ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ ՀԱՄԱԼՍԱՐԱՆ

Ա. ԱԼԵՔՍԱՆՅԱՆ

ՀԱՆՐԱՀԱՇԻՎ
(ԽՄԲԵՐ, ՕՂԱԿՆԵՐ, ԴԱՇՏԵՐ)

ԵՐԵՎԱՆ

ԵՐԵՎԱՆԻ ՀԱՄԱԼՍԱՐԱՆԻ ՀՐԱՏԱՐԱԿՉՈՒԹՅՈՒՆ

2006

ՀՏԴ 512 (07)
ԳՄԴ 22.14 y73
Ա 296

Երաշխավորված է տպագրության Երևանի պետական համալսարանի Ինֆորմատիկայի և կիրառական մաթեմատիկայի ֆակուլտետի խորհրդի կողմից

Ալեքսանյան Ա.
Հանրահաշիվ (խմբեր, օղակներ, դաշտեր), Եր., Երևանի համալս. հրատ., էջ. 204

Դասագիրքն ամփոփում է վերջին տասնամյակում հեղինակի կողմից **ԵՊՀ** *Ինֆորմատիկայի և կիրառական մաթեմատիկայի ֆակուլտետում կարդացվող դասախոսությունները: Ֆակուլտետի ուսումնական պլանով հաստատված «Հանրահաշիվ» առարկայի ծրագիրը հիմնված է հեղինակի այս և «Գծային հանրահաշիվ» դասագրքերում ներառված նյութի վրա:*

Ա $\frac{1602040000}{704(02)-2006}$

ԳՄԴ 22.14 y73

ISBN 5-8084-0807-5

ԽՄԲԵՐ

Խմբի սահմանումը

Դիցուք տրված է որևէ G բազմություն: Ընդունված է ասել, որ այդ բազմության վրա սահմանված է գործողություն, եթե տրված է արտապատկերում $G \times G$ դեկարտյան արտադրյալից G բազմություն: Այլ կերպ ասած G-ի տարրերի յուրաքանչյուր կարգավորված զույգին՝ (a,b)-ին համապատասխանության մեջ է դրված միարժեքորեն որոշված G-ի որոշակի տարր: (a,b)-ին համապատասխանող տարրը սովորաբար նշանակում են $a \cdot b$-ով (կամ ուղղակի ab-ով բաց թողնելով $\cdot$ նշանը) և ասում են, որ G բազմության վրա սահմանված է բազմապատկման գործողություն:

Սահմանում: Դիցուք G բազմության վրա սահմանված է բազմապատկման գործողություն: G բազմությունը կոչվում է ***խումբ*** բազմապատկման գործողության նկատմամբ, եթե բավարարված են հետևյալ պայմանները.

1. $(ab)c = a(bc)$ - ***ասոցիատիվության*** պայման

2. $\exists e \in G \quad \forall a \in G \quad ae = ea = a$ - ***միավոր*** տարրի գոյության պայման

3. $\forall a \in G \ \exists b \in G \quad ab = ba = e$ - ***հակադարձ*** տարրի գոյության պայման

Ասոցիատիվության պայմանից բխում է, որ եթե սկզբից հաշվենք ab-ն հետո արդյունքը բազմապատկենք c-ով կստանանք ճիշտ նույն քանն ինչ կստացվի, եթե սկզբից Հաշվենք bc-ն և Հետո արդյունքը ձախից բազմապատկենք a-ով: Այսինքն կարելի է գրել ուղղակի abc առանց փակագծեր օգտագործելու, քանի որ արդյունքը կախված չէ Հաշվման կարգից:

Երկրորդ պայմանն ասում է, որ գոյություն ունի մեկ Հատուկ տարր, որը նշանակվում է e տառով և կոչվում է **միավոր**, որը բազմապատկելիս G բազմության որևէ տարրով արդյունքում տալիս է Հենց այդ նույն տարրը (այսինքն միավորը խաղում է 1 թվի դերը): Միավոր տարրը միակն է: Եթե ունենք երկու միավոր e_1 և e_2, ապա պարզ է, որ $e_1 = e_1e_2 = e_2$:

