միավորից տարբեր երկրորդ կարգի տարր ($a^2{=}e$, $a{\neq}e$): Այստեղից բխեցնել, որ Լագրանժի թեորեմը (թեորեմ 18.22) վերջավոր լուպաների դեպքում տեղի չունի, այսինքն՝ վերջավոր լուպայի կարգը կարող է չբաժանվել նրա ենթալուպայի կարգի վրա (ենթալուպայի գաղափարը ենթադրվում է ինքնըստինքյան հասկանալի):

22. Ապացուցել, որ խմբի $a \circ b$ և $b \circ a$ տարրերն ունեն նույն կարգը: Հետևաբար, նույն կարգը կունենան նաև խմբի $a \circ b \circ c$, $b \circ c \circ a$ և $c \circ a \circ b$ տարրերը:

23. Ապացուցել, որ եթե $p < q$ բնական թվերը պարզ են, ապա $p \cdot q$ կարգի խումբը չի կարող ունենալ միմյանցից տարբեր q-րդ կարգի երկու ենթախմբեր:

24. Ապացուցել, որ եթե վերջավոր $Q(\circ)$ աբելյան խմբի կարգը բաժանվում է m բնական թվի վրա, ապա գոյություն ունի $Q(\circ)$ խմբի m կարգի ենթախումբ:

25. Ապացուցել, որ եթե վերջավոր խմբի n կարգը բաժանվում է m բնական թվի վրա և այդ խմբում գոյություն չունի m-տարրանի ենթախումբ, ապա $n \geqslant 12$:

26. Օգտվելով թեորեմ 18.21-ից ապացուցել, որ կոմպլեքս թվերի $\mathbb{C}(\cdot)$ կիսախմբի ցանկացած վերջավոր ենթախումբ միածին է (համեմատել թեորեմ 18.18-ի վերջին պնդման հետ):

27. Ապացուցել, որ եթե միևնույն խմբի երկու ենթախմբեր օժտված են վերջավոր նշիչներով, ապա նրանց հատումը ևս օժտված է վերջավոր նշիչով (Պուանկարե):

28. Ապացուցել, որ եթե $Q(\circ)$ խմբի Q բազմությունը համընկնում է իր $H_1, \ldots, H_n$ ենթախմբերի վերջավոր թվով ձախ հարակից դասերի միավորման հետ, ապա H_i ենթախմբերից որևէ մեկի նշիչը $Q(\circ)$ խմբում վերջավոր է (D. Passman).

29. Դիցուք $Q(\circ)$-ը կամայական խումբ է, $H \leqslant Q$, $a \in Q$: Ապացուցել, որ
$$a \in N_Q(H) \longleftrightarrow aH = Ha :$$

30. Դիցուք $Q(\cdot)$-ը կամայական խումբ է՝ $H \leqslant Q$ կամայական ենթախմբով: Ապացուցել, որ Q խմբի ոչ դատարկ ենթաբազմությունների $S(Q)$ կիսախմբի $H \in S(Q)$ ինքնահամընկնող տարրին համապատասխանող $S(Q)^*_H$ ենթախումբը համընկնում է $N_Q(H)/_H$ ֆակտոր-խմբի հետ, որտեղ $N_Q(H)$-ը H-ի նորմալացնող ենթախումբն է $Q(\cdot)$ խմբում:

(Ցուցում. ակնհայտ է, որ $N_Q(H)/_H \subseteq S(Q)^*_H$: Մնում է ապացուցել հակառակ ներդրումը: Եթե $X \in S(Q)^*_H$ և $x, t \in X$, ապա ինչպես և թեորեմ 18.25-ի ապացուցման ժամանակ, կստանանք $X = xH$: Այնուհետև, $H \cdot X = X$ պայմանից բխում է, $Hx \subseteq X$: Այնուհետև, $t \cdot x^{-1} \in X \cdot Y = H$ և $t \in Hx$, այսինքն՝ $X \subseteq Hx$: Այսպիսով, նաև $X = Hx$: Ուստի, $Hx = xH$: Հետևաբար, $X = xH$, որտեղ $x \in N_Q(H)$, և $X \in N_Q(H)/_H$:)

31. Կառուցել այնպիսի $Q(\circ)$ խմբի օրինակ, որն օժտված լինի այնպիսի $H \trianglelefteq K \trianglelefteq Q$ ենթախմբերով, որ H-ը ինվարիանտ չէ $Q(\circ)$ խմբում:

32. Որպեսզի $Q(\circ)$ խմբի $H \leqslant Q$ ենթախումբը լինի ինվարիանտ $Q(\circ)$ խմբում անհրաժեշտ է և բավարար, որ $x^{-1} \circ h \circ x \in H$ ցանկացած $x \in Q$ և ցանկացած $h \in H$ տարրերի համար:

33. Դիցուք $Q(\circ)$ -ը կամայական խումբ է՝ կամայական $H \leqslant Q$ ենթախմբով: Որպեսզի $H \trianglelefteq Q$ անհրաժեշտ է և բավարար, որ
$$xH = x'H,\ yH = y'H \longrightarrow (x \circ y)H = (x' \circ y')H,$$
որտեղ $x, x', y, y' \in Q$: Հետևաբար, որպեսզի $xH * yH = (x \circ y)H$, $x, y \in Q$, սահմանումով որոշվի գործողություն $Q/_{H_l} = \{xH |\ x \in Q\}$ բազմության վրա, անհրաժեշտ է և բավարար, որ $H \trianglelefteq Q$:

(Ցուցում. Եթե $H \trianglelefteq Q$ և $xH = x'H$, $yH = y'H$, ապա $x = x' \circ h_1$, $y = y' \circ h_2$, որտեղ $h_1, h_2 \in H$: Հետևաբար, համաձայն թեորեմ 18.24-ի, կունենանք՝

$$x \circ y = x' \circ h_1 \circ y' h_2 = x' \circ y' \circ \left((y')^{-1} \circ h_1 \circ y'\right) \circ h_2 =$$

$$= x' \circ y' \circ h_3 \circ h_2 = x' \circ y' \circ h_4,$$

որտեղ $h_3 = (y')^{-1} \circ h_1 \circ y' \in H$, $h_4 = h_3 \circ h_2 \in H$: Հետևաբար,

$$(x \circ y)H = (x' \circ y' \circ h_4)\, H = (x' \circ y')\, H :$$

Բավարարություն: Քանի որ $xH = (x \circ h)H$ և $x^{-1}H = x^{-1}H$, ապա $\left(x \circ x^{-1}\right) H = \left(x \circ h \circ x^{-1}\right) H$, այսինքն՝ $eH = \left(x \circ h \circ x^{-1}\right) H$ և $x \circ h \circ x^{-1} \in H$ ցանկացած $x \in Q$ և ցանկացած $h \in H$ տարրերի համար: Մնում է օգտվել թեորեմ 18.24-ից:)

34. Եթե $Q(\circ)$ վերջավոր խմբի ցանկացած երկու մաքսիմալ ենթախմբերի հատումը հավասար է $\{e\}$-ի, ապա մաքսիմալ ենթախմբերից որևէ մեկը կլինի ինվարիանտ $Q(\circ)$ խմբում (Միլլեր, Մորենո):

35. Եթե $Q(\circ)$-ը կամայական խումբ է, $H \leqslant K \leqslant Q$ և $(Q : K)$, $(Q : H)$, $(K : H)$ նշիչներից երկուսը վերջավոր են, ապա երրորդ նշիչը ևս կլինի վերջավոր և

$$(Q : H) = (Q : K) \cdot (K : H) :$$

36. Օգտվելով Կոշիի թեորեմից ապացուցել, որ կամայական վերջավոր p-խմբի կարգը հավասար է p^k-ի, որտեղ $k \in \mathbb{N}$:

37. Դիցուք $Q(\circ)$-ը խումբ է, իսկ τ-ն տոպոլոգիա է՝ որոշված Q-ի վրա: $Q(\circ, \tau)$ եռյակը կոչվում է **տոպոլոգիական խումբ**, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա) $(x, y) \to x \circ y$ արտապատկերումը անընդհատ է, այսինքն՝ կամայական $x, y \in Q$ տարրերի և նրանց $x \circ y$ արտադրյալի կամայական U շրջակայքի համար գոյություն ունեն x-ի և y-ի համապատասխանաբար այնպիսի V և W շրջակայքեր, որ $V \circ W \subseteq U$;

բ) $x \to x^{-1}$ արտապատկերումը անընդհատ է, այսինքն՝ կամայական $x \in Q$ տարրի և նրա $x^{-1} \in Q$ հակադարձի կամայական U շրջակայքի համար գոյություն ունի x-ի այնպիսի V շրջակայք, որ $V^{-1} \subseteq U$, որտեղ

$$V^{-1} = \left\{x^{-1} |\, x \in V\right\} :$$

Ապացուցել, որ $\mathbb{Z}(+, \tau)$ եռյակը տոպոլոգիական խումբ է, որտեղ τ-ն $\mathbb{Z}$-ի մնացքային տոպոլոգիան է:

Ապացուցել, որ եթե $Q(\circ, \tau)$ եռյակը տոպոլոգիական խումբ է, ապա (Q, τ) տոպոլոգիական տարածությունը կլինի T_3-տարածություն:

38. Դիցուք $Q(\circ)$-ը խումբ է, իսկ "$\leqslant$" հարաբերությունը մասնակի կարգ է՝ որոշված Q-ի վրա: $Q(\circ, \leqslant)$ եռյակը կոչվում է **մասնակի կարգավորված խումբ**, եթե տեղի ունի հետևյալ պայմանը.

$$a \leqslant b \longrightarrow a \circ c \leqslant b \circ c, \quad c \circ a \leqslant c \circ b,$$

որտեղ $a, b, c \in Q$: *Օրինակ,* $\mathbb{Z}(+, \leqslant)$, $\mathbb{Q}(+, \leqslant)$, $\mathbb{R}(+, \leqslant)$, $\mathbb{R}_+(\cdot, \leqslant)$ եռյակները մասնակի կարգավորված խմբեր են, որտեղ "$\leqslant$" հարաբերությունը թվերի բնական կարգն է:

Ապացուցել, որ եթե $Q(\circ, \leqslant)$ եռյակը մասնակի կարգավորված խումբ է, ապա

1) $a < b \longrightarrow c^{-1} \circ a \circ c < c^{-1} \circ b \circ c$,
2) $a < b \longrightarrow b^{-1} < a^{-1}$,
3) $a < b,\ c < d \longrightarrow ac < bd$,

որտեղ $a, b, c, d \in Q$:

$a \in Q$ տարրը կոչվում է **դրական**, եթե $a \geqslant e$, որտեղ e-ն $Q(\circ)$ խմբի միավորն է:

Ապացուցել, որ

$$a \leqslant b \longleftrightarrow b \circ a^{-1} \geqslant e,$$

այսինքն՝ "$\leqslant$" մասնակի կարգը միարժեքորեն որոշվում է դրական տարրերի բազմությամբ:

Ապացուցել, որ $Q(\circ,\leqslant)$ մասնակի կարգավորված խմբի բոլոր դրական տարրերի $P \subseteq Q$ ենթաբազմությունը բավարարում է հետևյալ երեք պայմաններին.

(1) $P \circ P \subseteq P$, այսինքն՝ $P(\circ)$-ը $Q(\circ)$ խմբի ենթակիսախումբն է;

(2) $P \cap P^{-1} = \{e\}$;

(3) $x^{-1} \circ P \circ x \subseteq P$ կամայական $x \in Q$ տարրի համար:

Եվ հակառակը, եթե $Q(\circ)$ խմբի $P \subseteq Q$ ենթաբազմությունը բավարարում է (1)–(3) պայմաններին, ապա գոյություն ունի այնպիսի $Q(\circ,\leqslant)$ մասնակի կարգավորված խումբ, որի բոլոր դրական տարրերի բազմությունը համընկնում է P-ի հետ:

39. $Q(\circ,\leqslant)$ մասնակի կարգավորված խումբը կոչվում է **գծայնորեն** (կամ գծային) **կարգավորված**, եթե "$\leqslant$" մասնակի կարգը գծային կարգ է, այսինքն՝ ցանկացած $x, y \in Q$ տարրերի համար՝ կամ $x \leqslant y$ կամ $y \leqslant x$:

Ապացուցել, որ $Q(\circ,\leqslant)$ գծայնորեն կարգավորված խմբում (1)–(3) պայմանների հետ մեկտեղ տեղի ունի նաև

(4) $Q = P \cup P^{-1}$

պայմանը: Ձևակերպել և ապացուցել հակառակ պնդումը:

40. Դիցուք $\mathbb{C}(+)$-ը բոլոր կոմպլեքս թվերի (գումարային) խումբն է, և

$$a + bi \leqslant a' + b'i \longleftrightarrow a < a' \quad \text{կամ} \quad a = a', b \leqslant b' :$$

Ապացուցել, որ $\mathbb{C}(+,\leqslant)$ եռյակը գծայնորեն կարգավորված խումբ է:

41. Դիցուք $Q(\cdot,\leqslant)$ եռյակը մասնակի կարգավորված խումբ է, իսկ $H \subseteq Q$ ենթաբազմությունը ուռուցիկ է $Q(\leqslant)$ մասնակի կարգավորված բազմության մեջ և H-ը $Q(\circ)$ խմբի ինվարիանտ ենթախումբն է: ${Q}/{H}(\cdot)$ ֆակտոր-խմբում սահմանենք հետևյալ մասնակի կարգը.

$$aH \leqslant bH \longleftrightarrow a' \leqslant b' \quad \text{որևէ} \quad a' \in aH \quad \text{և} \quad b' \in bH \quad \text{տարրերի համար;}$$

Ապացուցել, որ ${Q}/{H}(\cdot,\leqslant)$ եռյակը մասնակի կարգավորված խումբ է (որի տարրերը նույնպես ուռուցիկ բազմություններ են):

Գ լ ու խ 19

ՕՂԱԿՆԵՐ ԵՎ ԴԱՇՏԵՐ

19.1. Օղակի, մարմնի, դաշտի, կիսաօղակի, քվազիօղակի գաղափարները: Վերջավոր դաշտեր: Վան դեր Վարդենի թեորեմը

Օղակի և դաշտի գաղափարները ներմուծվել են 14.7 վերնագրում:

$Q(+,\cdot)$-ը, այսինքն՝ $Q \neq \emptyset$ բազմությունն իր մեջ սահմանված (որոշված) երկու գործողությունների հետ մեկտեղ, որոնցից մեկն անվանվում է գումար և նշանակվում է $+$ նշանով, իսկ մյուսը՝ արտադրյալ և նշանակվում է $\cdot$ նշանով, կոչվում է **օղակ**, եթե տեղի ունեն հետևյալ երկու պայմանները.

ա) $Q(+)$-ն աբելյան խումբ է;

բ) $+$ և $\cdot$ գործողությունները կապված են ձախ և աջ բաշխական նույնություններով՝

$$x(y+z) = xy + xz, \quad \text{(ձախ բաշխականություն)}$$

$$(y+z)x = yx + zx \quad \text{(աջ բաշխականություն)}$$

ցանկացած $x, y, z \in Q$ տարրերի համար:

Եթե $Q(+,\cdot)$-ը օղակ է, ապա $+$ և $\cdot$ գործողությունները կոչվում են օղակային գործողություններ՝ որոշված Q-ի վրա (մեջ):

$Q(+,\cdot)$ օղակի $Q(+)$ աբելյան խմբի միավորը սովորաբար նշանակվում է զրոյով՝ 0, որն ըստ միավորի սահմանման բնութագրվում է հետևյալ կերպ՝

$$x + 0 = 0 + x = x$$

ցանկացած $x \in Q$ տարրի համար, իսկ $Q(+)$ աբելյան խմբի $x \in Q$ տարրի հակադիրը նշանակվում է $-x$-ով, որն ըստ սահմանման բնութագրվում է հետևյալ կերպ՝

$$x + (-x) = (-x) + x = 0,$$

որտեղից հակադիրի միակության համաձայն՝ $-(-x) = x$:

Օղակի զրոյից տարբեր բոլոր տարրերը կոչվում են նրա ոչ զրոյական տարրեր:

Լեմմ 19.1: *$Q(+,\cdot)$ օղակի յուրաքանչյուր $x, y \in Q$ տարրերի համար՝*

$$x \cdot 0 = 0 \cdot x = 0,$$

$$x(-y) = (-x)y = -(xy),$$

$$(-x)(-y) = xy \ :$$

Ապացուցում: Իրոք՝

$$x \cdot a = x(a+0) = xa + x0,$$

$$-(xa) + xa = -(xa) + xa + x0,$$

$$0 = 0 + x0 = x0 :$$

Ելնելով $ax = (a+0)x = ax + 0x$ հավասարությունից, կստանանք $0x = 0$ հավասարությունը: Այնուհետև,

$$y + (-y) = 0,$$

$$x(y + (-y)) = x0 = 0,$$

$$xy + x(-y) = 0,$$

$$x(-y) = -(xy) :$$

Նույն եղանակով ստացվում է նաև $(-x)y = -(xy)$ հավասարությունը, իսկ

$$(-x)(-y) = -(x(-y)) = -(-(xy)) = xy : \qquad \square$$

Յուրաքանչյուր $Q(+,\cdot)$ օղակում կարելի է սահմանել նաև **հանման գործողություն**, հետևյալ կերպ՝

$$x - y = x + (-y), \quad x, y \in Q :$$

Ընդ որում, հեշտությամբ ստուգվում է հետևյալ լեմմը:

Լեմմ 19.2: *Եթե $Q(+,\cdot)$-ը օղակ է, ապա $Q(-)$-ը կլինի քվազիխումբ և տեղի ունեն հետևյալ նույնությունները՝*

$$x(y - z) = xy - xz,$$

$$(x-y)z = xz - yz,$$

$$(x-y)-(u-v) = (x-u)-(y-v) \ :$$

Դեռ ավելին, կամայական $f, g \in \{+, -\}$ գործողությունների համար տեղի ունի հետևյալ նույնությունը՝

$$f\left(g(x,y), g(u,v)\right) = g\left(f(x,u), f(y,v)\right),$$

որը հաճախ կոչվում է f և g գործողությունների աբելյանության (երկսիմետրիկության, մեդիալության կամ էնտրոպիկության) պայման:

Ապացուցում: Ակնհայտ է, որ ցանկացած $a, b \in Q$ տարրերի համար՝

$$a - x = b \longleftrightarrow x = a - b\,,$$

$$y - a = b \longleftrightarrow y = a + b\ :$$

Հետևաբար, $Q(-)$-ը քվազիխումբ է: Մնացած հատկություններն ապացուցվում են անմիջական ստուգման եղանակով: □

$Q(+,\cdot)$ օղակը կոչվում է **զրոյական**, եթե Q բազմությունը 1-տարրանի է՝ $Q = \{0\}$: Հակառակ դեպքում օղակը կոչվում է **ոչ զրոյական**: Այնուհետև, վերհիշենք օղակների հետևյալ կարևորագույն դասերի սահմանումները:

$Q(+,\cdot)$ օղակը կոչվում է **միավորով** օժտված, եթե նրա արտադրյալ գործողությունն ունի միավոր, այսինքն՝ գոյություն ունի այնպիսի $e \in Q$ տարր, որ $x\cdot e = e\cdot x = x$ ցանկացած $x \in Q$ տարրի դեպքում:Այս դեպքում e-ն որոշվում է միարժեքորեն և կոչվում է տրված օղակի միավոր: Հակառակ դեպքում օղակը կոչվում է **առանց միավորի**: Օրինակ, առանց միավորի է բոլոր զույգ թվերի օղակը:

Որպեսզի օղակը լինի զրոյական անհրաժեշտ է և բավարար, որ այն լինի օժտված $e = 0$ միավորով:

Օղակը կոչվում է **տեղափոխական**, եթե նրա արտադրյալ գործողությունը տեղափոխական է: Հակառակ դեպքում օղակը կոչվում է **ոչ տեղափոխական:**

Օղակը կոչվում է **զուգորդական**, եթե նրա արտադրյալ գործողությունը զուգորդական է: Հակառակ դեպքում օղակը կոչվում է **ոչ զուգորդական:**

$Q(+,\cdot)$ օղակը կոչվում է (օժտված) **զրոյի բաժանարարներով**, եթե գոյություն ունեն նրա այնպիսի $a, b \in Q$ ոչ զրոյական տարրեր, որ $a\,\cdot$

$b = 0$ (և այս դեպքում a, b ոչ զրոյական տարրերը կոչվում են զրոյի բաժանարարներ): Հակառակ դեպքում $Q(+,\cdot)$ օղակը կոչվում է **առանց զրոյի բաժանարարների**՝ (կամ զրոյի բաժանարարներ չունեցող)՝

$$a \cdot b = 0 \to a = 0 \text{ կամ } b = 0,$$

որտեղ $a, b \in Q$:

Լեմմ 19.3: *Զրոյի բաժանարարներ չունեցող յուրաքանչյուր $Q(+,\cdot)$ օղակում կարելի է կատարել կրճատում ոչ զրոյական տարրով, այսինքն՝*

$$a \cdot x = a \cdot y \longrightarrow x = y,$$

$$x \cdot a = y \cdot a \longrightarrow x = y,$$

որտեղ $a, x, y \in Q$, $a \neq 0$:

Ապացուցում: Իրոք, եթե $a \neq 0$, ապա

$$ax = ay \longrightarrow a(x-y) = 0 \longrightarrow x - y = 0 \longrightarrow x = y : \qquad \square$$

Ոչ զրոյական օղակը կոչվում է **ամբողջության** կամ **ամբողջականության տիրույթ**, եթե այն բավարարում է հետևյալ չորս պայմաններին. զուգորդական է, տեղափոխական, ունի միավոր և չունի զրոյի բաժանարարներ: *Օրինակ,* բոլոր ամբողջ թվերի $\mathbb{Z}(+,\cdot)$ օղակը, ինչպես նաև բոլոր ամբողջ p-ադիկ թվերի $\mathcal{O}_p(+,\cdot)$ օղակը այդպիսին են (թեորեմ 9.16):

Ներմուծենք բաժանման և բաղդատման գաղափարները օղակներում: Կասենք, որ $K(+,\cdot)$ ամբողջության տիրույթի a տարրը բաժանվում է նրա b տարրի վրա և կգրենք ${}^{a}/_{b}$, եթե գոյություն ունի այնպիսի $c \in K$ տարր, որ $a = b \cdot c$: Այդ դեպքում a-ն կոչվում է **բաժանելի**, b-ն **բաժանարար**, իսկ c-ն **քանորդ** (եթե $b \neq 0$): Եթե $b \neq 0$, ապա ամբողջության տիրույթում c-ն որոշվում է միարժեքորեն: Այնուհետև, $x, y \in K$ տարրերը կոչվում են բաղդատելի ըստ $a \in K$ հենքի (տարրի) և գրվում է

$$x \equiv y (mod\, a),$$

եթե ${}^{x-y}/_{a}$: Ակնհայտ է, որ բաղդատման սահմանված «$\equiv$» հարաբերությունը համարժեքություն է: Յուրաքանչյուր $x \in K$ տարրի համար

$$[x] = \{t \in K |\ t \equiv x (mod\, a)\}$$

համարժեքության դասը կոչվում է x-ի մնացքների դաս ըստ a հենքի: Ըստ որում, x-ը կոչվում է $[x]$ դասի ներկայացուցիչ: Ակնհայտ է, որ

$$[x] = [y] \longleftrightarrow x \equiv y(mod\, a) :$$

Այսպիսով, միևնույն մնացքների դասը կարող է ունենալ տարբեր ներկայացուցիչներ:

Բոլոր մնացքների դասերի բազմությունը ըստ $a \in K$ հենքի նշանակվում է $K/_{(a)}$-ով, այսինքն՝

$$K/_{(a)} = \{[x] |\, x \in K\} :$$

Բնական եղանակով սահմանվում է մնացքների դասերի գումարը և արտադրյալը (բազմապատկումը)՝

$$[x] + [y] = [x + y],$$

$$[x] \cdot [y] = [x \cdot y],$$

և հեշտությամբ ստուգվում է, որ այս գումարման և բազմապատկման արդյունքները որոշվում եմ միարժեքորեն, այսինքն՝ կախված չեն մնացքների դասերում ներկայացուցիչների ընտրություններից: Արդյունքում $K/_{(a)}(+,\cdot)$-ը դառնում է զուգորդական, տեղափոխական և $[e]$ միավորով օժտված օղակ, որը կոչվում է սկզբնական $K(+,\cdot)$ օղակի մնացքների օղակ՝ ըստ a հենքի:

e միավորով օժտված $Q(+,\cdot)$ օղակի $a \in Q$ տարրը կոչվում է հակադարձելի, եթե գոյություն ունի այնպիսի $a' \in Q$ տարր, որ

$$a \cdot a' = a' \cdot a = e :$$

Միավորով օժտված զուգորդական օղակում a' տարրը (եթե այն գոյություն ունի, ապա) որոշվում է միարժեքորեն, նշանակվում է՝ $a' = a^{-1}$ և կոչվում է a-ի հակադարձ (տարր) տրված օղակում: Միավորով օժտված զուգորդական օղակի երկու (հետևաբար և վերջավոր թվով) հակադարձելի տարրերի արտադրյալը ևս կլինի հակադարձելի, ընդ որում՝

$$(a_1 \cdot a_2)^{-1} = a_2^{-1} \cdot a_1^{-1},$$

$$(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdot a_{n-1}^{-1} \cdots a_2^{-1} \cdot a_1^{-1} :$$

Լեմմ 19.4: *Միավորով օժտված յուրաքանչյուր $Q(+,\cdot)$ զուգորդական օղակի բոլոր հակադարձելի տարրերի $Q^{\times}$ բազմությունը խումբ է՝ օղակի արտադրյալ գործողության նկատմամբ: Այդ $Q^{\times}(\cdot)$ խումբը կոչվում է տրված օղակի* **հակադարձելի տարրերի խումբ** *կամ տրված օղակի արտադրյալային խումբ (համառոտ՝ էյլերի խումբ):* □

Համաձայն թեորեմ 14.18-ի (տես նաև հետևություն 3.5-ը), $\mathbb{Z}_n(+,\cdot)$ օղակի $[a]\in\mathbb{Z}_n$ տարրը կլինի հակադարձելի այն և միայն այն դեպքում, երբ $(a,n) = 1$, այսինքն՝ $\mathbb{Z}_n(+,\cdot)$ օղակի հակադարձելի տարրերի քանակը հավասար է $\varphi(n)$-ի, որտեղ φ-ն էյլերի ֆունկցիան է: Ուստի, $|\mathbb{Z}_n^{\times}| = \varphi(n)$ և, հետևաբար, հետևություն 18.9-ի համաձայն՝ $[a]^{\varphi(n)} = [1]$, եթե $(a,n) = 1$: Այսպիսով, նորից հանգում ենք էյլերի թեորեմին (թեորեմ 9.1):

Ոչ զրոյական $Q(+,\cdot)$ օղակը կոչվում է **մարմին**, եթե նրա բոլոր ոչ զրոյական տարրերի Q^* բազմությունը խումբ է՝ օղակի արտադրյալ գործողության նկատմամբ:

Ոչ զրոյական $Q(+,\cdot)$ օղակը կոչվում է **դաշտ**, եթե նրա բոլոր ոչ զրոյական տարրերի Q^* բազմությունը աբելյան խումբ է՝ օղակի արտադրյալ գործողության նկատմամբ, որը կոչվում է դաշտի արտադրյալային խումբ: Հետևաբար, յուրաքանչյուր դաշտ ամբողջության տիրույթ է, իսկ ամբողջության տիրույթը կլինի դաշտ այն և միայն այն դեպքում, երբ նրա յուրաքանչյուր ոչ զրոյական տարր հակադարձելի է:

Առանց ապացուցման նշենք հետևյալ դասական արդյունքը:

Թեորեմ 19.1: *Վերջավոր բազմության վրա սահմանված (տրված) յուրաքանչյուր մարմին դաշտ է, այսինքն՝ վերջավոր մարմինը դաշտ է (Վեդդերբառն): Եթե $Q(+,\cdot)$ զուգորդական օղակի ցանկացած $a\in Q$ տարրի համար գոյություն ունի այնպիսի $n(a) > 1$ բնական թիվ, որ $a^{n(a)} = a$, ապա $Q(+,\cdot)$ օղակը տեղափոխական է (Ջեկոբսոն):* □

Վերհիշենք հետևյալ արդյունքը (թեորեմ 14.17, թեորեմ 14.18) :

Թեորեմ 19.2: *Վերջավոր բազմության վրա սահմանված (տրված) յուրաքանչյուր ամբողջության տիրույթ դաշտ է, այսինքն՝ վերջավոր ամբողջության տիրույթը դաշտ է: Եթե q-ն վերջավոր F դաշտի կարգն է, ապա $a^q = a$ ցանկացած $a\in F$ տարրի համար: Մնացքների $\mathbb{Z}_n(+,\cdot)$ օղակը կլինի դաշտ այն և միայն այն դեպքում, երբ n-ը պարզ թիվ է:* □

Այս պնդման երկրորդ մասը բխում է նաև խմբերի տեսության հետևություն 18.9 հատկությունից: Իրոք, վերջավոր F դաշտի արտադրյալային խմբի կարգը կլինի հավասար $q-1$-ի: Հետևաբար, այդ հետևության համաձայն, $a^{q-1}=e$ ցանկացած ոչ զրոյական $a \in F$ տարրի համար, որտեղից՝ $a^q = a$ արդեն ցանկացած $a \in F$ տարրի համար:

Ապացուցենք պարզ թվերի վերաբերյալ Վիլսոնի թեորեմի հետևյալ ընդհանրացումը:

Թեորեմ 19.3 (Վիլսոն): *Վերջավոր դաշտի բոլոր ոչ զրոյական տարրերի արտադրյալը հավասար է $-e$-ի, որտեղ e-ն դաշտի միավորն է:*

Ապացուցում: Դիցուք $F(+,\cdot)$-ը վերջավոր դաշտ է: Եթե $|F| \leqslant 3$, ապա պնդումն ակնհայտ է: Եթե $|F| > 3$ և $x \in F$, $x \neq 0$, e, $-e$, ապա $x \neq x^{-1}$ և $\{x, x^{-1}\}$ տեսքի բոլոր 2-տարրանի ենթաբազմությունները կկազմեն $F\backslash\{0, e, -e\} = \{x_1, \ldots, x_t\}$ բազմության տրոհում, որովհետև ցանկացած $x \in F\backslash\{0, e, -e\}$ տարրի համար՝ $x \in \{x, x^{-1}\}$ և, եթե $\{x, x^{-1}\} \cap \{y, y^{-1}\} \neq \emptyset$, ապա $\{x, x^{-1}\} = \{y, y^{-1}\}$: Հետևաբար,

$$x_1 \cdots x_t = e,$$
$$x_1 \cdots x_t \cdot e \cdot (-e) = -e:$$

Նկատենք, որ $char(F) = 2$ դեպքում՝ $e = -e$, իսկ հակառակ դեպքում՝ $e \neq -e$: (Հետևաբար, զույգ թվով տարրեր ունեցող դաշտի բնութագրիչը հավասար է 2-ի, իսկ կենտ թվով տարրեր ունեցող դաշտի բնութագրիչը հավասար չէ 2-ի:) □

Ապացուցենք վերջավոր դաշտերին վերաբերող հետևյալ երկու դասական արդյունքները, որոնք հայտնի են նաև իրենց կիրառություններով:

Թեորեմ 19.4*: Դաշտի արտադրյալային խմբի ցանկացած վերջավոր ենթախումբ միածին խումբ է: Մասնավորապես, վերջավոր դաշտի արտադրյալային խումբը կլինի միածին խումբ:*

Ապացուցում: Բխում է թեորեմ 18.21-ից, քանի որ դաշտի մեջ բազմանդամի արմատների թիվը չի գերազանցում բազմանդամի աստիճանը: □

Կարելի է ապացուցել, որ $\mathbb{Z}_n(+,\cdot)$ օղակի հակադարձելի տարրերի $\mathbb{Z}_n^\times(\cdot)$ խումբը միածին է այն և միայն այն դեպքում, երբ $n = 2, 4, p^k, 2p^k$, որտեղ p-ն կենտ պարզ թիվ է:

Վերջավոր F դաշտի ոչ զրոյական a տարրը կոչվում է **պրիմիտիվ**, եթե այն հանդիսանում է ծնիչ տարր F-ի միածին արտադրյալային խմբի համար:

Թեորեմ 19.5: *Ցանկացած P վերջավոր դաշտի և ցանկացած $n \geqslant 1$ բնական թվի համար գոյություն ունի P-ի նկատմամբ չբերվող n-րդ աստիճանի $\varphi \in P[x]$ բազմանդամ:*

Ապացուցում: Քանի որ P դաշտը վերջավոր է, ապա նրա բնութագրիչը հավասար է որևէ p պարզ թվի: Հետևաբար, $|P| = p^t$, որտեղ $t \in \mathbb{N}$ (թեորեմ 17.11): Նշանակենք՝ $q = p^{tn}$ և դիտարկենք $f = x^q - x \in P[x]$ բազմանդամը: Համաձայն Կրոնեկերի թեորեմի (թեորեմ 16.25), գոյություն ունի P դաշտի ընդլայնում հանդիսացող այնպիսի P' դաշտ, որի նկատմամբ f-ը վերլուծվում է գծային բազմանդամների արտադրյալի: F-ով նշանակենք f-ի բոլոր արմատների բազմությունը P' դաշտում՝

$$F = \{c \in P' \mid f(c) = 0\} \ :$$

Քանի որ $f' = qx^{q-1} - 1 = -1$, ապա f-ը չունի բազմապատիկ արմատ (թեորեմ 16.19), այսինքն՝ $|F| = q$: Այնուհետև, դժվար չէ նկատել, որ F-ը P'-ի ենթադաշտ է և պարունակում է P-ն, այսինքն՝ $\alpha^{p^{tn}} = \alpha$ ցանկացած $\alpha \in P$ տարրի համար (այսպիսով, F-ը կլինի դիտարկվող $f \in P[x]$ բազմանդամի վերլուծության դաշտը): Քանի որ F դաշտը վերջավոր է, ապա այն օժտված է որևէ $\alpha_0 \in F$ պրիմիտիվ տարրով (թեորեմ 19.4), որի աստիճաններով սպառվում են F-ի բոլոր ոչ զրոյական տարրերը: Հետևաբար, F-ը կլինի P-ի պարզ ընդլայնումը $\alpha_0 \in F$ հանրահաշվական տարրի օգնությամբ, այսինքն՝ F-ը կլինի P-ի հանրահաշվական ընդլայնումը՝ $F = P_F[\alpha_0]$: Համաձայն թեորեմ 16.24-ի, $F = P_F[\alpha_0]$ դաշտը իզոմորֆ է $P[x]\big/(\varphi)$ մնացքների դաշտին, որտեղ $\varphi \in P[x]$ բազմանդամը չբերվող է P-ում և $\varphi(\alpha_0) = 0$: Քանի որ $|F| = q = p^{tn}$ և $\left|P[x]\big/(\varphi)\right| = (p^t)^{deg(\varphi)}$, ապա $p^{tn} = (p^t)^{deg(\varphi)}$, որտեղից $deg(\varphi) = n$: □

$Q(+,\cdot)$-ը կոչվում է **կիսաօղակ**, եթե $Q(+)$-ը տեղափոխական կիսախումբ է, իսկ $+$ և $\cdot$ գործողությունները կապված են ձախ և աջ բաշխական նույնություններով:

Օրինակ, $\mathbb{N}(+,\cdot)$-ը, $2\mathbb{N}(+,\cdot)$-ը, $3\mathbb{N}(+,\cdot)$-ը, $\ldots$ կիսաօղակներ են, որտեղ $m\mathbb{N} = \{mn|\ n \in \mathbb{N}\}$: Յուրաքանչյուր թվակերպ բազմություն կիսաօղակ է:

Եթե $Q(+,\cdot)$ կիսաօղակի $Q(+)$ կիսախումբն օժտված է միավորով, ապա այն, ինչպես և օղակների դեպքում, նշանակվում է 0-ով, իսկ $Q \setminus \{0\}$-ով նշանակվում է Q-ի բոլոր $x \neq 0$ (ոչ զրոյական) տարրերի բազմությունը: Եթե $Q(+)$-ը չի օժտված միավորով, ապա ենթադրվում է՝ $Q \setminus \{0\} = Q$:

$Q(+,\cdot)$ կիսաօղակը կոչվում է **կիսամարմին** (կիսադաշտ), եթե $Q \setminus \{0\}$ բազմությունը խումբ է (աբելյան խումբ է) կիսաօղակի արտադրյալ գործողության նկատմամբ:

Օրինակ $\mathbb{Q}_+(+,\cdot)$-ը, $\mathbb{R}_+(+,\cdot)$-ը կիսադաշտեր են, որտեղ $\mathbb{Q}_+$-ը ($\mathbb{R}_+$-ը) բոլոր դրական կամ ոչ բացասական ռացիոնալ (իրական) թվերի բազմությունն է:

Կասենք, որ $Q(+,\cdot)$ կիսաօղակը կարելի է ընդլայնել մինչև կիսադաշտի (դաշտի), եթե գոյություն ունի այնպիսի $Q'(\#,\circ)$ կիսադաշտ (դաշտ), որ $Q \subseteq Q'$ և

$$x + y = x \# y,$$

$$x \cdot y = x \circ y$$

ցանկացած $x, y \in Q$ տարրերի համար: Այս դեպքում կասենք, որ $Q(+,\cdot)$ կիսաօղակը ընդլայնվում է մինչև $Q'(\#,\circ)$ կիսադաշտի (դաշտի): Սովորաբար, Q-ի և Q'-ի համապատասխան գործողությունները նշանակվում են նույն նշանով:

Համանման իմաստով հասկացվում է նաև կիսախմբի ընդլայնումը մինչև խմբի:

Օրինակ, պատմականորեն $\mathbb{N}(+,\cdot)$ կիսաօղակը ընդլայնվել է մինչև $\mathbb{Q}_+(+,\cdot)$ կիսադաշտի, իսկ $\mathbb{Q}_+(+,\cdot)$ կիսադաշտը՝ մինչև $\mathbb{Q}(+,\cdot)$ դաշտի:

Թեորեմ 19.6 (Վան դեր Վարդեն): *1) Կրճատումներով օժտված յուրաքանչյուր տեղափոխական կիսախումբ ընդլայնվում է մինչև աբելյան խմբի: 2) Եթե $Q(\cdot)$-ը կրճատումներով օժտված տեղափոխական կիսախումբ է, ապա յուրաքանչյուր $Q(+,\cdot)$ կիսաօղակ կարելի է ընդլայնել մինչև կիսադաշտի: 3) Եթե $Q(+)$-ը կրճատումներով օժտված տեղափոխական կիսախումբ է, ապա յուրաքանչյուր $Q(+,\cdot)$ կիսադաշտ կարելի է ընդլայնել մինչև դաշտի: 4) Յուրաքանչյուր ամբողջության տիրույթ կարելի է ընդլայնել մինչև դաշտի: 5)*

Զուգորդական, տեղափոխական և առանց զրոյի բաժանարարների յուրաքանչյուր օղակ կարելի է ընդլայնել մինչև դաշտի:

Ապացուցում: 1) Դիցուք $Q(+)$-ը տեղափոխական կիսախումբ է՝ օժտված կրճատումներով, այսինքն՝

$$a + x = a + y \longrightarrow x = y,$$

որտեղ $a, x, y \in Q$: Կազմենք $Q^2 = Q \times Q$ բազմությունը և նրա մեջ սահմանենք հետևյալ համարժեքությունը.

$$(a, b) \sim (c, d) \longleftrightarrow a + d = b + c,$$

որտեղ $a, b, c, d \in Q$: Հեշտությամբ ստուգվում է, որ «$\sim$» հարաբերությունը համարժեքություն է: Իրոք, նրա ռեֆլեքսիվությունը և սիմետրիկությունը ակնհայտ են, ապացուցենք փոխանցականությունը: Դիցուք $(a, b) \sim (c, d)$ և $(c, d) \sim (u, v)$: Հետևաբար, $a + d = b + c$, $c + v = d + u$ և $a + d + c + v = b + c + d + u$: Կատարելով կրճատում, այստեղից կստանանք՝ $a + v = b + u$, այսինքն՝ $(a, b) \sim (u, v)$: (a, b) զույգի համարժեքության դասը այստեղ հարմար է նշանակել $\overline{(a, b)}$-ով: Այսպիսով, կարելի է կազմել համապատասխան քանորդ-բազմությունը՝

$$Q' = Q^2/_{\sim} = \left\{ \overline{(a, b)} \middle| \, (a, b) \in Q^2 \right\}:$$

Այս Q' քանորդ-բազմության մեջ այժմ սահմանենք գումարման գործողություն՝

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}$$

և նախ համոզվենք, որ այս գումարման արդյունքը որոշվում է միարժեքորեն, այսինքն՝ գումարման արդյունքը կախված չէ համարժեքության դասերում ներկայացուցիչների ընտրությունից: Իրոք, եթե $(a, b) \sim (a', b')$ և $(c, d) \sim (c', d')$, ապա $a + b' = b + a'$, $c + d' = d + c'$ և հետևաբար՝ $(a + c) + (b' + d') = (b + d) + (a' + c')$, այսինքն՝ $(a + c, b + d) \sim (a' + c', b' + d')$: Հեշտությամբ ստուգվում է նաև, որ $Q'(+)$-ը տեղափոխական կիսախումբ է: Ապացուցենք, որ ստացված տեղափոխական կիսախումբը խումբ է: Իրոք, որպես $Q'(+)$-ի միավոր կարելի է վերցնել $\overline{(x, x)} = \overline{(y, y)}$ համարժեքության դասը, որովհետև՝

$$\overline{(a, b)} + \overline{(x, x)} = \overline{(a + x, b + x)} = \overline{(a, b)},$$

իսկ $-\overline{(a,b)} = \overline{(b,a)}$, որովհետև՝

$$\overline{(a,b)} + \overline{(b,a)} = \overline{(a+b,b+a)} = \overline{(x,x)} :$$

Մնում է յուրաքանչյուր $a \in Q$ տարր նույնականացնել Q'-ի $\overline{(a+x,x)}$ տարրի հետ: Այդ դեպքում՝

$$a \neq b \longrightarrow \overline{(a+x,x)} \neq \overline{(b+x,x)},$$
$$\overline{(a+b+x,x)} = \overline{(a+x,x)} + \overline{(b+x,x)},$$

այսինքն՝ $Q'(+)$ խումբը դառնում է սկզբնական $Q(+)$ կիսախմբի ընդլայնումը:

2) Դիցուք $Q(+,\cdot)$-ը այնպիսի կիսաօղակ է, որտեղ $Q(\cdot)$-ը կրճատումներով օժտված տեղափոխական կիսախումբ է: Համաձայն 1) պնդման, $Q(\cdot)$ կիսախումբը կարելի է ընդլայնել մինչև $Q'(\cdot)$ աբելյան խմբի: 1) պնդման ապացուցման ընթացքում ստացվող $Q'(\cdot)$ կիսախմբի կամայական $\overline{(a,b)}$ տարրը այստեղ հարմար է նշանակել $\left[\dfrac{a}{b}\right]$-ով: Հետևաբար՝

$$\left[\frac{a}{b}\right] = \left[\frac{c}{d}\right] \longleftrightarrow a \cdot d = b \cdot c,$$
$$\left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{a \cdot c}{b \cdot d}\right] :$$

Պահանջվում է Q'-ում սահմանել այնպիսի գումարման գործողություն, որ $Q'(+,\cdot)$-ը լինի կիսադաշտ: Սահմանելով գումարման գործողությունը հետևյալ կերպ՝

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{ad+bc}{bd}\right],$$

նախ նկատենք, որ այս գումարման արդյունքը որոշվում է միարժեքորեն, այսինքն՝ գումարման արդյունքը կախված չէ համարժեքության դասերում (գումարելիներում) ներկայացուցիչների ընտրությունից: Հեշտությամբ ստուգվում է նաև, որ $Q'(+)$-ը տեղափոխական կիսախումբ է և Q'-ի վրա սահմանված գումարման ու բազմապատկման գործողությունները կապված են բաշխական օրենքով: Քանի որ $Q(\cdot)$ կիսախմբի յուրաքանչյուր $a \in Q$ տարր նույնականացվում է $Q'(\cdot)$ կիսախմբի $\left[\dfrac{a \cdot x}{x}\right]$ տարրի հետ, ապա այստեղ անհրաժեշտ է նաև նկատել

$$\left[\frac{(a+b)x}{x}\right] = \left[\frac{ax}{x}\right] + \left[\frac{bx}{x}\right]$$

հավասարությունը: Այսպիսով, $Q'(+,\cdot)$-ը կիսադաշտ է և այս կիսադաշտը հանդիսանում է սկզբնական $Q(+,\cdot)$ կիսաօղակի ընդլայնումը:

3) Դիցուք $Q(+,\cdot)$-ը այնպիսի կիսադաշտ է, որտեղ $Q(+)$-ը կրճատումներով օժտված տեղափոխական կիսախումբ է: 1) պնդման համաձայն $Q(+)$ կիսախումբը կարելի է ընդլայնել մինչև $Q'(+)$ խմբի, որի $\overline{(a,b)}$ տարրերը գումարվում են ըստ

$$\overline{(a,b)}+\overline{(c,d)}=\overline{(a+c,b+d)}$$

բանաձևի: Q'-ի մեջ սահմանվում է բազմապատկման գործողություն հետևյալ կերպ՝

$$\overline{(a,b)}\cdot\overline{(c,d)}=\overline{(ac+bd,ad+bc)}:$$

Հեշտությամբ ստուգվում է, որ $Q'(+,\cdot)$-ը որոնելի դաշտն է:

4) Դիցուք $Q(+,\cdot)$-ը ամբողջության տիրույթ է, $Q_0 = Q\setminus\{0\}$ և $Q_1 = Q\times Q_0$: Այս Q_1 բազմության վրա սահմանենք հետևյալ «$\sim$» համարժեքությունը՝

$$(a,b)\sim(c,d)\longleftrightarrow ad=bc:$$

Հեշտությամբ ստուգվում է, որ «$\sim$» հարաբերությունն իրոք համարժեքություն է: Նշանակելով (a,b) զույգի համարժեքության դասը $[a,b]$-ով, կունենանք՝

$$[a,b]=[c,d]\longleftrightarrow ad=bc:$$

Համապատասխան քանորդ-բազմությունը նշանակենք Q'-ով՝

$$Q'=Q_1/_\sim=\{[a,b]|\,(a,b)\in Q_1\}$$

և Q'-ի մեջ սահմանենք գումարման և բազմապատկման հետևյալ գործողությունները՝

$$[a,b]+[c,d]=[ad+bc,bd],$$

$$[a,b]\cdot[c,d]=[ac,bd]:$$

Արդյունքում Q'-ը վերածվում է դաշտի (ստուգման մանրամասնությունները թողնվում է ընթերցողին), իսկ եթե Q-ի յուրաքանչյուր $a\in Q$ տարր նույնականացվի Q'-ի $[a,e]$ տարրի հետ

(e-ն $Q(+,\cdot)$ օղակի միավորն է), ապա $Q'(+,\cdot)$ դաշտը դառնում է $Q(+,\cdot)$ ամբողջության տիրույթի ընդլայնումը:

5) Դիցուք $Q(+,\cdot)$-ը զուգորդական, տեղափոխական և առանց զրոյի բաժանարարների օղակ է: Կրկնելով 4)-ի ապացուցումը, նկատում ենք, որ այս դեպքում Q'-ի միավորի դերը կարող է կատարել ցանկացած $[\ell,\ell]$ զույգ, որտեղ $\ell \in Q$, $\ell \neq 0$, իսկ Q-ի յուրաքանչյուր $a \in Q$ տարր պետք է նույնականացվի Q'-ի $[a\ell,\ell]$ տարրի հետ: $\square$

Հետևություն 19.1*: Որպեսզի օղակը կարելի լինի ընդլայնել մինչև որևէ դաշտի անհրաժեշտ է և բավարար, որ այն լինի զուգորդական, տեղափոխական և չունենա զրոյի բաժանարարներ:* $\square$

$Q(+,\cdot)$-ը կոչվում է **քվազիօղակ**, եթե $Q(+)$-ը քվազիխումբ է, իսկ $+$ և $\cdot$ գործողությունները կապված են ձախ և աջ բաշխական նույնություններով:

Օրինակ, $\mathbb{Z}(-,\cdot)$-ը քվազիօղակ է: Ընդհանրապես, եթե $Q(+,\cdot)$-ը օղակ է, ապա $Q(-,\cdot)$-ը կլինի քվազիօղակ:

$Q(+)$ քվազիխմբի սահմանումից բխում է, որ նրա $0 \in Q$ ձախ (կամ աջ) միավորը, գոյության դեպքում, որոշվում է միարժեքորեն:

Դիցուք $Q(+,\cdot)$-ը քվազիօղակ է և դիցուք $Q(+)$ քվազիխումբը օժտված է $0 \in Q$ ձախ (կամ աջ) միավորով: Ինչպես և վերևում, $Q \setminus \{0\}$-ով նշանակվում է Q-ի բոլոր $x \neq 0$ տարրերի բազմությունը: Այդ դեպքում, $Q(+,\cdot)$ քվազիօղակը կոչվում է քվազիմարմին (քվազիդաշտ), եթե $Q \setminus \{0\}$ բազմությունը խումբ է (աբելյան խումբ է) քվազիօղակի արտադրյալ գործողության նկատմամբ: Եթե $Q(+,\cdot)$-ը մարմին (դաշտ) է, ապա $Q(-,\cdot)$-ը քվազիմարմին (քվազիդաշտ) է: Յուրաքանչյուր մարմին քվազիմարմին է, իսկ յուրաքանչյուր դաշտ քվազիդաշտ է և կիսադաշտ:

Օրինակ, $\mathbb{Z}_2(-,\cdot)$-ը, $\mathbb{Z}_3(-,\cdot)$-ը, $\mathbb{Q}(-,\cdot)$-ը, $\mathbb{R}(-,\cdot)$-ը, $\mathbb{C}(-,\cdot)$-ը քվազիդաշտեր են:

19.2. Ենթաօղակի, իդեալի և քանորդ-օղակի գաղափարները

$K(+,\cdot)$ օղակի ոչ դատարկ $K' \subseteq K$ ենթաբազմությունը կոչվում է K-ի **ենթաօղակ** և գրվում է $K' \leqslant K$, եթե այն իր յուրաքանչյուր $x, y \in K'$ տարրերի հետ մեկտեղ պարունակում է նաև նրանց $x-y$ տարբերությունը և $x\cdot y$ արտադրյալը՝

$$x, y \in K' \longrightarrow x-y, x\cdot y \in K' :$$

Հետևաբար, $K' \leqslant K$ ենթաօղակը կլինի օղակ՝ սկզբնական $K(+,\cdot)$ օղակի $+$ և $\cdot$ գործողությունների նկատմամբ, որովհետև K'-ը կլինի $K(+)$ խմբի ենթախումբ:

Օրինակ, $\mathbb{Z}(+)$ խմբի ցանկացած ենթախումբ կլինի $\mathbb{Z}(+,\cdot)$ օղակի ենթաօղակ:

Դժվար չէ համոզվել, որ միևնույն օղակի ցանկացած թվով ենթաօղակների հատումը ենթաօղակ է:

$K(+,\cdot)$ օղակի ոչ դատարկ $K' \subseteq K$ ենթաբազմությունը կոչվում է այդ օղակի **իդեալ** և գրվում է $K' \trianglelefteq K$, եթե տեղի ունեն հետևյալ երկու պայմանները.

1) $K' \leqslant K$, այսինքն՝ K'-ը $K(+,\cdot)$ օղակի ենթաօղակ է,

2) $x \cdot z \in K'$ և $z \cdot x \in K'$, եթե $x \in K'$, $z \in K$:

Օրինակ, եթե $K' = \{0\}$ կամ $K' = K$, ապա $K' \trianglelefteq K$: Առաջին դեպքում K' իդեալը կոչվում է զրոյական, իսկ երկրորդ դեպքում՝ միավոր: Օղակը կոչվում է **պարզ**, եթե այն զրոյական և միավոր իդեալներից բացի ուրիշ իդեալներով չի օժտված: Օրինակ, բոլոր մարմինները (հետևաբար և դաշտերը) պարզ օղակներ են: Իրոք, եթե $K(+,\cdot)$-ը մարմին է և $K' \trianglelefteq K$, $K' \neq \{0\}$, ապա գոյություն ունի $h \in K'$, $h \neq 0$ տարր և, հետևաբար, յուրաքանչյուր $x \in K$ տարրի համար կունենանք՝

$$x = (xh)h^{-1} \in K',$$

այսինքն՝ $K' = K$:

Միևնույն $K(+,\cdot)$ օղակի K_1 և K_2 իդեալների գումարը և տարբերությունը սահմանվում են հետևյալ կերպ՝

$$K_1 + K_2 = \{x + y |\, x \in K_1, y \in K_2\},$$

$$K_1 - K_2 = \{x - y |\, x \in K_1, y \in K_2\} :$$

Նույն եղանակով սահմանվում է նաև վերջավոր թվով իդեալների գումարը՝

$$K_1 + K_2 + \cdots + K_n = \{x_1 + x_2 + \cdots + x_n |\, x_1 \in K_1, x_2 \in K_2, \ldots, x_n \in K_n\} :$$

$K(+,\cdot)$ օղակի K_1 և K_2 իդեալները կոչվում են **փոխադարձաբար պարզ**, եթե $K_1 + K_2 = K$: Ակնհայտ է, որ $K_1 - K_2 = K_1 + K_2$:

Լեմմ 19.5: *Միևնույն օղակի երկու իդեալների գումարը և հատումը նույնպես իդեալներ են: Ցանկացած թվով իդեալների հատումը իդեալ է, վերջավոր թվով իդեալների գումարը նորից իդեալ է:*

Ապացույց: Իդեալի սահմանման 1) և 2) պայմանները հեշտությամբ ստուգվում են երկու իդեալների գումարի, ցանկացած թվով իդեալների հատման, ինչպես նաև վերջավոր թվով իդեալների գումարի համար: □

Եթե դիտարկվող $K(+,\cdot)$ օղակը տեղափոխական և զուգորդական է, ապա հեշտությամբ ստուգվում է, որ յուրաքանչյուր $a \in K$ տարրի համար

$$(a) = \{x \cdot a | \, x \in K\} \subseteq K$$

ենթաբազմությունը կլինի իդեալ: Այդ իդեալը կոչվում է a տարրով ծնված **գլխավոր իդեալ**: Նկատենք նաև, որ $e \in K$ միավորի առկայության դեպքում (a) իդեալը կպարունակի a տարրը և այն կլինի a տարրը պարունակող «ամենափոքր» իդեալը և, հետևաբար, այն կհամընկնի a տարրը պարունակող բոլոր իդեալների հատման հետ:

Օրինակ, եթե ε-ը հակադարձելի տարր է, ապա $(\varepsilon) = K$, որովհետև $e \in (\varepsilon)$:

$K(+,\cdot)$ օղակի $H \trianglelefteq K$ իդեալը կոչվում է գլխավոր, եթե այն համընկնում է որևէ $a \in K$ տարրով ծնված գլխավոր իդեալի հետ՝ $H = (a)$: Օրինակ, ամբողջ թվերի $Z(+,\cdot)$ օղակի բոլոր իդեալները գլխավոր են: Այդպիսին է նաև յուրաքանչյուր դաշտ:

Եթե $K(+,\cdot)$-ը կամայական օղակ է, իսկ $H \trianglelefteq K$, ապա H-ը լինելով $K(+)$ աբելյան խմբի ենթախումբը, կլինի նաև նրա ինվարիանտ ենթախումբը և, հետևաբար, կարելի է դիտարկել (կազմել) ${}^{K}\!/_{H}(+)$ քանորդ-խումբը, որտեղ

$$(x + H) + (y + H) = (x + y) + H, \quad x, y \in K:$$

${}^{K}\!/_{H} = \{x + H| \;\; x \in K\}$ բազմության մեջ սահմանվում է նաև արտադրյալ (բազմապատկման) գործողություն հետևյալ կերպ՝

$$(x + H) \cdot (y + H) = (x \cdot y) + H, \quad x, y \in K;$$

Հեշտությամբ ստուգվում է, որ այս բազմապատկման արդյունքը որոշվում է միարժեքորեն, այսինքն՝ կախված չէ հարակից դասերում ներկայացուցիչների ընտրությունից՝

$$x + H = x' + H, \; y + H = y' + H \longrightarrow (x \cdot y) + H = (x' \cdot y') + H:$$

Իրոք, եթե $x + H = x' + H$ և $y + H = y' + H$, ապա $x = x' + h_1$, $y = y' + h_2$, $h_1, h_2 \in H$ և $x \cdot y = (x' + h_1)(y' + h_2) = x'y' + x'h_2 + h_1y' + h_1h_2 = x'y' + h_3$, որտեղ $h_3 = x'h_2 + h_1y' + h_1h_2 \in H$ ըստ իդեալի սահմանման: Ուստի, $(x \cdot y) + H = (x'y' + h_3) + H = (x' \cdot y') + H$:

Հեշտությամբ ստուգվում է նաև, որ K/H բազմության մեջ սահմանված $+$ և $\cdot$ գործողությունները կապված են բաշխական նույնություններով: Այսպիսով, $K/H(+,\cdot)$-ը օղակ է, որը և կոչվում է $K(+,\cdot)$ օղակի **քանորդ-օղակ** կամ **ֆակտոր-օղակ** ըստ $H \trianglelefteq K$ իդեալի:

Օրինակ, $\mathbb{Z}/(m)(+,\cdot) = \mathbb{Z}_m(+,\cdot)$, որտեղ $m \in \mathbb{N}$, $(m) = \{mx \mid x \in \mathbb{Z}\}$:

Անմիջական ստուգման եղանակով ապացուցվում են հետևյալ պնդումները.

1) Եթե $K(+,\cdot)$ օղակը զուգորդական է, ապա նրա բոլոր K/H քանորդ-օղակները կլինեն զուգորդական օղակներ, որտեղ $H \trianglelefteq K$:

2) Եթե $K(+,\cdot)$ օղակը տեղափոխական է, ապա նրա բոլոր K/H քանորդ-օղակները կլինեն տեղափոխական օղակներ, որտեղ $H \trianglelefteq K$:

3) Եթե $K(+,\cdot)$ օղակը օժտված է միավորով, ապա նրա բոլոր K/H քանորդ-օղակները կլինեն օժտված միավորով, որտեղ $H \trianglelefteq K$:

4) Մարմնի (դաշտի) քանորդ-օղակը կամ զրոյական օղակ է կամ մարմին (դաշտ) է:

Դիցուք $K(+,\cdot)$-ը կամայական օղակ է, իսկ $H \trianglelefteq K$: $x, y \in K$ տարրերը կոչվում են **բաղդատելի** ըստ H հենքի (մոդուլի) և գրվում է

$$x \equiv y(mod\, H),$$

եթե $x - y \in H$: Հեշտությամբ ստուգվում է, որ սահմանված բաղդատման հարաբերությունը համարժեքություն է: Յուրաքանչյուր $x \in K$ տարրի համար

$$[x] = \{t \in K |\ t \equiv x(mod\, H)\} \subseteq K$$

համարժեքության դասը կոչվում է x-ի մնացքների դաս ըստ H հենքի: Ըստ որում՝

$$[x] = [y] \longleftrightarrow x \equiv y(mod\, H) \quad \text{և} \quad [x] = x + H :$$

19.3. Գլխավոր իդեալներով օղակներ: Ամենամեծ ընդհանուր բաժանարարը, ամենափոքր ընդհանուր բազմապատիկը և թվաբանության հիմնական թեորեմի ընդհանրացումը գլխավոր իդեալներով օղակներում: Փոխադարձաբար պարզ տարրեր

Ամբողջության տիրույթը կոչվում է **գլխավոր իդեալներով օղակ**, եթե նրա յուրաքանչյուր իդեալ գլխավոր է: Օրինակ, $\mathbb{Z}$, $\mathbb{Z}[i]$, $P[x]$ օղակները գլխավոր իդեալներով օղակներ են, որտեղ P-ն դաշտ է (բխում է այդ օղակներից յուրաքանչյուրում ապացուցված մնացորդով բաժանման վերաբերյալ թեորեմից):

Այս սահմանման մեջ միավորի գոյությունը կարելի է նախապես չպահանջել, քանի որ այն բխում է մնացած աքսիոմների առկայությունից: Իրոք, $K(+,\cdot)$ օղակը, լինելով իր իդեալը, պետք է լինի գլխավոր իդեալ: Այսինքն՝ գոյություն կունենա այնպիսի $a \in K$ տարր, որ $K = (a)$: Այդ դեպքում, յուրաքանչյուր $b \in K$ տարրի համար գոյություն կունենան այնպիսի $x \in K$ և $f \in K$ տարրեր, որ $b = a \cdot x$, $a = a \cdot f$: Հետևաբար,

$$b \cdot f = (a \cdot x) \cdot f = a \cdot (x \cdot f) = a \cdot (f \cdot x) = (a \cdot f) \cdot x = a \cdot x = b$$

և $f \in K$ տարրը կլինի դետարկվող օղակի միավորը:

Եթե $K(+,\cdot)$-ը ամբողջության տիրույթ է, իսկ $a_1, a_2, \ldots, a_n \in K$, ապա

$$(a_1, a_2, \ldots, a_n) = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n | \, x_1, x_2, \ldots, x_n \in K\} \subseteq K$$

ենթաբազմությունը, լինելով $(a_1), (a_2), \ldots, (a_n)$ գլխավոր իդեալների գումարը, կլինի $K(+,\cdot)$ օղակի իդեալը և այն կոչվում է $a_1, a_2, \ldots, a_n \in K$ տարրերով ծնված իդեալ:

Կասենք, որ $K(+,\cdot)$ ամբողջության տիրույթի a և b տարրերը **զուգորդված** են և կգրենք $a \sim b$, եթե գոյություն ունի $K(+,\cdot)$ օղակի այնպիսի $\delta \in K$ հակադարձելի տարր, որ

$$a = b \cdot \delta :$$

Հակառակ դեպքում, օղակի a և b տարրերը կոչվում են **ոչ զուգորդված** կամ **չզուգորդված** և գրվում է $a \not\sim b$:

Սահմանված «$\sim$» հարաբերությունը կոչվում է **զուգորդման հարաբերություն** (որոշված $K(+,\cdot)$ ամբողջության տիրույթում):

Լեմմ 19.6: *Յուրաքանչյուր ամբողջության տիրույթում զուգորդման հարաբերությունը համարժեքության հարաբերություն է, որի բոլոր համարժեքության դասերը կլինեն վերջավոր այն և միայն այն դեպքում, երբ օղակի բոլոր հակադարձելի տարրերի խումբը վերջավոր է:*

Ապացուցում: Քանի որ յուրաքանչյուր $a \in K$ տարրի համար՝ $a = a \cdot e$, որտեղ e-ն $K(+, \cdot)$ օղակի միավորն է, ապա $a \sim a$: Եթե $a \sim b$, ապա $a = b \cdot \delta$, որտեղ δ-ն հակադարձելի է, այսինքն՝ գոյություն ունի այնպիսի $\delta' \in K$ տարր, որ $\delta \cdot \delta' = e$: Հետևաբար, $a \cdot \delta' = b$ և $b \sim a$: Ի վերջո, համոզվենք, որ «$\sim$» հարաբերությունը օժտված է նաև փոխանցական հատկությամբ. եթե $a \sim b$ և $b \sim c$, այսինքն՝ $a = b \cdot \delta_1$, $b = c \cdot \delta_2$, որտեղ $\delta_1 \cdot \delta_1' = e$ և $\delta_2 \cdot \delta_2' = e$, ապա $a = c \cdot (\delta_2 \delta_1)$, որտեղ $(\delta_2 \delta_1)(\delta_1' \delta_2') = e$, ուստի $a \sim c$: □

Լեմմ 19.7: *Եթե ամբողջության տիրույթում a/b և b/a, ապա $a \sim b$:*

Ապացուցում: Քանի որ $a = b \cdot c$ և $b = a \cdot l$, ապա $a = alc$ և $a(e - lc) = 0$: Այժմ, եթե $a = 0$, ապա՝ $b = a \cdot l = 0$ և ակներևորեն՝ $a \sim b$, իսկ եթե $a \neq 0$, ապա $e - lc = 0$ և $e = lc$: Այսպիսով, c տարրը կլինի հակադարձելի և հետևաբար $a = b \cdot c$ հավասարությունից կունենանք՝ $a \sim b$: □

Հետևություն 19.2: *Ամբողջության տիրույթում $(a) = (b)$ այն և միայն այն դեպքում, երբ $a \sim b$:*

Ապացուցում: Եթե $(a) = (b)$, ապա $a \in (b)$ և $b \in (a)$, այսինքն՝ a/b և b/a և ըստ նախորդ լեմմի $a \sim b$:

Եվ հակառակը, եթե $a \sim b$ և $x \in (a)$, ապա $a = b \cdot \delta$, որտեղ δ-ն հակադարձելի է, և $x = a \cdot t = (b\delta)t = b(\delta t) \in (b)$, այսինքն՝ $(a) \subseteq (b)$: Հակառակ ներդրումը ստացվում է նույն դատողություններով: □

Կասենք, որ $K(+, \cdot)$ ամբողջության տիրույթի $d \in K$ տարրը նրա $a, b \in K$ տարրերի **ընդհանուր բաժանարարն է** , եթե a/d և b/d: Եվ $d \in K$ տարրը կոչվում է $a, b \in K$ տարրերի համար **ընդհանուր ամենամեծ** (կամ ամենամեծ ընդհանուր) **բաժանարար** և գրվում է $d \rightleftharpoons (a, b)$, եթե

1. d -ն a և b տարրերի համար ընդհանուր բաժանարար է,
2. d -ն բաժանվում է a և b տարրերի բոլոր ընդհանուր բաժանարարների վրա:

Նույն եղանակով սահմանվում է նաև օղակի վերջավոր թվով տարրերի ամենամեծ ընդհանուր բաժանարարը:

$\mathbb{Z}(+,\cdot)$ ամբողջության տիրույթում երկու տարրերի (ամբողջ թվերի) ընդհանուր ամենամեծ բաժանարարը որոշվում է նշանի ճշտությամբ և դրա հաշվումը կատարվում է հայտնի եղանակներով (գլուխ 2, գլուխ 5): Դաշտի յուրաքանչյուր ոչ զրոյական տարր նրա կամայական երկու ոչ զրոյական տարրերի համար ընդհանուր ամենամեծ բաժանարար է: Այս խրթին իրավիճակին լույս է սփռում զուգորդման հարաբերությունը:

Եթե $d \rightleftharpoons (a,b)$ և $d' \sim d$, ապա ակնհայտ է, որ $d' \rightleftharpoons (a,b)$: Եվ հակառակը, եթե ամբողջության տիրույթում՝ $d \rightleftharpoons (a,b)$ և $d' \rightleftharpoons (a,b)$, ապա d/d', d'/d և հետևաբար (լեմմ 19.7)՝ $d \sim d'$: Այսպիսով, եթե ամբողջության տիրույթում երկու տարրերի ընդհանուր ամենամեծ բաժանարարը գոյություն ունի, ապա կարելի է ասել, որ այն զուգորդման ճշտությամբ որոշվում է միարժեքորեն:

Թեորեմ 19.7 (Է. Նյոթեր)*: Գլխավոր իդեալներով օղակի կամայական երկու տարրեր օժտված են ամենամեծ ընդհանուր բաժանարարով, որը զուգորդման ճշտությամբ որոշվում է միարժեքորեն: Նույն պնդումը տեղի ունի նաև գլխավոր իդեալներով օղակի կամայական վերջավոր թվով տարրերի համար:*

Ապացուցում: Դիտարկենք $K(+,\cdot)$ գլխավոր իդեալներով օղակի կամայական $a, b \in K$ տարրերով ծնված գլխավոր իդեալների գումարը՝

$$(a) + (b) = \Delta,$$

որը, համաձայն լեմմ 19.5-ի, կլինի իդեալ՝ $\Delta \trianglelefteq K$: Քանի որ դիտարկվող $K(+,\cdot)$ օղակի յուրաքանչյուր իդեալ գլխավոր է, ապա գոյություն ունի այնպիսի $d \in K$ տարր, որ $\Delta = (d)$, այսինքն՝

$$(a) + (b) = (d) :$$

Համոզվենք, որ այս ձևով ընտրված $d \in K$ տարրը կլինի a և b տարրերի համար ամենամեծ ընդհանուր բաժանարար: Իրոք, քանի որ

$$a \in (a) \subseteq (a) + (b) = (d)$$

և

$$b \in (b) \subseteq (a) + (b) = (d),$$

ապա $a = dx$ և $b = dy$, որտեղ $x, y \in K$, այսինքն՝ d-ն a և b տարրերի համար ընդհանուր բաժանարար է: Այժմ ենթադրենք, թե a/d' և b/d', ուստի $a = d's$ և $b = d't$: Միաժամանակ, հաշվի առնելով

$$d \in (d) = (a) + (b)$$

առնչությունը, կունենանք՝

$$d = au + bv, \quad u, v \in K :$$

Որտեղից,

$$d = d'su + d'tv = d'(su + tv) = d'w, \quad w \in K :$$

Այսպիսով, d ընդհանուր բաժանարարը բաժանվում է a և b տարրերի յուրաքանչյուր d' ընդհանուր բաժանարարի վրա: □

Հետևություն 19.3: *Գլխավոր իդեալներով օղակի a և b տարրերի ցանկացած d ամենամեծ ընդհանուր բաժանարարի համար գոյություն ունեն օղակի այնպիսի u և v տարրեր, որ*

$$d = au + bv : \qquad \square$$

$K(+, \cdot)$ ամբողջության տիրույթի a և b տարրերը կոչվում են **փոխադարձաբար պարզ** և նշանակվում (գրվում) է $(a, b) = e$, եթե գոյություն ունեն այնպիսի $x, y \in K$ տարրեր, որ

$$ax + by = e,$$

որտեղ e-ն օղակի միավորն է:

Թեորեմ 19.8: *Որպեսզի գլխավոր իդեալներով օղակի a և b տարրերը լինեն փոխադարձաբար պարզ անհրաժեշտ է և բավարար, որ օղակի e միավորը լինի a և b տարրերի ամենամեծ ընդհանուր բաժանարարը, այսինքն՝ $e \rightleftharpoons (a, b)$:*

Ապացուցում: Ակնհայտ է: □

Հատկություն 19.1: *Եթե ամբողջության տիրույթի a տարրը փոխադարձաբար պարզ է նրա b և c տարրերի հետ, ապա a-ն փոխադարձաբար պարզ է նաև դրանց $b \cdot c$ արտադրյալի հետ:*

Ապացուցում: Հատկություն 3.1-ի ապացուցման կրկնությունն է:

Հատկություն 19.2: *Եթե ամբողջության տիրույթի a տարրը փոխադարձաբար պարզ է նրա $b_1, b_2, \ldots, b_n$ տարրերից յուրաքանչյուրի հետ, ապա a-ն կլինի փոխադարձաբար պարզ նաև դրանց $b_1 \cdot b_2 \cdots b_n$ արտադրյալի հետ, որտեղ $n \geqslant 2$:*

Ապացուցում: Վերհանգման եղանակով: □

Հատկություն 19.3: *Եթե ամբողջության տիրույթի $a_1, a_2, \ldots, a_n$ տարրերից յուրաքանչյուրը փոխադարձաբար պարզ է նրա $b_1, b_2, \ldots, b_m$ տարրերից յուրաքանչյուրի հետ, ապա $a_1 a_2 \cdots a_n$ և $b_1 b_2 \cdots b_m$ արտադրյալները կլինեն փոխադարձաբար պարզ:*

Ապացուցում: Հատկություն 3.3-ի ապացուցման կրկնությունն է: □

Հատկություն 19.4: *Եթե ամբողջության տիրույթի a և b տարրերը փոխադարձաբար պարզ են, ապա a^n և b^m տարրերը ևս կլինեն փոխադարձաբար պարզ՝ ցանկացած n, m բնական թվերի դեպքում:*

Ապացուցում: Բխում է նախորդ հատկությունից, եթե $a_1 = a_2 = \cdots = a_n = a$ և $b_1 = b_2 = \cdots = b_m = b$: □

Հատկություն 19.5: *Եթե ամբողջության տիրույթի a և b տարրերի $a \cdot b$ արտադրյալը բաժանվում է իր c տարրի վրա և a-ն փոխադարձաբար պարզ է c-ի հետ, ապա b տարրը բաժանվում է c-ի վրա:*

Ապացուցում: Հատկություն 3.4-ի ապացուցման կրկնությունն է: □

Հատկություն 19.6: *Եթե ամբողջության տիրույթի a տարրը բաժանվում է իր b և c փոխադարձաբար պարզ տարրերից յուրաքանչյուրի վրա, ապա a-ն կբաժանվի նաև դրանց $b \cdot c$ արտադրյալի վրա: Նույն պնդումը տեղի ունի նաև վերջավոր թվով զույգ առ զույգ փոխադարձաբար պարզ տարրերի համար:*

Ապացուցում: Հատկություն 3.5-ի ապացուցման կրկնությունն է: □

Հատկություն 19.7 (Չինական թեորեմ): *Եթե $K(+,\cdot)$-ը ամբողջության տիրույթ է, իսկ $a_1, \ldots, a_n \in K$ տարրերը զույգ առ զույգ փոխադարձաբար պարզ են, ապա կամայական $x_1, \ldots, x_n \in K$ տարրերի համար կգտնվի այնպիսի $x \in K$ տարր, որ*

$$x \equiv x_1 (mod\, a_1),$$

$$\ldots \quad \ldots \quad \ldots$$

$$x \equiv x_n (mod\, a_n) :$$

Ապացուցում: Թեորեմ 3.5-ի ապացուցման կրկնությունն է: □

Կասենք, որ $K(+,\cdot)$ ամբողջության տիրույթի $q \in K$ տարրը նրա $a, b \in K$ տարրերի ընդհանուր բազմապատիկն է, եթե q/a և q/b: Եվ $q \in K$ տարրը կոչվում է $a, b \in K$ տարրերի համար ամենափոքր ընդհանուր (կամ ընդհանուր ամենափոքր) բազմապատիկ և նշանակվում է $q \rightleftharpoons [a, b]$, եթե տեղի ունեն հետևյալ երկու պայմանները.

1') q-ն a և b տարրերի համար ընդհանուր բազմապատիկ է;

2') a ու b տարրերի բոլոր ընդհանուր բազմապատիկները բաժանվում են q-ի վրա:

Նույն եղանակով սահմանվում է նաև ամբողջության տիրույթի վերջավոր թվով տարրերի ամենափոքր ընդհանուր բազմապատիկը: Եթե $q \rightleftharpoons [a, b]$ և $q' \sim q$, ապա $q' \rightleftharpoons [a, b]$: Եվ հակառակը, եթե ամբողջության տիրույթում` $q \rightleftharpoons [a, b]$ և $q' \rightleftharpoons [a, b]$, ապա $q' \sim q$: Այսպիսով, եթե ամբողջության տիրույթում երկու տարրերի ամենափոքր ընդհանուր բազմապատիկը գոյություն ունի, ապա կարելի է ասել, որ այն զուգորդման ճշտությամբ որոշվում է միարժեքորեն:

Թեորեմ 19.9: *Գլխավոր իդեալներով $K(+,\cdot)$ օղակի յուրաքանչյուր երկու $a, b \in K$ տարրեր օժտված են ամենափոքր ընդհանուր բազմապատիկով, որը զուգորդման ճշտությամբ որոշվում է միարժեքորեն: Ըստ որում, եթե $d \rightleftharpoons (a, b)$ (համաձայն թեորեմ 19.7 -ի) և*

$$a \cdot b = d \cdot q, \quad \text{ապա} \ \ q \rightleftharpoons [a, b] :$$

Հետևաբար a և b տարրերի ցանկացած ամենամեծ ընդհանուր բաժանարարի և ցանկացած ամենափոքր ընդհանուր բազմապատիկի արտադրյալը զուգորդված է $a \cdot b$-ի հետ:

Ապացուցում: Գլխավոր իդեալներով $K(+,\cdot)$ օղակի (a) և (b) գլխավոր իդեալների հատումը ևս կլինի իդեալ, հետևաբար և գլխավոր իդեալ`

$$(a) \cap (b) = (q), \qquad q \in K :$$

Այստեղից բխում է, որ q-ն a և b տարրերի ամենափոքր ընդհանուր բազմապատիկն է: Իրոք, $(q) \subseteq (a) \cap (b)$ ներդրումից հետևում է, որ q-ն a ու b տարրերի համար ընդհանուր բազմապատիկ է, իսկ $(a) \cap (b) \subseteq (q)$ ներդրումից հետևում է, որ a ու b տարրերի ցանկացած q' ընդհանուր բազմապատիկ բաժանվում է q-ի վրա:

Եթե $a = 0$ կամ $b = 0$, ապա 0-ն կլինի նրանց միակ ընդհանուր բազմապատիկը՝ $0 \rightleftharpoons [0, 0]$ և $0 = d \cdot 0$: Հետևաբար, այս դեպքում $a \cdot b = d \cdot q$, որտեղ $q \rightleftharpoons [a, b]$: Դիցուք $a \neq 0$, $b \neq 0$, $d \rightleftharpoons (a, b)$ և դիցուք $a \cdot b = d \cdot q$, որտեղ $q \in K$ և $d \neq 0$: Ապացուցենք, որ $q \rightleftharpoons [a, b]$: Քանի որ $K(+, \cdot)$ օղակը առանց զրոյի բաժանարարների է և a/d ու b/d, ապա $a \cdot b = d \cdot q$ հավասարությունից բխում է, որ q/a և q/b: *Օրինակ,* $a = d \cdot a'$ պայմանից կունենանք՝ $da'b = dq$, $d(a'b - q) = 0$, որտեղից (քանի որ $d \neq 0$)՝ $a'b - q = 0$ և $a'b = q$: Այսպիսով, q տարրի համար տեղի ունի 1’) պայմանը: Մնում է համոզվել, որ q տարրը բավարարում է նաև 2’) պայմանին: Դիցուք f-ը a և b տարրերի կամայական ընդհանուր բազմապատիկն է, այսինքն՝ $f = a \cdot s$ և $f = b \cdot t$, որտեղ $s, t \in K$: Քանի որ $d = ax + by$, $x, y \in K$ (հետևություն 19.3) և $a = d \cdot a'$, $b = d \cdot b'$, որտեղ $a', b' \in K$, ապա

$$d = da'x + db'y$$

և կրճատելով $d \neq 0$ տարրով, կստանանք՝

$$e = a'x + b'y,$$

որտեղ e-ն օղակի միավորն է:

Այսպիսով, a' և b' տարրերը կլինեն փոխադարձաբար պարզ: Այնուհետև,

$$a \cdot s = b \cdot t,$$

$$d \cdot a' \cdot s = d \cdot b' \cdot t, \quad d \neq 0,$$

$$a' \cdot s = b' \cdot t$$

և համաձայն հատկություն 19.5-ի, s-ը կբաժանվի b'-ի վրա, այսինքն՝ $s = b' \cdot l$, $l \in K$: Ուստի, $sd = lb'd = l \cdot b$, $f \cdot d = (as)d = a(sd) = alb = ab \cdot l = dql$ և $f = q \cdot l$, այսինքն՝ f/q: □

$K(+, \cdot)$ ամբողջության տիրույթի $p \in K$ տարրը կոչվում է **պարզ** կամ **է քստրեմալ** (ըստ Ն. Բուրբակիի), եթե այն օժտված է հետևյալ երեք հատկություններով՝

ա) $p \neq 0$,

բ) p տարրը հակադարձելի չէ,

գ) p տարրի յուրաքանչյուր $p = a \cdot b$ վերլուծության մեջ a, b տարրերից որևէ մեկը հակադարձելի է:

Օրինակ, ամբողջ թվերի $\mathbb{Z}(+,\cdot)$ օղակում պարզ տարրի գաղափարը նշանի ճշտությամբ համընկնում է պարզ թվի գաղափարի հետ: Եթե p-ն պարզ թիվ է, ապա այն կլինի ամբողջ p-ադիկ թվերի $\mathcal{O}_p(+,\cdot)$ օղակի պարզ տարրը, և հակառակը. ամբողջ p-ադիկ թվերի $\mathcal{O}_p(+,\cdot)$ օղակի յուրաքանչյուր պարզ տարր զուգորդված է p-ի հետ (բխում է թեորեմ 9.15-ից): Դաշտի մեջ պարզ տարրեր չկան: Եթե P-ն դաշտ է, ապա բազմանդամների $P[x]$ օղակում պարզ տարրի գաղափարը համընկնում է չբերվող բազմանդամի գաղափարի հետ:

Լեմմ 19.8*: Եթե ամբողջության տիրույթի p տարրը պարզ է, ապա նրա հետ զուգորդված յուրաքանչյուր q տարր ևս կլինի պարզ:*

Ապացուցում: Քանի որ $q \sim p$, ապա՝ $q = p\delta$, որտեղ $p \neq 0$, $\delta \neq 0$ և հետևաբար՝ $q \neq 0$: Եթե q տարրը լինի հակադարձելի, ապա կունենանք՝ $p = q \cdot \delta^{-1}$, որտեղ $\delta \cdot \delta^{-1} = e$, և p-ն կլինի հակադարձելի՝ որպես երկու հակադարձելի տարրերի արտադրյալ, որը հակասում է p-ի ընտրությանը: Այժմ ենթադրենք, թե

$$q = a \cdot b,$$

որտեղ a և b տարրերը միաժամանակ հակադարձելի չեն: Այդ դեպքում, $p\delta = a \cdot b$ հավասարությունից կունենանք՝

$$p = \left(\delta^{-1}a\right) b,$$

որտեղ $\delta^{-1}a$ և b տարրերը ևս կլինեն ոչ հակադարձելի, որը հակասում է p-ի պարզ տարր լինելուն: $\square$

Լեմմ 19.9*: Գլխավոր իդեալներով օղակի a տարրը չի բաժանվի նրա p պարզ տարրի վրա այն և միայն այն դեպքում, երբ a և p տարրերը փոխադարձաբար պարզ են:*

Ապացուցում: Անհրաժեշտություն: a և p տարրերի ամենամեծ ընդհանուր բաժանարարը (որը գոյություն ունի համաձայն թեորեմ 19.7-ի) նշանակենք d-ով: Քանի որ $p = d \cdot l$ տարրը պարզ է, ապա կամ d-ն է հակադարձելի, կամ՝ l-ը; Սակայն երկրորդ դեպքը տեղի ունենալ չի կարող, որովհետև a/d և d/p պայմաններից կհետևեր a/p փաստը, որը հնարավոր չէ: Հետևաբար, d-ն է հակադարձելի և $e \rightleftharpoons (a,p)$: Մնում է օգտվել թեորեմ 19.8-ից: *Բավարարությունն* ակնհայտ է: $\square$

Թեորեմ 19.10 (Էվկլիդես): *Գլխավոր իդեալներով օղակի a և b տարրերի $a \cdot b$ արտադրյալը բաժանվում է նրա p պարզ տարրի վրա այն և միայն այն դեպքում, երբ a, b արտադրիչներից գոնե մեկը բաժանվում է p-ի վրա:*

Ապացուցում: Դիցուք $a \cdot b/p$, բայց a-ն չի բաժանվում p-ի վրա: Ըստ նախորդ լեմմի a և p տարրերը այդ դեպքում կլինեն փոխադարձաբար պարզ, այսինքն՝

$$au + pv = e;$$

Որտեղից՝

$$(ab)u + p(vb) = b$$

և, հետևաբար, b/p: □

Ապացուցված պնդումը մնում է ուժի մեջ նաև կամայական վերջավոր թվով արտադրիչների համար: Այս ընդհանուր դեպքում ապացուցումը կատարվում է վերհանգման եղանակով (ինդուկցիայով):

Թեորեմ 19.11 (Է. Նյոթեր)*: Գլխավոր իդեալներով $K(+,\cdot)$ օղակում իդեալների ամեն մի աճող շղթա՝*

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \ldots$$

ընդհատվում է, այսինքն՝ գոյություն ունի այնպիսի m համար, որ

$$(a_m) = (a_{m+1}) = (a_{m+2}) = \cdots$$

Ապացուցում: Դիտարկենք հետևյալ Δ բազմությունը՝

$$\Delta = (a_1) \cup (a_2) \cup \cdots \cup (a_n) \cup \cdots = \bigcup_{i=1}^{\infty}(a_i)$$

և նախ համոզվենք, որ Δ-ն սկզբնական $K(+,\cdot)$ օղակի իդեալն է: Իրոք, եթե $x, y \in \Delta$ և $r \in K$, ապա գոյություն կունենան այնպիսի i և j համարներ, որ $x \in (a_i)$ և $y \in (a_j)$: Ընդսմին $i \leqslant j$ դեպքում կունենանք՝ $x, y \in (a_j)$, իսկ $i > j$ դեպքում կունենանք՝ $x, y \in (a_i)$: Առաջին դեպքում կունենանք՝ $x - y \in (a_j)$, իսկ երկրորդ դեպքում՝ $x - y \in (a_i)$: Այսպիսով, ընդհանուր դեպքում՝ $x - y \in \Delta$: Միաժամանակ, $x \cdot r \in (a_i) \subseteq \Delta$: Ուստի Δ-ն $K(+,\cdot)$ օղակի իդեալն է:

Քանի որ $K(+,\cdot)$-ը գլխավոր իդեալներով օղակ է, ապա գոյություն կունենա այնպիսի $a \in K$ տարր, որ $\Delta = (a)$: Հետևաբար,

$$(a) = \bigcup_{i=1}^{\infty} (a_i)$$

և գոյություն կունենա այնպիսի m համար, որ $a \in (a_m)$, այսինքն՝ a/a_m, որտեղից բխում է $(a) \subseteq (a_m)$ ներդրումը: Այսպիսով՝ $(a) = (a_m) = (a_{m+1}) = \cdots$: □

Հետևություն 19.4: *Եթե գլխավոր իդեալներով օղակի տարրերի*

$$a_1, a_2, \ldots, a_n, \ldots$$

անվերջ հաջորդականությունն օժտված է a_i/a_{i+1} հատկությամբ ($i = 1, 2, \ldots$), ապա գոյություն կունենա այնպիսի m համար, որ $a_m \sim a_{m+1} \sim a_{m+2} \sim \cdots$

Ապացուցում: Տրված պայմանից բխում է, որ $(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \ldots$ և համաձայն նախորդ թեորեմի գոյություն կունենա այնպիսի m համար, որ $(a_m) = (a_{m+1}) = (a_{m+2}) = \cdots$: Հետևաբար, համաձայն հետևություն 19.2-ի, կունենանք՝ $a_m \sim a_{m+1} \sim a_{m+2} \sim \cdots$: □

Թեորեմ 19.12: *Գլխավոր իդեալներով օղակի յուրաքանչյուր ոչ զրոյական և ոչ հակադարձելի տարր բաժանվում է նրա որևէ պարզ տարրի վրա:*

Ապացուցում: Ենթադրենք, թե ոչ զրոյական a տարրը հակադարձելի չէ: Հնարավոր է երկու դեպք՝

ա) a տարրը պարզ է և, հետևաբար, նրա համար թեորեմի եզրակացությունը ճիշտ է ($a = a \cdot e$);

բ) a տարրը պարզ չէ: Հետևաբար, այն վերածվում է երկու ոչ հակադարձելի տարրերի արտադրյալի՝ $a = a_1 \cdot b_1$, որտեղ $a_1 \neq 0$, $b_1 \neq 0$: Եթե a_1 տարրը լինի պարզ, ապա թեորեմը կլինի ապացուցված, իսկ հակառակ դեպքում կունենանք՝ $a_1 = a_2 \cdot b_2$, որտեղ $a_2 \neq 0$, $b_2 \neq 0$ տարրերը հակադարձելի չեն: Եթե a_2-ը լիներ պարզ, ապա պնդումը կլիներ ապացուցված, իսկ հակառակ դեպքում կունենանք՝ $a_2 = a_3 \cdot b_3$ և այսպես շարունակ: Այժմ համոզվենք, որ դատողությունների այս շղթան անվերջորեն շարունակվել չի կարող, այսինքն՝ գոյություն կունենա այնպիսի n համար, որ

$$a_n = a_{n+1} \cdot b_{n+1}, \quad a_{n+1} \neq 0, \ \ b_{n+1} \neq 0,$$

հավասարության մեջ a_{n+1}-ը պարզ տարր է:

Իրոք, հակառակ դեպքում, կստանայինք ոչ զրոյական տարրերի

$$a_1, a_2, \ldots, a_n, \ldots$$

անվերջ հաջորդականությունը, որտեղ a_1/a_2, a_2/a_3, … և, հետևաբար (հետևություն 19.3), սկսած որևէ m համարից

$$a_m \sim a_{m+1} \sim a_{m+2} \sim \cdots :$$

Այսպիսով, մի կողմից $a_m = a_{m+1} \cdot \delta$, որտեղ δ-ն հակադարձելի է, իսկ մյուս կողմից $a_m = a_{m+1} \cdot b_{m+1}$, որտեղ b_{m+1}-ը հակադարձելի չէ, որը հնարավոր չէ ամբողջության տիրույթում: □

Թեորեմ 19.13 (Գաուս): *Գլխավոր իդեալներով օղակի յուրաքանչյուր ոչ զրոյական և ոչ հակադարձելի տարր վերածվում է պարզ տարրերի արտադրյալի:*

Ապացույց: Եթե $a \neq 0$ և a-ն ոչ հակադարձելի է, ապա ըստ նախորդ թեորեմի a-ն բաժանվում է որևէ p_1 պարզ տարրի վրա՝ $a = p_1 \cdot b_1$, որտեղ $b_1 \neq 0$: Եթե b_1-ը լիներ նաև ոչ հակադարձելի, ապա նորից նախորդ թեորեմի համաձայն՝ $b_1 = p_2 \cdot b_2$, որտեղ p_2-ը պարզ է, իսկ $b_2 \neq 0$: Եթե b_2-ը լիներ ոչ հակադարձելի, ապա նրան նույնպես կարելի էր տարալուծել համանման եղանակով, և այսպես շարունակ: Ինչպես և նախորդ թեորեմի ապացուցման ժամանակ, դժվար չէ այժմ համոզվել, որ այս երևույթը անվերջորեն շարունակվել չի կարող, այսինքն՝ գոյություն կունենա այնպիսի n համար, որ $b_n = p_{n+1} \cdot b_{n+1}$, որտեղ p_{n+1}-ը պարզ տարր է, իսկ $b_{n+1} \neq 0$ տարրը հակադարձելի է: Այսպիսով՝

$$a = p_1 b = p_1 p_2 b = \cdots = p_1 p_2 \cdots p_{n+1} b_{n+1} = p_1 p_2 \cdots p^*_{n+1},$$

որտեղ $p^*_{n+1} = p_{n+1} \cdot b_{n+1}$ տարրը, համաձայն լեմմ 19.8-ի, ևս կլինի պարզ, քանի որ այն զուգորդված է p_{n+1} պարզ տարրի հետ՝ $p^*_{n+1} \sim p_{n+1}$: □

Թեորեմ 19.14: *Թեորեմ 19.13-ում ապացուցված վերլուծությունը զուգորդման ճշտությամբ որոշվում է միարժեքորեն, այսինքն՝ եթե գլխավոր իդեալներով օղակի ոչ զրոյական և ոչ հակադարձելի a տարրը օժտված է երկու վերլուծություններով՝*

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

որտեղ p_i և q_j տարրերը պարզ են, ապա $n = m$ և գոյություն ունի այնպիսի $\alpha : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ փոխմիարժեք (բիեկտիվ) արտապատկերում, որ $p_i \sim q_{\alpha(i)}$, $i = 1, 2, \ldots, n$:

Ապացուցում: Ենթադրենք $n > m$, այդ դեպքում

$$p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

հավասարությունից բխում է (թեորեմ 19.10), որ q_j տարրերից որևէ մեկը (դիցուք q_1-ը) բաժանվում է p_1 պարզ տարրի վրա՝ q_1 / p_1: Բայց քանի որ q_1-ը ևս պարզ տարր է, ապա $q_1 = \varepsilon_1 \cdot p_1$, որտեղ ε_1-ը հակադարձելի է, հետևաբար՝ $q_1 \sim p_1$: Օգտվելով q_1-ի ստացված ներկայացումից, կունենանք՝

$$p_1 p_2 \cdots p_n = \varepsilon_1 p_1 q_2 \cdots q_m,$$

որտեղից՝ $p_2 \cdots p_m = \varepsilon_1 q_2 \cdots q_m$: Ստացված հավասարությունից այժմ բխում է, որ մնացած q տարրերից որևէ մեկը (դիցուք q_2-ը) բաժանվում է p_2-ի վրա: Հետևաբար, $q_2 = \varepsilon_2 \cdot p_2$, որտեղ ε_2-ը հակադարձելի է: Այժմ ելնելով q_2-ի այս ներկայացումից, հանգում ենք հետևյալ հավասարությանը՝

$$p_2 \cdots p_m = \varepsilon_1 \varepsilon_2 p_2 q_3 \cdots q_m,$$

որտեղից՝ $p_3 \cdots p_m = \varepsilon_1 \varepsilon_2 q_3 \cdots q_m$, և այսպես շարունակ: Վերջավոր թվով քայլերից հետո, ի վերջո դիտարկվող հավասարության աջ մասից կարտաքսվեն բոլոր q տարրերը և կառաջանա

$$p_{m+1} \cdots p_n = \varepsilon_1 \cdots \varepsilon_m = \delta$$

հավասարությունը, որտեղ $\varepsilon_1, \ldots, \varepsilon_m$ տարրերը, ինչպես և նրանց δ արտադրյալը, հակադարձելի են: Հետևաբար, մնացած p պարզ տարրերից յուրաքանչյուրը կլինի հակադարձելի: Օրինակ, $p_{m+1} \left(p_{m+2} \cdots p_n \delta^{-1}\right) = e$: Հակասություն:

Համանման եղանակով քննարկվում է նաև $n < m$ դեպքը: Այսպիսով, $n = m$ և թեորեմն ապացուցված է: □

Ամբողջության տիրույթը կոչվում է **ֆակտորիալ** օղակ, եթե նրա յուրաքանչյուր ոչ զրոյական և ոչ հակադարձելի տարր վերածվում է պարզ տարրերի արտադրյալի և այդ վերլուծությունը զուգորդման ճշտությամբ որոշվում է միարժեքորեն (տես թեորեմ 19.14-ի ձևակերպումը): Այսպիսով, յուրաքանչյուր գլխավոր իդեալներով օղակ հանդիսանում է ֆակտորիալ օղակ: Սակայն գոյություն ունի ֆակտորիալ օղակ, որը գլխավոր իդեալներով օղակ չէ: Օրինակ, ամբողջ գործակիցներով բազմանդամների $\mathbb{Z}[x]$ օղակը, կամ P դաշտից վերցրած գործակիցներով և երկու փոփոխականներից կախված բազմանդամների $P[x, y]$ օղակը այդպիսին են:

Ամբողջության տիրույթը կոչվում է **ֆակտորիզացվող** օղակ, եթե նրա յուրաքանչյուր ոչ զրոյական և ոչ հակադարձելի տարր վերածվում է պարզ տարրերի արտադրյալի: Գոյություն ունի ֆակտորիզացվող օղակ, որը սակայն ֆակտորիալ չէ: Օրինակ, կոմպլեքս թվերի

$$\mathbb{Z}\left[i\sqrt{5}\right] = \left\{x + yi\sqrt{5} |\, x, y \in \mathbb{Z}\right\}$$

օղակը այդպիսին է:

Թեորեմ 19.15: *Որպեսզի $K(+,\cdot)$ ֆակտորիզացվող օղակը լինի ֆակտորիալ օղակ անհրաժեշտ է և բավարար, որ տեղի ունենա հետևյալ պայմանը (որը կոչվում է էվկլիդեսի պայման). եթե $a \cdot b \in K$ արտադրյալը բաժանվում է $p \in K$ պարզ տարրի վրա, ապա $a, b \in K$ արտադրիչներից գոնե մեկը կբաժանվի p-ի վրա:*

Ապացուցում: Անհրաժեշտություն: Դիցուք $ab = pc$, $c \in K$ և դիցուք՝

$$a = p_1 \cdots p_k, \quad b = q_1 \cdots q_s, \quad c = t_1 \cdots t_l,$$

որտեղ p_i, q_j և t_m տարրերը $K(+,\cdot)$ օղակի պարզ տարրերն են: Այսպիսով,

$$p_1 \cdots p_k \cdot q_1 \cdots q_s = p \cdot t_1 \cdots t_l$$

և $K(+,\cdot)$ օղակի ֆակտորիալությունից բխում է, որ գոյություն ունի $i = 1, \ldots, k$ կամ $j = 1, \ldots, s$ այնպիսին, որ $p \sim p_i$ կամ $p \sim q_j$, այսինքն՝ p_i/p կամ q_j/p: Հետևաբար, a/p կամ b/p:

Բավարարություն: Ապացուցենք $K(+,\cdot)$ ֆակտորիզացվող օղակի ֆակտորիալությունը, որտեղ

$$a \cdot b/p \to a/p \quad \text{կամ} \quad b/p :$$

Պահանջվում է ապացուցել, որ ֆակտորիզացվող օղակի յուրաքանչյուր ոչ զրոյական և ոչ հակադարձելի a տարր զուգորդման ճշտությամբ միարժեքորեն է վերլուծվում պարզ տարրերի արտադրյալի: Ապացուցումը կատարենք վերհանգման եղանակով՝ ըստ n բնական թվի, որտեղ n-ը ոչ զրոյական և ոչ հակադարձելի տարրի որևէ վերլուծության մեջ եղած պարզ թվերի քանակն է: $n = 1$ դեպքում պնդումը ճիշտ է, որովհետև, եթե

$$p = q_1 \cdots q_r,$$

որտեղ $r \geqslant 2$ և $q_1, \ldots, q_r$-ը պարզ տարրեր են, ապա ըստ տված պայմանի, q_j տարրերից որևէ մեկը (դիցուք q_1-ը) կբաժանվի p-ի վրա, այսինքն՝ $q_1 = \varepsilon_1 \cdot p$, որտեղ ε_1-ը հակադարձելի է (քանի որ q_1-ը ևս պարզ է): Հետևաբար,

$$p = \varepsilon_1 p q_2 \cdots q_r,$$

կրճատելով p-ով, կստանանք՝

$$e = \varepsilon_1 q_2 \cdots q_r,$$

այսինքն՝ մնացած q_j պարզ տարրերից յուրաքանչյուրը դառնում է հակադարձելի, որը հակասություն է: Այսպիսով, $r = 1$:

Այժմ ենթադրենք, թե բոլոր այն ոչ զրոյական և ոչ հակադարձելի տարրերը, որոնց որևէ վերլուծության մեջ մասնակցում են n-ից քիչ թվով պարզ տարրեր, օժտված են զուգորդման ճշտությամբ միարժեքորեն որոշվող վերլուծությամբ: Ապացուցենք այս պնդումը բոլոր այն ոչ զրոյական և ոչ հակադարձելի a տարրերի համար, որոնց որևէ վերլուծության մեջ մասնակցում են n թվով պարզ տարրեր: Դիցուք՝

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m, \quad m \geqslant n,$$

որտեղ p_i և q_j տարրերը պարզ են: Թեորեմում տված պայմանից բխում է, որ q_j տարրերից որևէ մեկը (դիցուք q_m-ը) բաժանվում է p_n-ի վրա, այսինքն՝ $q_m = \varepsilon \cdot p_n$, որտեղ ε-ը հակադարձելի է: Այսպիսով, հանգում ենք հետևյալ հավասարությանը՝

$$p_1 p_2 \cdots p_{n-1} = \varepsilon \cdot q_1 q_2 \cdots q_{m-1} = q_1^* q_2 \cdots q_{m-1},$$

և համաձայն վերհանգման ենթադրության՝ $m-1=n-1$, որտեղից $m=n$ և համապատասխան պարզ տարրերը կլինեն զուգորդված: □

Եթե $K(+,\cdot)$-ը ֆակտորիալ օղակ է, ապա նրա յուրաքանչյուր ոչ զրոյական և ոչ հակադարձելի $a\in K$ տարր վերածվում է պարզ տարրերի արտադրյալի՝

$$a=p_1p_2\cdots p_n:$$

Հավասարության աջ մասում հնարավոր է լինեն զուգորդված տարրեր: Դիցուք սկզբի s արտադրիչները զույգ առ զույգ զուգորդված չեն, իսկ մնացած պարզ տարրերից յուրաքանչյուրը զուգորդված է սկզբի s պարզ տարրերից որևէ մեկի հետ՝

$$p_i=\varepsilon_{i,j}p_j,$$

որտեղ $i\in\{s+1,\ldots,n\}$, $j\in\{1,\ldots,s\}$, իսկ $s_{i,j}$-ն հակադարձելի է $K(+,\cdot)$ օղակում: Կատարելով այս հավասարություններով տրված $p_{s+1},\ldots,p_n$ տարրերի փոխարինումները, հանգում ենք a տարրի հետևյալ ներկայացմանը՝

$$a=\varepsilon p_1^{k_1}\cdots p_s^{k_s},$$

որտեղ $k_1>0,\ldots,k_s>0$, իսկ s-ը հակադարձելի տարր է: Այս ներկայացումը կոչվում է a-ի **կանոնական ներկայացում** (վերլուծություն): Սակայն հաճախ անհրաժեշտ է լինում դիտարկել

$$a=\varepsilon p_1^{k_1}\cdots p_t^{k_t}$$

տեսքի ներկայացումը, որտեղ $k_1\geqslant 0,\ldots,k_t\geqslant 0$, ε-ը հակադարձելի է, իսկ $p_1,\ldots,p_t$ պարզ տարրերը զույգ առ զույգ զուգորդված չեն: Այս ներկայացումը կոչվում է a-ի **ընդլայնված ներկայացում**: Մասնավորապես կարելի է պնդել, որ $K(+,\cdot)$ ֆակտորիալ օղակի յուրաքանչյուր ոչ զրոյական տարր օժտված է ընդլայնված ներկայացմամբ, որովհետև յուրաքանչյուր հակադարձելի տարր օժտված է այդպիսի ներկայացմամբ՝

$$\varepsilon=\varepsilon\cdot p_1^0\cdots p_t^0:$$

Այնուհետև, եթե $K(+,\cdot)$ ֆակտորիալ օղակի $a,b\in K$ ոչ զրոյական տարրերը օժտված են

$$a=\varepsilon p_1^{k_1}\cdots p_t^{k_t}$$

և

$$b = \delta p_1^{l_1} \cdots p_t^{l_t}$$

ընդլայնված ներկայացումներով (որոնց կարելի է հասնել ավելացնելով պարզ տարրերը զրոյական աստիճաններով), ապա

1) $a/b \longleftrightarrow l_i \leqslant k_i$, $i = 1, 2, \ldots, t$;

2) $p_1^{s_1} \cdots p_t^{s_t} \rightleftharpoons (a, b)$, որտեղ $s_i = \min\{k_i, l_i\}$, $i = 1, 2, \ldots, t$;

3) $p_1^{r_1} \cdots p_t^{r_t} \rightleftharpoons [a, b]$, որտեղ $r_i = \max\{k_i, l_i\}$, $i = 1, 2, \ldots, t$:

Մասնավորապես, ֆակտորիալ օղակի ցանկացած երկու ոչ զրոյական տարրեր օժտված են ամենամեծ ընդհանուր բաժանարարով և ամենափոքր ընդհանուր բազմապատիկով: Սակայն ֆակտորիզացվող օղակները, ընդհանուր դեպքում, այս հատկությամբ չեն օժտված: Օրինակ, կարելի է ապացուցել, որ վերոհիշյալ $\mathbb{Z}[i\sqrt{5}]$ ֆակտորիզացվող օղակում $a = 9$ և $b = 3(2 + i\sqrt{5})$ տարրերի ամենամեծ ընդհանուր բաժանարարը գոյություն չունի, որովհետև դրանց բոլոր ընդհանուր բաժանարարներն են՝ ± 1, ± 3, $\pm(2 + i\sqrt{5})$ կոմպլեքս թվերը և սրանց մեջ չկա մեկը, որ բաժանվի մյուսների վրա:

Թեորեմ 19.16 (Պարզ թվերի քանակի վերաբերյալ Էվկլիդեսի թեորեմի ընդհանրացումը): *Եթե $K(+, \cdot)$ ամբողջության տիրույթը դաշտ չէ (հետևաբար և վերջավոր չէ), նրա յուրաքանչյուր ոչ զրոյական և ոչ հակադարձելի տարր բաժանվում է իր որևէ պարզ տարրի վրա և $K(+, \cdot)$ օղակի հակադարձելի տարրերի $K^*(\cdot)$ խումբը վերջավոր է կամ $K^* \cup \{0\}$ բազմությունը $K(+)$ խմբի ենթակիսախումբն է, ապա $K(+, \cdot)$ օղակի զույգ առ զույգ չզուգորդված բոլոր պարզ տարրերի քանակն անվերջ է:*

Ապացուցում: Ակնհայտ է, որ տված $K(+, \cdot)$ օղակի պարզ տարրերի բազմությունը դատարկ չէ: Ենթադրենք հակառակը, որ տված օղակում զույգ առ զույգ չզուգորդված բոլոր պարզ տարրերի քանակը վերջավոր է և դիցուք դրանք են՝ $p_1, \ldots, p_s$:

1) Դիցուք $K^*(\cdot)$ խումբը վերջավոր է և $|K^*| = n$: Սահմանենք հետևյալ $n + 1$ հատ տարրերը՝

$$q_i = (p_1 \cdots p_s)^i - e, \quad i = 1, \ldots, n + 1 :$$

Եթե որևէ i նշիչի համար $q_i = 0$, ապա կստանանք $(p_1 \cdots p_s)^i = e$, որտեղից՝ $p_j \cdot u = e$, այսինքն՝ p_j պարզ տարրերից յուրաքանչյուրը կլինի հակադարձելի, որը հակասում է պարզ տարրի սահմանմանը: Հետևաբար, $q_i \neq 0$, որտեղ $i = 1, \ldots, n+1$: Այժմ ապացուցենք, որ բոլոր q_i տարրերը հակադարձելի լինել չեն կարող: Իրոք, այդ դեպքում, քանի որ օղակի բոլոր հակադարձելի տարրերի քանակը հավասար է n-ի, ապա գոյություն կունենան այնպիսի $1 \leqslant t < l \leqslant n+1$, որ $q_l = q_t$: Որտեղից կունենանք $(p_1 \cdots p_s)^{l-t} = e$, այսինքն՝ p_j պարզ տարրերից յուրաքանչյուրը կլինի հակադարձելի: Հակասություն:

Ուստի, $q_1, \ldots, q_{n+1}$, տարրերի շարքում գոյություն կունենա որևէ ոչ հակադարձելի և ոչ զրոյական q_j տարր: Համաձայն թեորեմի պայմանի, q_j տարրը կբաժանվի $K(+, \cdot)$ օղակի որևէ պարզ տարրի վրա: Եթե p-ն այդ պարզ տարրն է, ապա պարզվում է $p \not\sim p_i$, $i = 1, \ldots, s$: Իրոք, հակառակ դեպքում, եթե որևէ i նշիչի համար՝ $p \sim p_i$, ապա կունենանք՝ $p = p_i\varepsilon$, $\varepsilon \in K^*$, $q_j = px = p_i\varepsilon x$, $x \in K$ և

$$q_j = (p_1 \cdots p_s)^j - e = p_i\varepsilon x,$$

$$(p_1 \cdots p_s)^j - p_i\varepsilon x = e,$$

$$p_i \cdot y = e, \quad y \in K,$$

այսինքն՝ p_i պարզ տարրը դառնում է հակադարձելի: Հակասություն:

Այսպիսով, եթե $K^*(\cdot)$ խումբը վերջավոր է, ապա թեորեմն ապացուցված է:

2) Դիցուք $K^* \cup \{0\}$ բազմությունը $K(+)$ խմբի ենթակիսախումբն է, այսինքն՝ $K^* \cup \{0\}$ բազմության կամայական երկու տարրերի գումարը նորից պատկանում է այդ բազմությանը: Ինչպես և նախորդ դեպքում՝ $q_1 \neq 0$: Նկատենք, որ q_1-ը նաև հակադարձելի չէ, այսինքն՝ $q_1 \notin K^*$, որովհետև հակառակ դեպքում կունենանք $q_1 + e \in K^* \cup \{0\}$: Հետևաբար $q_1 + e = (p_1 \cdots p_s - e) + e = p_1 \cdots p_s \neq 0$ տարրը կլինի հակադարձելի, որտեղից բխում է նաև $p_1, \ldots, p_s$ պարզ տարրերից յուրաքանչյուրի հակադարձելի լինելը: Հակասություն: Ուստի, համաձայն թեորեմի պայմանի՝ q_1-ը կունենա որևէ p պարզ բաժանարար, որի համար, ինչպես և նախորդ դեպքում, ապացուցվում է, որ $p \not\sim p_i$, $i = 1, \ldots, s$: Հակասություն: □

Հետևություն 19.5: *Եթե դաշտից տարբեր ֆակտորիզացվող (մասնավորապես ֆակտորիալ) $K(+, \cdot)$ օղակի հակադարձելի տարրերի*

$K^*(\cdot)$ խումբը վերջավոր է կամ $K^* \cup \{0\}$ բազմությունը $K(+)$ խմբի ենթակիսախումբն է, ապա $K(+,\cdot)$ օղակի զույգ առ զույգ չզուգորդված բոլոր պարզ տարրերի քանակն անվերջ է: □

Դեռևս պարզ չէ, թե ինչ կարելի պնդել ֆակտորիզացվող օղակի չզուգորդված պարզ տարրերի քանակի վերաբերյալ, եթե օղակի հակադարձելի տարրերի խումբը ոչ թե վերջավոր է, այլ պարբերական է կամ p-խումբ է: Մինչ այժմ չի հայտնաբերված նաև անհրաժեշտ և բավարար պայմաններ, որոնց դեպքում ամբողջության տիրույթի (գլխավոր իդեալներով օղակի, ֆակտորիզացվող կամ ֆակտորիալ օղակի) զույգ առ զույգ չզուգորդված պարզ տարրերի քանակն անվերջ է:

19.4. Էվկլիդյան օղակներ

Սահմանենք գլխավոր իդեալներով օղակների մի կարևոր դաս, որի հիմքում ընկած է մնացորդով բաժանման կանոնը:

$K(+,\cdot)$ ամբողջության տիրույթը կոչվում է **էվկլիդյան** կամ **էվկլիդեսյան** օղակ, եթե կարելի է ընտրել $\delta : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերումն այնպես, որ տեղի ունենան հետևյալ երկու պայմանները.

E1) $\delta(ab) \geqslant \delta(a)$ բոլոր $a,b \in K$, $a \neq 0$, $b \neq 0$ տարրերի համար;

E2) Ցանկացած $a,b \in K$, $b \neq 0$ տարրերի համար գոյություն ունեն այնպիսի $q,r \in K$ տարրեր, որ

$$a = bq + r,$$

որտեղ կամ $r = 0$ կամ $\delta(r) < \delta(b)$:

Այդ դեպքում, δ ֆունկցիան կոչվում է $K(+,\cdot)$ (էվկլիդյան) օղակի էվկլիդյան նորմ: Օղակի էվկլիդյան նորմը E1) և E2) աքսիոմներով միարժեքորեն չի որոշվում: Օրինակ, եթե δ-ն $K(+,\cdot)$ օղակի էվկլիդյան նորմն է, իսկ $n \in \mathbb{N}$, ապա $\delta_n(x) = n \cdot \delta(x)$ ֆունկցիան ևս կլինի էվկլիդյան նորմ $K(+,\cdot)$ օղակի համար: Հանգում ենք հետևյալ գաղափարին:

$K(+,\cdot)$ էվկլիդյան օղակի $\delta_0 : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ էվկլիդյան նորմը կոչվում է **մինիմալ**, եթե այդ օղակի ցանկացած $\delta : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ էվկլիդյան նորմի համար՝ $\delta_0(x) \leqslant \delta(x)$ կամայական $x \in K \setminus \{0\}$

տարրի դեպքում: Կարելի է ապացուցել (տես գլխի վերջում զետեղված 9-րդ խնդիրը), որ յուրաքանչյուր էվկլիդյան օղակ օժտված է մինիմալ էվկլիդյան նորմով:

Էվկլիդյան օղակների դասական օրինակներ են հանդիսանում ամբողջ թվերի $\mathbb{Z}(+,\cdot)$ և (դաշտից վերցված գործակիցներով) մեկ փոփոխականից կախված բազմանդամների օղակները: Առաջին օրինակում որպես էվկլիդյան նորմ կարելի է վերցնել ամբողջ թվի մոդուլը (տես թեորեմ 1.1-ը), կամ` այդ մոդուլի 2-ական համակարգում ունեցած ներկայացման երկարությունը (հետևություն 1.3): Երկրորդ օրինակում որպես էվկլիդյան նորմ կարելի է վերցնել ոչ զրոյական բազմանդամի աստիճանը:

Թեորեմ 19.17: *Բոլոր էվկլիդյան օղակները հանդիսանում են գլխավոր իդեալներով օղակներ, հետևաբար և ֆակտորիալ օղակներ են:*

Ապացուցում: Դիցուք $K(+,\cdot)$-ը էվկլիդյան օղակ է` δ էվկլիդյան նորմով, $\Delta \trianglelefteq K$ և $\Delta \neq (0)$: Ենթադրենք, թե ոչ զրոյական $a_\Delta \in \Delta$ տարրն այնպիսին է, որ ցանկացած ոչ զրոյական $x \in \Delta$ տարրի համար, $\delta(a_\Delta) \leqslant \delta(x)$ (a_Δ տարրի ընտրությունը հնարավոր է, որովհետև բնական թվերի $\{\delta(x)|\ x \in \Delta, x \neq 0\}$ բազմությունն ունի փոքրագույն տարր): Ապացուցենք $\Delta = (a_\Delta)$ հավասարությունը: Քանի որ $(a_\Delta) \subseteq \Delta$ ներդրումն ակներև է, մնում է ապացուցել $\Delta \subseteq (a_\Delta)$ ներդրումը:

Յուրաքանչյուր $x \in \Delta$ տարրի համար գոյություն կունենան այնպիսի $q, r \in K$ տարրեր, որ $x = a_\Delta q + r$, որտեղ կամ $r = 0$ կամ $\delta(r) < \delta(a_\Delta)$: Եթե $r \neq 0$, ապա $\delta(r) < \delta(a_\Delta)$ և $r = x - a_\Delta q \in \Delta$, որը հակասում է a_Δ տարրի ընտրությունը: Ուստի, $r = 0$, $x = a_\Delta q$ և հետևաբար` $\Delta \subseteq (a_\Delta)$: $\square$

Սակայն գոյություն ունի գլխավոր իդեալներով օղակ, որը էվկլիդյան չէ (T. S. Motzkin, Վ. Լենլեյն): Օրինակ, կոմպլեքս թվերի

$$\mathcal{D}[i\sqrt{19}] = \left\{ \frac{x + yi\sqrt{19}}{2} \,\middle|\, x, y \in \mathbb{Z},\ x\text{-}y/2 \right\}$$

օղակը այդպիսին է:

Քանի որ գլխավոր իդեալներով օղակներում, համաձայն թեորեմ 19.7-ի և թեորեմ 19.9-ի, ամենամեծ ընդհանուր բաժանարարը և ամենափոքր ընդհանուր բազմապատիկը գոյություն ունեն ցանկացած երկու (հետևաբար և վերջավոր թվով) տարրերի համար, ապա նույնը վերաբերվում է նաև էվկլիդյան օղակներին: Սակայն էվկլիդյան օղակներում, ի տարբերություն մյուս գլխավոր իդեալներով օղակների, ցանկացած երկու ոչ զրոյական տարրերի ամենամեծ ընդհանուր բաժանարարը կարելի է հաշվել (որոշել) էվկլիդից եկող ալգորիթմով:

Էվկլիդյան օղակի ցանկացած երկու ոչ զրոյական a և b տարրերի համար կարելի է գրել՝

$$a = q_1 b + r_1, \quad \text{եթե } r_1 \neq 0, \text{ ապա}$$

$$b = q_2 r_1 + r_2, \quad \text{եթե } r_2 \neq 0, \text{ ապա}$$

$$r_1 = q_3 r_2 + r_3, \quad \text{եթե } r_3 \neq 0, \text{ ապա}$$

$$\dots \quad \dots \quad \dots \quad \dots \quad \dots \quad \dots$$

Վերջավոր թվով քայլերից հետո, կունենանք՝

$$r_{k-1} = q_{k+1} r_k + r_{k+1}, \quad \text{որտեղ } r_{k+1} = 0,$$

քանի որ հակառակ դեպքում կառաջանա բնական թվերի անվերջ նվազող հաջորդականություն՝

$$\varphi(b) > \varphi(r_1) > \varphi(r_2) > \dots,$$

որը հնարավոր չէ:

Էվկլիդեսի ալգորիթմը: *Էվկլիդյան օղակի ցանկացած ոչ զրոյական* a *և* b *տարրերի համար*՝

$$r_k \rightleftharpoons (a,b) :$$

Ապացուցում: Նախ նկատենք, որ r_k-ն հանդիսանում է a և b տարրերի ընդհանուր բաժանարարը, քանի որ՝

$$r_{k-1}/r_k \to r_{k-2}/r_k \to \dots \to r_1/r_k \to b/r_k \to a/r_k :$$

Եվ հակառակը, եթե d-ն a և b տարրերի համար ընդհանուր բաժանարար է, ապա՝

$$a/d, b/d \to r_1/d \to r_2/d \to \dots \to r_{k-1}/d \to r_k/d :$$

Այսպիսով,

$$r_k \rightleftharpoons (a,b) :$$

Ապացուցենք $K(+,\cdot)$ էվկլիդյան օղակի δ էվկլիդյան նորմի հետևյալ հատկությունները, որտեղ «$\sim$»-ը զուգորդման հարաբերությունն է:

Թեորեմ 19.18*: 1) Եթե $c \sim a$ և $a \neq 0$, ապա $c \neq 0$ և $\delta(c) = \delta(a)$;*

2) Եթե c/a և $\delta(c) = \delta(a)$, $c \neq 0$, $a \neq 0$, ապա $c \sim a$;

3) $\delta(c) = \delta(e) \longleftrightarrow c$-ն էվկլիդյան օղակի հակադարձելի տարր է, որտեղ e-ն օղակի միավորն է;

4) Եթե c/a և $c \not\sim a$, ապա $\delta(c) > \delta(a)$;

5) Եթե ε-ը հակադարձելի է, ապա $\delta(\varepsilon) = \delta_1$, որտեղ δ_1-ը δ ֆունկցիայի փոքրագույն արժեքն է, այսինքն՝ $\delta_1 = \min\{\delta(x) |\ x \in K, x \neq 0\}$;

6) Եթե c-ն հակադարձելի չէ և $c \neq 0$, ապա $\delta(c) > \delta_1$;

7) Եթե էվկլիդյան օղակում գոյություն ունի որևէ ոչ զրոյական և ոչ հակադարձելի տարր, ապա նրա δ էվկլիդյան նորմի արժեքների բազմությունն անվերջ է;

8) էվկլիդյան օղակի $\delta : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերման միջուկի բոլոր համարժեքության դասերը կլինեն վերջավոր այն և միայն այն դեպքում, երբ օղակի բոլոր հակադարձելի տարրերի խումբը վերջավոր է:

Ապացուցում: 1) Քանի որ $c \sim a$, ապա $c = a \cdot \varepsilon$ և $a = c \cdot \varepsilon^{-1}$, որտեղ ε-ը դիտարկվող էվկլիդյան օղակի հակադարձելի տարրն է: Հետևաբար, էվկլիդյան օղակի սահմանման E1) աքսիոմի համաձայն՝

$$\delta(c) = \delta(a \cdot \varepsilon) \geqslant \delta(a),$$

$$\delta(a) = \delta(c \cdot \varepsilon^{-1}) \geqslant \delta(c)$$

և $\delta(c) = \delta(a)$:

2) Եթե c/a, ապա գոյություն ունի այնպիսի $t \in K$, որ $c = at$: Դիցուք $c \neq 0$ և $a = cq + r$, որտեղ $r \neq 0$: Հետևաբար, էվկլիդյան օղակի սահմանման համաձայն՝ $\delta(r) < \delta(c) = \delta(a)$, $r = a - cq = a - atq = a(e - tq)$ և E1) աքսիոմի համաձայն՝ $\delta(r) \geqslant \delta(a)$: Ստացված հակասությունից բխում է $r = 0$ հավասարությունը: Մնում է օգտվել լեմմ 18.7-ից:

3) Անհրաժեշտությունը բխում է 2) -ից, երբ $a = e$: Բավարարությունը բխում է 1)-ից, երբ $a = e$:

4) Բխում է 2)-ից և E1) աքսիոմից:

5) Գոյություն ունի այնպիսի $k \in K$, որ $\delta(k) = \delta_1$: Քանի որ ε-ը հակադարձելի է և $k = \varepsilon\left(\varepsilon^{-1}k\right)$, ապա E1)-ի համաձայն՝ $\delta(k) \geqslant \delta(\varepsilon)$, այսինքն՝ $\delta_1 \geqslant \delta(\varepsilon)$ և δ_1-ի մինիմալությունից բխում է $\delta_1 = \delta(\varepsilon)$ հավասարությունը:

6) Ենթադրենք հակառակը, որ $\delta(c) = \delta_1$, $c \neq 0$: Այդ դեպքում, համաձայն նախորդ հատկության, $\delta(c) = \delta(\varepsilon)$, որտեղ ε-ը հակադարձելի է: Մասնավորապես, $\delta(c) = \delta(e)$ և հետևաբար, համաձայն 3)-ի՝ c-ն կլինի հակադարձելի է: Հակասություն:

7) Դիցուք a-ն դիտարկվող $K(+,\cdot)$ էվկլիդյան օղակի ոչ զրոյական և ոչ հակադարձելի տարրն է: Հատկություն 4)-ի համաձայն՝

$$\delta(a) < \delta(a^2) < \delta(a^3) < \cdots < \delta(a^n) < \cdots$$

8) *Անհրաժեշտություն:* Բխում է 1)-ից: *Բավարարություն:* Եթե էվկլիդյան օղակի յուրաքանչյուր ոչ զրոյական x տարր հակադարձելի է, ապա 5)-ի համաձայն՝ $\delta(x) = \delta_1 = \delta(y)$, այսինքն՝ օղակի բոլոր ոչ զրոյական տարրերը կազմում են δ արտապատկերման միջուկի մի համարժեքության դաս, որը համընկնելով օղակի բոլոր հակադարձելի տարրերի խմբի հետ, կլինի վերջավոր: Իսկ եթե դիտարկվող էվկլիդյան օղակում գոյություն ունի ոչ զրոյական և ոչ հակադարձելի տարր, ապա 7)-ի համաձայն δ ֆունկցիայի արժեքների բազմությունը կլինի անվերջ: Այս դեպքում, δ ֆունկցիայի արժեքների բազմությունը նախ դասավորենք աճման կարգով՝

$$\delta_1 < \delta_2 < \cdots < \delta_n < \cdots$$

և վերհանգման եղանակով ապացուցենք, որ էվկլիդյան օղակի բոլոր այն $x \neq 0$ տարրերի բազմությունը, որոնց համար տեղի ունի

$$\delta(x) \leqslant \delta_n$$

անհավասարությունը, կլինի վերջավոր: Իրոք, $n = 1$ դեպքում պնդումն ակնհայտորեն ճիշտ է, որովհետև $\delta(x) \leqslant \delta_1$ պայմանին բավարարող բոլոր $x \neq 0$ տարրերի բազմությունը համընկնում է օղակի բոլոր հակադարձելի տարրերի բազմության հետ, որը ըստ պայմանի վերջավոր է: Ենթադրելով պնդումը ճիշտ $\delta(x) \leqslant \delta_n$ անհավասարության համար, ապացուցենք այն $\delta(x) \leqslant \delta_{n+1}$ անհավասարության դեպքում: Դիցուք $\delta(x) \leqslant \delta_{n+1}$ անհավասարությանը բավարարում են անվերջ թվով (միմյանցից տարբեր)

$$x_1, x_2, \ldots, x_m, \ldots$$

տարրեր: Քանի որ օղակի հակադարձելի տարրերի քանակը վերջավոր է, ապա կարելի է ենթադրել, որ այս հաջորդականության բոլոր տարրերը հակադարձելի չեն (նախապես ջնջելով բոլոր հակադարձելիները): Դիցուք օղակի $a \neq 0$ տարրը բավարարում է $\delta(a) \geqslant \delta_{n+1} > \delta_1$ պայմանին և

$$a = x_m q_m + r_m, \quad m \in \mathbb{N},$$

որտեղ կամ $r_m = 0$ կամ $\delta(r_m) < \delta(x_m) \leqslant \delta_{n+1}$, հետևաբար կամ $r_m = 0$ կամ $\delta(r_m) \leqslant \delta_n$: Համաձայն վերհանգման ենթադրության, գոյություն ունեն օղակի միայն վերջավոր թվով r_m տարրեր, որ $\delta(r_m) \leqslant \delta_n$: Հնարավոր են հետևյալ երկու դեպքերը. ա) գոյություն ունեն անվերջ թվով $m \in \mathbb{N}$ բնական թվեր, որոնց համար $r_m = 0$, և բ) գոյություն ունեն վերջավոր թվով $m \in \mathbb{N}$ բնական թվեր, որոնց համար $r_m = 0$: Երկրորդ դեպքում, գոյություն կունենա $\{x_m\}$ հաջորդականության այնպիսի անվերջ $\{x_{m_s}\}$ ենթահաջորդականություն, որի տարրերի համար՝ $r_{m_s} = r \neq 0$, $s \in \mathbb{N}$: Այսպիսով, կունենանք $a - r \neq 0$ (որովհետև $\delta(a) \neq \delta(r)$),

$$a - r = x_{m_1} q_{m_1} = x_{m_2} q_{m_2} = \cdots = x_{m_s} q_{m_s} = \cdots ,$$

որտեղից՝ $\delta(a-r) \geqslant \delta(x_{m_1}) > \delta_1$ և $a-r$ տարրը հակադարձելի չէ (բխում է 3) և 5) հատկություններից): Հետևաբար, էվկլիդյան օղակի $a - r$ ոչ զրոյական և ոչ հակադարձելի տարրի համար կունենանք անվերջ թվով

$$x_{m_1}, x_{m_2}, \ldots, x_{m_s}, \ldots$$

բաժանարարներ, որը հնարավոր չէ հակադարձելի տարրերի վերջավոր խումբ ունեցող ֆակտորիալ օղակում, որովհետև ինչպես գիտենք ֆակտորիալ օղակում՝

$$a - r = \varepsilon \cdot p_1^{k_1} \cdots p_t^{k_t},$$

որտեղ ε-ը օղակի հակադարձելի տարր է, իսկ $p_1, \ldots, p_t$ տարրերը պարզ են (և զույգ առ զույգ չզուգորդված), ուստի $a - r$ տարրի բոլոր բաժանարարների թիվը կլինի վերջավոր: Ավելի ճիշտ, այդ թիվը կլինի հավասար՝

$$\tau(a-r) = l(k_1+1) \cdots (k_t+1),$$

որտեղ l-ը օղակի հակադարձելի տարրերի քանակն է: Հակասություն:

Նույն ձևով, հակասության ենք հանգում նաև ա) դեպքում: Այս դեպքում, անվերջ թվով բաժանարարների գոյությանն ենք հանգում ոչ հակադարձելի $a \neq 0$ տարրի համար (որովհետև կունենանք՝ $a = x_{m_t} q_{m_t}$, $t \in \mathbb{N}$), որը հնարավոր չէ դիտարկվող օղակում: □

19.5. Թվաբանական օղակներ: Ֆերմայի և Էյլերի ֆունկցիաները թվաբանական օղակներում: Օղակների վրա որոշված արտադրյալային ֆունկցիաներ

$K(+,\cdot)$ ամբողջության տիրույթը կանվանենք **թվաբանական օղակ**, եթե նրա յուրաքանչյուր ոչ զրոյական $m \in K$ տարրով ծնված (m) գլխավոր իդեալի համար $K/(m) = \{x + (m) | \ x \in K\}$ քանորդ-օղակը վերջավոր է:

Օրինակ, $\mathbb{Z}$ օղակը և դաշտերը թվաբանական օղակի պարզագույն օրինակներ են:

Թեորեմ 19.19*: Եթե էվկլիդյան օղակի հակադարձելի տարրերի խումբը վերջավոր է, ապա այն թվաբանական օղակ է:*

Ապացուցում: Դիցուք $K(+,\cdot)$-ը տրված պայմանին բավարարող և δ էվկլիդյան նորմով էվկլիդյան օղակ է, $m \in K$, $m \neq 0$ և $K/(m) = \{x + (m) | \ x \in K\}$: Եթե $[x] = x + (m)$, $[x] \neq [0]$ և $\delta(x) \geqslant \delta(m)$, ապա

$$x = mq + r,$$

որտեղ $r = x - mq \in [x]$, $r \neq 0$ և $\delta(r) < \delta(m)$: Հետևաբար, $[r] = [x]$ և

$$K/(m) = \{r + (m) | \ r \in K, \delta(r) < \delta(m)\} \cup \{0 + (m)\} :$$

Մնում է օգտվել թեորեմ 19.18-ի հատկություն 8)-ից, որի համաձայն $K(+,\cdot)$ էվկլիդյան օղակի բոլոր այն r տարրերի բազմությունը, որոնց համար $\delta(r) < \delta(m)$, կլինի կամ վերջավոր կամ դատարկ (եթե m-ը հակադարձելի է): □

Օրինակ, վերջավոր $P(+,\cdot)$ դաշտից վերցրած գործակիցներով և մեկ փոփոխականից կախված $P[x]$ բազմանդամների օղակը բավարարում է ապացուցված թեորեմի պայմաններին և հետևաբար այն կլինի թվաբանական օղակ: Ընդ որում, կարելի է ապացուցել, որ n-րդ աստիճանի յուրաքանչյուր $f \in P[x]$, $f \neq 0$ բազմանդամի համար $\left| P[x]/(f) \right| = q^n$, որտեղ $q = |P|$ (բխում է բազմանդամների մնացորդով բաժանման թեորեմից):

Գոյություն ունի այնպիսի էվկլիդյան և թվաբանական օղակ, որի հակադարձելի տարրերի խումբը անվերջ է: Օրինակ, իրական թվերի

$$\mathbb{Z}\left[\sqrt{2}\right]=\left\{x+y\sqrt{2}\right|\ x,y\in\mathbb{Z}\right\}$$

օղակը թվաբանական է, էվկլիդյան է՝ $\delta\left(x+y\sqrt{2}\right) = \left|x^2-2y^2\right|$ էվկլիդյան նորմով և որի $\left(1+\sqrt{2}\right)^m$, $m\in\mathbb{Z}$ տարրերը ակնհայտորեն հակադարձելի են (Հ. Հասսե): Սակայն գոյություն ունեն նաև էվկլիդյան օղակներ, որոնք թվաբանական օղակներ չեն (օրինակ, անվերջ $P(+,\cdot)$ դաշտից վերցրած գործակիցներով և մեկ փոփոխականից կախված բազմանդամների $P[x]$ օղակը):

Դիցուք $K(+,\cdot)$-ը թվաբանական օղակ է; Քանի որ յուրաքանչյուր $m\in K$, $m\neq 0$ տարրի համար համապատասխան $K/(m)$ քանորդ-օղակը վերջավոր է, ապա սահմանելով՝

$$\nu(m)=\left|K/(m)\right|,$$

ստանում ենք $\nu : K\setminus\{0\}\to\mathbb{N}$ ֆունկցիան, որը կոչվում է $K(+,\cdot)$ թվաբանական **օղակի Ֆերմայի ֆունկցիա**:

Օրինակ, եթե $m=\varepsilon\in K$ տարրը հակադարձելի է, ապա $(m)=K$, $\left|K/(m)\right|=1$ և $\nu(m)=1$: Հետևաբար, եթե $K(+,\cdot)$-ը դաշտ է, ապա $\nu(m)=1$ բոլոր $m\in K$, $m\neq 0$ տարրերի համար, իսկ $\mathbb{Z}(+,\cdot)$ օղակի համար՝ $(m)=(-m)$ և $\nu(m)=|m|$:

Թեորեմ 19.20*: $K(+,\cdot)$ թվաբանական օղակի Ֆերմայի ֆունկցիան լիովին արտադրյալային է, այսինքն՝*

$$\nu(a\cdot b)=\nu(a)\cdot\nu(b)$$

կամայական ոչ զրոյական $a,b\in K$ տարրերի համար: Մասնավորապես $\nu\left(a^n\right)=(\nu a)^n$, $n\in\mathbb{N}$:

Ապացուցում: Եթե

$$K/(a)=\{x+(a)|\,x\in K\}$$

քանորդ-օղակին պատկանող և միմյանցից տարբեր $x+(a)$ հարակից դասերից մեկական վերցրած տարրերի ցանկացած բազմություն անվանենք $K(+,\cdot)$ օղակի **մնացքների լրիվ համակարգ** ըստ a հենքի և նշանակենք $K(mod\, a)$-ով, ապա կունենանք՝ $\nu(a) = |K(mod\, a)|$, ${}^{K}/_{(a)} = \{x + (a)|\, x \in K(mod\, a)\}$,

$$K = \bigcup_{x \in K(mod\, a)} x + (a) :$$

Յուրաքանչյուր $t \in K$ տարրի համար գոյություն ունի այնպիսի $y \in K(mod\, b)$, որ $t \in y + (b)$, այսինքն՝ $t = y + bz$, $z \in K$: Հետևաբար,

$$x + (a) = \{x + at|\, t \in K\} = \{x + ay + abz|\, y \in K(mod\, b), z \in K\} =$$

$$= \bigcup_{y \in K(mod\, b)} \{x + ay\} + (ab)$$

և

$$K = \bigcup_{x \in K(mod\, a)} x + (a) = \bigcup_{x \in K(mod\, a)} \left(\bigcup_{y \in K(mod\, b)} \{x + ay\} + (ab) \right) =$$

$$= \bigcup_{\substack{x \in K(mod\, a) \\ y \in K(mod\, b)}} \{x + ay\} + (ab),$$

այսինքն՝

$${}^{K}/_{(ab)} = \{\{x + ay\} + (ab)|\, x \in K(mod\, a), y \in K(mod\, b)\},$$

որտեղ, եթե $x + ay \equiv x' + ay'(mod\, ab)$, ապա $x = x'$ և $y = y'$: Իրոք, եթե $x + ay \equiv x' + ay'(mod\, ab)$ և $x \neq x'$, ապա

$$x + ay - (x' + ay') = ab \cdot q, \quad q \in K,$$

$$x - x' = ay' - ay + abq = a \cdot l, \quad l \in K,$$

$$x \equiv x'(mod\, a),$$

որը հակասում է $x, x' \in K(mod\, a)$ պայմանին: Հետևաբար, $x = x'$: Եթե այժմ $y \neq y'$, ապա օգտվելով $x = x'$ հավասարությունից, նորից հանգում ենք հակասության՝

$$x + ay - (x' + ay') = ab \cdot q,$$

$$a\,(y' - y) = ab \cdot q,$$

$$y - y' = b \cdot q,$$

որը հակասում է $y, y' \in K(mod\, b)$ տարրերի ընտրությանը:

Այսպիսով`

$$K(mod\, ab) = \{x + ay |\, x \in K(mod\, a), y \in K(mod\, b)\}$$

և հետևաբար`

$$|K(mod\, ab)| = |\{x + ay |\, x \in K(mod\, a), y \in K(mod\, b)\}| =$$

$$= |\{(x, y) |\, x \in K(mod\, a), y \in K(mod\, b)\}| = |K(mod\, a)| \cdot |K(mod\, b)|\,,$$

այսինքն`

$$\nu(a \cdot b) = \nu(a) \cdot \nu(b) : \qquad \square$$

Եթե $K(+, \cdot)$ ամբողջության տիրույթի $a, m \in K$ տարրերը փոխադարձաբար պարզ են, այսինքն` $e = (a, m)$, ապա $e = (a + mt, m)$ կամայական $t \in K$ տարրի համար, որովհետև եթե $ax + my = e$, $x, y \in K$, ապա

$$ax + mtx - mtx + my = e,$$

$$(a + mt)x + m(y - tx) = e :$$

Հետևաբար, եթե $e = (a, m)$ և $x \equiv a(mod\, m)$, ապա $e = (x, a)$: Այդ պատճառով, օղակի $[a]$ մնացքների դասը ևս կոչվում է փոխադարձաբար պարզ m-ի հետ: Հաշվի առնելով նաև $[a] = a + (m)$ հավասարությունը, հանգում ենք հետևյալ գաղափարին:

Դիցուք $K(+, \cdot)$-ը թվաբանական օղակ է, $m \in K$, $m \neq 0$ և

$$K/_{(m)} = \{x + (m) |\, x \in K\} :$$

Սահմանելով $\varphi(m)$-ը հավասար $K/_{(m)}$ քանորդ-օղակի բոլոր այն $[x] = x + (m)$ հարակից դասերի թվին, որոնք փոխադարձաբար պարզ են m-ի հետ, ստանում ենք $\varphi : K \setminus \{0\} \to \mathbb{N}$ ֆունկցիան, որը կոչվում է տրված $K(+, \cdot)$ թվաբանական **օղակի էյլերի ֆունկցիա**:

Օրինակ, դաշտի դեպքում էյլերի ֆունկցիան համընկնում է Ֆերմայի ֆունկցիայի հետ` $\varphi(m) = 1$, $m \neq 0$, իսկ $\mathbb{Z}(+, \cdot)$ օղակի դեպքում $\varphi(m)$-ը հավասար է էյլերի $\mathbb{N} \to \mathbb{N}$ սովորական ֆունկցիայի (գլուխ 9) արժեքին $|m|$-ի վրա: Եթե դիտարկվող $K(+, \cdot)$ օղակի $m \neq 0$ տարրի հետ փոխադարձաբար պարզ և միմյանցից տարբեր բոլոր հարակից դասերն են՝

$$[x_1] = x_1 + (m), \ldots, [x_{\varphi(m)}] = x_{\varphi(m)} + (m),$$

ապա այս դասերից մեկական վերցված տարրերի ցանկացած բազմություն կոչվում է $K(+,\cdot)$ **օղակի մնացքների բերված համակարգ** ըստ m հենքի և նշանակվում է $K^*(mod\, m)$-ով: Ուստի՝

$$\varphi(m) = |K^*(mod\, m)| :$$

Թեորեմ 19.21*: Յուրաքանչյուր $K(+,\cdot)$ թվաբանական օղակի էյլերի ֆունկցիան արտադրյալային է, այսինքն՝՝*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

որտեղ $a, b \in K$ ոչ զրոյական տարրերը փոխադարձաբար պարզ են:

Ապացուցում: Ինչպես տեսանք, $K(+,\cdot)$ թվաբանական օղակի համար՝

$$K = \bigcup_{\substack{x \in K(mod\, a) \\ y \in K(mod\, b)}} \{x + ay\} + (ab) = \bigcup_{\substack{x \in K(mod\, a) \\ y \in K(mod\, b)}} \{bx + ay\} + (ab);$$

Երկրորդ հավասարությունը այստեղ տեղի ունի այն պատճառով, որ եթե x-ը ընդունում է $K(+,\cdot)$ օղակի մնացքների լրիվ համակարգի բոլոր արժեքները (ըստ a հենքի), ապա bx արտադրյալի համապատասխան արժեքները նորից կկազմեն մնացքների լրիվ համակարգ (ըստ նույն հենքի): Իրոք, եթե $x \not\equiv x'(mod\, a)$, ապա $bx \not\equiv bx'(mod\, a)$, որովհետև հակառակ դեպքում կունենայինք՝

$$bx - bx' = at, \quad t \in K,$$

$$b(x - x') = at$$

և քանի որ a, b տարրերը փոխադարձաբար պարզ են, ապա $x - x'$ տարբերությունը կբաժանվի a-ի վրա, այսինքն՝ $x \equiv x'(mod\, a)$: Հակասություն:

Հեշտությամբ ստուգվում է նաև, որ օղակի $bx + ay$ տարրը կլինի փոխադարձաբար պարզ ab արտադրյալի հետ այն և միայն այն դեպքում, երբ a, x և b, y զույգերը փոխադարձաբար պարզ են՝

$$e = (bx + ay, ab) \longleftrightarrow e = (a, x), \;\; e = (b, y) :$$

Իրոք, եթե $e = (bx + ay, ab)$, այսինքն՝ գոյություն ունեն $K(+, \cdot)$ օղակի այնպիսի $s, t \in K$ տարրեր, որ

$$(bx + ay)s + abt = e,$$

ապա կունենանք՝

$$x(bs) + a(bt + ys) = e,$$

$$y(as) + b(at + xs) = e,$$

այսինքն՝ $(a, x) = e$ և $(b, y) = e$: Եվ հակառակը, եթե $(a, x) = e$ և $(b, y) = e$, ապա (հատկություն 19.1) $(a, xb) = e$ և $(b, ay) = e$, այսինքն՝ գոյություն կունենան այնպիսի $u, v, u', v' \in K$ տարրեր, որ

$$au + xbv = e,$$

$$bu' + ayv' = e,$$

և հետևաբար,

$$a(u - yv) + (xb + ay)v = e,$$

$$b\,(u' - xv') + (ay + xb)v' = e,$$

այսինքն՝ $(a, xb + ay) = e$ և $(b, xb + ay) = e$: Ուստի, $(ab, xb + ay) = e$:

Մնում է նկատել, որ

$$bx + ay \equiv bx' + ay'(mod\, ab) \longrightarrow x = x', \;\; y = y' :$$

Իրոք, $bx + ay \equiv bx' + ay'(mod\, ab)$ բաղդատումից կունենանք՝

$$bx + ay - (bx' + ay') = ab \cdot l, \quad l \in K,$$

$$b(x - x') = a(bl + y' - y),$$

$$a(y - y') = b(al + x' - x)$$

և քանի որ a, b զույգը փոխադարձաբար պարզ է, ապա այստեղից կբխի ${}^{x\text{-}x'}/_{a}$ և ${}^{y\text{-}y'}/_{b}$, այսինքն՝ $x \equiv x'(mod\, a)$ և $y \equiv y'(mod\, b)$, որտեղ $x, x' \in K(mod\, a)$, $y, y' \in K(mod\, b)$: Հետևաբար, $x = x'$ և $y = y'$:

Այսպիսով,

$$|K^*(\mod ab)| = |\{(x, y)|\, x \in K^*(mod\, a), y \in K^*(mod\, b)\}| =$$

$$= |K^*(mod\, a)| \cdot |K^*(mod\, b)|\,,$$

այսինքն՝

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) : \qquad \square$$

Թեորեմ 19.22 (էյլերի թեորեմը թվաբանական օղակներում): *Եթե $K(+,\cdot)$ թվաբանական օղակի a և $m \neq 0$ տարրերը փոխադարձաբար պարզ են, ապա*

$$a^{\varphi(m)} \equiv e(mod\, m),$$

որտեղ e-ն օղակի միավորն է, իսկ φ-ն նրա էյլերի ֆունկցիան:

Ապացուցում: Թեորեմ 9.1-ի ապացուցման կրկնությունն է: Իրոք, եթե $a = 0$, ապա $e = (a, m)$ պայմանից բխում է $0x + my = e$ հավասարությունը, որտեղ $x, y \in K$, այսինքն՝ $my = e$ և m-ը հակադարձելի է: Ուստի, $\varphi(m) = 1$ և $-e = m(-y)$, որը հավասարազոր է $0^{\varphi(m)} \equiv e(mod\, m)$ բաղդատմանը:

Եթե $a \neq 0$ և տարրերի

$$x_1, x_2, \ldots, x_{\varphi(m)}$$

հաջորդականությունը $K(+,\cdot)$ օղակի մնացքների որևէ բերված համակարգ է ըստ m հենքի, ապա այդպիսին կլինի նաև

$$ax_1, ax_2, \ldots, ax_{\varphi(m)}$$

հաջորդականությունը: Հետևաբար, առաջին բերված համակարգի յուրաքանչյուր տարր կլինի բաղդատելի երկրորդ բերված համակարգի որևէ տարրի հետ և

$$ax_1 ax_2 \cdots ax_{\varphi(m)} \equiv x_1 x_2 \cdots x_{\varphi(m)} (mod\, m) :$$

Մնում է կրճատել ստացված բաղդատումը $x_1 x_2 \cdots x_{\varphi(m)}$ արտադրյալով (որովհետև $\left(m, x_1 x_2 \cdots x_{\varphi(m)}\right) = e$):

Լեմմ 19.10: *Եթե p-ն $K(+,\cdot)$ թվաբանական օղակի պարզ տարրն է, ապա*

$$\varphi\left(p^k\right) = \varphi(p) \cdot (\nu p)^{k-1}, \quad k \in \mathbb{N},$$

որտեղ ν-ն և φ-ն $K(+,\cdot)$ օղակի Ֆերմայի և էյլերի ֆունկցիաներն են: Մասնավորապես, թվաբանական և գլխավոր իդեալներով օղակում՝

$$\varphi\left(p^k\right) = (\nu p)^k - (\nu p)^{k-1}, \quad k \in \mathbb{N} :$$

Ապացուցում: Օգտվենք

$$K = \bigcup_{\substack{x \in K(mod\, a) \\ y \in K(mod\, b)}} \{x + ay\} + (ab)$$

ներկայացումից, որն ապացուցվել է վերևում: Եթե այստեղ վերցնենք՝ $a = p$, $b = p^{k-1}$, ապա կունենանք՝

$$K = \bigcup_{\substack{x \in K(mod\, p) \\ y \in K\left(mod\, p^{k-1}\right)}} \{x + py\} + \left(p^k\right) :$$

Օղակի $x + py$ տարրը կլինի փոխադարձաբար պարզ p^k-ի հետ այն և միայն այն դեպքում, երբ x, p զույգը փոխադարձաբար պարզ է: Իրոք, եթե $e = \left(x + py, p^k\right)$, ապա գոյություն կունենան այնպիսի $t, s \in K$ տարրեր, որ

$$(x + py)t + p^k s = e,$$
$$xt + p\left(yt + p^{k-1}s\right) = e,$$

այսինքն՝ $(x, p) = e$: Եվ հակառակը, եթե $(x, p) = e$, ապա $(x + py, p) = e$ և (հատկություն 19.2) $\left(x + py, p^k\right) = e$:

Այդպիսի x-երի թիվը կլինի հավասար $\varphi(p)$-ի, իսկ y-ների թիվը հավասար է $\nu\left(p^{k-1}\right)$-ի: Այսպիսով՝ $\varphi\left(p^k\right) = \varphi(p)\cdot\nu\left(p^{k-1}\right) = \varphi(p)\cdot(\nu p)^{k-1}$:

Գլխավոր իդեալներով օղակում x, p զույգը կլինի փոխադարձաբար պարզ այն և միայն այն դեպքում, երբ x-ը չի բաժանվում p-ի վրա (լեմմ 19.9): Հետևաբար, այդ դեպքում՝ $\varphi(p) = \nu(p) - 1$, իսկ

$$\varphi\left(p^k\right) = \varphi(p)\cdot(\nu p)^{k-1} = (\nu p - 1)\cdot(\nu p)^{k-1} = (\nu p)^k - (\nu p)^{k-1} : \quad \square$$

***Հետևություն 19.6* (Ֆերմայի փոքր թեորեմը օղակներում):** *Եթե p-ն $K(+,\cdot)$ թվաբանական և գլխավոր իդեալներով օղակի պարզ տարրն է և $a \in K$ տարրը չի բաժանվում p-ի վրա, ապա*

$$a^{\nu(p)-1} \equiv e(mod\, p),$$

որտեղ ν-ն $K(+,\cdot)$ օղակի Ֆերմայի ֆունկցիան է: $\square$

Հետևություն 19.7: *Եթե թվաբանական և գլխավոր իդեալներով օղակի ոչ զրոյական և ոչ հակադարձելի a տարրը օժտված է*

$$a = \varepsilon \cdot p_1^{k_1} \cdots p_s^{k_s}$$

կանոնական վերլուծությամբ, որտեղ ε-ը հակադարձելի է, իսկ $p_1, \ldots, p_s$ տարրերը պարզ են և զույգ առ զույգ չզուգորդված, ապա

$$\varphi(a) = \nu(a)\left(1 - \frac{1}{\nu\left(p_1\right)}\right)\cdots\left(1 - \frac{1}{\nu\left(p_s\right)}\right) :$$

Ապացուցում: Բխում է էյլերի ֆունկցիայի արտադրյալային հատկությունից (թեորեմ 19.21) և լեմմ 19.10-ից: □

Դիցուք $K(+,\cdot)$-ը կամայական ամբողջության տիրույթ է, իսկ Q-ն կամայական թվակերպ բազմություն է (գլուխ 9): $\Theta: K\setminus\{0\}\to Q$ ֆունկցիան կոչվում է **օղակային արտադրյալային ֆունկցիա**, եթե այն բավարարում է հետևյալ պայմաններին.

ա) $\Theta(\varepsilon)=1$ ցանկացած $\varepsilon\in K$ հակադարձելի տարրի համար;

բ) $\Theta(a\cdot b)=\Theta(a)\cdot\Theta(b)$ կամայական $a,b\in K$ փոխադարձաբար պարզ տարրերի համար:

Օրինակ, թվաբանական օղակի Ֆերմայի և էյլերի ֆունկցիաները օղակային արտադրյալային ֆունկցիաներ են, որտեղ $Q=\mathbb{N}$: Կամայական $\alpha: K\setminus\{0\}\to\mathbb{N}$ օղակային արտադրյալային ֆունկցիայի և կամայական Q թվակերպ բազմության համապատասխան սահմանելով $\Theta_\alpha: K\setminus\{0\}\to Q$ ֆունկցիան հետևյալ կերպ՝

$$\Theta_\alpha(a)=\alpha(a)\circ 1=\underbrace{1+1+\cdots+1}_{\alpha(a)},\quad a\neq 0,$$

կստանանք նոր օղակային արտադրյալային ֆունկցիա: Մասնավորապես, որպես α կարելի է վերցնել թվաբանական օղակի Ֆերմայի և էյլերի ֆունկցիաները:

Գլուխ 9-ում $\mathbb{N}\to Q$ տեսքի արտադրյալային ֆունկցիաների վերաբերյալ ապացուցված արդյունքները վերաձևակերպվում և ապացուցվում են $K\setminus\{0\}\to Q$ տեսքի օղակային արտադրյալային ֆունկցիաների համար, որտեղ Q-ն թվակերպ բազմություն է: Ասվածը վերաբերվում է նաև Դիրիխլեի արտադրյալին և Մյոբիուսի թեորեմին: Մասնավորապես, այս ընդհանուր դեպքում, Մյոբիուսի ֆունկցիան սահմանվում է հետևյալ կերպ:

Դիցուք $K(+,\cdot)$-ը ֆակտորիալ օղակ է, իսկ Q թվակերպ բազմությունն օժտված է $-1\in Q$ հատկությամբ, այսինքն՝ Q-ն միավորով օժտված (որը նշանակվում է 1-ով) զուգորդական և տեղափոխական օղակ է: **Մյոբիուսի օղակային** $\mu: K\setminus\{0\}\to Q$ **ֆունկցիան** սահմանվում է հետևյալ կերպ՝

$$\mu(a) = \begin{cases} 1, & \text{եթե } a \in K \text{ տարրը հակադարձելի է,} \\ (-1)^k, & \text{եթե } a = \varepsilon \cdot p_1 \cdots p_k, \text{ որտեղ } \varepsilon\text{-ը հակադարձելի է,} \\ & \quad \text{իսկ } p_1, \ldots, p_k \text{ տարրերը պարզ են ,} \\ & \quad \text{և զույգ առ զույգ չզուգորդված,} \\ 0, & \text{եթե } a\text{-ն բաժանվում է որևէ } p \text{ պարզ տարրի :} \\ & \quad \text{քառակուսու վրա,} \end{cases}$$

19.6. Օղակային հոմոմորֆիզմներ: Օղակային հոմոմորֆիզմի միջուկ: Հոմոմորֆիզմների և իզոմորֆիզմների թեորեմները օղակներում

Դիցուք $K(+,\cdot)$-ը և $K'(+,\cdot)$-ը կամայակն օղակներ են: $\varphi : K \to K'$ արտապատկերումը կոչվում է **հոմոմորֆիզմ**, **հոմոմորֆություն**, **հոմոմորֆ արտապատկերում** կամ **նմանաձնություն**՝ $K(+,\cdot)$ օղակից $K'(+,\cdot)$ օղակի մեջ կամ $K(+,\cdot)$ և $K'(+,\cdot)$ օղակների միջև, եթե

$$\varphi(x+y) = \varphi(x) + \varphi(y)$$

և

$$\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$$

ցանկացած $x, y \in K$ տարրերի համար, այսինքն՝ φ արտապատկերումը համաձայնեցված է դիտարկվող օղակների օղակային գործողությունների հետ: Օղակների միջև գործող հոմոմորֆիզմը հաճախ կոչվում է նաև օղակային հոմոմորֆիզմ:

Դժվար չէ ստուգել, որ երկու (հետևաբար և վերջավոր թվով) օղակային հոմոմորֆիզմների արտադրյալը նորից օղակային հոմոմորֆիզմ է (եթե այն գոյություն ունի), այսինքն՝ եթե $K(+,\cdot)$-ը, $K'(+,\cdot)$-ը և $K''(+,\cdot)$-ը կամայական օղակներ են, իսկ $\varphi : K \to K'$ և $\varphi' : K' \to K''$ արտապատկերումները օղակային հոմոմորֆիզմներ են, ապա $\varphi \cdot \varphi' : K \to K''$ արտապատկերումը ևս կլինի օղակային հոմոմորֆիզմ, որովհետև

$$(\varphi \cdot \varphi')\,(x+y) = \varphi'\,(\varphi(x+y)) = \varphi'\,(\varphi x + \varphi y) = \varphi'(\varphi x) + \varphi'(\varphi y) =$$

$$= (\varphi \cdot \varphi')\,x + (\varphi \cdot \varphi')\,y,$$

$$(\varphi\cdot\varphi')\,(x\cdot y)=\varphi'\,(\varphi(x\cdot y))=\varphi'\,(\varphi x\cdot\varphi y)=\varphi'(\varphi x)\cdot\varphi'(\varphi y)=$$
$$=(\varphi\cdot\varphi')\,x\cdot(\varphi\cdot\varphi')\,y:$$

$\varphi : K \to K'$ օղակային հոմոմորֆիզմը կոչվում է **ներդրող հոմոմորֆիզմ** կամ օղակային **մոնոմորֆիզմ**, եթե φ արտապատկերումը նաև ներդրող (ինյեկտիվ) արտապատկերում է: Ակնհայտ է, որ երկու (հետևաբար և վերջավոր թվով) ներդրող օղակային հոմոմորֆիզմների արտադրյալը նորից ներդրող օղակային հոմոմորֆիզմ է:

$\varphi : K \to K'$ օղակային հոմոմորֆիզմը կոչվում է **վերադրող հոմոմորֆիզմ** կամ օղակային **էպիմորֆիզմ**, եթե φ արտապատկերումը նաև վերադրող (սյուրեկտիվ) արտապատկերում է: Ակնհայտ է, որ երկու (հետևաբար և վերջավոր թվով) վերադրող օղակային հոմոմորֆիզմների արտադրյալը նորից վերադրող օղակային հոմոմորֆիզմ է:

$\varphi : K \to K'$ օղակային հոմոմորֆիզմը կոչվում է օղակային **իզոմորֆիզմ**, **իզոմորֆություն**, **նույնաձևություն** կամ **իզոմորֆ արտապատկերում**, եթե φ արտապատկերումը նաև փոխմիարժեք (բիեկտիվ) արտապատկերում է: Ակնհայտ է, որ երկու (հետևաբար և վերջավոր թվով) օղակային նույնաձևությունների արտադրյալը նորից օղակային նույնաձևություն է և, եթե $\varphi : K \to K'$ արտապատկերումը օղակային նույնուձևություն է, ապա այդպիսին է նաև $\varphi^{-1} : K' \to K$ արտապատկերումը:

$\varphi : K \to K$ տեսքի օղակային նույնաձևությունը կոչվում է $K(+,\cdot)$ օղակի օղակային **ինքնաձևություն** կամ **ավտոմորֆիզմ**: Ակնհայտ է, որ միևնույն $K(+,\cdot)$ օղակի բոլոր օղակային ինքնաձևությունների բազմությունը խումբ է արտապատկերումների արտադրյալի նկատմամբ: Այդ խումբը նշանակվում է $Aut\,K$-ով:

Երկու $K(+,\cdot)$ և $K'(+,\cdot)$ օղակներ կոչվում են **նույնաձև** կամ **իզոմորֆ** և գրվում է $K \simeq K'$ կամ $K \cong K'$, եթե գոյություն ունի որևէ $\varphi : K \to K'$ օղակային նույնաձևություն: Սահմանված «$\simeq$» հարաբերությունը կոչվում է օղակների նույնաձևության կամ իզոմորֆության հարաբերություն:

Լեմմ 19.11: *Օղակների նույնաձևության «$\simeq$» հարաբերությունը բավարարում է համարժեքության հարաբերության սահմանման բոլոր երեք պայմաններին:* □

Օղակների տեսությունը կարելի է բնութագրել որպես գիտություն, որն ուսումնասիրում է օղակների և դրանց հոմոմորֆիզմների հանրահաշվական հատկությունները: Օղակների և դրանց միջև գործող արտապատկերումների հանրահաշվական հատկությունները սահմանվում են ճիշտ այնպես, ինչպես խմբերի դեպքում (տես 18.3 վերնագիրը):

Եթե $K(+,\cdot)$-ը կամայական օղակ է, իսկ $H \trianglelefteq K$, այսինքն՝ H-ը K օղակի իդեալն է, ապա

$$\pi(x) = x + H, \quad x \in K,$$

բանաձևով (արտապատկերումով) որոշվում է $\pi : K \to K/H$ օղակային հոմոմորֆիզմ՝ $K(+,\cdot)$ օղակից $K/H(+,\cdot)$ քանորդ-օղակի մեջ, որը կոչվում է **բնական** (կամ քանորդ-) օղակային հոմոմորֆիզմ: $\pi : K \to K/H$ բնական հոմոմորֆիզմը անհրաժեշտության դեպքում նշանակվում է նաև π_H-ով: Ակնհայտ է, որ բնական օղակային հոմոմորֆիզմը վերադրող օղակային հոմոմորֆիզմ (էպիմորֆիզմ) է:

Լեմմ 19.12*: Եթե $\varphi : K \to K'$ արտապատկերումը օղակային հոմոմորֆիզմ է $K(+,\cdot)$ օղակից $K'(+,\cdot)$ օղակի մեջ, ապա*

1) *$\varphi(0) = 0'$, որտեղ 0-ն և $0'$-ը K և K' օղակների զրոներն են;*

2) *$\varphi(-x) = -\varphi(x)$ ցանկացած $x \in K$ տարրի համար;*

3) *$\varphi(x_1 + x_2 + \cdots + x_n) = \varphi(x_1) + \varphi(x_2) + \cdots + \varphi(x_n)$ ցանկացած $n \in \mathbb{N}$ և ցանկացած $x_1, \ldots, x_n \in K$ տարրերի համար: Այնուհետև,*

$$\varphi(mx) = m\varphi(x)$$

ցանկացած $m \in \mathbb{Z}$ և ցանկացած $x \in K$ տարրերի համար;

4) *Եթե $H \leqslant K$, այսինքն՝ H-ը K օղակի ենթաօղակ է, ապա*

$$\varphi(H) = \{\varphi(h) \mid h \in H\} \leqslant K';$$

5) *Եթե $K(+,\cdot)$ օղակը օժտված է $e \in K$ միավորով, ապա $\varphi(e) \in K'$ տարրը կլինի $\varphi(K) \leqslant K'$ ենթաօղակի միավորը;*

6) *Եթե $K(+,\cdot)$ օղակը զուգորդական (տեղափոխական) է, ապա $\varphi(K) \leqslant K'$ ենթաօղակը ևս կլինի զուգորդական (տեղափոխական);*

7) *Եթե $K(+,\cdot)$ զուգորդական օղակը օժտված է միավորով և $a \in K$ տարրը հակադարձելի է, ապա ցանկացած $m \in \mathbb{Z}$ ամբողջ թվի համար՝*

$$\varphi\left(a^m\right) = (\varphi(a))^m\,;$$

8) *Եթե $H' \leqslant K'$, ապա*

$$\varphi^{-1}(H') = \{h \in K \mid \varphi(h) \in H'\} \leqslant K;$$

9) *Եթե $H \trianglelefteq K$, այսինքն՝ H-ը K օղակի իդեալ է, ապա $\varphi(H) \trianglelefteq \varphi(K)$;*

10) *Եթե $H' \trianglelefteq K'$, ապա $\varphi^{-1}(H') \trianglelefteq K$:*

Ապացուցում: Անմիջական ստուգման եղանակով: □

$\varphi : K \to K'$ օղակային հոմոմորֆիզմի **միջուկը** և **պատկերը**, ինչպես և խմբերի, գծային տարածությունների և գծային հանրահաշիվների դեպքում, նշանակվում են $Ker(\varphi)$-ով և $Im(\varphi)$-ով ու սահմանվում են հետևյալ կերպ՝

$$Ker(\varphi) = \{x \in K \mid \varphi(x) = 0'\},$$

$$Im(\varphi) = \{\varphi x \mid x \in K\} = \varphi(K);$$

$\varphi(K)$-ն կոչվում է նաև $K(+,\cdot)$ օղակի հոմոմորֆ պատկեր:

Լեմմ 19.13: *1) Օղակային հոմոմորֆիզմի միջուկը իդեալ է՝ $Ker(\varphi) \trianglelefteq K$: 2) Եվ հակառակը, յուրաքանչյուր $H \trianglelefteq K$ իդեալ հանդիսանում է որևէ $\varphi : K \to K'$ օղակային հոմոմորֆիզմի միջուկ:*

Ապացուցում: 1) $Ker(\varphi) \neq \emptyset$, որովհետև $0 \in Ker(\varphi)$: Եթե $x, y \in Ker\,\varphi$, ապա $x - y \in Ker\,\varphi$: Եթե $x \in Ker\,\varphi$ և $r \in K$, ապա $r \cdot x \in Ker\,\varphi$ և $x \cdot r \in Ker\,\varphi$:

2) Ընտրելով $K' = K/H$ և $\varphi = \pi_H : K \to K/H$ կունենանք՝

$$Ker\,(\varphi) = Ker\,(\pi_H) = H\,:$$ □

Թեորեմ 19.23 (Օղակային հոմոմորֆիզմների առաջին թեորեմը) : *Եթե $\varphi : K \to K'$ արտապատկերումը կամայական օղակային էպիմորֆիզմ է կամայական $K(+,\cdot)$ և $K'(+,\cdot)$ օղակների միջև, իսկ $Ker(\varphi) = H$, ապա $K' \simeq K/H$: Ավելի ճշգրիտ, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\mu : K' \to K/H$ օղակային իզոմորֆիզմ, որ տեղափոխական է օղակային հոմոմորֆիզմների հետևյալ եռանկյունը՝*

$$\begin{tikzcd} K \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & K' \arrow[d, "\mu"] \\ & K/H \end{tikzcd} \quad ,$$

այսինքն՝ $\pi = \varphi \cdot \mu$, որտեղ π-ն բնական օղակային հոմոմորֆիզմն է:

Ապացույց: Եթե սահմանափակվենք դիտարկվող երեք օղակների գումարային խմբերով, ապա համաձայն խմբային հոմոմորֆիզմների առաջին թեորեմի (թեորեմ 18.28), գոյություն կունենա այնպիսի $\mu : K' \to K/H$ խմբային իզոմորֆիզմ՝ $K'(+)$ խմբից $K/H(+)$ քանորդ-խմբի մեջ, որ $\varphi \cdot \mu = \pi$: Ըստ որում՝

$$\mu(x') = x + H \longleftrightarrow x' = \varphi x,$$

որտեղ $x' \in K'$, $x \in K$: Մնում է ապացուցել, որ μ խմբային իզոմորֆիզմը նաև օղակային իզոմորֆիզմ է, այսինքն՝

$$\mu\left(x' \cdot y'\right) = \mu(x') \cdot \mu(y'), \quad x', y' \in K' :$$

Դիցուք $x' = \varphi x$ և $y' = \varphi y$: Հետևաբար, $x' \cdot y' = \varphi x \cdot \varphi y = \varphi(x \cdot y)$ և $\mu\left(x' \cdot y'\right) = (x \cdot y) + H = (x + H)(y + H) = \mu(x') \cdot \mu(y')$: μ-ի միակությունն ակնհայտ է: $\square$

Թեորեմ 19.24 (օղակային հոմոմորֆիզմների երկրորդ թեորեմը): *Կամայական $\varphi_1 : K \to K'$ և $\varphi_2 : K \to K''$ օղակային էպիմորֆիզմների համար, որտեղ $Ker(\varphi_1) \subseteq Ker(\varphi_2)$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\varphi_3 : K' \to K''$ օղակային էպիմորֆիզմ, որ $\varphi_1 \cdot \varphi_3 = \varphi_2$, այսինքն՝ տեղափոխական է հոմոմորֆիզմների հետևյալ եռանկյունը.*

$$\begin{tikzcd} K \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & K' \arrow[d, "\varphi_3"] \\ & K'' \end{tikzcd} \quad :$$

Ըստ որում, φ_3-ը կլինի իզոմորֆիզմ այն և միայն այն դեպքում, երբ $Ker(\varphi_1) = Ker(\varphi_2)$:

Ապացուցում: Կրկնվում է խմբային հոմոմորֆիզմների երկրորդ թեորեմի ապացուցումը (կամ բխեցվում է այդ թեորեմից): □

Թեորեմ 19.25 (Օղակային իզոմոմորֆիզմների առաջին թեորեմը) : *Եթե $K(+,\cdot)$-ը կամայական օղակ է, $L \leqslant K$ և $H \trianglelefteq K$, ապա*

$$L + H = \{x + y \mid x \in L, y \in H\} \leqslant K,$$

$H \trianglelefteq L + H$, $L \cap H \trianglelefteq L$ և

$$L\big/L \cap H \simeq L + H\big/H$$

Ապացուցում: Առաջին երեք պնդումներն ակնհայտ են: Մնում է ապացուցել վերջին պնդումը՝ քանորդ-օղակների իզոմորֆիզմի վերաբերյալ: Եթե $z \in L + H$, ապա $z = x + y$, որտեղ $x \in L$, $y \in H$: Հետևաբար,

$$z + H = (x + y) + H = x + H, \quad x \in L:$$

Այժմ կառուցենք $f : L \to L + H\big/H$ օղակային էպիմորֆիզմը հետևյալ կերպ՝ $f(x) = x + H$, $x \in L$: Համաձայն օղակային հոմոմորֆիզմների առաջին թեորեմի՝

$$L + H\big/H \simeq L\big/Ker(f),$$

որտեղ $Ker(f) = L \cap H$: □

Թեորեմ 19.26 (Օղակային իզոմոմորֆիզմների երկրորդ թեորեմը) : *Եթե $K(+,\cdot)$-ը կամայական օղակ է, $L, H \trianglelefteq K$ և $H \subseteq L$, ապա $H \trianglelefteq L$, $L\big/H \trianglelefteq K\big/H$ և*

$$K/H\big/L/H \simeq K/L:$$

Ապացուցում: Նկատենք, որ $f(x+H) = x+L$, $x \in K$, օրենքով որոշվում է $f : K\big/H \to K\big/L$ օղակային էպիմորֆիզմ և, հետևաբար, համաձայն օղակային հոմոմորֆիզմների առաջին թեորեմի՝

$$K/L \simeq K/H\big/Ker(f),$$

որտեղ $Ker(f) = L\big/H$: □

19.7. Քելիի թեորեմը զուգորդական և միավորով օղակների համար

Կասենք, որ $K(+,\cdot)$ օղակը ներդրվում է $K'(+,\cdot)$ օղակում (կամ օղակի մեջ), եթե գոյություն ունի որևէ $\varphi : K \to K'$ օղակային մոնոմորֆիզմ: Նույնն է, թե գոյություն ունենա այնպիսի $H \leqslant K'$ ենթաօղակ, որ $K \simeq H$: Իրոք, նշանակելով $H = \varphi(K)$, կունենանք՝ $K \simeq H$:

Դիցուք $G(+)$-ը աբելյան խումբ է: $G(+)$ խմբի հոմոմորֆիզմն իր մեջ կոչվում է $G(+)$ խմբի էնդոմորֆիզմ: $G(+)$ խմբի բոլոր էնդոմորֆիզմների բազմությունը նշանակվում է $EndG(+)$-ով: Այս բազմությունը օղակ է հետևյալ գործողությունների նկատմամբ՝

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x),$$

$$(\varphi \cdot \psi)(x) = \psi(\varphi(x)),$$

որտեղ $x \in G$, $\varphi, \psi \in EndG(+)$: Ստացված $EndG(+)$ օղակը կլինի զուգորդական և միավորով օժտված և կոչվում է $G(+)$ աբելյան խմբի էնդոմորֆիզմների օղակ:

Թեորեմ 19.27 (Քելի): *Զուգորդական և միավորով օժտված յուրաքանչյուր $K(+,\cdot)$ օղակ ներդրվում է $EndK(+)$ օղակում:*

Ապացուցում: Դիցուք $a \in K$ և $T_a(x) = x \cdot a$, որտեղ $x \in K$: Կունենանք՝

$$T_a(x + y) = (x + y)a = xa + ya = T_a(x) + T_a(y),$$

այսինքն $T_a \in EndK(+)$: Սահմանենք $\Phi : K \to EndK(+)$ արտապատկերումը հետևյալ կերպ՝

$$\Phi(a) = T_a, \quad a \in K :$$

Կունենանք՝

$$T_{a+b}(x) = x(a + b) = xa + ab = T_a(x) + T_b(x) = (T_a + T_b)(x),$$
$$T_{a\cdot b}(x) = x(a \cdot b) = (xa) \cdot b = T_b(T_a(x)) = (T_a \cdot T_b)(x),$$

այսինքն՝

$$T_{a+b} = T_a + T_b\,,$$
$$T_{a\cdot b} = T_a \cdot T_b\ :$$

Այսպիսով,

$$\Phi(a+b) = T_{a+b} = T_a + T_b = \Phi(a) + \Phi(b)\,,$$
$$\Phi(a \cdot b) = T_{a \cdot b} = T_a \cdot T_b = \Phi(a) \cdot \Phi(b)\,,$$
$$\Phi(a) = \Phi(b) \to T_a = T_b \to T_a(x) = T_b(x) \to xa = xb \to a = b\,,$$

եթե $x = e$, որտեղ e-ն $K(+,\cdot)$ օղակի միավորն է: □

Նկատենք, որ եթե $K(+,\cdot)$ օղակը նաև տեղափոխական է և ինքնահամընկնող, այսինքն՝ $x \cdot x = x$ ցանկացած $x \in K$ տարրի համար, ապա ապացուցված թեորեմում կառուցված $T_a : K \to K$ արտապատկերումը դառնում է նաև $K(+,\cdot)$ օղակի հոմոմորֆիզմ իր մեջ, որովհետև

$$T_a(x \cdot y) = (x \cdot y)a = xyaa = (xa)(ya) = T_a(x) \cdot T_a(y)\ :$$

19.8. Պարզ և մաքսիմալ իդեալներ

$K(+,\cdot)$ օղակի $H \trianglelefteq K$ իդեալը կոչվում է **պարզ**, եթե ցանկացած $a, b \in K$ տարրերի համար տեղի ունի հետևյալ պայմանը՝

$$a \cdot b \in H \to a \in H \quad \text{կամ} \quad b \in H\ :$$

Այլ կերպ ասած, $H \trianglelefteq K$ իդեալը կոչվում է պարզ, եթե այն K օղակի երկու տարրերի արտադրյալի հետ մեկտեղ պարունակում է նաև դրանցից գոնե մեկը:

Յուրաքանչյուր օղակ ակներևորեն հանդիսանում է իր պարզ իդեալը: Որպեսզի տեղափոխական, զուգորդական և միավորով օժտված օղակը հանդիսանա ամբողջության տիրույթ անհրաժեշտ է և բավարար, որ նրա զրոյական իդեալը լինի պարզ իդեալ: Ավելի ճիշտ, որպեսզի օղակը չունենա զրոյի բաժանարարներ անհրաժեշտ է և բավարար, որ նրա զրոյական իդեալը լինի պարզ իդեալ:

Օղակի $H \trianglelefteq K$ իդեալը կոչվում է **ճշգրիտ**, եթե այն տարբեր է զրոյական և միավոր իդեալներից, այսինքն՝ $H \neq (0)$ և $H \neq K$:

Պնդում 19.1: *1) $\mathbb{Z}(+,\cdot)$ օղակի $H \trianglelefteq \mathbb{Z}$ ճշգրիտ իդեալը կլինի պարզ իդեալ այն և միայն այն դեպքում, երբ այն ծնվում է որևէ պարզ թվով: 2) Ընդհանրապես, գլխավոր իդեալներով օղակի (p) ճշգրիտ իդեալը կլինի պարզ այն և միայն այն դեպքում, երբ p-ն պարզ տարր է:*

Ապացուցում: 1) $\mathbb{Z}(+,\cdot)$ օղակի բոլոր իդեալները գլխավոր իդեալներ են: Եթե $H \trianglelefteq \mathbb{Z}$ իդեալը ծնվում է որևէ $p \in \mathbb{Z}$ պարզ թվով՝ $H = (p)$ և $a \cdot b \in H$, ապա $a \cdot b$-ն բաժանվում է p-ի վրա: Հետևաբար, կամ a-ն կբաժանվի p-ի վրա, կամ՝ b-ն: Առաջին դեպքում կունենանք $a \in (p) = H$, իսկ երկրորդ դեպքում՝ $b \in (p) = H$:

Եվ հակառակը, եթե $H = (m)$ և H-ը ճշգրիտ իդեալ է, ապա $m \neq 0, 1$, այսինքն՝ $m > 1$: Եթե m-ը բաղադրյալ թիվ է, այսինքն՝ $m = s \cdot t$, որտեղ $1 < s < m$, $1 < t < m$, ապա $s \cdot t \in (m)$, որտեղ s-ը և t-ն չեն բաժանվում m-ի վրա, այսինքն՝ $s \notin (m)$ և $t \notin (m)$:

2)-ի ապացուցումը 1)-ի դատողությունների կրկնությունն է: □

Թեորեմ 19.28: *Տեղափոխական, զուգորդական և միավորով օժտված $K(+,\cdot)$ օղակի $H \trianglelefteq K$ իդեալը կլինի պարզ իդեալ այն և միայն այն դեպքում, երբ K/H քանորդ-օղակը ամբողջության տիրույթ է:*

Ապացուցում: Նախ ենթադրենք, թե $H \trianglelefteq K$ իդեալը պարզ է և K/H քանորդ-օղակում տեղի ունի հետևյալ հավասարությունը՝

$$(x + H)(y + H) = H, \quad x, y \in K,$$

որտեղ H-ը K/H քանորդ-օղակի զրոն է: Ուստի $xy + H = H$, հետևաբար, $xy \in H$, որտեղից $x \in H$ կամ $y \in H$: Առաջին դեպքում կունենանք $x + H = H$, իսկ երկրորդ դեպքում՝ $y + H = H$: Այսպիսով K/H քանորդ-օղակը չունի զրոյի բաժանարարներ:

Եվ հակառակը, եթե K/H քանորդ-օղակը ամբողջության տիրույթ է և $x \cdot y \in H$, ապա

$$xy + H = H,$$

$$(x + H)(y + H) = H,$$

որտեղից $x + H = H$ կամ $y + H = H$: Առաջին դեպքում կունենանք $x \in H$, իսկ երկրորդ դեպքում՝ $y \in H$: □

Սովորաբար, եթե $H \trianglelefteq K$ և $H \neq K$, ապա գրվում է $H \triangleleft K$: $K(+,\cdot)$ օղակի $H \trianglelefteq K$ իդեալը կոչվում է **մաքսիմալ**, եթե $H \triangleleft K$ և գոյություն չունի K օղակի այնպիսի $H' \triangleleft K$ իդեալ, որ $H \triangleleft H'$, այսինքն՝ $H \neq K$ իդեալը հնարավոր չէ ընդգրկել իրենից և ամբողջ օղակից տարբեր որևէ այլ իդեալի մեջ:

Պնդում 19.2: *Որպեսզի տեղափոխական, զուգորդական և միավորով օժտված օղակը լինի դաշտ անհրաժեշտ է և բավարար, որ նրա զրոյական իդեալը լինի մաքսիմալ:*

Ապացուցում: Անհրաժեշտությունը բխում է այն փաստից, որ դաշտը չի օժտված ճշգրիտ իդեալներով: Ապացուցենք բավարարությունը: Դիցուք դիտարկվող $K(+,\cdot)$ օղակի զրոյական իդեալը մաքսիմալ է: Ուստի, այդ օղակը կլինի ոչ զրոյական (և, մասնավորապես, օղակի e միավորը կլինի ոչ զրոյական՝ $e \neq 0$): Այնուհետև, յուրաքանչյուր ոչ զրոյական $a \in K$ տարրի համար $a \in (a)$ և $(a) \neq (0)$: Հետևաբար, $(a) = K$ և $a \cdot x = e$ հավասարումն օժտված է լուծումով: □

Լեմմ 19.14 (հիմնական): *Որպեսզի զուգորդական, տեղափոխական և e միավորով օժտված $K(+,\cdot)$ օղակի $H \neq K$ իդեալը լինի մաքսիմալ անհրաժեշտ է և բավարար, որ յուրաքանչյուր $r \in K \setminus H$ տարրի համար գոյություն ունենա այնպիսի $x \in K$ տարր, որ $e - rx \in H$:*

Ապացուցում: Անհրաժեշտություն: Ենթադրենք թե $H \trianglelefteq K$, $H \neq K$ իդեալը մաքսիմալ է և $r \in K \setminus H$: Քանի որ $H \triangleleft H' = (r) + H$, ապա $(r) + H = K$ և հետևաբար գոյություն կունենա այնպիսի $x \in K$ տարր, որ $rx + \delta = e$, որտեղ $\delta \in H$: Ուստի $e - rx \in H$:
Բավարարություն: Եթե $H \neq K$ և $H \triangleleft H^* \trianglelefteq K$, ապա որևէ $r_0 \in H^* \setminus H$ տարրի համար սահմանենք $H' = (r_0) + H$ իդեալը: Ըստ լեմմի պայմանի, գոյություն կունենա այնպիսի $x_0 \in K$ տարր, որ $e - r_0 x_0 \in H$, այսինքն՝

$$e = r_0 x_0 + \delta_0, \quad \delta_0 \in H,$$

որտեղից $e \in H'$ և հետևաբար՝ $H' = K$: Միաժամանակ, շնորհիվ $H' \subseteq H^* \subseteq K$ ներդրումների, կունենանք նաև $H^* = K$ հավասարությունը: Այսպիսով H-ը մաքսիմալ իդեալ է: □

Թեորեմ 19.29: *Զուգորդական, տեղափոխական և միավորով օժտված $K(+,\cdot)$ օղակի H իդեալը կլինի մաքսիմալ այն և միայն այն դեպքում, երբ K/H քանորդ-օղակը դաշտ է:*

Ապացուցում: Եթե K/H քանորդ-օղակը դաշտ է, ապա այն կլինի ոչ զրոյական և հետևաբար $H \neq K$: Կամայական $r \in K \setminus H$ տարրի համար գոյություն կունենա այնպիսի $x \in K$ տարր, որ

$$(r + H)(x + H) = e + H,$$

$$rx + H = e + H,$$

որտեղից $e - rx \in H$ և ըստ նախորդ լեմմի $H \triangleleft K$ իդեալը կլինի մաքսիմալ:

Եվ հակառակը, եթե $H \triangleleft K$ իդեալը մաքսիմալ է և $r + H \in K/H$ տարրը ոչ զրոյական է, այսինքն՝ $r + H \neq H$, ապա $r \in K \setminus H$ և, նախորդ լեմմի համաձայն, գոյություն կունենա այնպիսի $x \in K$ տարր, որ $e - rx \in H$, որտեղից

$$rx + H = e + H,$$

$$(r + H)(x + H) = e + H :$$

Այսպիսով, զուգորդական, տեղափոխական և միավորով օժտված K/H քանորդ-օղակի յուրաքանչյուր ոչ զրոյական տարր հակադարձելի է: Հետևաբար, այն դաշտ է: □

Հետևություն 19.8: *Զուգորդական, տեղափոխական և միավորով օժտված օղակի մաքսիմալ իդեալները պարզ իդեալներ են:* □

Նույնիսկ ամբողջության տիրույթներում գոյություն ունեն այնպիսի $H \neq K$ պարզ իդեալներ, որոնք մաքսիմալ չեն: Օրինակ, բոլոր ամբողջ թվերի $\mathbb{Z}(+, \cdot)$ օղակում $H = (0)$ զրոյական իդեալը պարզ է, բայց մաքսիմալ չէ:

Այս տեսակետից հետաքրքրական է հետևյալ արդյունքը:

Թեորեմ 19.30: *Գլխավոր իդեալներով օղակի յուրաքանչյուր ճշգրիտ պարզ իդեալ մաքսիմալ իդեալ է:*

Ապացույցում: Համաձայն պնդում 19.1-ի, $K(+, \cdot)$ գլխավոր իդեալներով օղակի յուրաքանչյուր ճշգրիտ $H = (c)$ պարզ իդեալի դեպքում՝ c-ն պարզ տարր է: Այնուհետև, եթե $(c) \trianglelefteq H' \trianglelefteq K$, ապա $H' = (a)$ որևէ $a \in K$ տարրի համար, որովհետև $K(+, \cdot)$-ը գլխավոր իդեալներով օղակ է: Հետևաբար, $c \in (a)$ և $c = a \cdot x$, որտեղ $x \in K$: Ուստի, կամ a-ն է հակադարձելի, կամ՝ x-ը: Առաջին դեպքում՝ $H' = K$, իսկ երկրորդ դեպքում՝ $a = c \cdot x^{-1}$ և $H' = (c)$, այսինքն՝ $H = (c) \trianglelefteq K$ իդեալը մաքսիմալ է: □

Օրինակ: Եթե $F(+, \cdot)$-ը դաշտ է, իսկ $f \in F[x]$ բազմանդամը չբերվող է F-ում, ապա $F[x]/(f)$ քանորդ-օղակը դաշտ է և այդ դաշտը համընկնում է F-ի մնացքների դաշտի հետ՝ ըստ f չբերվող բազմանդամի (թեորեմ 16.23):

$K(+,\cdot)$ օղակը կոչվում է բուլյան օղակ (G. Boole), եթե այն զուգորդական է, տեղափոխական, օժտված e միավորով և $x\cdot x=x$ ցանկացած $x\in Q$ տարրի համար:

Հատկություն 19.8: *Կամայական $K(+,\cdot)$ բուլյան օղակի յուրաքանչյուր $H\neq K$ պարզ իդեալ մաքսիմալ է:*

Ապացուցում: Դիցուք $H\neq K$ և $r\in K\setminus H$: Քանի որ

$$r(e-r)=r-r^2=r-r=0\in H$$

և $H\trianglelefteq K$ իդեալը պարզ է, ապա $e-r\in H$: Ուստի, ցանկացած $r\in K\setminus H$ տարրի համար գոյություն ունի այնպիսի $x\in K$ տարր $(x=e)$, որ $e-rx\in H$: Մնում է օգտվել լեմմ 19.14 -ից: □

Օգտվելով Ցոռնի աքսիոմից, կարելի է ապացուցել, որ միավորով օժտված յուրաքանչյուր օղակ օժտված է մաքսիմալ իդեալով: Ավելի ճիշտ տեղի ունի հետևյալ արդյունքը:

Թեորեմ 19.31: *Միավորով օժտված յուրաքանչյուր $K(+,\cdot)$ օղակի ամեն մի $H\neq K$ իդեալ ընկած է որևէ մաքսիմալ իդեալում, այսինքն՝ գոյություն ունի այնպիսի $H'\vartriangleleft K$ մաքսիմալ իդեալ, որ $H\subseteq H'$:*

Ապացուցում: M_H-ով նշանակենք $K(+,\cdot)$ օղակի K-ից տարբեր բոլոր այն իդեալների բազմությունը, որոնցից յուրաքանչյուրը պարունակում է H-ը: Քանի որ $H\in M_H$, ապա $M_H\neq\emptyset$: M_H-ը մասնակի կարգավորված բազմություն է՝ ըստ «$\subseteq$» մասնակի կարգի: Դժվար չէ նկատել, որ M_H մասնակի կարգավորված բազմության մեջ յուրաքանչյուր $\{H_i\}_{i\in I}$ գծային կարգավորված ենթաբազմություն (շղթա) օժտված է վերին եզրով: Իրոք, եթե կամայական $r,s\in I$ տարրերի համար, կամ $H_r\subseteq H_s$ կամ $H_s\subseteq H_r$, ապա

$$S=\bigcup_{i\in I}H_i$$

տեսա-բազմային միավորումը կլինի K օղակի իդեալ: Ընդսմին $S\neq K$, որովհետև եթե $S=K$, ապա $K(+,\cdot)$ օղակի $e\in K$ միավորը կպարունակվեր որևէ H_{i_0} իդեալի մեջ, որտեղ $i_0\in I$, և հետևաբար, $H_{i_0}=K$, որը հակասում է նրա ընտրությանը: Այսպիսով, $S\in M_H$, որովհետև $H\subseteq S$ և $S\neq K$: Միաժամանակ, S-ը $\{H\}_{i\in I}$ համակարգի (շղթայի) վերին եզրն է, այսինքն՝ $H_i\subseteq S$ յուրաքանչյուր $i\in I$ նշիչի համար: Մնում է օգտվել Ցոռնի աքսիոմից, համաձայն որի M_H մասնակի կարգավորված բազմությունն օժտված է $H' \in M_H$ մաքսիմալ տարրով, որը և կլինի $K(+,\cdot)$ օղակի այն H' մաքսիմալ իդեալը, որը պարունակում է H-ը: $\square$

Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ

1. Ապացուցել, որ չորս-տարրանի վերջավոր դաշտի գումարային խումբը միածին չէ:

2. Ապացուցել, որ $\mathbb{Z}_n(+,\cdot)$ օղակի հակադարձելի տարրերի $\mathbb{Z}_n^{\times}(\cdot)$ խումբը կլինի միածին, եթե $n \leqslant 7$ և չի լինի միածին, եթե $n = 8$:

3. Ապացուցել, որ $K(+,\cdot)$ ամբողջության տիրույթի $a, b \in K$ տարրերը կլինեն փոխադարձաբար պարզ այն և միայն այն դեպքում, երբ $K(+,\cdot)$ օղակի (a) և (b) գլխավոր իդեալները փոխադարձաբար պարզ են, այսինքն՝ $(a)+(b)=K$:

4. (Չինական թեորեմ): Ապացուցել, որ եթե $K(+,\cdot)$ ամբողջության տիրույթի $H_1, \ldots, H_n$ իդեալները զույգ առ զույգ փոխադարձաբար պարզ են, ապա կամայական $x_1, \ldots, x_n \in K$ տարրերի համար գոյություն ունի այնպիսի $x \in K$ տարր, որ
$$x \equiv x_1 (mod\, H_1),$$
$$\ldots \quad \ldots \quad \ldots \quad \ldots$$
$$x \equiv x_n (mod\, H_n):$$

5. Բնութագրել
$$\mathbb{Z}[i] = \{a + bi |\ a, b \in \mathbb{Z}\}$$
ամբողջության տիրույթի պարզ տարրերը: Ապացուցել, որ $\alpha \in \mathbb{Z}[i]$ տարրը կլինի պարզ այն և միայն այն դեպքում, երբ $Nr(\alpha) \in \mathbb{N}$ թիվը պարզ է կամ α-ն զուգորդված է $p = 4n + 3$ տեսքի $\mathbb{Z}$-ում պարզ որևէ ամբողջ թվի հետ:

6. Ապացուցել, որ կոմպլեքս թվերի

$$\mathbb{Z}\left[i\sqrt{3}\right] = \left\{x + iy\sqrt{3} | \, x, y \in \mathbb{Z}\right\}$$

օղակը ֆակտորիզացվող է, բայց ֆակտորիալ չէ: Նույն պնդումն ապացուցել կոմպլեքս թվերի $\mathbb{Z}\left[i\sqrt{5}\right]$ օղակի դեպքում:

7. Ապացուցել, որ կոմպլեքս թվերի

$$\mathcal{D}\left[i\sqrt{19}\right] = \left\{ \frac{x + iy\sqrt{19}}{2} \right| \left. x, y \in \mathbb{Z}, x \equiv y(mod\, 2) \right\}$$

օղակը գլխավոր իդեալներով օղակ է, բայց էվկլիդյան չէ:

8. Դիցուք $k \in \mathbb{Z}$ և k-ն չի բաժանվում որևէ պարզ թվի քառակուսու վրա և $\sqrt{k} = i\sqrt{|k|}$, եթե $k < 0$: Համաձայն հետևություն 3.3-ի, $\sqrt{k}$-ն իռացիոնալ թիվ է, եթե $k > 0$: Հետևաբար,

$$x + y\sqrt{k} = x' + y'\sqrt{k} \longleftrightarrow x = x', y = y',$$

որտեղ $x, x', y, y' \in \mathbb{Z}$: Ապացուցել, որ եթե $k \equiv 3(mod\, 4)$ կամ $k \equiv 2(mod\, 4)$, ապա

$$\mathbb{Z}\left[\sqrt{k}\right] = \left\{x + y\sqrt{k} \right| \left. x, y \in \mathbb{Z}\right\}$$

ամբողջության տիրույթը թվաբանական օղակ է:

9. Դիցուք $K(+, \cdot)$ ամբողջության տիրույթի համար գոյություն ունի այնպիսի $\rho : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերում, որ տեղի ունի հետևյալ պայմանը.