Երրորդ պայմանը Հաստատում է, որ ամեն մի $a \in G$ տարրի Համար կգտնվի մեկ $b \in G$, որ $ab = ba = e$: Այդպիսի b-ն կոչվում է a-ի **Հակադարձ** տարր և այն նշանակվում է a^{-1} նշանով (թեև ընդՀանուր դեպքում որևէ կապ չունի թվի Հակադարձի Հետ): Պարզ է, որ a-ն էլ իր Հերթին b-ի Հակադարձն է: Հակարդարձը միակն է: Եթե b_1-ը և b_2-ը a-ի Հակադարձներն են, ապա $b_1 = b_1(ab_2) = (b_1a)b_2 = b_2$:

Եթե բացի (1)-(3) պայմաններից ճիշտ է նաև

4. $\forall a,b \in G \;\; ab = ba$

պայմանը, ապա G խումբը կոչվում է **տեղափոխելի** կամ **աբելյան**:

Եթե ի սկզբանե ցանկանում են նշել, որ խումբը աբելյան է, բազմապատկման $\cdot$ նշանի փոխարեն օգտագործում են գումարման $+$ նշանը: Այդ դեպքում միավոր տարրը նշանակվում է 0-ով, իսկ a-ի Հակադարձը՝ $-a$-ով և այն անվանում են **Հակադիր**:

G խմբի գործողությունն "բազմապատկում" անվանելը և *ab*-ով նշանակելն արդարացված է այն բանով, որ գործողության կանոնները շատ նման են թվերի բազմապատկման կանոններին (և թվերի բազմապատկումն իրոք խումբ է սահմանում ոչ զրոյական իրական թվերի բազմության վրա)։ Դա թույլ է տալիս գործել օգտվելով հարմար դարձած թվաբանության ավանդական բանաձևերից։ Օրինակ, եթե ընդունենք որ $a^0 = e$ և նշանակենք a^n-ով (բնական n թվի համար) $\underbrace{a \cdot a \cdot \ldots \cdot a}_{n}$ արտադրյալը, իսկ a^{-n}-ով $\underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{n}$-ը, ապա դյուրին է համոզվել, որ կամայական ամբողջ m և n թվերի համար կիրառելի են հետևյալ ստանդարտ կանոնները.

$$a^m a^n = a^{m+n}$$
$$(a^m)^n = a^{mn}$$

Օրինակներ

1. Նշանակենք $\mathbb{Z}$-ով ամբողջ թվերի բազմությունը և որպես խմբի բազմապատկման գործողություն դիտարկենք ամբողջ թվերի գումարումը։ Նշանակենք ստացված համակարգը $(\mathbb{Z},+)$-ով։ Դյուրին ստուգվում է, որ $(\mathbb{Z},+)$-ն աբելյան խումբ է (որպես միավոր տարր վերցնում ենք 0 թիվը)։

2. Այժմ դիտարկենք $(\mathbb{Z},\cdot)$ համակարգը, որտեղ $\cdot$ -ը ամբողջ թվերի բազմապատկման գործողությունն է։ Ակնհայտ է, որ խմբի սահմանման (1) և (2) պայմանները բավարարվում են (որպես միավոր վերցնում ենք 1 թիվը)։ Սակայն (3) պայմանը տեղի չունի, քանի որ 0 թիվը չունի հակադարձ։ Եթե նույնիսկ հեռացնենք 0-ն և դիտարկենք $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ բազմությունը, ապա կրկին (3)-ը չի բավարարվում, քանի որ օրինակ 2-ը չունի հակադարձ ($\frac{1}{2}$ -ն ամբողջ թիվ չէ)։ Միայն 1-ը և -1-ն ունեն հակադարձ ըստ բազմապատկման։ Ուստի, ոչ $(\mathbb{Z},\cdot)$-ն ոչ էլ $(\mathbb{Z}^*,\cdot)$-ը խումբ չեն։