   Ցանկացած $a, b \in K$, $b \neq 0$ տարրերի համար գոյություն ունեն այնպիսի $q, r \in K$ տարրեր, որ

$$a = bq + r,$$

   որտեղ $r = 0$ կամ $\rho(r) < \rho(b)$: Ապացուցել, որ $K(+, \cdot)$ ամբողջության տիրույթը էվկլիդյան օղակ է, այսինքն՝ նրա համար գոյություն ունի որևէ էվկլիդյան նորմ:

10. Ապացուցել, որ յուրաքանչյուր էվկլիդյան օղակ օժտված է մինիմալ էվկլիդյան նորմով:

11. Ապացուցել, որ $P[x]$ բազմանդամների օղակի մինիմալ էվկլիդյան նորմը որոշվում է հետևյալ կերպ՝ $\delta_0(f) = deg(f)$, որտեղ $deg(f)$-ը $f \neq 0$ բազմանդամի աստիճանն է:

12. Ապացուցել, որ $\mathbb{Z}(+,\cdot)$ էվկլիդյան օղակի մինիմալ էվկլիդյան նորմը որոշվում է հետևյալ կերպ՝ $\delta_0(x) = [\log_2 |x|]$, որը համընկնում է 2-ական համակարգում $|x|$-ի ունեցած ներկայացման երկարության հետ:

13. Դիցուք $K(+,\cdot)$-ը ամբողջության տիրույթ է, $X_0 = \{0\}$ և ցանկացած $n \in \mathbb{N}$ բնական թվի համար՝

$$X_n = \{x \in K | \forall a \in K, \exists b \in K, a - bx \in X_{n-1} \cup X_0\} :$$

Ստանում ենք K բազմության ենթաբազմությունների հետևյալ

$$X_0, X_1, \ldots, X_n, \ldots$$

հաջորդականությունը, որի տարրերը կոչվում են $K(+,\cdot)$ օղակի X-բազմություններ: Ապացուցել X-բազմությունների հետևյալ հատկությունները.

1) X_1-ը համընկնում է $K(+,\cdot)$ օղակի հակադարձելի տարրերի բազմության հետ;
2) $X_n \subseteq X_{n+1}$, որտեղ $n = 1, 2, \ldots$;
3) Եթե որևէ k բնական թվի դեպքում $X_k = X_{k+1}$, ապա $X_{k+l} = X_k$ ցանկացած $l \geqslant 1$ բնական թվի համար;
4) Եթե $x \in X_k$, $k \geqslant 1$, ապա գոյություն ունի միարժեքորեն որոշվող այնպիսի $n \in \mathbb{N}$ բնական թիվ, որ $x \in X_n \setminus X_{n-1}$, որտեղ $n \leqslant k$;
5) Եթե $x \in X_{n+1} \setminus X_n$ և $xz \in X_{m+1} \setminus X_m$, որտեղ $n, m \in \mathbb{N}$, ապա $n \leqslant m$;
6) Եթե $x \in X_{n+1} \setminus X_n$, որտեղ $n \geqslant 1$, ապա $\varepsilon x \in X_{n+1} \setminus X_n$ օղակի ցանկացած ε հակադարձելի տարրի համար:

14. Ապացուցել, որ ամբողջ թվերի $\mathbb{Z}(+,\cdot)$ օղակի համար՝

$$X_n = \{\pm 1, \pm 2, \pm 3, \ldots, \pm (2^n - 1)\},$$

որտեղ $n \geqslant 1$: Հետևաբար, $x \in X_n \setminus X_{n-1} \leftrightarrow 2^{n-1} \leqslant |x| < 2^n$:

15. Ապացուցել, որ բազմանդամների $P[x]$ օղակի համար, որտեղ P-ն դաշտ է,

$$X_1 = P \setminus \{0\},$$

$$X_n = \{f \in P[x] |\, deg(f) \leqslant n-1\},$$

որտեղ $n \geqslant 2$: Հետևաբար, $f \in X_n \setminus X_{n-1} \leftrightarrow deg(f) = n-1$:

16. Ապացուցել, որ եթե ρ արտապատկերումը բավարարում է 9-րդ խնդրի պայմանին և $x \notin X_n \cup X_0$, ապա $\rho(x) \geqslant n$:

17. Ապացուցել, որ եթե $K(+,\cdot)$ ամբողջության տիրույթը բավարարում է 9-րդ խնդրի պայմանին, ապա ցանկացած $x \in K$, $x \neq 0$ տարրի համար գոյություն կունենա միարժեքորեն որոշվող այնպիսի n համար, որ $x \in X_n \setminus X_{n-1}$: Այս դեպքում, սահմանելով $\delta_0(x) = n-1$, ստանում ենք էվկլիդյան նորմի սահմանման E_1) և E_2) աքսիոմներին բավարարող ֆունկցիա: Ըստ որում, $\delta_0(x) \leqslant \rho(x)$, որտեղ ρ-ն 8-րդ խնդրի պայմանին բավարարող ցանկացած ֆունկցիա է: Մասնավորապես, $K(+,\cdot)$-ը կլինի էվկլիդյան օղակ, իսկ $\delta_0 : K \setminus \{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերումը կլինի նրա մինիմալ էվկլիդյան նորմը:

18. Ամբողջության տիրույթը կլինի էվկլիդյան օղակ այն և միայն այն դեպքում, երբ նրա յուրաքանչյուր տարր պատկանում է որևէ X-բազմության:

19. Ձևակերպել և ապացուցել Մյոբիուսի շրջման թեորեմը $K \setminus \{0\} \to Q$ տեսքի ֆունկցիաների համար, որտեղ $K(+,\cdot)$-ը ֆակտորիալ օղակ է, իսկ Q-ն միավորով օժտված զուգորդական և տեղափոխական օղակ է:

20. Դիցուք $Q(+,\cdot)$-ը օղակ է, իսկ τ-ն տոպոլոգիա է՝ որոշված Q-ի վրա: $Q(+,\cdot,\tau)$ քառյակը կոչվում է **տոպոլոգիական օղակ**, եթե

    ա) $Q(+,\tau)$ եռյակը տոպոլոգիական խումբ է, և

    բ) $(x,y) \to x \cdot y$ արտապատկերումը անընդհատ է, այսինքն՝ կամայական $x, y \in Q$ տարրերի և նրանց $x \cdot y$ արտադրյալի կամայական U շրջակայքի համար գոյություն ունեն x-ի և y-ի համապատասխանաբար այնպիսի V և W շրջակայքեր, որ $V \cdot W \subseteq U$:

Ապացուցել, որ $\mathbb{Z}(+,\cdot,\tau)$ քառյակը տոպոլոգիական օղակ է, որտեղ τ-ն $\mathbb{Z}$-ի մնացքային տոպոլոգիան է:

21. Դիցուք $Q(+,\cdot)$-ը օղակ է, իսկ «$\leqslant$» հարաբերությունը մասնակի կարգ է, որոշված Q-ի վրա: $Q(+,\cdot,\leqslant)$ քառյակը կոչվում է **մասնակի կարգավորված օղակ**, եթե տեղի ունեն հետևյալ պայմանները.

ա) $a \leqslant b \to a+c \leqslant b+c$, այսինքն՝ $Q(+,\leqslant)$ եռյակը մասնակի կարգավորված խումբ է,

բ) $a \leqslant b,\ 0 \leqslant c \to ac \leqslant bc,\ ca \leqslant cb$,

որտեղ $a,b,c \in Q$:

Օրինակ, $\mathbb{Z}(+,\cdot,\leqslant)$ քառյակը մասնակի կարգավորված օղակ է, որտեղ «$\leqslant$» հարաբերությունը ամբողջ թվերի բնական կարգն է:

$a \geqslant 0$ պայմանին բավարարող բոլոր տարրերի բազմությունը կոչվում է $Q(+,\cdot,\leqslant)$ մասնակի կարգավորված օղակի **դրական կոն**: Ապացուցել հետևյալ պնդումը.

Որպեսզի $P \subseteq Q$ ոչ դատարկ ենթաբազմությունը լինի որևէ $Q(+,\cdot,\leqslant)$ մասնակի կարգավորված օղակի դրական կոն անհրաժեշտ է և բավարար, որ $P(+,\cdot)$-ը լինի $P \cap (-P) = \{0\}$ պայմանին բավարարող կիսաօղակ:

22. $Q(+,\cdot,\leqslant)$ մասնակի կարգավորված օղակը կոչվում է **գծայնորեն կարգավորված օղակ**, եթե «$\leqslant$» մասնակի կարգը գծային կարգ է, այսինքն՝ ցանկացած $x,y \in Q$ տարրերի համար՝ կամ $x \leqslant y$ կամ $y \leqslant x$: Կասենք, որ $Q(+,\cdot)$ օղակը հնարավոր է գծայնորեն կարգավորել, եթե գոյություն ունի այնպիսի «$\leqslant$» գծային կարգ՝ որոշված Q-ի վրա, որ $Q(+,\cdot,\leqslant)$ քառյակը լինի գծայնորեն կարգավորված օղակ: Հակառակ դեպքում կասենք, որ $Q(+,\cdot)$ օղակը հնարավոր չէ գծայնորեն կարգավորել:

1) Ապացուցել, որ կոմպլեքս թվերի $\mathbb{C}(+,\cdot)$ դաշտը հնարավոր չէ գծայնորեն կարգավորել:

2) Ապացուցել, որ $Z_5(+,\cdot)$ դաշտը հնարավոր չէ գծայնորեն կարգավորել:

(Ցուցում. Երկու դաշտերում էլ գոյություն ունի այնպիսի ε տարր, որ $\varepsilon^2 = -1$: Սակայն գծայնորեն կարգավորված դաշտում՝ $t^2 > 0$, եթե $t \neq 0$: Հետևաբար, $\varepsilon^2 = -1 > 0$ և երկու մասերին գումարելով 1 կստանանք՝ $0 \geqslant 1$, այսինքն՝ $0 > 1$ և $1 = 1^2 > 0 > 1$: Հակասություն:)

23. Ձևակերպել և ապացուցել Մյոբիուսի շրջման թեորեմը մասնակի կարգավորված օղակների համար:

Գ լ ու խ 20

ԿԱՎԱՐՆԵՐ, ԲԱՇԽԱԿԱՆ ԵՎ ՄՈԴՈՒԼՅԱՐ (ԴԵԴԵԿԻՆԴՅԱՆ) ԿԱՎԱՐՆԵՐ, ԲՈՒԼՅԱՆ ԵՎ ԴԵ ՄՈՐԳԱՆԻ ՀԱՆՐԱՀԱՇԻՎՆԵՐ

20.1. Կավարի գաղափարը

Ինչպես նշել ենք, ոչ դատարկ բազմությունն իր մեջ սահմանված ցանկացած թվով գործողությունների հետ մեկտեղ կոչվում է հանրահաշիվ (կամ ունիվերսալ հանրահաշիվ):

Երկու երկտեղ գործողությամբ $Q(+,\cdot)$ հանրահաշիվը կոչվում է **կավար** (lattice, решётка), եթե նրա կամայական $x, y, z \in Q$ տարրերի համար`

$$x + x = x, \;\; x \cdot x = x, \;\; \text{(ինքնահամընկնման նույնություններ)}$$

$$x + y = y + x, \;\; x \cdot y = y \cdot x, \;\; \text{(տեղափոխական նույնություններ)}$$

$$(x{+}y){+}z = x{+}(y{+}z), \;\; (x{\cdot}y){\cdot}z = x{\cdot}(y{\cdot}z), \;\; \text{(զուգորդական նույնություններ)}$$

$$x(x + y) = x, \;\; x + xy = x : \;\; \text{(կլանման նույնություններ)}$$

Եթե $Q(+,\cdot)$-ը կավար է, ապա $+$ և $\cdot$ գործողությունները կոչվում են կավարային գործողություններ որոշված Q-ի վրա (մեջ): $Q(+,\cdot)$ կավարը համառոտ նշանակվում է նաև Q-ով:

Սևեռված թվով գործողություններ պարունակող հանրահաշիվների դասը կոչվում է **բազմաձևություն**, եթե այն որոշվում է նույնություններով (այսինքն` այդ դասը կազմված է բոլոր այն սևեռված թվով գործողություններ պարունակող հանրահաշիվներից, որոնք բավարարում են որոշ քանակի նույնությունների): Ուստի, բոլոր կավարների դասը բազմաձևություն է:

Հետևյալ արդյունքով ստեղծվում է բնական փոխմիարժեք համապատասխանություն բոլոր կավարների դասի և բոլոր կավարաձև կարգավորված բազմությունների դասի միջև:

Թեորեմ 20.1: *1) Եթե $Q(+,\cdot)$-ը կավար է և սահմանենք*

$$x \leqslant y \longleftrightarrow x + y = y,$$

ապա $Q(+,\cdot)^{\vee} = Q(\leqslant)$ *զույգը կլինի կավարաձև կարգավորված բազմություն, որտեղ*

$$\sup\{x,y\} = x + y,$$

$$\inf\{x,y\} = x \cdot y :$$

2) Եվ հակառակը, եթե $Q(\leqslant)$ *զույգը կավարաձև կարգավորված բազմություն է և սահմանենք*

$$x + y = \sup\{x,y\},$$

$$x \cdot y = \inf\{x,y\},$$

ապա $Q(\leqslant)^{\wedge} = Q(+,\cdot)$*-ը կլինի կավար:*

3) $(Q(+,\cdot)^{\vee})^{\wedge} = Q(+,\cdot)$ *և* $(Q(\leqslant)^{\wedge})^{\vee} = Q(\leqslant)$*:*

Ապացուցում: 1) Նախ նկատենք, որ $Q(\leqslant)$ զույգը մասնակի կարգավորված բազմություն է, այսինքն՝

ա) $x \leqslant x$,

բ) $x \leqslant y,\ y \leqslant x \longrightarrow x = y$,

գ) $x \leqslant y,\ y \leqslant z \longrightarrow x \leqslant z$;

Իրոք, ա) պայմանը բխում է $x + x = x$ նույնությունից, բ) պայմանը՝ գումարման տեղափոխականությունից, իսկ գ) պայմանը՝ նրա զուգորդականությունից:

Այժմ ապացուցենք, որ $Q(\leqslant)$ զույգը կավարաձև կարգավորված բազմություն է, այսինքն՝ Q-ում գոյություն ունեն $\sup\{a,b\}$-ն և $\inf\{a,b\}$-ն՝ բոլոր $a,b \in Q$ տարրերի համար: Ավելի ճիշտ, ապացուցենք

$$\sup\{a,b\} = a + b$$

և

$$\inf\{a,b\} = a \cdot b$$

հավասարությունները: Նախ ապացուցենք առաջին հավասարությունը:

$$a + (a + b) = a + b \longrightarrow a \leqslant a + b,$$

$$b + (a + b) = a + b \longrightarrow b \leqslant a + b,$$

այսինքն՝ $a + b$ տարրը $\{a,b\}$ ենթաբազմության համար վերին եզր է:

$$a \leqslant c,\ b \leqslant c \longrightarrow a + c = c,\ b + c = c \longrightarrow (a + b) + c = c \longrightarrow a + b \leqslant c,$$

այսինքն՝ $a+b$-ն $\{a,b\}$ ենթաբազմության վերին ճշգրիտ եզրն է:

Այժմ ապացուցենք երկրորդ հավասարությունը:

$$ab+a=a\longrightarrow ab\leqslant a,$$

$$ab+b=b\longrightarrow ab\leqslant b,$$

այսինքն՝ ab-ն $\{a,b\}$ ենթաբազմության համար ստորին եզր է: Մնում է ապացուցել, որ ab-ն $\{a,b\}$ ենթաբազմության ստորին ճշգրիտ եզրն է՝

$$c\leqslant a,\ c\leqslant b\longrightarrow c\leqslant ab:$$

Իրոք,

$$c\leqslant a,\ c\leqslant b\longrightarrow c+a=a,\ c+b=b\longrightarrow c+ab=$$
$$=c(c+b)+ab=cb+ab=c(c+a)b+ab=c(ab)+ab=ab\longrightarrow c\leqslant ab:$$

2) պնդումը նույնպես ապացուցվում է անմիջական ստուգման եղանակով: Իրոք, սահմանվող $+$ և $\cdot$ գործողությունների ինքնահամընկնման և տեղափոխական նույնություններն ակնհայտ են: Ապացուցենք, օրինակ, $+$ գործողության զուգորդականությունը:

$$\begin{aligned}&(x+y)+z\geqslant x+y\geqslant x,\\&(x+y)+z\geqslant x+y\geqslant y,\\&(x+y)+z\geqslant z:\end{aligned}$$

Հետևաբար, $(x+y)+z\geqslant y+z$ և $(x+y)+z\geqslant x+(y+z)$: Նույն դատողություններով ստացվում է նաև հակառակ անհավասարությունը՝ $x+(y+z)\geqslant(x+y)+z$: Մնում է օգտվել մասնակի կարգի հակահամաչափությունից:

Այնուհետև, $x(x+y)=\inf\{x,x+y\}\leqslant x$: Միաժամանակ, $x\leqslant x$, $x\leqslant\sup\{x,y\}=x+y$: Հետևաբար, $x\leqslant\inf\{x,x+y\}=x(x+y)$ և $x(x+y)=x$, այսինքն՝ տեղի ունի առաջին կլանման նույնությունը: Նման դատողություններով ապացուցվում է նաև երկրորդ կլանման նույնությունը:

3) պնդումն ակնհայտորեն բխում է սահմանումներից: □

$Q(+,\cdot)$ **կավարի գրաֆ** ասելով հասկացվում է համապատասխան $Q^{\vee}=Q(\leqslant)$ կավարածև կարգավորված բազմության գրաֆը: Այսպիսով, կավարները պատկերվում են գրաֆների տեսքով:

Ակնհայտ է, որ եթե $Q(\leqslant)$ զույգը կավարածև կարգավորված բազմություն է, ապա $Q(\leqslant^{-1})$ զույգը ևս կլինի կավարածև կարգավորված բազմություն:

Հետևություն 20.1*: 1) Եթե $Q(\leqslant)^\wedge = Q(+,\cdot)$, ապա $Q(\leqslant^{-1})^\wedge = Q(\cdot,+)$; 2) եթե $Q(+,\cdot)^\vee = Q(\leqslant)$, ապա $Q(\cdot,+)^\vee = Q(\leqslant^{-1})$:* $\square$

$Q(+,\cdot)^\vee$ և $Q(\leqslant)^\wedge$ նշանակումների փոխարեն երբեմն կօգտագործենք $Q^\vee$ և $Q^\wedge$ համառոտ նշանակումները:

Հետևություն 20.2*: Դիցուք $Q(\leqslant)$ զույգը կավարածև կարգավորված բազմություն է, իսկ $Q(+,\cdot)$-ը դրա համապատասխան կավարն է: Եթե $a \leqslant c$ և $b \leqslant d$, ապա $a+b \leqslant c+d$ և $ab \leqslant cd$:*

Ապացուցում: Ըստ սահմանման, $a+c = \sup\{a,c\} = c$, $a\cdot c = \inf\{a,c\} = a$, $b+d = \sup\{b,d\} = d$, $b\cdot d = \inf\{b,d\} = b$: Հետևաբար,

$$(a+b)+(c+d) = (a+c)+(b+d) = c+d,$$

$$(ab)(cd) = (ac)(bd) = ab$$

և $a+b \leqslant c+d$, $ab \leqslant cd$: $\square$

Լեմմ 20.1*: Ցանկացած $Q(+,\cdot)$ կավարում տեղի ունեն հետևյալ նույնությունները՝*

$$(xy+z)(y+z) = xy+z,$$

$$(x+y)z+yz = (x+y)z :$$

Ապացուցում: Ապացուցենք, օրինակ, առաջին հավասարությունը ցանկացած $x,y,z \in Q$ տարրերի համար: Քանի որ $a\cdot b = \inf\{a,b\} \leqslant a$, ապա

$$(xy+z)(y+z) \leqslant xy+z :$$

Առինքնության համաձայն՝ $xy+z \leqslant xy+z$, իսկ նախորդ հետևության համաձայն $xy+z \leqslant y+z$: Հետևաբար, $xy+z \leqslant (xy+z)(y+z)$: Մնում է կիրառել «$\leqslant$» մասնակի կարգի հակասիմետրիկության պայմանը: $\square$

Հետևություն 20.3: *Կամայական $Q(+,\cdot)$ կավարում տեղի ունի*

$$X(Y(X(x,y),z),Y(y,z)) = Y(X(x,y),z)$$

հավասարությունը ցանկացած $x,y,z \in Q$ տարրերի և ցանկացած $X,Y \in \{+,\cdot\}$ գործողությունների համար:

Ապացույց: Անմիջական ստուգման եղանակով, երբ $(X,Y)=(+,\cdot)$, $(X,Y)=(\cdot,+)$, $(X,Y)=(+,+)$, $(X,Y)=(\cdot,\cdot)$: $\square$

Այսպիսի հավասարությունները կոչվում են **գերնույնություններ**, որտեղ փոքրատառերը կոչվում են **առարկայական** փոփոխականներ, իսկ մեծատառերը՝ **ֆունկցիոնալ** փոփոխականներ: Այսպիսով, գերնույնությունները առարկայական և ֆունկցիոնալ փոփոխականներ պարունակող հավասարություններ են, ի տարբերություն (սովորական) նույնությունների, որոնք պարունակում են միայն առարկայական փոփոխականներ և տրված գործողությունների նշաններ:

Օրինակներ: Խմբի բոլոր (ինվարիանտ) ենթախմբերի դասը կավար է, որտեղ երկու (ինվարիանտ) ենթախմբերի արտադրյալ ասելով հասկացվում է դրանց հատումը, իսկ երկու (ինվարիանտ) ենթախմբերի գումար ասելով հասկացվում է այն ամենափոքր (ինվարիանտ) ենթախումբը, որը պարունակում է տրված երկու (ինվարիանտ) ենթախմբերին (այսինքն՝ երկու (ինվարիանտ) ենթախմբերի գումարը կլինի հավասար դրանց պարունակող բոլոր (ինվարիանտ) ենթախմբերի հատմանը): Նման եղանակով սահմանվում է օղակի բոլոր ենթաօղակների (իդեալների) կավարը: Բոլոր բնական թվերի $\mathbb{N}$ բազմությունը բնական թվերի սովորական գումարման և բազմապատկման գործողությունների նկատմամբ կիսաօղակ է, բայց կավար չէ: Սակայն, եթե երկու $x,y\in\mathbb{N}$ բնական թվերի գումար և արտադրյալ ասելով հասկանանք $\max\{x,y\}$-ը և $\min\{x,y\}$-ը, ապա կստանանք կավար: Մենք, ըստ էության, ծանոթ ենք $\mathbb{N}$ բազմությունը կավարի վերածելու մեկ այլ բնական եղանակի հետ ևս, որտեղ որպես կավարային գործողություններ վերցվում են երկու բնական թվերի ամենափոքր ընդհանուր բազմապատիկը և ամենամեծ ընդհանուր բաժանարարը: Համապատասխան կավարաձև կարգավորված բազմության մասնակի կարգը կլինի բաժանման հարաբերությունը: Կավարի այս երկու օրինակները բավարարում են նաև $+$ և $\cdot$ գործողությունների բաշխականության պայմանին (թեորեմ 6.5):

20.2. Մոդուլյար (Դեդեկինդյան) կավարներ

Դիցուք $Q(+,\cdot)$-ը կավար է, իսկ $Q(\leqslant)$ զույգը դրա համապատասխան կավարաձև կարգավորված բազմությունն է (թեորեմ 20.1):

$Q(+,\cdot)$ կավարը կոչվում է **մոդուլյար** կամ **դեդեկինդյան**, եթե տեղի ունի հետևյալ պայմանը՝

$$x \leqslant z \longrightarrow (x+y)z = x + yz$$

որտեղ $x, y, z \in Q$: $Q(\leqslant)$ կավարաձև կարգավորված բազմությունը կոչվում է **մոդուլյար** կամ **դեդեկինդյան**, եթե համապատասխան $Q^{\wedge} = Q(+,\cdot)$ կավարը մոդուլյար է: Նշված պայմանը կոչվում է մոդուլյարության պայման և այն կարելի նաև գրել հետևյալ կերպ՝

$$x \cdot z = x \longrightarrow (x+y)z = x + yz,$$

կամ

$$x + z = z \longrightarrow (x+y)z = x + yz,$$

որտեղ $x, y, z \in Q$: Այսպիսի պայմանները կոչվում են նաև քվազինույնություններ, իսկ քվազինույնություններով որոշվող և սևեռված թվով գործողություններ պարունակող հանրահաշիվների դասը կոչվում է **քվազիբազմաձևություն**: Ուստի, բոլոր մոդուլյար կավարների դասը քվազիբազմաձևություն է:

Օրինակ, գծային տարածության բոլոր ենթատարածությունների դասը մոդուլյար կավար է, որտեղ երկու ենթատարածությունների արտադրյալ ասելով հասկացվում է դրանց հատումը, իսկ երկու ենթատարածությունների գումար ասելով պետք է հասկանալ գծային հանրահաշվում սահմանվող դրանց գումարը: Աբելյան խմբի բոլոր ենթախմբերի կավարը մոդուլյար է:

Մոդուլյար կավարի կարևոր օրինակ է խմբի բոլոր ինվարիանտ ենթախմբերի կավարը (Ռ. Դեդեկինդ, 1900թ.), որտեղ երկու ինվարիանտ ենթախմբերի արտադրյալ ասելով հասկացվում է դրանց հատումը, իսկ երկու ինվարիանտ ենթախմբերի գումար ասելով հասկացվում է այն ամենափոքր ինվարիանտ ենթախումբը, որը պարունակում է տրված երկու ինվարիանտ ենթախմբերին: Այլ կերպ ասած, եթե $G(*)$-ը կամայական խումբ է, ապա տեղի ունի հետևյալ հավասարությունը՝

$$(X * Y) \cap Z = X * (Y \cap Z),$$

որտեղ X, Y, Z-ը $G(*)$ խմբի ցանկացած ինվարիանտ ենթախմբեր են, $X \subseteq Z$, իսկ $X * Y = \{x * y \,|\, x \in X,\, y \in Y\} = \sup\{X, Y\}$ (հատկություն 18.21):

Լեմմ 20.2: *Որպեսզի $Q(+,\cdot)$ կավարը լինի մոդուլյար անհրաժեշտ է և բավարար, որ*

$$x(xy+z) = xy + xz$$

ցանկացած $x, y, z \in Q$ տարրերի համար: Հետևաբար, բոլոր մոդուլյար կավարների դասը բազմաձևություն է:

Ապացուցում: Անհրաժեշտություն: Եթե $Q(+,\cdot)$ կավարը մոդուլյար է, ապա հաշվի առնելով $xy \leqslant x$ առնչությունը, կունենանք՝

$$x(xy+z) = (xy+z)x = xy + zx = xy + xz :$$

Բավարարություն: Ելնելով տրված նույնությունից հաշվենք $(a+b)c$-ն, որտեղ $a \leqslant c$, այսինքն՝ երբ $ac = a$.

$$(a+b)c = (ac+b)c = c(ca+b) = ca + cb = a + bc : \qquad \square$$

Լեմմ 20.3: *Որպեսզի $Q(+,\cdot)$ կավարը լինի մոդուլյար անհրաժեշտ է և բավարար, որ*

$$(x+yz)(y+z) = x(y+z) + yz$$

ցանկացած $x, y, z \in Q$ տարրերի համար:

Ապացուցում: Դիցուք $Q(+,\cdot)$ կավարը մոդուլյար է: Քանի որ համապատասխան կավարաձև կարգավորված բազմություն մեջ‘ $yz \leqslant y+z$, ապա

$$(x+yz)(y+z) = (yz+x)(y+z) = yz + x(y+z) :$$

Եվ հակառակը, եթե $Q(+,\cdot)$ կավարը բավարարում է նշված նույնությանը և $y \leqslant z$, ապա $yz = y$, $y+z = z$ և

$$(y+x)z = (x+yz)(y+z) = x(y+z) + yz = xz + y = y + xz : \qquad \square$$

Հետևություն 20.4: *Եթե $Q(\leqslant)$ կավարաձև կարգավորված բազմությունը մոդուլյար է , ապա $Q(\leqslant^{-1})$ կավարաձև կարգավորված բազմությունը ևս կլինի մոդուլյար:*

Ապացուցում: Եթե լեմմ 20.3-ում նշված նույնության մեջ $+$-ը փոխարինենք $\cdot$ -ով, իսկ $\cdot$ -ը՝ $+$-ով, ապա կստանանք նույն նույնությունը:
$\square$

Հետևություն 20.5: *Կամայական $Q(+,\cdot)$ մոդուլյար կավարում տեղի ունեն*

$$X(Y(x,X(y,z)),Y(y,z)) = Y(X(x,Y(y,z)),X(y,z)),$$

$$X(x,Y(X(x,y),z)) = Y(X(x,y),X(x,z))$$

հավասարությունները ցանկացած $x,y,z \in Q$ տարրերի և ցանկացած $X,Y \in \{+,\cdot\}$ գործողությունների համար: Այսինքն՝ կամայական $Q(+,\cdot)$ մոդուլյար կավարում տեղի ունեն նշված զերնույնությունները:

Ապացուցում: Անմիջական ստուգման եղանակով, երբ $(X,Y) = (+,\cdot)$, $(X,Y) = (\cdot,+)$, $(X,Y) = (+,+)$, $(X,Y) = (\cdot,\cdot)$: □

$Q(+,\cdot)$ կավարի ոչ դատարկ $Q' \subseteq Q$ ենթաբազմությունը կոչվում է $Q(+,\cdot)$-ի ենթակավար և նշանակվում է $Q' \leqslant Q$, եթե Q'-ը փակ է $+$ և $\cdot$ գործողությունների նկատմամբ, այսինքն՝

$$x,y \in Q' \longrightarrow x+y \in Q',$$

$$x,y \in Q' \longrightarrow x\cdot y \in Q' :$$

Ակնհայտ է, որ կավարի ենթակավարը կլինի կավար նույն գործողությունների նկատմամբ, իսկ մոդուլյար կավարի ենթակավարը կլինի մոդուլյար կավար:

Ապացուցենք կավարի մոդուլյարության Դեդեկինդի հետևյալ հայտանիշը:

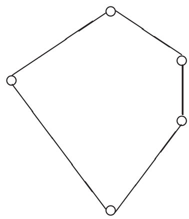
Թեորեմ 20.2 (Ռ. Դեդեկինդ) : *Որպեսզի կավարը լինի մոդուլյար անհրաժեշտ է և բավարար, որ այն օժտված չլինի նկ. 1 տեսքի ենթակավարով:*

Ապացուցում: Նախ նկատենք, որ եթե $Q(+,\cdot)$ կավարը մոդուլյար է, ապա այն չի կարող ունենալ նկ. 1-ում պատկերված տեսքի ենթակավար, որովհետև նկ. 1-ում պատկերված կավարը մոդուլյար չէ:

Եվ հակառակը, եթե $Q(+,\cdot)$ կավարը մոդուլյար չէ, ապա այն կունենա նկ. 1-ում պատկերված տեսքի ենթակավար: Իրոք, եթե $Q(+,\cdot)$ կավարը մոդուլյար չէ, ապա գոյություն կունենան այնպիսի $x,y,z \in Q$ տարրեր, որ $x \leqslant z$, բայց $(x+y)z \neq x+yz$: Սակայն $x+yz \leqslant (x+y)z$, որովհետև $x \leqslant z$, $x \leqslant x+y$, հետևաբար՝ $x \leqslant (x+y)z$: Բայց քանի որ $yz \leqslant (x+y)z$, ապա $x+yz \leqslant (x+y)z$: Նշանակելով $a = x+yz$, $b = (x+y)z$, կունենանք՝ $a < b$, $y+a \geqslant b$, $y+a \geqslant y+b$, $y+a \leqslant y+b$, $yb \leqslant a$, $yb \leqslant ya$,

$ya \leqslant yb$: Հետևաբար, $y + a = y + b$ և $ya = yb$: Այսպիսով, հանգում ենք $Q' = \{a, b, y, y + a, ya\}$ ենթակավարին, որը կունենա նկ. 1 տեսքը, որովհետև նշված 5 տարրերը զույգ առ զույգ միմյանցից տարբեր են: Իրոք, $y \nleqslant a$, $y \nleqslant b$, $b \nleqslant y$, $a \nleqslant y$: Ապացուցենք սրանք:
1) Եթե $y \leqslant a$, ապա $y + a = a \geqslant b$, բայց քանի որ $a \leqslant b$, հետևաբար՝ $a = b$: Հակասություն:
2) Եթե $y \leqslant b$, ապա $y \cdot b = y \leqslant a$, որն ինչպես տեսանք հնարավոր չէ:
3) Եթե $b \leqslant y$, ապա $b \cdot y = b \leqslant a$, հետևաբար՝ $a = b$: Հակասություն:
4) Եթե $a \leqslant y$, ապա $a + y = y \geqslant b$, որն ինչպես տեսանք հնարավոր չէ:

□



նկ. 1 (pentagon)

20.3. Բաշխական կավարներ

$Q(+, \cdot)$ կավարը կոչվում է **բաշխական**, եթե նրա մեջ տեղի ունի հետևյալ բաշխական նույնությունը՝

$$x(y + z) = xy + xz$$

բոլոր $x, y, z \in Q$ տարրերի համար: $Q(\leqslant)$ կավարաձև կարգավորված բազմությունը կոչվում է **բաշխական**, եթե համապատասխան $Q^{\vee} = Q(+, \cdot)$ կավարը բաշխական է:

Հետևաբար, բոլոր բաշխական կավարների դասը բազմաձևություն է և բաշխական կավարի ցանկացած ենթակավար նս կլինի բաշխական կավար:

Բաշխական կավարը նաև կիսաօղակ է:

Օրինակ, հետևյալ կավարաձև կարգավորված բազմությունները բաշխական են.

ա) X բազմության բոլոր ենթաբազմությունների 2^X բազմությունը՝ տեսա-բազմային ներդրման մկատմամբ;

բ) բոլոր իրական թվերի $\mathbb{R}$ բազմությունը՝ սովորական «$\leqslant$» հարաբերության նկատմամբ;

գ) յուրաքանչյուր շղթա (կամ գծայնորեն կարգավորված բազմություն);

դ) բոլոր բնական թվերի $\mathbb{N}$ բազմությունը՝ բաժանման հարաբերության նկատմամբ;

ե) միածին խմբի բոլոր ենթախմբերի բազմությունը՝ տեսա-բազմային ներդրման նկատմամբ:

Լեմմ 20.4: *Որպեսզի $Q(+,\cdot)$ կավարը լինի բաշխական անհրաժեշտ է և բավարար, որ*

$$(x+y)z \leqslant x+yz$$

ցանկացած $x,y,z \in Q$ տարրերի համար:

Ապացուցում: Եթե $Q(+,\cdot)$ կավարը բաշխական է, ապա

$$(x+y)z = xz+yz \leqslant x+yz:$$

Եվ հակառակը, եթե $(x+y)z \leqslant x+yz$, ապա

$$(x+y)z = (x+y)zz \leqslant (x+yz)z = (yz+x)z \leqslant yz+xz,$$

այսինքն՝ $(x+y)z \leqslant xz+yz$: Մնում է նկատել, որ հակառակ անհավասարությունը տեղի ունի բոլոր կավարներում: Իրոք,

$$xz \leqslant (x+y)z,$$

$$yz \leqslant (x+y)z,$$

հետևաբար, $xz+yz \leqslant (x+y)z$: □

Լեմմ 20.5*: Յուրաքանչյուր բաշխական կավար մոդուլյար է:*

Ապացուցում: Եթե $x \leqslant z$, ապա $xz = x$ և $(x+y)z = xz+yz = x+yz$: □

Սակայն, հակառակը ճիշտ չէ: Օրինակ, չորս տարրանի ոչ միածին (բայց աբելյան) խմբի բոլոր ենթախմբերի կավարը մոդուլյար է, բայց բաշխական չէ: Հարթության (այսինքն՝ երկչափանի գծային տարածության) բոլոր ենթատարածությունների կավարը լինելով մոդուլյար, բաշխական չէ (բխում է նաև հաջորդ լեմմից):

Լեմմ 20.6: *Եթե բաշխական կավարում* $x + x' = x + x''$ *և* $x \cdot x' = x \cdot x''$, *ապա* $x' = x''$*:*

Ապացուցում: Իրոք,

$$x' = x'(x' + x) = x'(x'' + x) = x'x'' + x'x = x''x' + x''x =$$

$$= x''(x' + x) = x''(x'' + x) = x'' :$$

Թեորեմ 20.3*: Կամայական* $Q(+, \cdot)$ *կավարի համար հետևյալ պնդումները համարժեք են.*

1) $Q(+, \cdot)$*-ը բաշխական է;*

2) $Q(+, \cdot)$*-ը բավարարում է*

$$x + yz = (x + y)(x + z) \quad \textit{(երկակի բաշխականություն)}$$

նույնությանը;

3) $Q(+, \cdot)$*-ը բավարարում է*

$$xy + yz + zx = (x + y)(y + z)(z + x)$$

նույնությանը:

Ապացուցում: 1)$\to$2): Իրոք,

$$(x + y)(x + z) = (x + y)x + (x + y)z = x(x + y) + z(x + y) =$$

$$= x + zx + zy = x + zy = x + yz :$$

2)$\to$3): Իրոք,

$$xy + yz + zx = (xy + yz) + zx = (xy + yz + z)(xy + yz + x) =$$

$$= (xy + z)(yz + x) = (x + z)(y + z)(y + x)(z + x) = (x + y)(y + z)(z + x) :$$

3)$\to$1): Նախ ապացուցենք, որ 3)-ից բխում է $Q(+, \cdot)$ կավարի մոդուլյարությունը: Իրոք, եթե $a \leqslant c$, ապա $ac = a$, $a + c = c$ և

$$a+bc = ab+a+bc = ab+ac+bc = (a+b)(a+c)(b+c) = (a+b)c(b+c) = (a+b)c :$$

Այժմ ապացուցենք 3)$\to$1) հետևությունը՝ ելնելով $Q(+, \cdot)$ կավարի մոդուլյարությունից: Նշանակելով $u = xy+yz+zx$, $v = (x+y)(y+z)(z+x)$, կունենանք՝ $u = v$, $xu = xv$, որտեղ

$$xu = x(xy + yz + zx) = ((xy + zx) + yz)x = xy + zx + yzx = xy + zx,$$

$$xv = x(x+y)(y+z)(z+x) = x(y+z)(z+x) = x(x+z)(y+z) = x(y+z):$$

Հետևաբար, $x(y+z) = xy + xz$:

Նկատենք, որ 2)→1) հետևությունը կարելի է նաև ստանալ ավելի հեշտ՝ $xy+xz = (xy+x)(xy+z) = x(xy+z) = x(x+z)(y+z) = x(y+z)$: □

Հետևություն 20.6: *Եթե $Q(\leqslant)$ կավարածև կարգավորված բազմությունը բաշխական է, ապա $Q(\leqslant^{-1})$ կավարածև կարգավորված բազմությունը ևս կլինի բաշխական:* □

Հետևություն 20.7: *Կամայական $Q(+,\cdot)$ բաշխական կավարում տեղի ունեն*

$$X(x, Y(y,z)) = Y(X(x,y), X(x,z)),$$

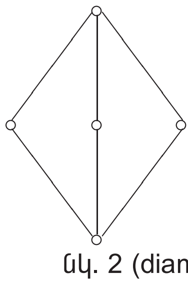
$$X(Y(x,y),z) = Y(X(x,z), X(y,z))$$

հավասարությունները ցանկացած $x,y,z \in Q$ տարրերի և ցանկացած $X, Y \in \{+,\cdot\}$ գործողությունների համար: Այսինքն՝ կամայական $Q(+,\cdot)$ բաշխական կավարում տեղի ունեն նշված գերնույնությունները, որոնք կոչվում են բաշխական գերնույնություններ:

Ապացուցում: Անմիջական ստուգման եղանակով, երբ $(X,Y) = (+,\cdot)$, $(X,Y) = (\cdot,+)$, $(X,Y) = (+,+)$, $(X,Y) = (\cdot,\cdot)$: □

Այժմ ապացուցենք կավարի բաշխականության Բիրկհոֆի հետևյալ հայտանիշը:

Թեորեմ 20.4 (Գ. Բիրկհոֆ) : *Որպեսզի կավարը լինի բաշխական անհրաժեշտ է և բավարար, որ այն օժտված չլինի նկ.1 և նկ.2 տեսքի ենթակավարներով՝*


:

նկ. 2 (diamond)

Ապացուցում: Անհրաժեշտությունն ակնհայտ է: Իրոք, բաշխական կավարի յուրաքանչյուր ենթակավար ևս բաշխական կավար է, իսկ յուրաքանչյուր բաշխական կավար մոդուլյար է: Հետևաբար, բաշխական կավարը չի կարող ունենալ նկ. 1 տեսքի ենթակավար, որը մոդուլյար չէ: Այնուհետև, յուրաքանչյուր բաշխական կավար չի կարող ունենալ նկ. 2 տեսքի ենթակավար, որովհետև նկ. 2-ում պատկերված կավարը բաշխական չէ:
Ապացուցենք *բավարարությունը:* Եթե $Q(+,\cdot)$ կավարը չունի նկ. 1 տեսքի ենթակավար, ապա, համաձայն մոդուլյարության Դեդեկինդի հայտանիշի, այն կլինի մոդուլյար: Վերցնենք կամայական $c_1, c_2, c_3 \in Q$ տարրեր և նշանակենք՝

$$a_1 = c_2 \cdot c_3, \quad a_2 = c_1 \cdot c_3, \quad a_3 = c_1 \cdot c_2,$$

$$b_1 = c_2 + c_3, \quad b_2 = c_1 + c_3, \quad b_3 = c_1 + c_2,$$

$$d_i = (a_i + c_i)b_i = a_i + c_ib_i, \quad a_i \leqslant b_i, \qquad i = 1, 2, 3,$$

$$u = b_1b_2b_3, \qquad v = a_1 + a_2 + a_3,$$

որտեղից (ըստ մոդուլյարության պայմանի)՝

$$d_1 + d_2 = a_1 + c_1b_1 + a_2 + c_2b_2 = (c_1b_1 + c_2b_2) + a_1 + a_2,$$

որտեղ $c_1b_1+c_2b_2 = (c_2b_2+c_1)b_1 = ((c_1+c_2)b_2)b_1 = b_3b_2b_1 = u$, որովհետև $c_2b_2 \leqslant b_1$, $c_1 \leqslant b_2$: Սակայն $a_i \leqslant u$ ցանկացած $i = 1, 2, 3$ արժեքի դեպքում: Օրինակ, $a_1 \leqslant b_1$, այսինքն՝ $c_2c_3 \leqslant c_2 + c_3$, որտեղից

$$c_2c_3(c_1 + c_3) \leqslant (c_2 + c_3)(c_1 + c_3),$$

$$c_2c_3 \leqslant (c_2 + c_3)(c_1 + c_3),$$

$$c_3c_2(c_1 + c_2) \leqslant (c_2 + c_3)(c_1 + c_3)(c_1 + c_2),$$

$$a_1 = c_2c_3 \leqslant (c_2 + c_3)(c_1 + c_3)(c_1 + c_2) = u:$$

Նույն ձևով ստացվում են $a_2 \leqslant u$ և $a_3 \leqslant u$ անհավասարությունները: Հետևաբար, $d_1 + d_2 = u + a_1 + a_2 = u$: Նույն եղանակով ապացուցվում են $d_1 + d_3 = u$, $d_2 + d_3 = u$, $d_1 \cdot d_2 = v$, $d_1 \cdot d_3 = v$, $d_2 \cdot d_3 = v$ հավասարությունները: Եթե $d_1, d_2, d_3 \in Q$ տարրերը զույգ առ զույգ համեմատելի չեն, ապա $Q(+,\cdot)$ կավարը կունենա նկ. 2 տեսքի $Q' = \{d_1, d_2, d_3, u, v\}$ ենթակավարը, որը հակասում է տրված պայմանին:

Հետևաբար, գոյություն կունենան այնպիսի $i \neq j$ համարներ, որ $d_i \leqslant d_j$: Դիցուք $d_1 \leqslant d_2$: Ուստի, $u = d_1 + d_2 = d_2$ և $v = d_1 \cdot d_2 = d_1$: Սակայն մոդուլյարության պայմանից բխում է ավելին՝

$$d_2 = u \cdot d_2 = (d_1 + d_3)d_2 = d_1 + d_3 d_2 = d_1 + v = d_1 :$$

Ուստի, $u = v$: Մնում է օգտվել թեորեմ 20.3-ից: □

Հետևություն 20.8: *Որպեսզի $Q(+,\cdot)$ կավարը լինի բաշխական անհրաժեշտ է և բավարար, որ*

$$x + y = x + z, \quad x \cdot y = x \cdot z \longrightarrow y = z,$$

որտեղ $x, y, z \in Q$:

Ապացուցում: Անհրաժեշտությունը բխում է լեմմ 20.6-ից, իսկ *բավարարությունը*՝ թեորեմ 20.4-ից: Իրոք, նշված պայմանի դեպքում $Q(+,\cdot)$ կավարը չի կարող ունենալ նկ. 1 կամ նկ. 2 տեսքի ենթակավար, որովհետև դրանցից յուրաքանչյուրի համար խախտվում է տրված պայմանը: □

20.4. Բուլյան հանրահաշվի գաղափարը

$Q(+,\cdot)$ կավարը կոչվում է **սահմանափակ**, եթե $+$ և $\cdot$ գործողությունները օժտված են միավորներով, որոնք համապատասխանաբար նշանակվում են 0-ով և 1-ով՝

$$x \cdot 1 = x,$$

$$x + 0 = x$$

ցանկացած $x \in Q$ տարրի համար և, հետևաբար,

$$1 + x = 1 + 1 \cdot x = 1,$$

$$0 \cdot x = 0(0 + x) = 0$$

համաձայն կլանման նույնությունների: Հետևաբար, համապատասխան $Q^{\vee} = Q(\leqslant)$ կավարաձև կարգավորված բազմության մեջ՝ $0 \leqslant x \leqslant 1$ ցանկացած $x \in Q$ տարրի համար, որով էլ հենց պայմանավորված է սահմանափակ կավարի անվանումը: Եվ հակառակը, եթե $Q(\leqslant)$ կավարաձև կարգավորված բազմությունն օժտված է մեծագույն և փոքրագույն տարրերով, ապա համապատասխան $Q^{\wedge} = Q(+,\cdot)$ կավարը կլինի սահմանափակ:

$Q(+,\cdot)$ կավարը կոչվում է **բուլյան հանրահաշիվ (G. Boole)**, եթե նրա համար տեղի ունեն հետևյալ երեք պայմանները.