3. Դիտարկենք $(\mathbb{Q},+)$, $(\mathbb{R},+)$ և $(\mathbb{C},+)$ համակարգերը, որտեղ $\mathbb{Q}$-ն ռացիոնալ թվերի, $\mathbb{R}$-ն իրական և $\mathbb{C}$-ն կոմպլեքս թվերի բազմություններն են, իսկ $+$ -ը թվերի գումարումն է։ Դյուրին ստուգվում է, որ այս երեք համակարգերն աբելյան խմբեր են։ Նաև հեշտությամբ կարելի է համոզվել, որ $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ և $(\mathbb{C}\setminus\{0\},\cdot)$ համակարգերը նույնպես աբելյան խմբեր են։

4. Նշանակենք մնացքների դասերն ըստ $mod\, n$-ի $\mathbb{Z}_n$-ով, այսինքն $\mathbb{Z}_n=\{0,1,\ldots,n-1\}$։ $(\mathbb{Z}_n,+mod\, n)$ համակարգն ակնհայտորեն աբելյան խումբ է։ Ավելի հետաքրքրական է $(\mathbb{Z}_n^*,\cdot mod\, n)$ համակարգի դեպքը, որտեղ $\mathbb{Z}_n^*=\mathbb{Z}_n\setminus\{0\}$։ Դյուրին է ստուգել, որ խմբի սահմանման (1) և (2) պայմանները բավարարված են ($e=1$)։ Եթե $a\in\mathbb{Z}_n^*$, ապա այն ունի հակադարձ $\Leftrightarrow$ a-ն ու n-ը փոխադարձաբար պարզ են (սա բխում է թվերի ամենամեծ ընդհանուր բաժանարարը գտնելու Էվկլիդեսի ալգորիթմի հետևանքից՝ գոյություն ունեն $x,y\in\mathbb{Z}$, որ $ax+ny=(a,n)=1$, ուստի $ax\equiv 1\, mod\, n$)։ Ուրեմն $(\mathbb{Z}_n^*,\cdot mod\, n)$ համակարգը խումբ է միայն այն դեպքում երբ n-ը պարզ թիվ է։ Սակայն եթե դիտարկենք միայն n-ի հետ փոխադարձաբար պարզ թվերը $\mathbb{Z}_n^*$-ից, ապա դրանք խումբ կկազմեն, քանի որ n-ի հետ փոխադարձաբար պարզ թվերի արտադրյալը նույնպես փոխադարձաբար պարզ է և այդպիսին է նաև n-ի հետ փոխադարձաբար պարզ թվի հակադարձը։

5. Նշանակենք S_n-ով $\{1,2,\ldots,n\}$ թվերի տեղադրությունների բազմությունը։ Այդ բազմությունը խումբ է տեղադրությունների բազմապատկման գործողության նկատմամբ։ Նույնաբար տեղադրությունը դա միավոր տարրն է, իսկ հակադարձ տարրի գոյությունը ապահովվում է հակադարձ տեղադրությամբ: Այս խումբը աբելյան չէ, քանի որ ընդհանուր դեպքում տեղադրությունների բազմապատկումը տեղափոխելի չէ: S_n խումբը կոչվում է **սիմետրիկ** խումբ:

6. Դիտարկենք $n \times m$ չափանի իրական թվերով մատրիցների բազմությունը: Այդ բազմությունը կազմում է աբելյան խումբ մատրիցների գումարման գործողության նկատմամբ: Եթե $n = m$, ապա այս բազմությունը փակ է մատրիցների բազմապատկման գործողության նկատմամբ, սակայն այն խումբ չի կազմում, քանի որ ոչ բոլոր մատրիցներն ունեն հակադարձ ըստ բազմապատկման: Հայտնի է, որ $n \times n$ չափանի իրական A մատրիցն ունի հակադարձ միայն և միայն այն դեպքում, երբ $det A \neq 0$: Քանի որ $det AB = det A \, det B$, ապա չվերասերված (0-ից տարբեր դետերմինանտով) $n \times n$ չափանի իրական մատրիցների բազմությունը փակ է մատրիցների բազմապատկման գործողության նկատմամբ և այն կազմում է խումբ մատրիցների բազմապատկման գործողության նկատմամբ: Այդ խումբն աբելյան չէ: Ոչ աբելյան խումբ է կազմում (ըստ բազմապատկման) նաև $det A = 1$ պայմանին բավարարող $n \times n$ չափանի իրական մատրիցների բազմությունը:

7. Ֆիքսենք հարթության վրա որևէ կետ և դիտարկենք հարթության բոլոր պտույտներն այդ կետի շուրջ: Պտույտների բազմության վրա սահմանենք հետևյալ գործողությունը. α և β անկյուններով պտույտների արտադրյալը դա $\alpha + \beta$ անկյունով պտույտն է: Որպես միավոր տարր վերցնում ենք 0 անկյունով պտույտը: Պարզ է, որ α անկյունով պտույտի հակադարձը կլինի $-\alpha$ անկյունով պտույտը: Դյուրին է ստուգել, որ պտույտների բազմությունն աբելյան խումբ է:

8. *Դիտարկենք "Ռուբիկի խորանարդ" Հայտնի գլուխկոտրուկը։ Դժվար չէ տեսնել, որ խորանարդի "շերտերի" պտույտները խումբ են կազմում։*

Ենթախմբեր

Շատ դեպքերում անհրաժեշտ է լինում գործել խմբի ենթաբազմության հետ, որը նույնպես խումբ է սահմանված բազմապատկման գործողության նկատմամբ:

Սահմանում: G խմբի H ենթաբազմությունը կոչվում է **ենթախումբ**, եթե

$$a,b \in H \Rightarrow ab$$
$$a \in H \Rightarrow a^{-1} \in H$$

Առաջին պայմանը նշանակում է, որ H ենթաբազմությունը "փակ" է G-ի բազմապատկման գործողության նկատմամբ, այսինքն, H-ի տարրերի արտադրյալը դուրս չի գալիս H-ից: Երկրորդ պայմանը նշանակում է, որ H-ը "փակ" է հակադարձին անցնելու գործողության նկատմամբ: Քանի որ խմբի սահմանման ասոցիատիվության պայմանը ճիշտ է ամբողջ G-ի համար, ապա այն ճիշտ է նաև H-ի համար: Հակադարձի գոյությունը H-ում ապահովված է երկրորդ պայմանով: Նկատենք, որ միավոր տարրը միշտ պատկանում է ենթախմբին: Իսկապես, համաձայն երկրորդ պայմանի $a \in H \Rightarrow a^{-1} \in H$, ուրեմն առաջին պայմանից ստանում ենք՝ $a,a^{-1} \in H \Rightarrow aa^{-1} = e \in H$: Uստի, H-ը բավարարում է խմբի սահմանման բոլոր պայմաններին:

Ենթախմբի սահմանման երկու պայմանները կարելի է փոխարինել մեկ համարժեքով.

$$a,b \in H \Rightarrow a^{-1}b \in H \qquad (1)$$

Ակնհայտ է, որ (1)-ը բխում է ենթախմբի սահմանման պայմաններից: Ցույց տանք հակառակը: Եթե (1)-ում վերցնենք $a = b$ կստացվի $a,a \in H \Rightarrow a^{-1}a = e \in H$: Այժմ $a \in H \Rightarrow a,e \in H \Rightarrow a^{-1}e = a^{-1} \in H$, այսինքն ստացանք ենթախմբի սահմանման երկրորդ պայմանը: Ստույգ է նաև առաջին պայմանը՝

$$a,b \in H \Rightarrow a^{-1},b \in H \Rightarrow (a^{-1})^{-1}b = ab \in H:$$

Յուրաքանչյուր G խումբ ունի առնվազն երկու ենթախումբ՝ $\{e\}$-ն, որ կազմված է միայն միավոր տարրից և կոչվում է **տրիվիալ** ենթախումբ, և ամբողջ խումբը՝ G-ն: Այն ենթախմբերը, որոնց համար ճիշտ է $\{e\} \subset H \subset G$ պայմանը կոչվում են **սեփական** ենթախմբեր: Այն փաստը, որ H-ը G-ի ենթախումբն է նշանակվում է հետևյալ կերպ՝ $H \leq G$:

Օրինակներ

1. Գտնենք $(\mathbb{Z},+)$-ի բոլոր ենթախմբերը: Համաձայն (1)-ի $H \leq \mathbb{Z}$ միայն երբ $m,n \in H \Rightarrow m - n \in H$: Պարզ է, որ $0 \in H$ և $m \in H \Rightarrow -m \in H$: Եթե H-ը պարունակում է ոչ զրոյական թիվ m, ապա այն պարունակում է դրական թիվ: Նշանակենք d-ով H-ում պարունակվող ամենափոքր դրական թիվը: Պարզ է, որ $\{dx \mid x \in \mathbb{Z}\} \subseteq H$: Իսկապես,

$$d,-d \in H \Rightarrow d - (-d) = 2d \in H:$$

Նմանապես $d,-2d \in H \Rightarrow d - (-2d) = 3d \in H$ և այլն: Ցույց տանք, որ $H = \{dx \mid x \in \mathbb{Z}\}$: Վերցնենք կամայական m թիվ

*H-ից և մնացորդով բաժանենք այն d-ի վրա $m = dn + p$, $0 \le p < d$: **Պարզ** է, որ $p = m - dp \in H$: **Եթե** $0 < p < d$, ապա H-ում կգտնվի d-ից փոքր դրական թիվ ինչն անհնար է, ուստի $p = 0$ և $m = dn$, ուրեմն $H \subseteq \{dx \mid x \in \mathbb{Z}\}$: Այսպիսով, գտանք $(\mathbb{Z},+)$-ի բոլոր ենթախմբերը: Նրանք ունեն $\{dx \mid x \in \mathbb{Z}\}$ տեսքը, այսինքն ինչ որ մի որոշակի թվի (H-ում պարունակվող ամենափոքր դրական թվի կամ էլ 0-ի) բոլոր պատիկներից կազմված բազմություններն են:*

2. *Ակնհայտ է, որ $(\mathbb{Q},+) \le (\mathbb{R},+) \le (\mathbb{C},+)$ և $(\mathbb{Q}\setminus\{0\},\cdot) \le (\mathbb{R}\setminus\{0\},\cdot) \le (\mathbb{C}\setminus\{0\},\cdot)$:*

3. *Նշանակենք A_n-ով $\{1,2,\ldots,n\}$ թվերի զույգ տեղադրությունների բազմությունը (այն կոչվում է* ***Նշանափոխ*** *խումբ): Դյուրին է ստուգել, որ $A_n \le S_n$:*

4. *$detA = 1$ պայմանին բավարարող $n \times n$ չափանի իրական մատրիցների խումբը $detA \neq 0$ պայմանին բավարարող $n \times n$ չափանի իրական մատրիցների խմբի ենթախումբն է:*

5. *Ֆիքսած կետի շուրջ հարթության 60^o-ին պատիկ անկյուններով պտույտների բազմությունը ենթախումբ է բոլոր պտույտների բազմության մեջ:*

Իզոմորֆիզմ

Սահմանում: $f : G_1 \to G_2$ փոխմիարժեք արտապատկերումը G_1 խմբից G_2-ի վրա կոչվում է **իզոմորֆիզմ**, եթե

$$f(ab) = f(a)f(b) \quad \text{բոլոր } a,b \in G_1 \qquad (2)$$

G_1 և G_2 խմբերը կոչվում են **իզոմորֆ**: Եթե $G_1 = G_2$, ապա $f : G_1 \to G_2$ իզոմորֆիզմը կոչվում է **ավտոմորֆիզմ**:

Իզոմորֆիզմի ժամանակ միավոր տարրը միշտ անցնում է միավորի մեջ. $f(e) = f(ee) = f(e)f(e)$ ուստի $f(e) = e$: Հակադարձն անցնում է հակադարձի մեջ. $e = f(e) = f(aa^{-1}) = f(a)f(a^{-1})$ ուստի $f(a^{-1}) = (f(a))^{-1}$:

Դիտարկենք իզոմորֆիզմի հետևյալ օրինակը: Դիցուք $G_1 = (\mathbb{R}^+, \cdot)$ իրական դրական թվերի խումբն է ըստ բազմապատկման իսկ $G_2 = (\mathbb{R}, +)$ իրական թվերի խումբն է ըստ գումարման: Իզոմորֆիզմն իրականացվում է $y = \ln x$ ֆունկցիայի միջոցով, քանի որ տեղի ունեն $\ln(x_1x_2) = \ln x_1 + \ln x_2$, $\ln 1 = 0$ և $\ln x^{-1} = -\ln x$ հատկությունները:

Դիտարկենք մեկ այլ օրինակ ևս: $n \times n$ չափանի մատրիցը կոչվում է **տեղափոխության մատրից**, եթե մատրիցի տարրերը կամ զրոներ են կամ էլ մեկեր և յուրաքանչյուր տողում կամ սյունում բոլոր տարրերը բացի մեկից զրոյական են, այսինքն ամեն տողում կամ սյունում գոյություն ունի ճիշտ մեկ հատ 1 և մնացած տարրերը 0 են: Դիցուք $P = (a_{ij})_{n\times n}$-ն տեղափոխության մատրից է: Այդ մատրիցի հետ կարելի է կապել մի տեղադրություն, որը կնշանակենք π-ով և $\pi(i)$-ով կնշանակենք այն j թիվը, որի մեջ է տանում i-ն π տեղադրությունը, այսինքն՝

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}:$$

π տեղադրությունը կառուցվում է հետևյալ կերպ. որպեսզի որոշենք $\pi(1)$-ը, նախ գտնում ենք, թե մատրիցի առաջին տողում, որ տեղում է գտնվում 1-ը, այսինքն գտնում ենք այն j-ն, որ $a_{1j} = 1$ և $\pi(1)$-ը վերցնում ենք հավասար j-ին: $\pi(2)$-ը վերցնում ենք հավասար այն միակ j-ն, որ $a_{2j} = 1$, այսինքն երկրորդ տողում որոշում ենք մեկի տեղը: $\pi(2)$-ն անպայման կտարբերվի $\pi(1)$-ից, քանի որ հակառակ դեպքում կստացվի, որ միևնույն սյունում կա երկու հատ 1: Շարունակելով մեկերի տեղերը գտնելը տողերում որոշում ենք π տեղադրությունը: Ասում են, որ այս տեղադրությունը որոշվում է ըստ P մատրիցի տողերի: π տեղադրությունը լրիվին բնորոշվում է հետևյալ պայմանով

$$\pi(i) = j \Leftrightarrow a_{ij} = 1 \tag{3}$$

Նման եղանակով, որոշելով մեկերի տեղերը սյուներում, կարելի է կառուցել մեկ այլ տեղադրություն σ, որի համար կստանանք

$$\sigma(i) = j \Leftrightarrow a_{ji} = 1 \tag{4}$$

Համեմատելով (3)-ը և (4)-ը դյուրին է տեսնել, որ $\sigma = \pi^{-1}$: Որպեսզի նշենք P մատրիցի հետ կապված տեղադրությունները կօգտվենք հետևյալ նշանակումից՝ P_{π}^{σ}: Պարզ է, որ եթե տրված է որևէ տեղադրություն, ապա ընդունելով այն որպես ըստ տողերի տեղադրություն, հեշտությամբ կարելի է կառուցել այն միակ տեղափոխության մատրիցը, որի համար այդ տեղադրությունն ըստ տողերի տեղադրությունն է: Այսպիսով ստանում ենք փոխմիարժեք համապատասխանեցում տեղադրությունների և տեղափոխության մատրիցների միջև (հեշտությամբ կարելի է համոզվել, որ տեղափոխության մատրիցների քանակը $n!$ է՝ հավասար է տեղադրությունների քանակին):