1) այն բաշխական է;

2) այն սահմանափակ է;

3) նրա յուրաքանչյուր տարր օժտված է բուլյան լրացումով, այսինքն՝ ցանկացած $x \in Q$ տարրի համար գոյություն ունի այնպիսի $x' \in Q$ տարր, որ
$$\begin{cases} x + x' = 1, \\ x \cdot x' = 0, \end{cases}$$
որտեղ x'-ը կոչվում է x-ի **բուլյան լրացում**:

$Q(\leqslant)$ կավարաձև կարգավորված բազմությունը կոչվում է **բուլյան**, եթե համապատասխան $Q^{\vee} = Q(+,\cdot)$ կավարը բուլյան հանրահաշիվ է: Հետևաբար, եթե $Q(\leqslant)$ կավարաձև կարգավորված բազմությունը բուլյան է, ապա այդպիսին կլինի նաև $Q(\leqslant^{-1})$ կավարաձև կարգավորված բազմությունը:

Դժվար չէ նկատել, որ բուլյան հանրահաշվում x'-ը որոշվում է միարժեքորեն:

Իրոք, եթե նաև
$$\begin{cases} x + x'' = 1, \\ x \cdot x'' = 0, \end{cases}$$
ապա համաձայն լեմմ 20.6-ի՝ $x' = x''$: Հետևաբար, $x \to x'$ արտապատկերումը, որը նույնպես նշանակվում է $(')$-ով, կարելի է դիտել որպես բուլյան հանրահաշվի երրորդ գործողություն: Իսկ եթե 0-ն և 1-ը դիտենք որպես զրո-տեղանի գործողություններ, ապա բուլյան հանրահաշվի սահմանման պայմանները դառնում են նույնություններ՝ գրված $+$, $\cdot$, $'$, 0, 1 գործողություններով: Հետևաբար, բոլոր բուլյան հանրահաշիվների դասը բազմաձևություն է:

Լեմմ 20.7: *Ցանկացած բուլյան հանրահաշվում* $0' = 1$, $1' = 0$ *և տեղի ունեն հետևյալ նույնությունները՝*
$$(x')' = x,$$

$$\left.\begin{array}{l}(x+y)'=x'\cdot y',\\(x\cdot y)'=x'+y':\end{array}\right\}$$ (Դե Մորգանի նույնություններ (օրենքներ))

Ապացուցում: Բուլյան լրացման սահմանման համաձայն՝

$$\left\{\begin{array}{l}x'+x=1,\\x'\cdot x=0,\end{array}\right. \qquad \left\{\begin{array}{l}x'+(x')'=1,\\x'\cdot(x')'=0,\end{array}\right.$$

որտեղից, բուլյան լրացման միակության համաձայն՝ $(x')' = x$: Այնուհետև, $0' = 1$ և $1' = 0$ հավասարություններն ակնհայտ են: Ապացուցենք Դե Մորգանի նույնությունները: Երկակի բաշխականության համաձայն, կունենանք՝

$$(x+y)+(x'\cdot y')=(x+x'y')+y=(x+x')(x+y')+y=$$

$$=1(x+y')+y=x+y'+y=x+1=1,$$

$$(x+y)(x'y')=xx'y'+yx'y'=0+0=0:$$

Դե Մորգանի երկրորդ նույնությունն ակնհայտորեն բխում է նրա առաջին նույնությունից և $(x')'=x$ պայմանից: □

Թեորեմ 20.5: *Կամայական $Q(+,\cdot)$ բուլյան հանրահաշվում տեղի ունեն*

$$X(x,Y(y,z)')'=Y(X(x,y')',X(x,z')'),$$

$$X(Y(x,y)',z)'=Y(X(x',z)',X(y',z)')$$

հավասարությունները ցանկացած $x,y,z\in Q$ տարրերի և ցանկացած $X,Y\in\{+,\cdot\}$ գործողությունների համար: Այսինքն՝ կամայական $Q(+,\cdot)$ բուլյան հանրահաշվում տեղի ունեն նշված գերնույնությունները:

Ապացուցում: Անմիջական ստուգման եղանակով, երբ $(X,Y)=(+,\cdot)$, $(X,Y)=(\cdot,+)$, $(X,Y)=(+,+)$, $(X,Y)=(\cdot,\cdot)$: □

Կասենք, որ $Q(+,\cdot)$ սահմանափակ կավարը բավարարում է բուլյան լրացումների գոյության (միակության) պայմանին, եթե նրա յուրաքանչյուր տարր ունի (ունի միայն մեկ) բուլյան լրացում: Հետևյալ երկու արդյունքները կապված են բուլյան հանրահաշվի սահմանման հետ:

Թեորեմ 20.6 (Բիրկհոֆ, Ֆոն Նեյման): *Բուլյան լրացումների միակության պայմանին բավարարող ցանկացած սահմանափակ և մոդուլյար կավար կլինի բաշխական, հետևաբար, և բուլյան հանրահաշիվ:* □

Փոքրագույն (զրոյական) տարրով $Q(\leqslant)$ կավարաձև կարգավորված բազմության ատոմները կոչվում են նաև համապատասխան $Q^{\wedge} = Q(+, \cdot)$ կավարի ատոմներ:

Զրոյական տարրով կավարը կոչվում է **ատոմական**, եթե նրա յուրաքանչյուր $x \neq 0$ տարր պարունակում է որևէ a ատոմ, այսինքն՝ $a \leqslant x$: Օրինակ, յուրաքանչյուր վերջավոր կավար ատոմական է:

Թեորեմ 20.7 (Բիրկհոֆ, Ուօրդ): *Բուլյան լրացումների միակության պայմանին բավարարող ցանկացած սահմանափակ և ատոմական կավար կլինի բաշխական, հետևաբար, և բուլյան հանրահաշիվ:* □

Օրինակներ:

1) Բազմությունների յուրաքանչյուր հանրահաշիվ հանդիսանում է բուլյան հանրահաշիվ: Մասնավորապես, կամայական A բազմության բոլոր ենթաբազմությունների դասը բուլյան հանրահաշիվ է, որը նշանակվում է 2^A-ով (կամ $pow(A)$-ով) և որի կավարային գործողությունները որոշվում են հետևյալ կերպ՝

$$X + Y = X \cup Y,$$

$$X \cdot Y = X \cap Y,$$

$$X' = A \setminus X,$$

որտեղ $X, Y \in 2^A$:

2) Դիցուք p-ն պարզ թիվ է, իսկ N_p-ն բոլոր այն n բնական թվերի բազմությունն է, որոնց համար

$$n = 1 \cdot p_1 \cdot p_2 \cdots p_{k(n)},$$

որտեղ բոլոր p_i արտադրիչները միմյանցից տարբեր և p-ն չգերազանցող պարզ թվեր են: N_p-ն կլինի բուլյան հանրահաշիվ, եթե որպես $m, n \in N_p$ բնական թվերի գումար վերցնենք նրանց ամենափոքր ընդհանուր բազմապատիկը, իսկ որպես արտադրյալ՝ նրանց ամենամեծ ընդհանուր բաժանարարը:

3) Երկու տարրանի $\{0,1\}$ թվային բազմությունը դառնում է բուլյան հանրահաշիվ, եթե $x, y \in \{0,1\}$ թվերի գումար և արտադրյալ ասելով հասկանանք $\max\{x,y\}$-ը և $\min\{x,y\}$-ը, իսկ $x' = 1 - x$: Այս դեպքում ընդունված են նաև հետևյալ հանրահայտ նշանակումները՝

$$x \vee y = \max\{x,y\},$$

$$x \& y = \min\{x,y\},$$

որտեղ $x, y \in \{0,1\}$: Այսպիսով հանգում ենք 2-տարրանի բուլյան հանրահաշվի գումարման և բազմապատկման գործողությունների հետևյալ աղյուսակներին՝

$\vee$	0	1
0	0	1
1	1	1

,

$\&$	0	1
0	0	0
1	0	1

:

4) Որևէ փորձում (էքսպերիմենտ) հանդիպող բոլոր պատահարների (պատահական մեծությունների) բազմությունը կազմում է բուլյան հանրահաշիվ՝ պատահարների նկատմամբ սահմանվող հայտնի գործողությունների նկատմամբ:

5) Իրական թվերի $[a,b]$ հատվածի բոլոր այն ենթաբազմությունների դասը, որոնք չափելի են Լեբեգի իմաստով, կազմում է բուլյան հանրահաշիվ՝ տեսա-բազմային գործողությունների նկատմամբ: Այստեղ $[a,b]$ հատվածի փոխարեն կարելի է դետարկել իրական թվերի ցանկացած բազմություն, որը չափելի է Լեբեգի իմաստով: Մյուս կողմից, $[a,b]$ հատվածի բոլոր չափելի ենթաբազմությունների փոխարեն կարելի է դիտարկել նրա բոլոր բորելյան ենթաբազմությունների դասը, որը նույնպես կլինի բուլյան հանրահաշիվ (E. Borel):

6) X տոպոլոգիական տարածության բոլոր այն ենթաբազմությունների դասը, որոնք միաժամանակ բաց են և փակ, կազմում է բուլյան հանրահաշիվ՝ տեսա-բազմային գործողությունների նկատմամբ: Այս բուլյան հանրահաշիվը կոչվում է X տոպոլոգիական տարածության բաց-փակ ենթաբազմությունների բուլյան հանրահաշիվ:

Համեմատելով 2-տարրանի բուլյան հանրահաշվի գործողությունները $\mathbb{Z}_2(+,\cdot)$ մնացքների օղակի (դաշտի) գործողությունների հետ, նկատում ենք հետևյալ կապը՝

$$x \vee y = x + y + xy,$$

$$x\&y = x \cdot y,$$

$$x + y = (x\&y') \vee (y\&x') :$$

Ընդհանուր դեպքում, բուլյան հանրահաշիվները գտնվում են փոխադարձ կապի մեջ, այսպես կոչված, բուլյան օղակների հետ: $Q(+,\cdot)$ օղակը կոչվում է **բուլյան օղակ**, եթե այն զուգորդական է, տեղափոխական, օժտված e միավորով և $x^2 = x$ ցանկացած $x \in Q$ տարրի համար: Բուլյան օղակում $(x+x)^2 = x + x$ պայմանից բխում է $x + x = 0$ հավասարությունը:

Բուլյան հանրահաշիվների նկարագրության վերաբերյալ հիմնական արդյունքներն ապացուցվել են Ստոունի (M. H. Stone) կողմից:

Թեորեմ 20.8 (Ստոուն): *1) Եթե $Q(+,\cdot)$-ը բուլյան հանրահաշիվ է և*

$$x \oplus y = xy' + yx',$$

ապա $Q(\oplus,\cdot)$-ը բուլյան օղակ է : 2) Եվ հակառակը, եթե $Q(\oplus,\cdot)$-ը բուլյան օղակ է և

$$x + y = x \oplus y \oplus xy,$$

ապա $Q(+,\cdot)$-ը բուլյան հանրահաշիվ է , որտեղ $x' = e \oplus x$, իսկ e-ն բուլյան օղակի միավորն է :

Ապացուցում: 1) Անմիջական ստուգման եղանակով: Իրոք,

$$\begin{aligned} &x \oplus y = y \oplus x, \\ &(x \oplus y) \oplus z = xyz + xy'z' + yx'z' + zx'y' = x \oplus (y \oplus z), \\ &x \oplus 0 = x, \\ &x \oplus x = 0, \\ &x(y \oplus z) = xyz' + xzy' = xy \oplus xz, \end{aligned}$$

որտեղ 0-ն բուլյան հանրահաշվի փոքրագույն տարրն է: 2)-ը ևս ապացուցվում է անմիջական ստուգման եղանակով: □

20.5. Կավարների իզոմորֆիզմը

Դիցուք $Q(+,\cdot)$-ը և $Q^*(+,\cdot)$-ը կավարներ են: $\varphi : Q \to Q^*$ արտապատկերումը կոչվում է (կավարային) **նմանածնություն** կամ **հոմոմորֆ** արտապատկերում (**հոմոմորֆություն**, **հոմոմորֆիզմ**)՝ $Q(+,\cdot)$ կավարից $Q^*(+,\cdot)$ կավարի մեջ, եթե տեղի ունեն հետևյալ երկու պայմանները.

$$\varphi(x+y) = \varphi x + \varphi y,$$

$$\varphi(x \cdot y) = \varphi x \cdot \varphi y$$

ցանկացած $x, y \in Q$ տարրերի համար: Եթե այդ դեպքում φ արտապատկերումը նաև փոխմիարժեք (բիեկտիվ) է, ապա φ-ն կոչվում է (կավարային) **նույնածնություն** կամ **իզոմորֆ** արտապատկերում (իզոմորֆություն, իզոմորֆիզմ): $Q(+,\cdot)$ և $Q^*(+,\cdot)$ կավարները կոչվում են **իզոմորֆ** կամ **նույնածն** և գրվում է $Q \simeq Q^*$ կամ $Q \cong Q^*$, եթե գոյություն ունի որևէ $\varphi : Q \to Q^*$ իզոմորֆ արտապատկերում: Սահմանված «$\simeq$» հարաբերությունը կոչվում է **կավարների իզոմորֆության** կամ **նույնածնության հարաբերություն**: Հեշտությամբ ապացուցվում է, որ երկու (հետևաբար և վերջավոր թվով) հոմոմորֆիզմների (իզոմորֆիզմների) արտադրյալը նորից հոմոմորֆիզմ (իզոմորֆիզմ) է: Եթե $\varphi : Q \to Q^*$ արտապատկերումը (կավարային) իզոմորֆիզմ է, ապա այդպիսին կլինի նաև $\varphi^{-1} : Q^* \to Q$ արտապատկերումը:

Լեմմ 20.8: *Կավարների իզոմորֆության «$\simeq$» հարաբերությունը բավարարում է համարժեքության հարաբերության սահմանման բոլոր երեք պայմաններին:* □

Կասենք, որ $Q(+,\cdot)$ կավարը **ներդրվում է** $Q^*(+,\cdot)$ կավարի մեջ, եթե գոյություն ունի որևէ $\varphi : Q \to Q^*$ ներդրող (ինյեկտիվ) և հոմոմորֆ արտապատկերում:

Թեորեմ 20.9: *Դիցուք $Q(+,\cdot)$-ը և $Q^*(+,\cdot)$-ը կավարներ են: Որպեսզի $\varphi : Q \to Q^*$ փոխմիարժեք (բիեկտիվ) արտապատկերումը լինի նույնածնություն (իզոմորֆիզմ) տրված կավարների միջև անհրաժեշտ է և բավարար, որ համապատասխան $Q(\leqslant)$ և $Q^*(\leqslant)$ կավարածն կարգավորված բազմություններում տեղի ունենա հետևյալ պայմանը՝*

$$x \leqslant y \longleftrightarrow \varphi(x) \leqslant \varphi(y),$$

որտեղ $x, y \in Q$ (այսինքն՝ որ $\varphi : Q \to Q^*$ արտապատկերումը լինի նույնածնություն (իզոմորֆիզմ) համապատասխան կավարածն կարգավորված բազմությունների միջև):

Ապացուցում: Անհրաժեշտությունն ակնհայտ է, որովհետև եթե $\varphi : Q \to Q^*$ արտապատկերումն իզոմորֆիզմ է $Q(+,\cdot)$ կավարից $Q^*(+,\cdot)$ կավարի մեջ, ապա $\varphi^{-1} : Q^* \to Q$ արտապատկերումը կլինի իզոմորֆիզմ $Q^*(+,\cdot)$ կավարից $Q(+,\cdot)$ կավարի մեջ և հետևաբար՝

$$x \leqslant y \longrightarrow x + y = y \longrightarrow \varphi(x+y) = \varphi(y) \longrightarrow \varphi(x) + \varphi(y) =$$

$$= \varphi(y) \longrightarrow \varphi(x) \leqslant \varphi(y),$$

$$\varphi(x) \leqslant \varphi(y) \longrightarrow \varphi^{-1}(\varphi(x)) \leqslant \varphi^{-1}(\varphi(y)) \longrightarrow x \leqslant y:$$

Բավարարություն: Քանի որ $x \leqslant x + y$ և $y \leqslant x + y$, ապա $\varphi(x) \leqslant \varphi(x+y)$ և $\varphi(y) \leqslant \varphi(x+y)$, այսինքն՝ $\varphi(x+y)$-ը $\{\varphi(x), \varphi(y)\}$ բազմության վերին եզր է: Ապացուցենք, որ այն վերին ճշգրիտ եզր է, այսինքն՝ $\varphi(x+y) = \sup\{\varphi(x), \varphi(y)\} = \varphi(x) + \varphi(y)$: Իրոք, եթե $\varphi(x) \leqslant c'$ և $\varphi(y) \leqslant c'$, իսկ $c' = \varphi(c)$, ապա $x \leqslant c$ և $y \leqslant c$: Հետևաբար, $x+y \leqslant c$ և $\varphi(x+y) \leqslant \varphi(c) = c'$:

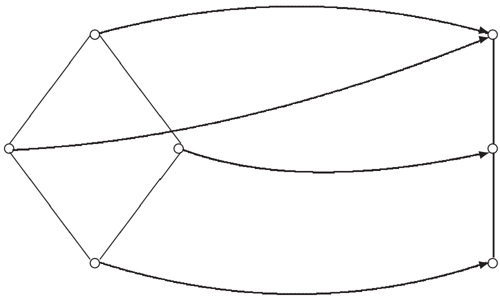
Երկակի դատողություններով ապացուցվում է $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ հավասարությունը ցանկացած $x, y \in Q$ տարրերի համար: □

Հետևություն 20.9: *Դիցուք $Q(+,\cdot)$-ը և $Q^*(+,\cdot)$-ը կավարներ են: $\varphi : Q \to Q^*$ փոխմիարժեք (բիեկտիվ) արտապատկերումը կլինի նույնածնություն (իզոմորֆիզմ) տրված կավարների միջև, եթե տեղի ունի հետևյալ պայմաններից որևէ մեկը՝*

ա) $\varphi(x+y) = \varphi(x) + \varphi(y)$ ցանկացած $x, y \in Q$ տարրերի համար;

բ) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ ցանկացած $x, y \in Q$ տարրերի համար: □

Սակայն այս պնդումը կամայական հոմոմորֆիզմի համար տեղի չունի, այսինքն՝ գոյություն ունեն այնպիսի Q և Q^* կավարներ և հոմոմորֆիզմ չհանդիսացող այնպիսի $\varphi : Q \to Q^*$ արտապատկերում, որը բավարարում է ա) (կամ բ)) պայմանին: Օրինակ,



նշված արտապատկերումը բավարարում է ա) պայմանին, բայց չի բավարարում բ) պայմանին:

Ակնհայտ է, որ կավարի ցանկացած ոչ դատարկ $[x, y]$ հատված ենթակավար է ($x \leqslant y$):

Թեորեմ 20.10 (Դեդեկինդ): *Եթե $Q(+,\cdot)$ կավարը մոդուլյար է, ապա $[ab, b]$ և $[a, a{+}b]$ հատվածներն իզոմորֆ են ցանկացած $a, b \in Q$ տարրերի համար:*

Ապացույց: Դիցուք $I = [ab, b]$ և $J = [a, a + b]$: Սահմանենք $\varphi : I \to J$ և $\varphi' : J \to I$ արտապատկերումները հետևյալ կերպ.

$$\varphi(x) = x + a, \qquad x \in I,$$

$$\varphi'(y) = y \cdot b, \qquad y \in J :$$

Քանի որ $ab \leqslant x \leqslant b$, ապա $a = ab + a \leqslant x + a \leqslant a + b$, այսինքն՝ $\varphi(x) \in J$: Նույն կերպ, քանի որ $a \leqslant y \leqslant a{+}b$, ապա $ab \leqslant yb \leqslant (a{+}b)b = b$, այսինքն՝ $\varphi'(y) \in I$: Օգտվելով մոդուլյարության պայմանից, նախ ապացուցենք $\varphi \cdot \varphi' = \varepsilon_I$ և $\varphi' \cdot \varphi = \varepsilon_J$ հավասարությունները, որտեղից կբխի φ-ի և φ'-ի փոխմիարժեքությունը (բիեկտիվությունը).

$$(\varphi \cdot \varphi')x = \varphi'(\varphi x) = \varphi'(x + a) = (x + a)b = x + ab = x = \varepsilon_I(x),$$

$$(\varphi' \cdot \varphi)y = \varphi(\varphi' y) = \varphi(y \cdot b) = yb + a = (a + b)y = y = \varepsilon_J(y) :$$

Այնուհետև,

$$\varphi(x + y) = x + y + a = x + y + a + a = (x + a) + (y + a) = \varphi(x) + \varphi(y),$$

$$\varphi(x \cdot y) = \varphi\left(\varphi'(x' \cdot y')\right) = (\varphi' \cdot \varphi)(x' \cdot y') = x' \cdot y' = \varphi(x) \cdot \varphi(y),$$

որտեղ $x' = \varphi(x)$, $y' = \varphi(y)$ և $x = \varphi'(x')$, $y = \varphi'(y')$, իսկ $x \cdot y = \varphi'(x') \cdot \varphi'(y') = x' \cdot b \cdot y' \cdot b = x' \cdot y' \cdot b = \varphi'(x' \cdot y')$: □

20.6. Բուլյան հանրահաշիվների իզոմորֆիզմը

Եթե $Q(+,\cdot)$-ը և $Q^*(+,\cdot)$-ը բուլյան հանրահաշիվներ են, ապա $\varphi : Q \to Q^*$ արտապատկերումը կոչվում է **նմանաձևություն** կամ **հոմոմորֆ** արտապատկերում (**հոմոմորֆություն**, **հոմոմորֆիզմ**)՝ $Q(+,\cdot)$ բուլյան հանրահաշվից $Q^*(+,\cdot)$ բուլյան հանրահաշվի մեջ, եթե տեղի ունեն հետևյալ պայմանները.

$$\varphi(x+y) = \varphi x + \varphi y,$$

$$\varphi(x \cdot y) = \varphi x \cdot \varphi y,$$

$$\varphi(x') = (\varphi x)'$$

ցանկացած $x, y \in Q$ տարրերի համար, որտեղ a'-ը միարժեքորեն որոշվող a-ի բուլյան լրացումն է: Եթե այդ դեպքում φ արտապատկերումը փոխմիարժեք (բիեկտիվ) է, ապա φ-ն կոչվում է **նույնաձևություն** կամ **իզոմորֆ** արտապատկերում (իզոմորֆություն, իզոմորֆիզմ): Երկու $Q(+,\cdot)$ և $Q^*(+,\cdot)$ բուլյան հանրահաշիվներ կոչվում են **իզոմորֆ** կամ **նույնաձև** և գրվում է $Q \simeq Q^*$ կամ $Q \cong Q^*$, եթե գոյություն ունի որևէ $\varphi : Q \to Q^*$ իզոմորֆ արտապատկերում: Սահմանված «$\simeq$» հարաբերությունը կոչվում է **բուլյան հանրահաշիվների իզոմորֆության հարաբերություն**: Հեշտությամբ ապացուցվումէ, որ երկու (հետևաբար և վերջավոր թվով) հոմոմորֆիզմների (իզոմորֆիզմների) արտադրյալը նորից հոմոմորֆիզմ (իզոմորֆիզմ) է:

Եթե $\varphi : Q \to Q^*$ արտապատկերումը բուլյան հանրահաշիվների իզոմորֆիզմ է, ապա այդպիսին կլինի նաև $\varphi^{-1} : Q^* \to Q$ արտապատկերումը:

Լեմմ 20.9: *Բուլյան հանրահաշիվների իզոմորֆության «$\simeq$» հարաբերությունը բավարարում է համարժեքության հարաբերության սահմանման բոլոր երեք պայմաններին:* □

Կասենք, որ $Q(+,\cdot)$ բուլյան հանրահաշիվը **ներդրվում է** $Q^*(+,\cdot)$ բուլյան հանրահաշվի մեջ, եթե գոյություն ունի որևէ $\varphi : Q \to Q^*$ ներդրող (ինյեկտիվ) և հոմոմորֆ արտապատկերում:

Լեմմ 20.10: *Դիցուք* $Q(+,\cdot)$*-ը և* $Q^*(+,\cdot)$*-ը բուլյան հանրահաշիվներ են:* $\varphi : Q \to Q^*$ *արտապատկերումը կլինի հոմոմորֆիզմ (նմանածնություն), եթե տեղի ունի հետևյալ պայմաններից որևէ մեկը՝*

ա) $\varphi(x+y) = \varphi(x) + \varphi(y)$,

$\varphi(x') = (\varphi x)'$

ցանկացած $x, y \in Q$ *տարրերի համար;*

բ) $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$,

$\varphi(x') = (\varphi x)'$

ցանկացած $x, y \in Q$ *տարրերի համար:*

Ապացուցում: ա) Իրոք,

$$\varphi(x\cdot y) = \varphi\left((x'+y')'\right) = \left(\varphi(x'+y')\right)' = \left(\varphi(x') + \varphi(y')\right)' =$$

$$\left(\varphi(x')\right)' \cdot \left(\varphi(y')\right)' = \varphi\left(x''\right)\cdot\varphi\left(y''\right) = \varphi(x)\cdot\varphi(y) :$$ □

Լեմմ 20.11: *Դիցուք* $Q(+,\cdot)$*-ը և* $Q^*(+,\cdot)$*-ը բուլյան հանրահաշիվներ են: Որպեսզի* $\varphi : Q \to Q^*$ *փոխմիարժեք (բիեկտիվ) արտապատկերումը լինի նույնածնություն (իզոմորֆիզմ) տրված բուլյան հանրահաշիվների միջև անհրաժեշտ է և բավարար, որ համապատասխան* $Q(\leqslant)$ *և* $Q^*(\leqslant)$ *կավարածն կարգավորված բազմություններում տեղի ունենա հետևյալ պայմանը՝*

$$x \leqslant y \longleftrightarrow \varphi(x) \leqslant \varphi(y),$$

որտեղ $x, y \in Q$*:*

Ապացուցում: Բխում է թեորեմ 20.9-ից: □

Թեորեմ 20.11 (Ստոուն): *Յուրաքանչյուր վերջավոր բուլյան հանրահաշիվ իզոմորֆ է* 2^A *տեսքի որևէ բուլյան հանրահաշվի: Ավելի ճիշտ,* A*-ն կարելի է վերցնել հավասար վերջավոր բուլյան հանրահաշվի ատոմների բազմությանը:*

Ապացուցում: Դիցուք $Q(+,\cdot)$-ը տրված վերջավոր բուլյան հանրահաշիվն է: $Q(+,\cdot)$-ի բոլոր ատոմների բազմությունը նշանակենք Q^+-ով: Ակնհայտ է, որ $Q(+,\cdot)$ վերջավոր բուլյան հանրահաշվի ցանկացած $x \in Q$, $x \neq 0$, տարրի համար գոյություն ունի այնպիսի $a \in Q^+$ ատոմ, որ $a \leqslant x$, այսինքն՝ վերջավոր բուլյան հանրահաշիվը ատոմական կավար է: Դիցուք

$$x^+ = \{a \in Q^+ |\, a \leqslant x\} :$$

Մասնավորապես, $1^+ = Q^+$, իսկ $0^+ = \emptyset$:

Այժմ մեզ անհրաժեշտ են հետևյալ օժանդակ պնդումները:

Լեմմ 20.12: *Եթե $x \in Q$, իսկ $a \in Q^+$, ապա կամ $a \leqslant x$ կամ $a \leqslant x'$: Ընդ որում, այս երկու առնչությունները միաժամանակ տեղի ունենալ չեն կարող:*

Ապացույցում: Քանի որ $ax \leqslant a$ և a-ն ատոմ է, ապա կամ $ax = a$ կամ $ax = 0$: Առաջին դեպքում կունենանք՝ $a \leqslant x$, իսկ երկրորդ դեպքում՝

$$(a + x')x = 0, \qquad a + x' + x = 1 :$$

Հետևաբար, $a + x' = x'$ և $a \leqslant x'$: Ի վերջո, եթե միաժամանակ $a \leqslant x$ և $a \leqslant x'$, ապա $a \leqslant x \cdot x' = 0$ և $a = 0$, որը հակասում է ատոմի սահմանմանը:

□

Լեմմ 20.13: *Եթե $x^+ = y^+$, ապա $x = y$:*

Ապացույցում: Նախ կապացուցենք, որ $x \cdot y' = 0$ և $x' \cdot y = 0$: Իրոք, դիցուք $x \cdot y' \neq 0$: Այդ դեպքում գոյություն կունենա այնպիսի $a \in Q^+$ ատոմ, որ $a \leqslant x \cdot y'$: Հետևաբար, $a \leqslant x$ և $a \leqslant y'$, որտեղից՝ $a \in x^+$, բայց $a \notin y^+$, որը հակասում է տրված պայմանին:

Նույն դատողություններով ապացուցվում է $x' \cdot y = 0$ հավասարությունը: Այսպիսով՝

$$\begin{cases} (x+y)y' = 0, \\ x + y + y' = 1, \end{cases} \qquad \begin{cases} (x+y)x' = 0, \\ x + y + x' = 1, \end{cases}$$

այսինքն՝ $x + y = (y')' = y$ և $x + y = (x')' = x$: Ուստի $x = y$: □

Լեմմ 20.14: *Ցանկացած $a_1, \ldots, a_n \in Q^+$ ատոմների համար՝*

$$(a_1 + \cdots + a_n)^+ = \{a_1, \ldots, a_n\} :$$

Ապացույցում: Ակնհայտ է, որ հավասարության աջ մասը պարունակվում է ձախ մասում: Ապացուցենք հակառակը, որ հավասարության ձախ մասը ընկած է աջ մասում: Ենթադրելով հակառակը, ստանում ենք հակասություն: Իրոք, դիցուք $a \in (a_1 + \cdots + a_n)^+$, բայց $a \neq a_i$, $i = 1, \ldots, n$: Դիտարկենք $a \cdot a_i$ արտադրյալը: Քանի որ $0 \leqslant a \cdot a_i \leqslant a$ և a-ն ատոմ է, ապա կամ $a \cdot a_i = a$ կամ $a \cdot a_i = 0$: Եթե $a \cdot a_i = a$, ապա $0 < a < a_i$, որը հակասում է a_i-ի ատոմ լինելուն: Հետևաբար, $a \cdot a_i = 0$, որտեղ $i = 1, \ldots, n$: Բայց քանի որ $a \in (a_1 + \cdots + a_n)^+$, ապա $a \leqslant a_1 + \cdots + a_n$ և

$$a = a\,(a_1 + \cdots + a_n) = aa_1 + \cdots + aa_n = 0 + \cdots + 0 = 0 :$$

Հակասություն: □

Շարունակենք թեորեմի ապացուցումը, սահմանելով $\varphi : Q \to 2^{Q^+}$ արտապատկերումը հետևյալ կերպ`

$$\varphi(x) = x^+ \subseteq Q^+ :$$

Ապացուցված պնդումների համաձայն φ-ն կլինի ինյեկտիվ (ներդրող) և սյուրեկտիվ (վերադրող), այսինքն` φ-ն փոխմիարժեք (բիեկտիվ) է: Մնում է նկատել, որ

$$x \leqslant y \longleftrightarrow \varphi(x) \leqslant \varphi(y),$$

որտեղ $x, y \in Q$: Իրոք,

$$x \leqslant y \longrightarrow \varphi(x) \leqslant \varphi(y)$$

հատկությունն ակնհայտ է: Ապացուցենք հակառակ հատկությունը: Դիցուք $\varphi(x) \subseteq \varphi(y)$: Եթե $x \cdot y' \neq 0$, ապա գոյություն կունենա այնպիսի $a \in Q^+$ ատոմ, որ $a \leqslant x \cdot y'$: Հետևաբար, $a \leqslant x$ և $a \leqslant y'$, այսինքն` $a \in x^+$, բայց $a \notin y^+$, որը հակասում է տրված պայմանին: Ուստի, $x \cdot y' = 0$ և

$$(x + y)y' = 0, \quad x + y + y' = 1,$$

այսինքն` $x + y = (y')' = y$ և $x \leqslant y$: □

Հետևություն 20.10: *Վերջավոր բուլյան հանրահաշվի տարրերի թիվը հավասար է 2-ի n աստիճանի, որտեղ n-ը տրված բուլյան հանրահաշվի ատոմների թիվն է:* □

Հետևություն 20.11: *Երկու վերջավոր բուլյան հանրահաշիվներ կլինեն իզոմորֆ (նույնաձև) այն և միայն այն դեպքում, երբ դրանց ատոմների թիվը նույնն է:* □

Հետևություն 20.12: *Երկու վերջավոր բուլյան հանրահաշիվներ կլինեն իզոմորֆ (նույնաձև) այն և միայն այն դեպքում, երբ դրանց տարրերի թիվը նույնն է: Մասնավորապես, միևնույն բազմության վրա սահմանված (որոշված) բոլոր բուլյան հանրահաշիվներն իզոմորֆ են:*

□

$Q(+,\cdot)$ կավարը (մասնավորապես բուլյան հանրահաշիվը) կոչվում է **լրիվ**, եթե համապատասխան $Q^\vee = Q(\leqslant)$ մասնակի կարգավորված բազմությունը լրիվ կավարանմ կարգավորված բազմություն է, այսինքն՝ $\sup(X)$-ը և $\inf(X)$-ը գոյություն ունեն ցանկացած ոչ դատարկ $X \subseteq Q$ ենթաբազմության համար:

Գոյություն ունի բուլյան հանրահաշիվ, որն իզոմորֆ չէ 2^A տեսքի որևէ բուլյան հանրահաշվի: Իրոք, յուրաքանչյուր $X \neq \emptyset$ բազմության համար նշանակենք՝

$$FC(X) = \{A \subseteq X \mid A \text{ -ն կամ } X \setminus A \text{ -ն վերջավոր է}\} :$$

$FC(X)$-ը կլինի բուլյան հանրահաշիվ՝ տեսա-բազմային գործողությունների նկատմամբ: Մասնավորապես, $FC(\mathbb{N})$ բուլյան հանրահաշիվը իզոմորֆ չէ 2^A տեսքի որևէ բուլյան հանրահաշվի, որովհետև $FC(\mathbb{N})$ բազմությունը հաշվելի է, իսկ 2^A բազմությունը, համաձայն Կանտորի թեորեմի, կամ վերջավոր է կամ հաշվելի չէ:

Թեորեմ 20.12 (Լինդենբաում, Տարսկի): *Որպեսզի $Q(+,\cdot)$ բուլյան հանրահաշիվը լինի իզոմորֆ 2^A տեսքի որևէ բուլյան հանրահաշվի անհրաժեշտ է և բավարար, որ այն լինի լրիվ և ատոմական:*

Ապացուցում: Անհրաժեշտությունն ակնհայտ է, որովհետև 2^A տեսքի բուլյան հանրահաշիվը լրիվ է և ատոմական: Հետևաբար, այդպիսին կլինի նաև դրան իզոմորֆ ցանկացած բուլյան հանրահաշիվ:

Բավարարության համար կրկնվում է նախորդ թեորեմի ապացուցումը, որտեղ ցանկացած թվով ատոմների գումար ասելով պետք է հասկանալ դրանց վերին ճշգրիտ եզրը: Բացի այդ, եթե $X \subseteq Q$, $X \neq \emptyset$, $a \in Q$ և $a \cdot X = \{a \cdot x | x \in X\}$,ապա կարելի է կիրառել նաև հետևյալ ընդհանրացված բաշխական նույնությունը՝

$a \cdot \sup(X) = \sup(a \cdot X)$: (ֆոն Նեյմանի նույնություն)

Իրոք, $a \cdot x \leqslant a$ և $a \cdot x \leqslant x \leqslant \sup(X)$ ցանկացած $x \in X$ տարրի համար: Հետևաբար,$a \cdot x \leqslant a \cdot \sup(X)$ և $a \cdot \sup(X)$ տարրը կլինի $a \cdot X$ բազմության վերին եզրը: Դիցուք այժմ u-ն այդ բազմության կամայական վերին եզր է, այսինքն՝ $a \cdot x \leqslant u$ ցանկացած $x \in X$ տարրի համար: Հետևաբար՝

$$x = x \cdot 1 = x(a + a') = xa + xa' \leqslant u + a',$$

այսինքն՝ $u + a'$ տարրը կլինի X բազմության վերին եզրը, և

$$a \cdot \sup(X) \leqslant a(u + a') = au + aa' = au + 0 = au \leqslant u : \qquad \square$$

20.7. Կավարի իդեալներ և ֆիլտրներ: Պարզ և մաքսիմալ իդեալներ

Դիցուք $Q(+,\cdot)$-ը կավար է, իսկ $I \subseteq Q$, $I \neq \emptyset$: I ենթաբազմությունը կոչվում է $Q(+,\cdot)$ **կավարի իդեալ** և նշանակվում է $I \trianglelefteq Q$, եթե այն բավարարում է հետևյալ երկու պայմաններին.
ա) $x, y \in I \longrightarrow x + y \in I$;
բ) $t \in Q$, $z \in I$, $t \leqslant z \longrightarrow t \in I$:

Կավարի իդեալը ենթակավար է: Միևնույն կավարի ցանկացած թվով իդեալների հատումը նորից իդեալ է:

Լեմմ 20.15: *Որպեսզի ոչ դատարկ $I \subseteq Q$ ենթաբազմությունը լինի $Q(+,\cdot)$ կավարի իդեալ անհրաժեշտ է և բավարար, որ տեղի ունենա հետևյալ պայմանը՝*

$$x + y \in I \longleftrightarrow x, y \in I,$$

որտեղ $x, y \in Q$:

Ապացուցում: Անմիջական ստուգման եղանակով: □

Երկակի եղանակով սահմանվում է **ֆիլտրի** գաղափարը (այսինքն՝ գումարը փոխարինվում է արտադրյալով, իսկ «$\leqslant$» նշանը՝ «$\geqslant$» նշանով): Ավելի ճիշտ, $F \subseteq Q$, $F \neq \emptyset$, ենթաբազմությունը կոչվում է $Q(+,\cdot)$ **կավարի ֆիլտր**, եթե այն բավարարում է հետևյալ երկու պայմաններին.
գ) $x, y \in F \longrightarrow x \cdot y \in F$;
դ) $t \in Q$, $z \in F$, $t \geqslant z \longrightarrow t \in F$:

Կավարի ֆիլտրը ենթակավար է: Միևնույն կավարի ցանկացած թվով ֆիլտրների հատումը նորից ֆիլտր է:

Լեմմ 20.16: *Որպեսզի ոչ դատարկ $F \subseteq Q$ ենթաբազմությունը լինի $Q(+,\cdot)$ կավարի ֆիլտր անհրաժեշտ է և բավարար, որ տեղի ունենա հետևյալ պայմանը՝*

$$x \cdot y \in F \longleftrightarrow x, y \in F,$$

որտեղ $x, y \in Q$:

Ապացուցում: Անմիջական ստուգման եղանակով: □

Օրինակ, եթե $a \in Q$ և

$$(a] = \{x \in Q \mid x \leqslant a\} \neq \emptyset,$$

ապա $(a] \trianglelefteq Q$: Այս իդեալը կոչվում է կավարի a տարրով ծնված **գլխավոր իդեալ**: Ակնհայտ է նաև, որ $Q \trianglelefteq Q$: Իսկ

$$[a) = \{x \in Q \mid x \geqslant a\} \neq \emptyset$$

ենթաբազմությունը կլինի Q կավարի ֆիլտր և այն կոչվում է a տարրով ծնված **գլխավոր ֆիլտր**:

Եթե $I \trianglelefteq Q$ և $I \neq Q$, ապա կգրենք $I \triangleleft Q$: $Q(+,\cdot)$ կավարի $I \trianglelefteq Q$ իդեալը կոչվում է **մաքսիմալ**, եթե $I \neq Q$ և գոյություն չունի այնպիսի $I' \trianglelefteq Q$ իդեալ, որ $I \triangleleft I' \triangleleft Q$: $Q(+,\cdot)$ կավարի $I \neq Q$ իդեալը կոչվում է **պարզ**, եթե այն բավարարում է հետևյալ պայմանին.

$$x \cdot y \in I \longrightarrow x \in I \quad \text{կամ} \quad y \in I,$$

որտեղ $x, y \in Q$: Երկակի եղանակով սահմանվում է **պարզ ֆիլտրի** գաղափարը: $Q(+,\cdot)$ կավարի $F \neq Q$ ֆիլտրը կոչվում է պարզ, եթե

$$x + y \in F \longrightarrow x \in F \quad \text{կամ} \quad y \in F,$$

որտեղ $x, y \in Q$:

Լեմմ 20.17: *Եթե $Q(+,\cdot)$-ը կավար է, իսկ $S \subseteq Q$, $S \neq \emptyset$, ապա*

$$(S] = \{x \in Q \mid \exists s_1, \ldots, s_k \in S,\ x \leqslant s_1 + \cdots + s_k\} \subseteq Q$$

ենթաբազմությունը կլինի $Q(+,\cdot)$ կավարի իդեալ, որը կոչվում է S-ով ծնված իդեալ: $(S]$ իդեալը կպարունակի S-ը և կլինի ընկած $Q(+,\cdot)$-ի բոլոր այն իդեալների մեջ, որոնք պարունակում են S-ը, այսինքն՝ $(S]$ իդեալը հանդիսանում է S-ը պարունակող $Q(+,\cdot)$-ի ամենափոքր իդեալը:

Ապացույց: Անմիջական ստուգման եղանակով: $\square$

Լեմմ 20.18: *$Q(+,\cdot)$ կավարի բոլոր իդեալների*

$$I(Q) = \{I \subseteq Q \mid I \trianglelefteq Q\} \neq \emptyset$$

բազմությունը կլինի կավար՝ հետևյալ գործողությունների նկատմամբ.

$$I_1 + I_2 = (I_1 \cup I_2] \trianglelefteq Q,$$

$$I_1 \cdot I_2 = I_1 \cap I_2 \trianglelefteq Q :$$

Ապացուցում: $I(Q)$ բազմությունը կավարածև կարգավորված բազմություն է` տեսա-բազմային ներդրման նկատմամբ, որտեղ

$$\sup\{I_1, I_2\} = (I_1 \cup I_2],$$

$$\inf\{I_1, I_2\} = I_1 \cap I_2 : \qquad \square$$

Թեորեմ 20.13: *Եթե $Q(+,\cdot)$-ը բաշխական կավար է, ապա նրա իդեալների $I(Q)$ բազմությունը ևս կլինի բաշխական կավար: Ըստ որում $x \to (x]$ արտապատկերման միջոցով Q բաշխական կավարը ներդրվում է $I(Q)$ բաշխական կավարի մեջ:*

Ապացուցում: Բավական է նկատել (լեմմ 20.4), որ եթե $I_1, I_2, I_3 \in I(Q)$, ապա

$$I_1 \cap (I_2 + I_3) \subseteq I_2 + (I_1 \cap I_3)$$

և $(x] \cap (y] = (xy]$, $(x] + (y] = (x + y]$ ցանկացած $x, y \in Q$ տարրերի համար: $\square$

Դժվար չէ նաև նկատել, որ բաշխական կավարի դեպքում իդեալների գումարը որոշվում է սովորական եղանակով`

$$I_1 + I_2 = \{x + y \,|\, x \in I_1, y \in I_2\} :$$

Թեորեմ 20.14: *Բաշխական կավարի յուրաքանչյուր մաքսիմալ իդեալ պարզ իդեալ է:*

Ապացուցում: Դիցուք $Q(+,\cdot)$-ը բաշխական կավար է, իսկ $I \trianglelefteq Q$ իդեալը մաքսիմալ է: Դիցուք $x \cdot y \in I$, բայց $x \notin I$: Դիտարկենք $I' = (\{x\} \cup I] \trianglelefteq Q$ իդեալը: Քանի որ I-ն մաքսիմալ իդեալ է և $I \triangleleft I'$, ապա $I' = Q$: Հետևաբար, $y \in I'$ և $y \leqslant s_1 + \cdots + s_k$, որտեղ $s_i \in \{x\} \cup I$, $i = 1, \ldots, k$: Հնարավոր է երեք դեպք.
1) $s_1, \ldots, s_k \in I$ և $y \leqslant s_1 + \cdots + s_k = s \in I$, ուստի $y \in I$;
2) $s_i = x$ որևէ i ճշիչի դեպքում և $s_j \neq x$ որևէ j ճշիչի համար ($i \neq j$): Այս դեպքում, $y \leqslant x + s$, որտեղ $s \in I$: Հետևաբար, $y = y(x+s) = yx + ys \in I$, որովհետև $yx \in I$, $ys \in I$ (քանի որ $ys \leqslant s \in I$):
3) $s_i = x$ բոլոր i ճշիչների համար: Հետևաբար, $y \leqslant x$ և

$$y = yx \in I : \qquad \square$$

Հետևություն 20.13: *Որպեսզի Բուլյան հանրահաշվի իդեալը լինի մաքսիմալ անհրաժեշտ է և բավարար, որ այն լինի պարզ իդեալ:*

Ապացուցում: Անհրաժեշտությունը բխում է նախորդ թեորեմից: Ապացուցենք *բավարարությունը*: Դիցուք I-ն պարզ իդեալ է $Q(+,\cdot)$ բուլյան հանրահաշվի համար: Եթե $a \notin I$, ապա $a' \in I$, քանի որ $a \cdot a' = 0 \in I$: Ուստի, եթե $I \lhd J \unlhd Q$, ապա J-ն կպարունակի որևէ $a \notin I$ և $a' \in I$ տարրերը: Հետևաբար, $1 = a + a' \in J$ և $J = Q$: □

Հետևություն 20.14: *Բուլյան լրացումների գոյության պայմանին բավարարող ցանկացած սահմանափակ կավարի յուրաքանչյուր պարզ իդեալ նաև մաքսիմալ իդեալ է:* □

Հետևություն 20.15: *Եթե I-ն $Q(+,\cdot)$ բուլյան հանրահաշվի մաքսիմալ իդեալ է, ապա ցանկացած $x \in Q$ տարրի համար կամ $x \in I$ կամ $x' \in I$: Ըստ որում, այս երկու ներդրումները միասին տեղի ունենալ չեն կարող:*

Ապացուցում: Քանի որ բուլյան հանրահաշվի մաքսիմալ իդեալը նաև պարզ է, ապա

$$x \cdot x' = 0 \in I \longrightarrow x \in I \quad \text{կամ} \quad x' \in I :$$

Եթե միաժամանակ $x \in I$ և $x' \in I$, ապա կունենանք՝ $1 = x + x' \in I$ և $I = Q$: Հակասություն: □

20.8. Բաշխական կավարի և բուլյան հանրահաշվի ներկայացումը ենթաբազմություններով: Բուլյան հանրահաշվի ներկայացումը տոպոլոգիական տարածության բաց-փակ բազմություններով

Հետևյալ արդյունքը կոչվում է պարզ իդեալների թեորեմ:

Թեորեմ 20.15 (Բիրկհոֆ, Ստոուն): *Դիցուք $Q(+,\cdot)$ -ը բաշխական կավար է, I-ն Q-ի իդեալ է, իսկ F-ը Q-ի ֆիլտր է, ըստ որում, $I \cap F = \emptyset$: Այդ դեպքում, գոյություն կունենա Q-ի այնպիսի P պարզ իդեալ, որ $I \subseteq P$ և $P \cap F = \emptyset$, այսինքն՝ P-ն պարունակում է I-ն և չի հատվում F-ի հետ:*

Ապացուցում: Դիցուք J-ն Q-ի բոլոր այն իդեալների բազմությունն է, որոնք պարունակում են I-ն և չեն հատվում F-ի հետ: J-ն դատարկ չէ, որովհետև պարունակում է I-ն: Ցոռնի աքսիոմի համաձայն, J-ն պարունակում է նշված պայմանին բավարարող P մաքսիմալ իդեալ (տարր): Բավական է այժմ ապացուցել, որ P-ն պարզ իդեալ է: Դիցուք $a \cdot b \in P$, բայց $a \notin P$ և $b \notin P$: P-ի մաքսիմալության պատճառով $P + (a]$ և $P + (b]$ իդեալները կհատվեն F-ի հետ, այսինքն՝

$$(P + (a]) \cap F \neq \emptyset, \qquad (P + (b]) \cap F \neq \emptyset :$$

Հետևաբար, գոյություն կունենան այնպիսի $p, q \in P$ տարրեր, որ $p + a \in F$ և $q + b \in F$: Դիցուք $x = (p + a)(q + b)$: Ֆիլտրի սահմանման համաձայն, կունենանք՝ $x \in F$, իսկ քանի որ $x = pq + pb + aq + ab$, ապա $x \in P$: Այսպիսով, $x \in P \cap F$ և $P \cap F \neq \emptyset$: Հակասություն: □

Հետևություն 20.16*: Դիցուք $Q(+, \cdot)$-ը բաշխական կավար է, I-ն Q-ի իդեալ է և $a \in Q \setminus I$: Այդ դեպքում, գոյություն կունենա Q-ի այնպիսի P պարզ իդեալ, որ $I \subseteq P$ և $a \notin P$:*

Ապացուցում: Բխում է նախորդ թեորեմից $F = [a)$ դեպքում, որովհետև $a \notin I$ պայմանի դեպքում կունենանք՝ $I \cap [a) = \emptyset$: □

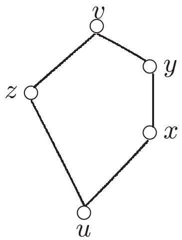
Հետևություն 20.17*: Բաշխական կավարի յուրաքանչյուր (իրենից տարբեր) իդեալ հավասար է իրեն պարունակող բոլոր պարզ իդեալների հատմանը:* □

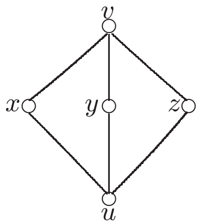
$Q(+, \cdot)$ կավարի I իդեալը կոչվում է $a, b \in Q$, $a \neq b$, տարրերին **անջատող**, եթե I-ն պարունակում է a, b տարրերից մեկին, բայց չի պարունակում մյուսին:

Հետևություն 20.18*: Որպեսզի $Q(+, \cdot)$ կավարը լինի բաշխական անհրաժեշտ է և բավարար, որ Q-ի ցանկացած $x \neq y$ տարրերի համար գոյություն ունենա դրանց անջատող Q-ի պարզ իդեալ:*

Ապացուցում: Անհրաժեշտություն: Եթե $Q(+, \cdot)$-ը բաշխական կավար է և $x \neq y$, ապա $x \leqslant y$ և $y \leqslant x$ պայմանները միաժամանակ տեղի ունենալ չեն կարող: Հետևաբար, կամ $(x] \cap [y) = \emptyset$ կամ $[x) \cap (y] = \emptyset$: Մնում է օգտվել նախորդ թեորեմից:

Բավարարություն: Եթե $Q(+, \cdot)$-ը բաշխական չէ, ապա համաձայն կավարի բաշխականության Բիրկհոֆի հայտանիշի, Q-ն կպարունակի հետևյալ տեսքի ենթակավարներից որևէ մեկը.



,


:

Դիցուք P պարզ իդեալը պարունակում է x-ը: Քանի որ $y \cdot z = u < x$, ապա $y \cdot z \in P$ և, հետևաբար, $y \in P$ կամ $z \in P$: Եթե $z \in P$, ապա $v = x + z \in P$ և $y \in P$: Այսպիսով, յուրաքանչյուր P պարզ իդեալ, որը պարունակում է x-ը կպարունակի նաև $y \neq x$ տարրը: Հակասություն: $\square$

Պարզվում է բաշխական կավարները կարելի է ներկայացնել որպես տեսա-բազմային գործողություններով բազմությունների կավարներ: Համապատասխան դասական արդյունքը կոչվում է բաշխական կավարների ներկայացման վերաբերյալ Բիրկհոֆի թեորեմ և ունի հետևյալ տեսքը:

Թեորեմ 20.16 (Բիրկհոֆ): *Յուրաքանչյուր $Q(+,\cdot)$ բաշխական կավար իզոմորֆ է 2^J բաշխական կավարի որևէ ենթակավարի, այսինքն՝ յուրաքանչյուր $Q(+,\cdot)$ բաշխական կավար ներդրվում է 2^J բաշխական կավարի մեջ, որտեղ $J = J(Q)$-ն Q-ի բոլոր պարզ իդեալների բազմությունն է:*

Ապացուցում: Յուրաքանչյուր $x \in Q$ տարրի համար $\mathcal{P}(x)$-ով նշանակենք Q-ի բոլոր այն P պարզ իդեալների բազմությունը, որոնք չեն պարունակում x-ը: Այնուհետև,

$$P \in \mathcal{P}(x \cdot y) \longleftrightarrow x \cdot y \notin P \longleftrightarrow x \notin P,\ \ y \notin P \longleftrightarrow P \in \mathcal{P}(x) \cap \mathcal{P}(y),$$

$$P \in \mathcal{P}(x + y) \longleftrightarrow x + y \notin P \longleftrightarrow x \notin P \text{ կամ } y \notin P \longleftrightarrow P \in \mathcal{P}(x) \cup \mathcal{P}(y),$$

այսինքն՝

$$\mathcal{P}(x \cdot y) = \mathcal{P}(x) \cap \mathcal{P}(y),$$
$$\mathcal{P}(x + y) = \mathcal{P}(x) \cup \mathcal{P}(y) :$$

Հետևաբար,

$$\mathcal{P} = \{\mathcal{P}(x) \mid x \in Q\} \subseteq 2^J$$

ենթաբազմությունը 2^J կավարի ենթակավար է: Այժմ $\Phi(x) = \mathcal{P}(x)$ բանաձևով սահմանելով $\Phi : Q \to \mathcal{P}$ արտապատկերումը, նկատենք, որ Φ-ի ինյեկտիվությունը բխում է նախորդ հետևությունից, իսկ նրա իզոմորֆիզմ լինելու մնացած պայմաններն ակնհայտ են: $\square$

Դիցուք այժմ $Q(+,\cdot)$-ը բուլյան հանրահաշիվ է, իսկ $Q' \subseteq Q$, $Q' \neq \emptyset$: Q'-ը կոչվում է Q բուլյան հանրահաշվի ենթահանրահաշիվ, եթե Q'-ը պարունակում է իր ցանկացած տարրի բուլյան լրացումը և իր ցանկացած երկու տարրերի գումարը և արտադրյալը: Նախորդ թեորեմի նման արդյունք տեղի ունի նաև բուլյան հանրահաշիվների համար և կոչվում է բուլյան հանրահաշիվների ներկայացման վերաբերյալ Ստոունի թեորեմ:

Թեորեմ 20.17 (Ստոուն): *Յուրաքանչյուր Q բուլյան հանրահաշիվ իզոմորֆ է 2^J բուլյան հանրահաշվի որևէ ենթահանրահաշվի, այսինքն՝ յուրաքանչյուր Q բուլյան հանրահաշիվ ներդրվում է 2^J բուլյան հանրահաշվի մեջ, որտեղ $J = J(Q)$-ն Q-ի բոլոր պարզ իդեալների բազմությունն է:*

Ապացուցում: Նախորդ թեորեմի ապացուցմանը բավական է այժմ ավելացնել հետևյալ հավասարությունը՝

$$\mathcal{P}(x') = (\mathcal{P}(x))' :$$

Իրոք, եթե P-ն Q բուլյան հանրահաշվի պարզ իդեալ է, ապա

$$x \in P \longleftrightarrow x' \notin P :$$

Այնուհետև,

$$P \in \mathcal{P}(x') \longleftrightarrow x' \notin P \longleftrightarrow x \in P \longleftrightarrow P \notin \mathcal{P}(x) \longleftrightarrow P \in J\backslash\mathcal{P}(x) = (\mathcal{P}(x))' :$$

Հետևաբար, $(\mathcal{P}(x))' = \mathcal{P}(x')$ և

$$\mathcal{P} = \{\mathcal{P}(x) \mid x \in Q\} \subseteq 2^J$$

ենթաբազմությունը այս դեպքում կլինի 2^J բուլյան հանրահաշվի ենթահանրահաշիվ, իսկ $\Phi : x \to \mathcal{P}(x)$ արտապատկերումը կլինի Q և $\mathcal{P}$ բուլյան հանրահաշիվների իզոմորֆիզմ: $\square$

Սահմանված Φ արտապատկերման $\Phi(Q)$ պատկերի լրացուցիչ հատկությունները (ավելի ճիշտ տոպոլոգիական հատկությունները) պարզաբանելու համար ներմուծենք հետևյալ հասկացությունները:

Դիցուք տրված է (X,τ) տոպոլոգիական տարածությունը: $A \subseteq X$ ենթաբազմություն կոչվում է **բաց-փակ**, եթե այն բաց և փակ բազմություն է տրված տոպոլոգիական տարածության համար: (X,τ) տոպոլոգիական տարածությունը կոչվում է **լիովին չկապակցված**, եթե նրա յուրաքանչյուր բաց բազմություն հավասար է որոշ քանակի բաց-փակ բազմությունների միավորմանը: (X,τ) տոպոլոգիական տարածությունը կոչվում է **բուլյան** կամ **ստոունյան տարածություն**, եթե այն հաուսդորֆյան է, կոմպակտ է և լիովին չկապակցված է:

Թեորեմ 20.18 (Ստոուն): *Յուրաքանչյուր $Q(+,\cdot)$ բուլյան հանրահաշիվ իզոմորֆ է որևէ ստոունյան տոպոլոգիական տարածության բոլոր բաց-փակ բազմությունների բուլյան հանրահաշվին:*

Ապացուցում: Ինչպես և նախորդ երկու թեորեմներում, J-ով կնշանակենք Q-ի բոլոր պարզ իդեալների բազմությունը, իսկ

$$\mathcal{P}(x) = \{P \in J \mid x \notin P\} \subseteq J:$$

Նախ նկատենք, որ $\mathcal{P}(x)$ բազմությունները փակ են վերջավոր տեսա-բազմային հատումների նկատմամբ, որովհետև

$$\mathcal{P}(x_1) \cap \mathcal{P}(x_2) \cap \cdots \cap \mathcal{P}(x_n) = \mathcal{P}(x_1 \cdot x_2 \cdots x_n):$$

Սահմանենք որոնելի (X,τ) տոպոլոգիական տարածությունը հետևյալ կերպ: Վերցնենք $X = J$, իսկ τ տոպոլոգիան կառուցենք $\mathcal{P}(x)$ տեսքի բազմություններից և դրանց բոլոր հնարավոր տեսա-բազմային միավորումներից, այսինքն՝ $\mathcal{P} = \{\mathcal{P}(x) \mid x \in Q\}$ բազմությունը հենք է կառուցված տոպոլոգիական տարածության համար: Այժմ ապացուցենք, որ ստացված տոպոլոգիական տարածությունը լիովին չկապակցված է, հաուսդորֆյան է, կոմպակտ է և դրա բաց-փակ բազմությունների բուլյան հանրահաշվին իզոմորֆ է սկզբնական բուլյան հանրահաշիվը:

1) Յուրաքանչյուր բաց բազմություն հավասար է $\mathcal{P}(x)$ տեսքի բազմությունների տեսա-բազմային միավորմանը, իսկ $\mathcal{P}(x)$ տեսքի յուրաքանչյուր բազմություն բաց է և փակ, որովհետև $\mathcal{P}(x)$-ի լրացումը բաց է՝ $(\mathcal{P}(x))' = \mathcal{P}(x')$: Հետևաբար, սահմանված տոպոլոգիական տարածությունը լիովին չկապակցված է:

2) Դիցուք $P_1, P_2 \in J$ և $P_1 \neq P_2$: Դիցուք $x \in P_1$, $x \notin P_2$: Հետևաբար, $P_2 \in \mathcal{P}(x)$ և $P_1 \notin \mathcal{P}(x)$, որտեղից $P_1 \in \mathcal{P}(x')$:

Այսպիսով, $P_1 \in \mathcal{P}(x')$, $P_2 \in \mathcal{P}(x)$ և $\mathcal{P}(x) \cap \mathcal{P}(x') = \emptyset$, այսինքն՝ տոպոլոգիական տարածության ցանկացած երկու տարբեր կետերի համար գտել ենք այդ կետերը պարունակող և միմյանց հետ չհատվող բաց բազմություններ: Հետևաբար, այն հաուսդորֆյան է:

3) Ապացուցենք տոպոլոգիական տարածության կոմպակտությունը: Դիցուք $J = \bigcup\limits_{i\in I} \mathcal{P}(x_i)$ և դիցուք $\Delta = (K]$, որտեղ $K = \{x_i \mid i \in I\}$: Եթե $\Delta \neq Q$, ապա, համաձայն հետևություն 20.16-ի, գոյություն կունենա Q-ի այնպիսի P_0 պարզ իդեալ, որ $\Delta \subseteq P_0$: Մյուս կողմից, քանի որ $x_i \in \Delta$, ապա $x_i \in P_0$, $i \in I$: Հետևաբար, $P_0 \notin \mathcal{P}(x_i)$, $i \in I$ և $P_0 \notin \bigcup\limits_{i\in I} \mathcal{P}(x_i) = J$: Մի կողմից $P_0 \in J$, իսկ մյուս կողմից՝ $P_0 \notin J$: Հակասություն:

Այսպիսով, $\Delta = Q$ և $1 \in \Delta$, որտեղ 1-ը Q բուլյան հանրահաշվի մեծագույն տարրն է: Ուստի, գոյություն կունենան վերջավոր թվով $x_1, \ldots, x_n \in K$ տարրեր (լեմմ 20.17), որ $1 = x_1 + \cdots + x_n$: Հետևաբար,

$$\mathcal{P}(x_1) \cup \cdots \cup \mathcal{P}(x_n) = \mathcal{P}(x_1 + \cdots + x_n) = \mathcal{P}(1) = J :$$

4) Պարզվում է նախորդ երկու թեորեմներում կառուցված իզոմորֆիզմը կլինի հենց այստեղ պահանջվող իզոմորֆիզմը: Որպեսզի $\Phi : x \to \mathcal{P}(x)$ արտապատկերումը լինի պահանջվող արտապատկերումը, բավական է միայն այստեղ ավելացնել, որ կառուցված տոպոլոգիական տարածության յուրաքանչյուր բաց-փակ բազմություն ունի $\mathcal{P}(x)$ տեսքը: Իրոք, դիցուք M-ը բաց-փակ բազմություն է: Քանի որ M-ը բաց է, ապա $M = \bigcup\limits_{i\in I} \mathcal{P}(x_i)$ և քանի որ M-ը փակ բազմություն է, իսկ տոպոլոգիական տարածությունը կոմպակտ է, ապա M-ը ևս կլինի կոմպակտ տոպոլոգիական (ենթա)տարածություն: Հետևաբար, գոյություն կունենան վերջավոր թվով $x_1, \ldots, x_n$ տարրեր, որ $M = \mathcal{P}(x_1) \cup \cdots \cup \mathcal{P}(x_n) = \mathcal{P}(x_1 + \cdots + x_n)$: □

Q բուլյան հանրահաշվին համապատասխան կառուցված (J, τ) տոպոլոգիական տարածությունը կոչվում է նաև Q-ի **երկակի** կամ **դուալ** տարածություն:

Նմանատիպ արդյունք տեղի ունի նաև սահմանափակ բաշխական կավարների դեպքում:

20.9. Դե Մորգանի հանրահաշիվներ

$Q(+,\cdot)$ կավարը կոչվում է **Դե Մորգանի հանրահաշիվ**, եթե այն բաշխական է, սահմանափակ է և օժտված Դե Մորգանի լրացումներով, այսինքն՝ յուրաքանչյուր $x \in Q$ տարրի համար գոյություն ունի այնպիսի $\overline{x} \in Q$ տարր, որ $\overline{(\overline{x})} = x$ և տեղի ունեն Դե Մորգանի նույնությունները՝

$$\overline{x+y} = \overline{x} \cdot \overline{y},$$

$$\overline{x \cdot y} = \overline{x} + \overline{y}$$

ցանկացած $x, y \in Q$ տարրերի համար: Այդ դեպքում, $\overline{x}$-ը կոչվում է x-ի **Դե Մորգանի լրացում**: Օրինակ, X բազմության բոլոր ոչ հստակ ենթաբազմությունների դասը կլինի Դե Մորգանի հանրահաշիվ: Դժվար չէ նկատել, որ երկու տարրանի Դե Մորգանի հանրահաշիվը բուլյան հանրահաշիվ է, որը նշանակվում է $\mathbf{2}$-ով: Սակայն $n \geqslant 3$ դեպքում գոյություն ունի n-տարրանի Դե Մորգանի հանրահաշիվ, որը բուլյան հանրահաշիվ չէ: Օրինակ, եթե $Q = \{1, 2, 3, \ldots, n\}$, $x + y = \max\{x, y\}$, $x \cdot y = \min\{x, y\}$, $\overline{x} = n + 1 - x$, ապա ստացվող $Q(+,\cdot)$ Դե Մորգանի հանրահաշիվը կլինի այդպիսին: Ի տարբերություն բուլյան հանրահաշվի, Դե Մորգանի հանրահաշվում $x \to \overline{x}$ արտապատկերումը միարժեքորեն չի որոշվում, այսինքն՝ տարրի Դե Մորգանի լրացումը միարժեքորեն չի որոշվում (տես ներքևում զետեղված 4-տարրանի Դե Մորգանի հանրահաշվի օրինակը, որն այդ հատկությամբ օժտված ամենափոքր Դե Մորգանի հանրահաշվի օրինակն է): Դե Մորգանի նույնություններից բխում է, որ յուրաքանչյուր Դե Մորգանի հանրահաշվում՝ $\overline{0} = 1$, $\overline{1} = 0$:

$Q(\leqslant)$ կավարածև կարգավորված բազմությունը կոչվում է Դե Մորգանի կավարածև կարգավորված բազմություն, եթե դրա համապատասխան $Q^{\wedge}$ կավարը Դե Մորգանի համրահաշիվ է: Ակնհայտ է, որ եթե $Q(\leqslant)$ զույգը Դե Մորգանի կավարածև կարգավորված բազմությունը, ապա այդպիսին կլինի նաև $Q(\leqslant^{-1})$ կավարածև կարգավորված բազմությունը:

Թեորեմ 20.5-ի պնդումը մնում է ուժի մեջ նաև Դե Մորգանի հանրահաշիվների դեպքում:

Եթե $Q(+,\cdot)$-ը և $Q^*(+,\cdot)$-ը Դե Մորգանի հանրահաշիվներ են, ապա $\varphi : Q \to Q^*$ արտապատկերումը կոչվում է **նմանաձևություն** կամ **հոմոմորֆ** արտապատկերում (**հոմոմորֆություն**, **հոմոմորֆիզմ**)՝ $Q(+,\cdot)$

Դե Մորգանի հանրահաշվից $Q^*(+,\cdot)$ Դե Մորգանի հանրահաշվի մեջ, եթե տեղի ունեն հետևյալ պայմանները.

$$\varphi(x+y) = \varphi x + \varphi y,$$

$$\varphi(x \cdot y) = \varphi x \cdot \varphi y$$

$$\varphi(\overline{x}) = \overline{\varphi x}$$

ցանկացած $x, y \in Q$ տարրերի համար: Եթե այդ դեպքում φ արտապատկերումը փոխմիարժեք (բիեկտիվ) է, ապա φ-ն կոչվում է **նույնաձևություն** կամ **իզոմորֆ** արտապատկերում (իզոմորֆություն, իզոմորֆիզմ): Երկու $Q(+,\cdot)$ և $Q^*(+,\cdot)$ Դե Մորգանի հանրահաշիվներ կոչվում են **իզոմորֆ** կամ **նույնաձև** և գրվում է $Q \simeq Q^*$ կամ $Q \cong Q^*$, եթե գոյություն ունի որևէ $\varphi : Q \to Q^*$ իզոմորֆ արտապատկերում: Սահմանված «$\simeq$» հարաբերությունը կոչվում է **Դե Մորգանի հանրահաշիվների իզոմորֆության** (կամ **նույնաձևության**) **հարաբերություն**: Հեշտությամբ ապացուցվում է, որ երկու (հետևաբար և վերջավոր թվով) հոմոմորֆիզմների (իզոմորֆիզմների) արտադրյալը նորից հոմոմորֆիզմ (իզոմորֆիզմ) է: Եթե $\varphi : Q \to Q^*$ արտապատկերումը նույնաձևություն է Դե Մորգանի հանրահաշիվների միջև, ապա այդպիսին կլինի նաև $\varphi^{-1} : Q^* \to Q$ արտապատկերումը:

Լեմմ 20.19: *Դե Մորգանի հանրահաշիվների իզոմորֆության «$\simeq$» հարաբերությունը բավարարում է համարժեքության հարաբերության սահմանման բոլոր երեք պայմաններին:* □

Կասենք, որ $Q(+,\cdot)$ Դե Մորգանի հանրահաշիվը **ներդրվում է** $Q^*(+,\cdot)$ Դե Մորգանի հանրահաշվի մեջ, եթե գոյություն ունի որևէ $\varphi : Q \to Q^*$ ներդրող (ինյեկտիվ) և հոմոմորֆ արտապատկերում:

Եթե $Q(+,\cdot)$-ը սահմանափակ բաշխական կավար է, ապա $Q \times Q$ դեկարտյան արտադրյալը վերածվում է Դե Մորգանի հանրահաշվի՝ հետևյալ գործողությունների նկատմամբ.

$$(x,y) + (x',y') = (x+x', y \cdot y'),$$

$$(x,y) \cdot (x',y') = (x \cdot x', y + y'),$$

$$\overline{(x,y)} = (y,x) :$$

Թեորեմ 20.19: *Յուրաքանչյուր* $\mathcal{D}(+,\cdot)$ *Դե Մորգանի հանրահաշվի համար գոյություն ունի այնպիսի* $Q(+,\cdot)$ *սահմանափակ բաշխական կավար, որ* $\mathcal{D}(+,\cdot)$*-ը ներդրվում է* $Q \times Q$ *Դե Մորգանի հանրահաշվի մեջ:* □

Դե Մորգանի հանրահաշվի a տարրը կոչվում է անշարժ կետ, եթե $\overline{a} = a$:

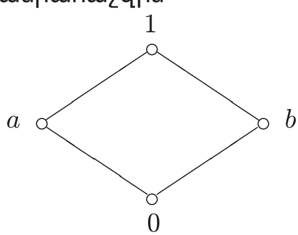
Երեք տարրանի Դե Մորգանի հանրահաշիվը օժտված է մեկ անշարժ կետով և իզոմորֆ է հետևյալ Դե Մորգանի հանրահաշվին՝

,

որտեղ $\overline{0} = 1$, $\overline{1} = 0$ և $\overline{a} = a$. Այս երեք տարրանի Դե Մորգանի հանրահաշիվը նշանակենք $\mathbf{3}$-ով: Չորս տարրանի Դե Մորգանի հանրահաշիվը կամ իզոմորֆ է չորս տարրանի բուլյան հանրահաշվին, կամ իզոմորֆ է հետևյալ Դե Մորգանի հանրահաշվին՝

,

որտեղ $\overline{0} = 1$, $\overline{1} = 0$, $\overline{a} = b$, $\overline{b} = a$, կամ իզոմորֆ է երկու անշարժ կետով հետևյալ Դե Մորգանի հանրահաշվին՝



,

որտեղ $\overline{a} = a$, $\overline{b} = b$, $\overline{0} = 1$, $\overline{1} = 0$: Այս վերջին Դե Մորգանի հանրահաշիվը կնշանակենք $\mathbf{4}$-ով: Հետևաբար, երկու անշարժ կետով չորս տարրանի Դե Մորգանի հանրահաշիվը իզոմորֆ է $\mathbf{4}$-ին:

Դիցուք X-ը կամայական ոչ դատարկ բազմություն է, իսկ $L(+,\cdot)$-ը կամայական Դե Մորգանի հանրահաշիվ է: L^X-ով նշանակենք $X \to L$ տեսքի բոլոր արտապատկերումների բազմությունը: Այս բազմությունը վերածվում է Դե Մորգանի հանրահաշվի՝ հետևյալ գործողությունների նկատմամբ.

$$(f \vee g)x = f(x) + g(x),$$
$$(f \wedge g)x = f(x) \cdot g(x),$$
$$\left(\overline{f}\right) x = \overline{f(x)} :$$

Մասնավորապես, եթե $L = [0,1]$, որտեղ $x + y = \max\{x,y\}$, $x \cdot y = \min\{x,y\}$, $\overline{x} = 1 - x$, ապա $L(+,\cdot)$-ը կլինի Դե Մորգանի հանրահաշիվ, իսկ L^X-ը այդ դեպքում կլինի X բազմության բոլոր ոչ հստակ ենթաբազմությունների Դե Մորգանի հանրահաշիվը: Այդ պատճառով, եթե $L(+,\cdot)$-ը կամայական Դե Մորգանի հանրահաշիվ է, ապա $X \to L$ տեսքի արտապատկերումները կոչվում են նաև ընդհանրացված ոչ հստակ ենթաբազմություններ կամ ոչ հստակ L-ենթաբազմություններ: Հետևյալ նկարագրության մեջ որպես $L(+,\cdot)$ Դե Մորգանի հանրահաշիվ վերցվում է $\mathbf{4}$-ը:

Թեորեմ 20.20: *Յուրաքանչյուր $\mathcal{D}(+,\cdot)$ Դե Մորգանի հանրահաշվի համար գոյություն ունի այնպիսի X բազմություն, որ $\mathcal{D}(+,\cdot)$-ը ներդրվում է $\mathbf{4}^X$ Դե Մորգանի հանրահաշվի մեջ:* □

$L(+,\cdot)$ Դե Մորգանի հանրահաշիվը կոչվում է **Քլինիի հանրահաշիվ** (S. C. Kleene), եթե $x \cdot \overline{x} \leqslant y + \overline{y}$ ցանկացած $x, y \in L$ տարրերի համար, այսինքն՝ տեղի ունի հետևյալ նույնությունը.

$$x \cdot \overline{x} \cdot (y + \overline{y}) = x \cdot \overline{x};$$

Օրինակ $\mathbf{3}$-ը Քլինիի հանրահաշիվ է, իսկ $\mathbf{4}$-ը՝ ոչ: Ցանկացած բուլյան հանրահաշիվ Քլինիի հանրահաշիվ է:

$L(+,\cdot)$ Դե Մորգանի (Քլինիի) հանրահաշիվը կոչվում է **համաձայնեցված անշարժ կետով Դե Մորգանի (Քլինիի) հանրահաշիվ**, եթե այն ունի այնպիսի $a \in L$ անշարժ կետ, որը բավարարում է հետևյալ նույնությանը՝

$$x + \overline{x} + a = x + \overline{x} :$$

Օրինակ, $\mathbf{3}$-ը հանդիսանում է համաձայնեցված անշարժ կետով Քլինիի հանրահաշիվ; Հետևաբար, այդպիսին կլինի նաև $\mathbf{3}^X$ Դե Մորգանի հանրահաշիվը, ցանկացած $X \neq \emptyset$ բազմության համար:

Թեորեմ 20.21*: 1) Համաձայնեցված անշարժ կետով վերջավոր Դե Մորգանի հանրահաշվի տարրերի թիվը հավասար է կենտ թվի: 2) Եվ հակառակը, յուրաքանչյուր n կենտ թվի համար գոյություն ունի n տարրանի համաձայնեցված անշարժ կետով Դե Մորգանի հանրահաշիվ:*

Ապացուցում: Նախ նկատենք, որ եթե Դե Մորգանի հանրահաշվում $x \leqslant y$, ապա $\overline{y} \leqslant \overline{x}$, որովհետև

$$x \leqslant y \longrightarrow x + y = y \longrightarrow \overline{x+y} = \overline{y} \longrightarrow \overline{x} \cdot \overline{y} = \overline{y} \longrightarrow \overline{y} \leqslant \overline{x} :$$

Ըստ սահմանման, համաձայնեցված անշարժ կետով Դե Մորգանի հանրահաշիվը օժտված է գոնե մեկ անշարժ կետով: Դիցուք $K(+,\cdot)$-ը համաձայնեցված անշարժ կետով Դե Մորգանի հանրահաշիվ է՝ $a \in K$ անշարժ կետով և դիցուք $b \in K$ տարրը ևս անշարժ կետ է, այսինքն՝ $\overline{b} = b$: Քանի որ՝

$$b + a = b + b + a = b + \overline{b} + a = b + \overline{b} = b + b = b\,,$$

ապա $a \leqslant b$: Հետևաբար, $\overline{a} \geqslant \overline{b}$, այսինքն՝ $a \geqslant b$: Ուստի, $a = b$:

1) Համաձայնեցված անշարժ կետով Դե Մորգանի վերջավոր $K(+,\cdot)$ հանրահաշվի վերջավոր K բազմությունը կարելի է ներկայացնել $\{x, \overline{x}\}$ չհատվող զույգերի միավորումով, որտեղ միայն $\{a, \overline{a}\}$ զույգն է մեկ տարրանի, որովհետև a-ն միակ անշարժ կետն է:

2) Բխում է վերոհիշյալ n-տարրանի Դե Մորգանի հանրահաշվի օրինակից, երբ n-ը կենտ թիվ է: □

Թեորեմ 20.22*: Յուրաքանչյուր $\mathcal{K}(+,\cdot)$ Քլինիի հանրահաշվի համար գոյություն ունի այնպիսի X բազմություն, որ $\mathcal{K}(+,\cdot)$-ը ներդրվում է $\mathbf{3}^X$ Քլինիի հանրահաշվի մեջ:* □

Եթե $L(+,\cdot)$ Դե Մորգանի հանրահաշիվը բուլյան հանրահաշիվ է, ապա L^X Դե Մորգանի հանրահաշիվը նույնպես կլինի բուլյան հանրահաշիվ:

20.10. σ-կավարներ և բուլյան σ-հանրահաշիվներ

$Q(+,\cdot)$ կավարը կոչվում է σ-**կավար**, եթե այն օժտված է նաև իր ցանկացած հաշվելի $X \subseteq Q$ ենթաբազմության վերին և ստորին ճշգրիտ եզրերով:

$Q(+,\cdot)$ բուլյան հանրահաշիվը կոչվում է **բուլյան** σ-**հանրահաշիվ** (կամ երբեմն **բորելյան հանրահաշիվ**), եթե այն նաև σ-կավար է:

Եթե $Q(+,\cdot)$-ը և $Q^*(+,\cdot)$-ը բուլյան σ-հանրահաշիվներ են, ապա $\varphi : Q \to Q^*$ արտապատկերումը կոչվում է դրանց σ-**հոմոմորֆ** արտապատկերում (σ-հոմոմորֆություն, σ-**հոմոմորֆիզմ**), եթե φ-ն հոմոմորֆ արտապատկերում է $Q(+,\cdot)$ և $Q^*(+,\cdot)$ բուլյան հանրահաշիվների միջև և

$$\sup \varphi(X) = \varphi(\sup X), \quad \inf \varphi(X) = \varphi(\inf X)$$

կամայական հաշվելի $X \subseteq Q$ ենթաբազմության համար: $Q^*(+,\cdot)$ բուլյան σ-հանրահաշիվը կոչվում է $Q(+,\cdot)$ բուլյան σ-հանրահաշվի σ-հոմոմորֆ պատկեր, եթե գոյություն ունի այնպիսի $\varphi : Q \to Q^*$ σ-հոմոմորֆ արտապատկերում, որը նաև վերադրող (սյուրեկտիվ) արտապատկերում է:

Թեորեմ 20.23 (Լյումիս, Սիկորսկի): *Յանկացած բուլյան σ-հանրահաշիվ հանդիսանում է բազմությունների որևէ σ-հանրահաշվի σ-հոմոմորֆ պատկերը:* □

20.11. Կոնգրուենցիաներ: Հոմոմորֆիզմների թեորեմը կավարներում

Դիցուք $Q(+,\cdot)$-ը կավար է: Q բազմության «$\sim$» համարժեքությունը կոչվում է $Q(+,\cdot)$ կավարի **կոնգրուենցիա**, եթե տեղի ունի հետևյալ պայմանը՝

$$x \sim y, u \sim v \longrightarrow x + u \sim y + v, x \cdot u \sim y \cdot v,$$

որտեղ $x, y, u, v \in Q$: Բուլյան (Դե Մորգանի) հանրահաշվի դեպքում այս պայմանին ավելացվում է հետևյալ պայմանը՝

$$x \sim y \longrightarrow x' \sim y',$$

որտեղ x'-ը x-ի բուլյան (Դե Մորգանի) լրացումն է:

Օրինակ, զրոյական և միավոր համարժեքությունները ցանկացած կավարի կոնգրուենցիաներ են: Երեք տարրանի

կավարի $\{0, a, 1\}$ բազմության $\{0\}$, $\{a, 1\}$ տրոհմանը համապատասխանող համարժեքությունը կլինի կոնգրուենցիա:

Վերհիշենք $\varphi : Q \to Q'$ արտապատկերման $Ker(\varphi) \subseteq Q \times Q$ միջուկի սահմանումը`

$$(x, y) \in Ker(\varphi) \longleftrightarrow \varphi(x) = \varphi(y), \quad x, y \in Q,$$

որն ակնհայտորեն համարժեքություն է, որոշված Q բազմության վրա:

Լեմմ 20.20: *Եթե $\varphi : Q \to Q'$ արտապատկերումը հոմոմորֆիզմ է $Q(+, \cdot)$ կավարից $Q'(+, \cdot)$ կավարի մեջ, ապա նրա $Ker(\varphi)$ միջուկը կլինի $Q(+, \cdot)$ կավարի կոնգրուենցիա:*

Ապացուցում: Իրոք, եթե $Ker(\varphi) = (\sim)$ և $x \sim y$, $u \sim v$, ապա $\varphi(x) = \varphi(y)$ և $\varphi(u) = \varphi(v)$: Հետևաբար,

$$\varphi(x + u) = \varphi(x) + \varphi(u) = \varphi(y) + \varphi(v) = \varphi(y + v),$$

$$\varphi(x \cdot u) = \varphi(x) \cdot \varphi(u) = \varphi(y) \cdot \varphi(v) = \varphi(y \cdot v),$$

որտեղից $x + u \sim y + v$ և $x \cdot u \sim y \cdot v$: □

Նույն պնդումը տեղի ունի նաև բուլյան (Դե Մորգանի) հանրահաշիվների դեպքում:

Միևնույն կավարի կամ բուլյան (Դե Մորգանի) հանրահաշվի ցանկացած թվով կոնգրուենցիաների հատումը նորից կոնգրուենցիա է:

Եթե «$\sim$» համարժեքությունը $Q(+, \cdot)$ կավարի կոնգրուենցիա է, ապա

$$Q/_{\sim} = \{[a] \mid a \in Q\}$$

քանորդ-բազմության վրա (մեջ) կարելի է սահմանել գումարման և բազմապատկման հետևյալ գործողությունները`

$$[a] + [b] = [a + b],$$

$$[a] \cdot [b] = [a \cdot b],$$

որտեղ $a, b \in Q$: Նախ նկատենք, որ գործողության արդյունքները կախված չեն համարժեքության դասերում ներկայացուցիչների ընտրությունից: Իրոք, եթե $[x] = [y]$ և $[u] = [v]$, ապա $x \sim y$ և $u \sim v$: Հետևաբար, ըստ կոնգրուենցիայի սահմանման՝ $x + u \sim y + v$ և $x \cdot u \sim y \cdot v$, ուստի $[x + u] = [y + v]$ և $[x \cdot u] = [y \cdot v]$:

Ստանում ենք երկու գործողությամբ $Q/_{\sim}(+, \cdot)$ հանրահաշիվ, որը բավարարում է կավարի սահմանման բոլոր նույնություններին (աքսիոմներին): Այսպիսով, $Q/_{\sim}(+, \cdot)$-ը կավար է, որը և կոչվում է տրված $Q(+, \cdot)$ **կավարի քանորդ-կավար** կամ **ֆակտոր-կավար ըստ տրված «$\sim$» կոնգրուենցիայի**:

Եթե «$\sim$» համարժեքությունը $Q(+, \cdot)$ բուլյան (Դե Մորգանի) հանրահաշվի կոնգրուենցիա է, ապա $Q/_{\sim}(+, \cdot)$ ֆակտոր-կավարը կլինի բուլյան (Դե Մորգանի) հանրահաշիվ, որտեղ

$$[a]' = [a'], \qquad a \in Q :$$

Դիցուք $Q(+, \cdot)$-ը և $Q'(+, \cdot)$-ը կավարներ են: $\varphi : Q \to Q'$ հոմոմորֆիզմը կոչվում է

ա) **մոնոմորֆիզմ**, եթե φ-ն ինյեկտիվ (ներդրող) արտապատկերում է;

բ) **էպիմորֆիզմ**, եթե φ-ն սյուրեկտիվ (վերադրող) արտապատկերում է;

գ) **իզոմորֆիզմ**, եթե φ-ն բիեկտիվ (փոխմիարժեք) արտապատկերում է:

Հեշտությամբ ապացուցվում է, որ երկու մոնոմորֆիզմների (էպիմորֆիզմների) արտադրյալը նորից մոնոմորֆիզմ (էպիմորֆիզմ) է:

$\pi(x) = [x]$ օրենքով որոշվող $\pi : Q \to Q/_{\sim}$ արտապատկերումը կլինի էպիմորֆիզմ, որովհետև այն սյուրեկտիվ է և

$$\pi(x + y) = \pi(x) + \pi(y),$$

$$\pi(x \cdot y) = \pi(x) \cdot \pi(y),$$

$$(\pi(x') = (\pi x)') :$$

Այս π հոմոմորֆիզմը (էպիմորֆիզմը) կոչվում է **բնական հոմոմորֆիզմ** (էպիմորֆիզմ) և երբեմն նշանակվում է $\pi_{\sim}$-ով: $Ker\,(\pi_{\sim}) = (\sim)$, որովհետև

$$(x, y) \in Ker\,(\pi_{\sim}) \longleftrightarrow \pi_{\sim}(x) = \pi_{\sim}(y) \longleftrightarrow [x] = [y] \longleftrightarrow x \sim y :$$

Այսպիսով, $Q(+,\cdot)$ կավարի ցանկացած «$\sim$» կոնգրուենցիա հանդիսանում է $\pi_\sim : Q \to Q/_\sim$ բնական հոմոմորֆիզմի միջուկ: Այսպիսով, որպեսզի Q բազմության «$\sim$» համարժեքությունը լինի $Q(+,\cdot)$ կավարի կոնգրուենցիա անհրաժեշտ է և բավարար, որ գոյություն ունենա այնպիսի $Q'(+,\cdot)$ կավար և այնպիսի $\varphi : Q \to Q'$ (կավարային) էպիմորֆիզմ, որ $(\sim) = Ker(\varphi)$, այսինքն՝ երբ «$(\sim)$»-ը լինի որևէ (կավարային) հոմոմորֆիզմի միջուկ:

Թեորեմ 20.24 (հոմոմորֆիզմների առաջին թեորեմը կավարներում): *Եթե $\varphi : Q \to Q'$ արտապատկերումը էպիմորֆիզմ է $Q(+,\cdot)$ կավարից $Q'(+,\cdot)$ կավարի մեջ և $Ker(\varphi) = (\sim)$, ապա $Q' \simeq Q/_\sim$: Ավելի ճշգրիտ, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\mu : Q' \to Q/_\sim$ իզոմորֆիզմ, որ $\pi = \varphi \cdot \mu$, այսինքն՝ տեղափոխական է հոմոմորֆիզմների հետևյալ եռանկյունը (դիագրամը).*

$$\begin{tikzcd} Q \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & Q' \arrow[d, "\mu"] \\ & Q/_\sim \end{tikzcd} :$$

Ապացուցում: Քանի որ $\varphi : Q \to Q'$ արտապատկերումը սյուրեկտիվ (վերադրող) է, ապա յուրաքանչյուր $z \in Q'$ տարրի համար գոյություն ունի այնպիսի $x \in Q$ տարր, որ $\varphi(x) = z$: Սահմանենք $\mu(z) = [x]$, որտեղ $\varphi(x) = z$: Նախ նկատում ենք, որ μ-ն իրոք արտապատկերում է, այսինքն՝ $\mu(z)$-ը կախված չէ $\varphi(x) = z$ պայմանին բավարարող x-ի ընտրությունից: Այնուհետև, ապացուցվում է μ-ի բիեկտիվությունը և հոմոմորֆությունը, իսկ վերջում՝ $\pi = \varphi \cdot \mu$ հավասարությունը և μ-ի միակությունը: $\square$

Թեորեմ 20.25 (հոմոմորֆիզմների երկրորդ թեորեմը կավարներում): *Ցանկացած $Q(+,\cdot)$, $Q'(+,\cdot)$ և $Q''(+,\cdot)$ կավարների կամայական $\varphi_1 : Q \to Q'$ և $\varphi_2 : Q \to Q''$ էպիմորֆիզմների համար, որտեղ $Ker(\varphi_1) \subseteq Ker(\varphi_2)$, գոյություն ունի միարժեքորեն որոշվող այնպիսի $\varphi_3 : Q' \to Q''$ էպիմորֆիզմ, որ $\varphi_1 \cdot \varphi_3 = \varphi_2$, այսինքն՝ տեղափոխական է հոմոմորֆիզմների հետևյալ եռանկյունը (դիագրամը).*

$$
\begin{tikzcd}
Q \arrow[r, "\varphi_1"] \arrow[dr, "\varphi_2"'] & Q' \arrow[d, "\varphi_3"] \\
& Q''
\end{tikzcd}
\quad :
$$

Ըստ որում, φ_3-ը կլինի իզոմորֆիզմ այն և միայն այն դեպքում, երբ $Ker(\varphi_1) = Ker(\varphi_2)$:

Ապացուցում: Տես թեորեմ 0.9-ի ապացուցումը: □

Նման արդյունքներ տեղի ունեն նաև բուլյան (Դե Մորգանի) հանրահաշիվների համար:

Յուրաքանչյուր $f : Q \to Q'$ արտապատկերմանը համապատասխանում է հետևյալ $\mathbf{f} \subseteq Q \times Q'$ հարաբերությունը՝

$$(x, y) \in \mathbf{f} \longleftrightarrow y = f(x),$$

որտեղ $x \in Q$, $y \in Q'$:

Եթե $Q(+,\cdot)$-ը և $Q'(+,\cdot)$-ը կավարներ են, ապա $Q \times Q'$ բազմությունը վերածվում է կավարի, եթե դրա վրա (մեջ) սահմանենք գումարման և բազմապատկման հետևյալ գործողությունները՝

$$(x, y) + (u, v) = (x + u, y + v),$$

$$(x, y) \cdot (u, v) = (x \cdot u, y \cdot v),$$

որտեղ $(x, y), (u, v) \in Q \times Q'$: Սահմանված $Q \times Q'(+,\cdot)$ կավարը կոչվում է Q և Q' կավարների **դեկարտյան** կամ **ուղիղ** արտադրյալ: Եթե $Q = Q'$, ապա հանգում ենք $Q^2(+,\cdot)$ կավարին, որտեղ $Q^2 = Q \times Q$: Բուլյան (Դե Մորգանի) հանրահաշիվների դեպքում սահմանվում է նաև

$$(x, y)' = (x', y')$$

լրացումը:

Լեմմ 20.21: *Որպեսզի $f : Q \to Q'$ արտապատկերումը լինի հոմոմորֆիզմ $Q(+,\cdot)$ կավարից $Q'(+,\cdot)$ կավարի մեջ անհրաժեշտ է և բավարար, որ $\mathbf{f} \subseteq Q \times Q'$ հարաբերությունը լինի $Q \times Q'(+,\cdot)$ կավարի ենթակավար:*

Ապացուցում: Անմիջական ստուգման եղանակով: □

Լեմմ 20.22: *Որպեսզի Q բազմության վրա որոշված «$\sim$» համարժեքությունը լինի $Q(+,\cdot)$ կավարի կոնգրուենցիա անհրաժեշտ է և բավարար, որ այն լինի $Q^2(+,\cdot)$ կավարի ենթակավար:*

Ապացուցում: Անմիջական ստուգման եղանակով: □

Նմանատիպ պնդումներ տեղի ունեն նաև բուլյան (Դե Մորգանի) հանրահաշիվների դեպքում:

Կասենք, որ $Q(+,\cdot)$ կավարն օժտված է **հարաբերական լրացումներով**, եթե նրա ցանկացած ոչ դատարկ $[a,b]$ հատված բավարարում է բուլյան լրացումների գոյության պայմանին (որպես սահմանափակ ենթակավար), այսինքն՝ կամայական $x\in[a,b]$ տարրի համար գոյություն ունի այնպիսի $y\in[a,b]$ տարր, որ $x+y=b$ և $x\cdot y=a$:

Լեմմ 20.23: *Եթե սահմանափակ և մոդուլյար (մասնավորապես բաշխական) կավարը բավարարում է բուլյան լրացումների գոյության պայմանին, ապա այն կլինի օժտված նաև հարաբերական լրացումներով:*

Ապացուցում: Դիցուք $Q(+,\cdot)$-ը 0 փոքրագույն տարրով և 1 մեծագույն տարրով մոդուլյար կավար է, որի յուրաքանչյուր $t\in Q$ տարրի համար գոյություն ունի այնպիսի $t'\in Q$ տարր, որ $t+t'=1$, $t\cdot t'=0$: Դիտարկենք կամայական $[a,b]\subseteq Q$ հատված, որտեղ $a\leqslant b$: Եթե $x\in[a,b]$ և $y=a+x'b$, ապա օգտվելով մոդուլյարության պայմանից, կստանանք՝

$$x+y=x+a+x'b=x+x'b=(x+x')b=1\cdot b=b,$$

$$x\cdot y=x(a+x'b)=(a+x'b)x=a+x'bx=a+0=a: \qquad \square$$

Թեորեմ 20.26 (R. P. Dilworth): *Հարաբերական լրացումներով օժտված $Q(+,\cdot)$ կավարի ցանկացած α և β կոնգրուենցիաների համար՝ $\alpha\cdot\beta=\beta\cdot\alpha$:*

Ապացուցում: Պահանջվում է ապացուցել $\alpha\cdot\beta\subseteq\beta\cdot\alpha$ և $\beta\cdot\alpha\subseteq\alpha\cdot\beta$ ներդրումները: Ապացուցենք, օրինակ, առաջին ներդրումը՝ $(a,b)\in\alpha\cdot\beta\to(a,b)\in\beta\cdot\alpha$: Դիցուք $\alpha=(\sim_1)$, $\beta=(\sim_2)$: Այսպիսով կապացուցենք, որ եթե $a\sim_1 x$ և $x\sim_2 b$, որտեղ $a,x,b\in Q$, ապա գոյություն ունի այնպիսի $y\in Q$ տարր, որ $a\sim_2 y$ և $y\sim_1 b$: Այս պնդումը նախ կապացուցենք

$x \in [a, b]$ դեպքում: Քանի որ $Q(+, \cdot)$ կավարն օժտված է հարաբերական լրացումներով, ապա գոյություն կունենա այնպիսի $y \in [a, b]$, որ

$$x + y = b,$$

$$x \cdot y = a :$$

Հետևաբար,

$$y = y \cdot b \sim_2 y \cdot x = a,$$

$$y = y + a \sim_1 y + x = b,$$

այսինքն՝ գտանք այնպիսի $y \in Q$ տարր, որ $a \sim_2 y$ և $y \sim_1 b$: Նույն եղանակով ապացուցվում է, որ եթե $a \sim_2 x$, $x \sim_1 b$ և $x \in [a, b]$, ապա գոյություն ունի այնպիսի $y \in [a, b]$, որ $a \sim_1 y$ և $y \sim_2 b$:

Անցնելով ընդհանուր դեպքին, դիտարկենք $[a, a+b+x]$ և $[b, a+b+x]$ հատվածները: Կունենանք՝

$$a = a + a \sim_1 a + x = a + x + x \sim_2 a + b + x,$$

$$b = b + b \sim_2 b + x = b + x + x \sim_1 b + a + x,$$

այսինքն՝ $a \sim_1 a + x \sim_2 a + b + x$ և $b \sim_2 b + x \sim_1 b + a + x$: Հետևաբար, գոյություն կունենան այնպիսի $u \in [a, a+b+x]$ և $v \in [b, a+b+x]$ տարրեր, որ

$$a \sim_2 u, \quad u \sim_1 a + b + x,$$

$$b \sim_1 v, \quad v \sim_2 a + b + x :$$

Օգտվելով այս տվյալներից, ստանում ենք՝

$$u = u(a + b + x) \sim_2 uv \sim_1 (a + b + x)v = v :$$

Այսպիսով,

$$a \sim_2 u \sim_2 uv,$$

$$uv \sim_1 v \sim_1 b : \qquad \square$$

Թեորեմ 20.27 (J. Hashimoto): *Հարաբերական լրացումներով օժտված կավարի ցանկացած կոնգրուենցիա միարժեքորեն է որոշվում իր կամայական համարժեքության դասով, այսինքն՝ նույն համարժեքության դասն ունեցող երկու կոնգրուենցիաներ հավասար են:* $\square$

Վարժություններ և խնդիրներ, լրացուցիչ արդյունքներ

1. Կառուցել Քլայնի չորս տարրանի ոչ միածին խմբի բոլոր ենթախմբերի կավարը: Ապացուցել, որ այն մոդուլյար է, բայց բաշխական չէ:

2. Ապացուցել, որ կավարի մինիմալ (մաքսիմալ) տարրը կլինի դրա փոքրագույն (մեծագույն) տարրը:

3. Ապացուցել, որ եթե կավարում $a + b = ab$, ապա $a = b$:

4. Ապացուցել, որ եթե կավարում $a + b + c = abc$, ապա $a = b = c$:

5. Ապացուցել, որ ցանկացած կավարում տեղի ունեն հետևյալ նույնությունները՝

$$(xy + xz)(xy + yz) = xy,$$

$$(x + y)(x + z) + (x + y)(y + z) = x + y :$$

6. $Q(+, \cdot)$ կավարի $Q' \neq Q$ ենթակավարը կլինի Q-ի պարզ իդեալ այն և միայն այն դեպքում, երբ $Q \setminus Q'$-ը Q-ի պարզ ֆիլտր է:

7. Յուրաքանչյուր կավարի ավելացնելով ամենաշատը երեք տարր, կարելի է ստանալ բուլյան լրացումների գոյության պայմանին բավարարող սահմանափակ կավար:

8. Ապացուցել, որ զույգ տեղադրությունների A_4 խմբի բոլոր ենթախմբերի կավարը մոդուլյար չէ:

9. Ապացուցել, որ 0 փոքրագույն տարրով մոդուլյար կավարում՝

$$(a + b)c = 0 \longrightarrow a(b + c) = ab :$$

10. Ապացուցել, որ սահմանափակ բաշխական կավարի բուլյան լրացումներ ունեցող բոլոր տարրերի ենթաբազմությունը կլինի բուլյան հանրահաշիվ:

11. Ապացուցել, որ յուրաքանչյուր բաշխական կավար հանդիսանում է որևէ բուլյան հանրահաշվի ենթակավար:

12. Ապացուցել, որ բուլյան հանրահաշվում տեղի ունի հետևյալ պնդումը.
$$a \leqslant b \longleftrightarrow ab' = 0 :$$

13. Ապացուցել, որ վերջավոր կավարի յուրաքանչյուր իդեալ (ֆիլտր) գլխավոր է:

14. Ապացուցել, որ 20.6-ում ներմուծված $FC(\mathbb{N})$ բուլյան հանրահաշիվը ատոմական է, բայց լրիվ չէ:

15. Ապացուցել, որ $Q \neq \emptyset$ բազմության բոլոր համարժեքությունների E_Q բազմությունը լրիվ կավարաձև կարգավորված բազմություն է (տեսա-բազմային ներդրման նկատմամբ): Այստեղ $\inf(X)$-ը և $\sup(X)$-ը ցանկացած ոչ դատարկ $X = \{\theta_i \mid i \in I\} \subseteq E_Q$ ենթաբազմության համար որոշվում են հետևյալ բանաձևերով՝
$$\inf(X) = \bigcap_{i \in I} \theta_i,$$
$$\sup(X) = \Psi \quad ,$$
որտեղ $(x, y) \in \Psi$ այն և միայն այն դեպքում, երբ գոյություն ունեն վերջավոր թվով $x_1, \ldots, x_n \in Q$ տարրեր և $i_1, \ldots, i_n \in I$ համարներ, որ $x = x_1\theta_{i_1}x_2\theta_{i_2}\cdots x_{n-1}\theta_{i_{n-1}}x_n = y$:

16. Ապացուցել, որ $Q(+, \cdot)$ կավարի բոլոր կոնգրուենցիաների $Con(Q)$ բազմությունը E_Q կավարի ենթակավար է:

17. Ապացուցել, որ $Con(Q)$ կավարը բաշխական է ցանկացած $Q(+, \cdot)$ կավարի համար (N. Funayama, T. Nakayama):

18. Ապացուցել հետևյալ պնդումը. որպեսզի $Q(+, \cdot)$ կավարի α, β կոնգրուենցիաների $\alpha \cdot \beta$ արտադրյալը լինի կոնգրուենցիա անհրաժեշտ է և բավարար, որ $\alpha \cdot \beta = \beta \cdot \alpha$:

19. Խումբը կոչվում է **ընդհանրացված միածին**, եթե դրա ցանկացած վերջավոր ենթաբազմությամբ ծնված ենթախումբը միածին է: Ակնհայտ է, որ այդպիսի խմբերը աբելյան են, որովհետև $\{x, y\}$ ենթաբազմությամբ ծնված ենթախումբը, լինելով միածին, կլինի աբելյան: Տեղի ունի հետևյալ հայտանիշը:

    Որպեսզի $Q(\circ)$ խմբի ենթախմբերի կավարը լինի բաշխական անհրաժեշտ է և բավարար, որ այն լինի ընդհանրացված միածին:

20. $Q(+,\cdot,')$ հանրահաշիվը, որտեղ $+$ և $\cdot$ գործողությունները երկտեղ գործողություններ են, իսկ $'$-ը 1-տեղանի գործողություն է (որի արժեքը $x \in Q$ տարրի վրա նշանակվում է x'-ով), կոչվում է **քվազիբուլյան հանրահաշիվ**, եթե

$$\begin{aligned} x+y=y+x, &\quad x\cdot y=y\cdot x,\\ x+(y+z)=(x+y)+z, &\quad x\cdot(y\cdot z)=(x\cdot y)\cdot z,\\ x+x=x, &\quad x\cdot x=x,\\ x(y+z)=xy+xz, &\quad x+(yz)=(x+y)(x+z),\\ (x')'=x, &\\ x'+y=(x+y)'+y, &\quad x'\cdot y=(x\cdot y)'\cdot y,\\ (x+y)'+(x+y')'=x', &\quad (x\cdot y)'\cdot(x\cdot y')'=x' \end{aligned}$$

ցանկացած $x, y, z \in Q$ տարրերի համար:

Ապացուցել, որ յուրաքանչյուր բուլյան հանրահաշիվ քվազիբուլյան հանրահաշիվ է, մինչդեռ հակառակը ճիշտ չէ (կառուցել օրինակ):

21. Եթե $(+) = (\cdot)$, ապա $Q(+,\cdot,')$ քվազիբուլյան հանրահաշիվը կոչվում է մեկ երկտեղ գործողությամբ: Հակառակ դեպքում քվազիբուլյան հանրահաշիվը կոչվում է երկու երկտեղ գործողությամբ:

Ապացուցել, որ երկու տարրանի և երկու երկտեղ գործողությամբ քվազիբուլյան հանրահաշիվը հանդիսանում է բուլյան հանրահաշիվ:

22. Ապացուցել, որ վերջավոր Q բազմության վրա կարելի է սահմանել քվազիբուլյան հանրահաշիվ այն և միայն այն դեպքում, երբ $|Q| = 2^n$, $n \geqslant 1$:

23. Դիցուք $Q = \left\{0, \frac{1}{2}, 1\right\}$, իսկ $x+y=\max\{x,y\}$, $x\cdot y=\min\{x,y\}$,

$$x' = \begin{cases} 1, & \text{եթե } x=0,\\ 0, & \text{եթե } x=1 \text{ կամ } x=\frac{1}{2} : \end{cases}$$

Հանգում ենք գումարման և բազմապատկման հետևյալ գործողություններին՝

$+$	0	$\frac{1}{2}$	1
0	0	$\frac{1}{2}$	1
$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{2}$	1
1	1	1	1

,

$\cdot$	0	$\frac{1}{2}$	1
0	0	0	0
$\frac{1}{2}$	0	$\frac{1}{2}$	$\frac{1}{2}$
1	0	$\frac{1}{2}$	1

:

Ստացված երեք տարրանի $Q(+,\cdot,')$ հանրահաշիվը կոչվում է Գյոդելի հանրահաշիվ (K. Gödel, 1932):

Ապացուցել, որ Գյոդելի հանրահաշիվը բավարարում է հետևյալ նույնություններին.

$$\begin{aligned}
x+y&=y+x, & x\cdot y&=y\cdot x,\\
x+(y+z)&=(x+y)+z, & x\cdot(y\cdot z)&=(x\cdot y)\cdot z,\\
x+x&=x, & x\cdot x&=x,\\
x(y+z)&=xy+xz, & x+(yz)&=(x+y)(x+z),\\
(x+y)'&=x'\cdot y', & (x\cdot y)'&=x'+y',\\
(x+y)'+(x+y')'&=x', & (x\cdot y)'\cdot(x\cdot y')'&=x' \ :
\end{aligned}$$

24. Դիցուք $A(\leqslant)$ զույգի «$\leqslant$» հարաբերությունն օժտված է առինքնության և հակահամաչափության հատկություններով և $\sup\{a,b\}$-ն, $\inf\{a,b\}$-ն գոյություն ունեն ցանկացած $a,b\in Q$ տարրերի համար: Ապացուցել, որ

$$x+y=\sup\{x,y\},\qquad x\cdot y=\inf\{x,y\},\qquad x,y\in A,$$

գործողությունները բավարարում են հետևյալ նույնություններին՝

(a) $x+x=x$, $x\cdot x=x$,

(b) $x+y=y+x$, $x\cdot y=y\cdot x$,

(c) $(xz+yz)+z=z$, $(x+z)(y+z)z=z$,

(d) $x(x+y)=x$, $x+xy=x$:

Չ լ ու ծ վ ա ծ խ ն դ ի ր ն ե ր

Դասագրքում ձևակերպված բազմաթիվ չլուծված խնդիրների հետ մեկտեղ նշենք նաև հետևյալները.

1. Բնութագրել անշարժ կետի հատկությամբ օժտված մասնակի կարգավորված բազմությունները:

2. Ձևակերպել և ապացուցել Մյոբիուսի շրջման թեորեմը մասնակի կարգավորված օղակների համար:

3. Յուրաքանչյուր $n > 0$ բնական թվի համար գոյություն ունեն արդյոք այնպիսի a և b բնական թվեր, որ
$$\varphi(a) + \varphi(b) = 2n,$$
որտեղ φ-ն էյլերի ֆունկցիան է (P. Erdős):

4. Դիցուք Q-ն P դաշտի վրա որոշված գծային տարածություն է, իսկ $f : Q \times Q \to P$ արտապատկերումը Q-ի երկգծային ձև է: (Q, f) զույգը կոչվում է Դե Մորգանի գծային տարածություն եթե $(U^{\perp})^{\perp} = U$ ցանկացած $U \leqslant Q$ ենթատարածության համար (որտեղ $U^{\perp}$-ը U-ի օրթոգոնալ լրացումն է f-ի նկատմամբ): Բնութագրել Դե Մորգանի գծային տարածությունները:

5. Ձևակերպել և ապացուցել Համիլտոն-Քելիի թեորեմը վերջավոր չափանի գծային տարածության երկգծային ձևափոխության համար:

6. Ձևակերպել և ապացուցել Համիլտոն-Քելիի թեորեմը վերջավոր չափանի գծային տարածության n-գծային ձևափոխության համար:

7. Ապացուցել Քելիի տիպի թեորեմ քվազիխմբերի (լուպաների) համար:

8. Ապացուցել Քելիի տիպի թեորեմ կավարների (մոդուլյար կավարների) համար:

9. Ապացուցել Քելիի տիպի թեորեմ էվկլիդյան օղակների համար:

10. Ապացուցել Քելիի տիպի թեորեմ քվազիբուլյան հանրահաշիվների համար:

11. Քելիի տիպի թեորեմի օգնությամբ բնութագրել անշարժ կետի հատկությամբ օժտված մասնակի կարգավորված բազմությունները:

12. Քելիի տիպի թեորեմի օգնությամբ բնութագրել տոպոլոգիական դաշտերի (մարմինների) արտադրյալային խմբերը:

13. Բնութագրել երկու օղակների (դաշտերի, մարմինների, ամբողջության տիրույթների, էվկլիդյան օղակների) սուպեր-արտադրյալը:

    Սահմանում: Երկու երկտեղ գործողությամբ $Q_1(A_1, B_1)$ և $Q_2(A_2, B_2)$ հանրահաշիվների սուպեր-արտադրյալ ասելով հասկացվում է չորս երկտեղ գործողությամբ հետևյալ հանրահաշիվը՝ $(Q_1 \times Q_2; \{A_1, B_1\} \times \{A_2, B_2\})$, որտեղ $\{A_1, B_1\} \times \{A_2, B_2\} = \{(A_1, A_2), (A_1, B_2), (B_1, A_2), (B_1, B_2)\}$, իսկ (X, Y) գործողությունը գործում է $Q_1 \times Q_2$ դեկարտյան արտադրյալի վրա ըստ բաղադրիչների, այսինքն՝

    $$(X, Y)\left((x_1, y_1), (x_2, y_2)\right) = (X(x_1, x_2), Y(y_1, y_2)) :$$

    Երկու կամայական $(Q_1; \Sigma_1)$ և $(Q_2; \Sigma_2)$ հանրահաշիվների սուպեր-արտադրյալ ասելով հասկացվում է $\left(Q_1 \times Q_2; \Sigma_1 \tilde{\times} \Sigma_2\right)$ հանրահաշիվը, որտեղ

    $$\Sigma \tilde{\times} \Sigma_2 = \{(X, Y) \mid X \in \Sigma_1,\ Y \in \Sigma_2,\ |X| = |Y|\} :$$

    Այստեղ $|X|$-ը նշանակում է X գործողության տեղայնությունը, իսկ (X, Y) գործողությունը նորից գործում է ըստ բաղադրիչների:

14. Բնութագրել երկու զրո $(p > 0)$ բնութագրիչով դաշտերի սուպեր-արտադրյալը:

15. Բնութագրել երկու քվազիխմբերի (լուպաների, խմբերի) սուպեր-արտադրյալը՝ դիտելով դրանց որպես երեք (երկտեղ) գործողությամբ հանրահաշիվներ:

16. Բնութագրել զուգորդական (զուգորդական և տեղափոխական) օղակների արտադրյալային կիսախմբերը:

17. Բնութագրել զրո $(p > 0)$ բնութագրիչով դաշտերի արտադրյալային խմբերը:

18. Զարգացնել թվային համակարգերի տեսություն՝ ելնելով հանման (բաժանման) գործողության քվազիխմբային հատկություններից:
19. Զարգացնել կրիպտոգրաֆիա՝ ելնելով տարբեր թվաբանական օղակներում էյլերի օղակային ֆունկցիայի հատկություններից:
20. Նկարագրել (բնութագրել) Գյոդելի հանրահաշվի բոլոր նույնությունները: Բնութագրել այդ նույնություններին բավարարող հանրահաշիվները:
21. Նկարագրել (բնութագրել) Գյոդելի հանրահաշվի բոլոր գերնույնությունները: Բնութագրել այդ գերնույնություններին բավարարող հանրահաշիվները:
22. Նկարագրել (բնութագրել) նկ. 1-ում (նկ. 2-ում) պատկերված կավարի բոլոր գերնույնությունները: Բնութագրել այդ գերնույնություններին բավարարող հանրահաշիվները:
23. Գոյություն ունի արդյոք բուլյան լրացումների միակության պայմանին բավարարող ոչ բաշխական լրիվ կավար:

Առարկայական ցանկ

Աբելյան խումբ 18.1
Ալգորիթմ Էվկլիդեսի 2
– մնացորդով բաժանման ամբողջ թվերի 1.1
– – – բազմանդամների 16.2
– Չինական համակարգի լուծման 3.2
Ամբողջ թվի կարգ ըստ տրված հենքի (հենաթվի, մոդուլի) 9.2
– մաս իրական թվի 8
– p-ադիկ թիվ 9.6
Ամբողջության տիրույթ 19.1
Ամենամեծ ընդհանուր բաժանարար 2, 5, 19.3
Ամենափոքր ընդհանուր բազմապատիկ 4, 5, 19.3
Անշարժ կետ 0.5
Աջ բաշխականություն 19.1
Աջից հակադարձելի արտապատկերում 0.3
Առինքնություն 0.1, 0.4
Ատոմ 0.4
Ատոմական կավար 20.4
Արմատային ենթատարածություն 17.22
Արտադրյալային հատկություն 9.4, 9.5
– ֆունկցիա 9.4, 9.5
Արտապատկերման միջուկ 0.3, 17.14, 20.11
Արտապատկերումների առաջին և երկրորդ թեորեմներ 0.3, 17.14
Աքսիոմային տեսություն թվերի 12.2
Ավտոմորֆիզմ դաշտի 14.7
– խմբի 18.7
– օղակի 19.6

Բազմանդամ 16.2
Բազմանդամի աստիճան 16.2
– ածանցյալ 16.6
Բազմանդամների օղակ 16.2
Բազմապատիկ արմատ 16.6
Բազմությունների կիսաօղակ 0.1
– հանրահաշիվ 0.1
– σ-հանրահաշիվ 0.1
– օղակ 0.1
Բաղադրյալ թիվ 6.1
Բաղդատելի թվեր 1.2
– տարրեր 19.1
Բաղդատման աստիճան 6.3
– լուծում 6.3
Բաղդատումների Չինական համակարգ 3.2
Բանախի թեորեմ 0.5
Բաշխական կավար 20.3
– նույնություններ 0.1, 9.4, 19.1, 20.3
Բաց բանալի 11
Բաց-փակ բազմություն 20.8
Բեզուի գործակիցներ 2
– թեորեմ 16.2
Բեռնսայդի լեմմ 18.9
Բերթրանի թեորեմ (հատկություն) 7
Բինեթի բանաձև 2
Բիրկհոֆի թեորեմ 20.3, 20.8
Բիրկհոֆ-Ստոունի թեորեմ 20.8
Բիրկհոֆ-Տարսկիի թեորեմ 0.5
Բնական արտապատկերում 0.3
– հոմոմորֆիզմ 18.6, 19.7, 20.11
Բնութագրիչ բազմանդամ 17.21

Բրունի հաստատուն 7
Բուլյան հանրահաշիվ 20.4
– լրացում 20.4
– օղակ 20.4
Բորելյան հանրահաշիվ 0.8
Բրաուերի թեորեմ 0.5

Գաղտնագրություն 11
Գաղտնի բանալի 11
Գալուայի թեորեմ 16.10
Գաուսի ալգորիթմ 14.6
Գաուսի թեորեմ 10.2
Գաուսի լեմմ 10.2
Գերկատարյալ թիվ 9
Գերնույնություն 20.1
Գլխավոր իդեալ 19.2, 20.7
– իդեալներով օղակ 19.3
– ֆիլտր 20.7
Գծային արտապատկերում 17.14
– Դիոֆանտյան հավասարում 3.1
– կախվածություն (անկախություն) 17.1
– հանրահաշիվ 17.16
– ձև 17.12
– տարածություն 17.1
Գծայնորեն կարգավորված բազմություն 0.4
– – խումբ 18
– – օղակ 19
Գյոդելի հանրահաշիվ 20
Գրեթե-կատարյալ թիվ 9
Գումարման աքսիոմ 0.1
Գոլդբախի թեորեմ 7
– պրոբլեմ 7
Գրքույկ հեռախոսային (համակարգչային, ինտերնետային) 11

Դաշտ 14.7
Դաշտի արտադրյալային խումբ 19.1
– բնութագրիչ 14.7
– պարզ ընդլայնում 16.9
Դասերի արտադրյալ 1.3
– գումար 1.3
Դեդեկինդի թեորեմ 20.2, 20.5
Դե Մորգանի նույնություններ 0.1, 20.9
– հանրահաշիվ 20.9
Դինամիկ համակարգ 12.2
Դիոֆանտյան հավասարում 3.1
– լուծում 3.1
Դիրիխլեի արտադրյալ 9.5
– թեորեմ 7
Դիսկրետ լոգարիթմ 18.13

Ենթադաշտ 14.7
Ենթախումբ 18.1
Ենթակավար 20.2
Ենթակիսախումբ 18.1
Ենթատարածություն 17.7
Ենթատարածությունների գումար 17.10
– ուղիղ գումար 17.10
Ենթաօղակ 14.7
Երկգծային ձև 17.16
– արտապատկերում 17.17
– ձևափոխություն 17.17
n-գծային արտապատկերում 17.17
n-գծային ձևափոխություն 17.17

Զրոյական դաս 1.3
– օղակ 14.7
Զուգորդականություն 1.4, 18.1
Զուգորդական օղակ 19.1
Զուգորդման հարաբերություն 19.4

Էյլերի թեորեմ 7, 9.1, 19.5
– խումբ 19.1
– ֆունկցիա 9.1
– – օղակային 19.5
Էվկլիդեսի ալգորիթմ 2
Էվկլիդի (Էվկլիդեսի) թեորեմ 1.1, 7
Էվկլիդյան թիվ 6.2
– նորմ 19.4
– տարածություն 17.20
– օղակ 19.4

Ժորդանյան հենք 17.22
– մատրից 17.22

Թեյլորի բանաձև 16.6
Թվաբանական օղակ 19.5
Թվակերպ բազմություն 9.4
– ֆունկցիա Մյոբիուսի 9.5
Թվաբանության հիմնական թեորեմ 6.2
– – – գլխավոր իդեալներով օղակներում 19.3

Իդեալ կավարի 20.7
– կիսախմբի 18.14
– օղակի 14.2
Իզոմորֆ բազմություններ 0.6, 12.2
– բուլյան հանրահաշիվներ 20.6
– դաշտեր 14.7
– խմբեր 18.3
– կավարներ 20.5
– կիսախմբեր 18.14
– օղակներ 14.7
Իզոմորֆիզմ 0.7, 17.11, 17.15, 17.20, 18.3, 19.7, 20.5, 20.6
Իզոմորֆիզմների թեորեմ 18.6, 19.7
Իներցիայի օրենք 17.18
Ինվարիանտ ենթախումբ 18.4
– ենթատարածություն 17.21, 17.22
Ինտերնետային ստորագրություն 11
Ինքնահամընկնող տարր 18.2

Լագրանժի թեորեմ 6.3, 18.4
Լամեի բանաձև 2
– թեորեմ 2
Լեժանդր-Դիրիխլեի թվաբանական պրոգրեսիա 7
Լեժանդրի թեորեմ 7, 8
– պայմանանշան 10.2
Լինդենբաում-Տարսկիի թեորեմ 20.6
Լրիվ կավար 20.6
– գծային խումբ 18.1
Լուկաս-Լեհմերի հաջորդականություն 7
Լուկասի թեորեմ 9.2
Լուպա 18.1

Խմբերի հոմոմորֆիզմ 18.6
– կիսաուղիղ արտադրյալ 18.8
– ուղիղ արտադրյալ 18.8
Խմբի կենտրոն 18.2
Խումբ 18.1

Կանոնական վերլուծություն 6.2, 16.5
Կավար 20.1
Կավարաձև կարգավորված բազմություն 0.4
Կավարի իդեալ 20.7
– ֆիլտր 20.7
Կանտորի թեորեմ 0.3
Կանտոր-Շրյոդեր-Բեռնշտայնի թեորեմ 0.5
Կատարյալ թիվ 9.4
Կոմպլեքս թիվ 15.1

– թվի կարգ 15.3
– թվից արմատ հանելը 15.3
Կոնգրուենտ մատրիցներ 17.17
Կոնգրուենցիա 18.14, 20.11
Կոտորակային մաս իրական թվի 8
Կիսախումբ 18.1
Կիսադաշտ 19.1
Կիսամարմին 19.1
Կիսաօղակ 19.1
Կոշի-Բունյակովսկու անհավասարություն 17.19
Կոշիի թեորեմ 18.4, 18.10
Կրամերի եղանակ 14.6
Կրոնեկերի թեորեմ 16.10
Կրոնեկեր-Կապելլիի թեորեմ 17.5

Հակադարձ արտապատկերում 0.4
– դաս 1.3
– հարաբերություն 0.6
– մատրից 14.2, 14.3
– տարր 18.1
Հակադարձելի աջից 18.1
– ամբողջ p-ադիկ թիվ 9.6
– արտապատկերում 0.3
– դաս 1.3
– մատրից 14.2
– տարր 18.1
– տարրերի խումբ 18.2
Հակադիր ամբողջ p-ադիկ թիվ 9.6
Հակահամաչափություն 0.4
Համարժեքության դաս 0.1
Համակարգի ռանգ 17.2
Համարժեքություն 0.1
Համալուծ տարածություն 17.12
Համիլտոն-Քելիի թեորեմ 17.21
Հանրահաշիվ 18.1
Հանրահաշվական բաղդատման աստիճան 6.3
– – լուծում 6.3
– լրացուցիչ 14.5
– տարր 16.4
– ընդլայնում 16.10
Հավասարազոր բազմություններ 0.3
Հարաբերական լրացումներով կավար 20.11
Հարաբերություն 0.1
Հաշվելի բազմություն 0.3
Հատուկ գծային խումբ 18.1
Հենաթիվ 1.2
Հենք 17.2
Հերմիտյան մատրից 17.20
Հիմնական թեորեմ հանրահաշվի՝ բաղդատումների վերաբերյալ 6.3
– – կոմպլեքս թվերի վերաբերյալ 16.2
Հոմոմորֆիզմների թեորեմ խմբերում 18.6
– – կավարներում 20.11
– – օղակներում 19.6

Ձախից հակադարձելի արտապատկերում 7
Ձետա-ֆունկցիա 7

Մասնակի կարգ 0.4
Մասնակի կարգավորված բազմություն 0.4
– – խումբ 18
– – օղակ 19
Մատրիցի որոշիչ 14.4
– ռանգ 17.3
Մարմին 14.1
Մաքսիմալ ենթախումբ 18.2
– իդեալ 19.7, 20.7

Մերսեննի թիվ 7
Միածին ենթախումբ 18.3
– խումբ 18.4
Միավորով օղակ 19.1
Մյոբիուսի թվակերպ ֆունկցիա 9.5
– ընդհանրացված ֆունկցիա 9.4
– ֆունկցիա 6.2
– թեորեմ 9.5
– օղակային ֆունկցիա 19.5
Մոդուլյար կավար 20.2

Նախնական արմատ 15.3
Ներքին ավտոմորֆիզմ 18.7
Նման մատրիցներ 17.15
Նորմալացնող ենթախումբ 18.2
Նույնություն աջ բաշխական 19.1
– երկակի-բաշխականության 20.3
– զուգորդական 18.1
– ինքնահամընկնման 20.1
– ձախ բաշխական 19.1
– տեղափոխական 18.1
– կլանման 20.1

Ոչ հստակ բազմություն 0.9

Չբերվող բազմանդամ 16.5
Չեբիշևի անհավասարություն 7
– թեորեմ 7
Չինական թեորեմ 3.2, 19.3
– համակարգ 3.2

Պարբերական խումբ 18.3
Պարզ թիվ 6.1
– ընդլայնում 16.9
– իդեալ 19.7, 20.7
– խումբ 18.5
– տարր 19.3
Պեանոյի աքսիոմներ 12.2

Պյութագորասի թեորեմ 17.19
Պոյայի թեորեմ 7
Պսևդոպարզ թիվ 9.1
p-ադիկ թիվ 9.7
p-խումբ 18.3

Սեպարաբել բազմանդամ 16.10
Սեփական արժեք 17.20
– վեկտոր 17.20
Սիլովի թեորեմներ 18.11
Սիլվեստրի հայտանիշ 17.18
Սիմետրիկ երկգծային ձև 17.17
– խումբ 18.1
– կիսախումբ 18.1
Սիմետրիկություն 0.1
Ստոունի թեորեմ 20.4, 20.6, 20.8

Վեդդերբառնի թեորեմ 19.1
Վերհանգման սկզբունք (եղանակ) 0.2
Վիետի բանաձևեր 16.6
Վիլսոնի թեորեմ 6.1, 19.1

Տարրի ամբողջ աստիճան 18.4
Տեղադրության նշան 13.1
Տեղափոխության նշան 13.2
Տեսա-բազմային գործողություններ 0.1
– ներդրում 0.4
Տոպոլոգիա 0.8
– դիսկրետ 0.8
– հակադիսկրետ 0.8
– մնացքային 1.2
Տոպոլոգիական խումբ 18
– տարածություն 0.8
– – Հաուսդորֆյան 0.8
– – նորմալ 0.8
– – ռեգուլյար 0.8

– – ստոունյան 20.8
– – T_1, T_2, T_3, T_4 0.8
– օղակ 19
Տրանսցենդենտ թիվ 3.1
– տարր 16.9
– ընդլայնում 16.9

Ցոռնի աքսիոմ 0.4

Փոխադարձաբար պարզ ամբողջ թվեր 3.1
– – բազմանդամներ 16.4
– – տարրեր 19.3
Փոխանցականություն 0.1
Փոքրագույն տարրի սկզբունք 0.2

Քաթալանի թիվ 1.4
Քառակուսային դաշտ 15.4
– ձև 17.18
– մնացք 10.1
– մնացքների փոխադարձության օրենք 10.2
– ոչ-մնացք 10.1
– օղակ 15.4
Քարմայքլի թիվ 9.1
Քելիի թեորեմ 0.7, 17.16, 18.3
– ընդհանրացված թեորեմ 18.6
Քլինիի հանրահաշիվ 20.9
Քնաստեր-Տարսկիի թեորեմ 0.5
Քվազիբուլյան հանրահաշիվ 20
Քվազիդաշտ 19.1
Քվազիխումբ 18.1
Քվազիկարգ 0.4
Քվազիմարմին 19.1
Քվազիօղակ 19.1

Օղակ 19.1
Օղակի հակադարձելի տարրերի խումբ 19.1
Օրթոգոնալ լրացում 17.18
– հենք 17.18
– մատրից 14.1
Օրթոնորմալ հենք 17.20

Ֆակտոր-կավար 20.11
Ֆակտոր-կիսախումբ 18.14
Ֆակտոր-խումբ 18.5
Ֆակտոր-տարածություն 17.13
Ֆակտոր-օղակ 19.2
Ֆակտորիզացվող օղակ 19.3
Ֆակտորիալ օղակ 19.3
Ֆերմայի թիվ 7
– մեծ թեորեմ 3.1
– փոքր թեորեմ 9.1
– – – օղակներում 19.5
– ֆունկցիա 19.5
Ֆիբոնաչիի հաջորդականություն 2
– թիվ 2
Ֆրոբենիուսի օրենք 16.10
– ընդհանրացված օրենք 16.10

Լրացուցիչ գրականություն

Մովսիսյան Յու. Մ., *Բարձրագույն Հանրահաշիվ,* Երևանի պետական համալսարանի հրատարակչություն, Երևան, 1983.

Մովսիսյան Յու. Մ., *Թվերի տեսություն,* Երևան, 2004, Զանգակ-97.

Մովսիսյան Յու. Մ., Թունիև Ա. Դ., *Գծային Հանրահաշվի և Գծային Ծրագրավորման Մեթոդներ, Տնտեսագիտության և Գործարարության Հանգունակներ,* «Ասողիկ», Երևան, 2002.

Մովսիսյան Յու. Մ. (խմբ.), Հանրահաշվի և երկրաչափության ամբիոնի կուրսային և ավարտական աշխատանքների թեմաների ժողովածու, Երևան, ԵՊՀ, 2008.

Աթաբեկյան Վ. Ս., *Հանրահաշվի ներածություն,* Երևան, 2005.

Անտոնյան Ս. Հ., *Տոպոլոգիական խմբեր և G-տարածություններ,* Երևան, ԵՊՀ, 1985.

Դալալյան Ս. Հ., *Գծային ձևափոխություններ,* Երևան, ԵՊՀ, 2005.

Դավիդով Ս. Ս., *Թվային համակարգեր,* Երևան, ԵՊՀ, 2007.

Առաքելյան Ա. Ս., *Թվային համակարգեր,* Վանաձոր, ԱՐՄԻՆՖՈ, 2006.

Մաշուրյան Ա. Ս., *Համարողության արվեստի արահետներում: Ասույթաբանություն, տրամաբանություն, թվաբանություն,* Երևան, 1997, Նոյյան Տապան.

Աբրահամյան Լ., *Քվազիխմբեր,* Ստեփանակերտ, 2010.

Միքայելյան Հ. Ս., *Բարձրագույն հանրահաշվի դասընթաց,* «էդիթ պրինթ», Երևան, 2000.

Адян С. И., *Проблема Бернсайда и тождества в группах,* "Наука", М., 1975.

Александрян Р. А., Мирзаханян Э. А. *Общая топология, М., Высшая школа,* 1979.

Арнаутов В. И., Водинчар М. И., Михалев А. В.,*Введение в теорию топологических колец и модулей,* "Штиинца", 1981.

Белоусов В. Д., *Основы теории квазигрупп и луп,* "Наука", 1967.

Биркгоф Г., *Теория решёток,* "Наука", М., 1984.

Боревич З. И., Шафаревич И. Р.,*Теория чисел,* "Наука", М., 1970.

Ван дер Варден Б. Л., *Алгебра,* "Наука", М., 1976.

Винберг Э. Б., *Курс алгебры,* "Факториал Пресс", М., 2002.

Виноградов И. М., *Основы теории чисел,* "Наука", М., 1981.

Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра,* т. I, II, М., 2003.

Клиффорд А., Престон. Г., *Алгебраическая теория полугрупп, "Мир",* М., 1972.

Кон П., *Универсальная алгебра,* "Мир", М., 1968.

Кострикин А. И., *Введение в алгебру,* "Наука", М., 1977.

Курош А. Г., *Лекции по общей алгебре,* "Наука", М., 1975.

Мальцев А. И., *Алгебраические системы,* "Наука", М., 1970.

Мендельсон Э., *Введение в математическую логику,* "Наука", М., 1984.

Мовсисян Ю. М., *Введение в теорию алгебр со сверхтождествами,* Изд-во ЕГУ, 1986.

Мовсисян Ю. М., *Сверхтождества и сверхмногообразия в алгебрах,* Изд-во ЕГУ, 1990.

Нечаев В. И., *Элементы криптографии. Основы теории защиты информации,* "Высшая школа", М., 1999.

Ноден П., Китте К., *Алгебраическая алгоритмика,* "Мир", М., 1999.

Проблемы Гильберта, "Наука", М., 1969.

Родосский К. А., *Алгоритм Эвклида,* "Наука", М., 1988.

Серпинский В., *250 задач по элементарной теории чисел,* "Просвещение", М., 1968.

Фаддеев Д. К., *Лекции по алгебре,* "Наука", М., 1984.

Bergman G.M., *An invitation on general algebra and universal constructions*, Second edition, Springer, 2015.

Buchmann J. A., *Introduction to Cryptography,* Springer-Verlag, 2001.

Burris S., Sankappanavar H.P., *A Course in Universal Algebra,* Springer-Verlag, 1981.

Crama Y. and Hammer P.L., *Boolean Functions: Theory*, Algorithms, and Applications, Cambridge University Press, New York, 2011.

Denecke K., Koppitz J., *M-solid varieties of Algebras*, Advances in Mathematic, 10, Spriger-Science+Business Media, New York, 2006

Denecke K., Wismath S.L., *Hyperidentities and Clones*, Gordon and Breach Science Publishers, 2000.

Euclid, *The Thirteen Books of the Elements,* 3 vols., 2nd ed., trans. Thomas

Heath, Dover, New-York, 1956.

Graczynska E., *Algebra of M-solid quasivarieties,* Siatras International Bookshop, Athens, 2014.

Grätzer G., *Lattice Theory: Foundation*, Springer Basel AG, 2011.

Grätzer G., *Universal Algebra*, Springer-Verlag, 2008.

Hazewinkel M. (Editor), *Handbook of algebra*, Vol. 2, North-Holland, 2000.

Kobliz N., *A Course in Number Theory and Cryptography,* Springer-Verlag, 1987.

Plotkin B.I., *Universal algebra, algebraic logic, and databases* , Kluwer Academic Publisher, 1994.

Romanowska A., Smith J.D.H., *Modes*, World Scientific, 2002.

Smith J.D.H., Romanowska A.B., *Post-modern algebra*, A Wiley-Interscience Publication, John Wiley and Sons, Inc., New York, 1999.

Strayer J. K., *Elementary Number Theory,* Waveland Press, 2002.

Tattersall J. J., *Elementary Number Theory in Nine Chapters,* Cambridge University Press, 1999.

Ušan J., *n-Groups in the light of the neutral operations*, Mathematica Moravica, 2006.

ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Յու. Մ. Մովսիսյան

ԲԱՐՁՐԱԳՈՒՅՆ ՀԱՆՐԱՀԱՇԻՎ ԵՎ ԹՎԵՐԻ ՏԵՍՈՒԹՅՈՒՆ

Երրորդ հրատարակություն

Մասնագիտական խմբագիր՝ Վ. Ս. Աթաբեկյան
Համակարգչային ձևավորումը՝ Լ. Ա. Էլբակյանի,
Կ. Չալաբյանի
Կազմի ձևավորումը՝ Ա. Պատվականյանի
Հրատ. սրբագրումը՝ Վ. Դերձյանի

Տպագրված է Time to Print օպերատիվ տպագրությունների սրահում
ք. Երևան, Խանջյան 15/55

Չափսը՝ 60x84 $^1/_{16}$: Տպ. մամուլը՝ 59:
Տպաքանակը՝ 100 օրինակ:

ԵՊՀ հրատարակչություն,

ք. Երևան, 0025, Ալեք Մանուկյան 1

ՀՐԱՏԱՐԱԿՉՈՒԹՅՈՒՆ
ԵՐԵՎԱՆ 2015