Դիցուք տրված են երկու տեղափոխության մատրիցներ՝ $P_{\pi}^{\sigma\pi} = (a_{ij})_{n\times n}$ և $P_{\mu}^{\tau} = (b_{ij})_{n\times n}$: Նշանակենք c_{ij}-ով $P_{\pi}^{\sigma}P_{\mu}^{\tau}$ արտադրյալի տարրը՝ $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$: Քանի որ c_{ij}-ն հաշվելու համար P_{π}^{σ}-ի i-րդ տողը բազմապատկվում է P_{μ}^{τ}-ի j-րդ սյունով, ապա կամ այդ տողի և սյան մեկերի տեղերը համընկնում են և արդյունքում $c_{ij} = 1$, կամ էլ մեկերի տեղերը չեն համընկնում և $c_{ij} = 0$: Օգտվելով (3)-ից ու (4)-ից ստանում ենք. $c_{ij} = 1 \Leftrightarrow \exists$ միակ k, որ $a_{ik} = b_{kj} = 1 \Leftrightarrow \pi(i) = k,\ \ \mu(k) = j \Leftrightarrow (\pi\mu)(i) = j$: Այսինքն տեղափոխության մատրիցների արտադրյալը նորից տեղափոխության մատրից է և

$$P_{\pi}^{\sigma}P_{\mu}^{\tau} = P_{\pi\mu}^{\tau\sigma} \qquad (5)$$

Պարզ է, որ P_{π}^{σ}-ի տրանսպոնացված (շրջված) մատրիցը դա P_{σ}^{π}-ն է: (5)-ից ստանում ենք՝

$$P_{\pi}^{\sigma}P_{\sigma}^{\pi} = P_{\pi\sigma}^{\pi\sigma} = E, \qquad (6)$$

որտեղ E-ն միավոր մատրիցն է, ուստի տեղափոխության մատրիցի հակադարձը դա տրանսպոնացված մատրիցն է:

Նկատենք, որ եթե բազմապատկենք P_{π}^{σ}-ն որևէ A մատրիցով, ապա արդյունքում $P_{\pi}^{\sigma}A$ մատրիցը կստացվի A-ից տողերի տեղափոխությամբ համաձայն σ տեղադրության: AP_{π}^{σ} էլ ստացվում է A-ից սյուների տեղափոխությամբ համաձայն π տեղադրության:

(5)-ից և (6)-ից հետևում է, որ $n \times n$ չափանի տեղափոխության մատրիցները խումբ են կազմում ըստ մատրիցների բազմապատկման գործողության:

Կառուցենք հետևյալ փոխմիարժեք արտապատկերումը S_n-ից $n \times n$ չափանի տեղափոխության մատրիցների խմբի վրա.

$$f(\pi) = P_\pi \tag{7}$$

(5)-ից անմիջապես ստանում ենք, որ (7)-ը իզոմորֆիզմ է:

Գոյություն ունի միակ եղանակ տեղափոխության մատրիցում ամեն տողից և ամեն սյունից տարրերն այնպես ընտրելու, որ արտադրյալը լինի ոչ զրոյական: Այդ պատճառով տեղափոխության մատրիցի դետերմինանտը հավասար է ± 1, ավելի ստույգ, այն հավասար է 1-ի եթե π տեղադրությունը զույգ է և -1-ի երբ π տեղադրությունը կենտ է: Ուստի (7)-ով տրված իզոմորֆիզմի ժամանակ զույգ տեղադրություններին համապատասխանում են 1 դետերմինանտով տեղափոխության մատրիցները, իսկ կենտերին՝ -1:

Վերը բերված օրինակներից և, իհարկե, իզոմորֆիզմի սահմանումից պարզ է դառնում, որ իզոմորֆ խմբերը մեկը մյուսի պատճենն են և բազմապատկման գործողության հետ կապված որևէ հատկություն ուսումնասիրելիս իզոմորֆ խմբերն իրարից չպետք է տարբերել: Կամայական փաստ, որ վերաբերվում է բազմապատկման գործողությանը և տեղի ունի մի խմբում տեղի ունի նաև նրան իզոմորֆ խմբում: Այդ իսկ պատճառով խմբերի տեսության մեջ իզոմորֆ խմբերը համարվում են համարժեք և նույնացվում են:

Թեորեմ 1 (Քելիի թեորեմ). Եթե G խմբի տարրերի քանակը վերջավոր է և հավասար է n-ի, ապա G խումբն իզոմորֆ է S_n-ի n տարրանոց ենթախմբերից մեկին:

Ապացույց. Յուրաքանչյուր $g \in G$ համար սահմանենք մի արտապատկերում $f_g : G \to G$ հետևյալ կերպ՝ $f_g(x) = gx$: Ակնհայտ է, որ $f_g(x_1) = f_g(x_2) \Rightarrow x_1 = x_2$, այսինքն f_g-ն փոխմիարժեք է: Եթե $y \in G$, ապա վերցնելով $x = g^{-1}y$ ստանում ենք՝ $f_g(x) = g(g^{-1}y) = y$: Ուրեմն f_g-ն փոխմիարժեքորեն արտապատկերում է G-ն G-ի վրա: Համարակալենք G-ի տարրերը՝ $G = \{a_1, \ldots, a_n\}$: Յուրաքանչյուր f_g-ն լրիվ նկարագրվում է n տարրանոց տեղադրությամբ՝

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ f_g(a_1) & f_g(a_2) & \ldots & f_g(a_n) \end{pmatrix} =$$

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ ga_1 & ga_2 & \ldots & ga_n \end{pmatrix} =$$

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_n \\ a_{i_1} & a_{i_2} & \ldots & a_{i_n} \end{pmatrix}:$$

Վերջին տեղադրությունը պարզապես կարելի է փոխարինել համարժեքով

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

որը կնշանակենք $\pi(f_g)$-ով:

Դյուրին է ստուգել, որ f_g արտապատկերումները խումբ են կազմում կոմպոզիցիայի (հաջորդաբար կիրառման) գործողության նկատմամբ (այնպես ինչպես նաև $\pi(f_g)$ տեղադրությունները)՝

$$\begin{gathered} (f_g \cdot f_h)(x) = f_g(f_h(x)) = g(hx) = (gh)x = f_{gh}(x) \\ \pi(f_g \cdot f_h) = \pi(f_{gh}) = \pi(f_g)\pi(f_h) \end{gathered} \qquad (8)$$

Պարզ է, որ միավոր տարրը f_e-ն նույնաբար արտապատկերում է և $f_{g^{-1}} = (f_g)^{-1}$ (սա անմիջապես հետևում է (8)-ից): f_g արտապատկերումներին համապատասխանող տեղադրությունների խումբը նշանակենք $F(G)$-ով: Պարզ է, որ $F(G) \le S_n$:

Կառուցենք այժմ φ փոխմիարժեք արտապատկերումը G-ից $F(G)$ հետևյալ կերպ.

$$\varphi(g) = \pi(f_g)$$

Դյուրին է համոզվել, որ $\varphi : G \to F(G)$ իզոմորֆիզմ է, իսկապես $\varphi(gh) = \pi(f_{gh}) = \pi(f_g)\pi(f_h) = \varphi(g)\varphi(h)$ և թեորեմն ապացուցված է:

Թեորեմ 1-ից հետևում է, որ վերջավոր խմբերի ուսումնասիրությունը հանգեցվում է սիմետրիկ խմբի՝ S_n-ի ենթախմբերի ուսումնասիրմանը: Հարկ է նշել, որ Թեորեմ 1-ը հեշտությամբ կարելի է ընդհանրացնել նաև անվերջ խմբերի համար:

Հոմոմորֆիզմ

Սահմանում: Դիցուք G_1-ը և G_2-ը խմբեր են: $f : G_1 \to G_2$ արտապատկերումը կոչվում է **հոմոմորֆիզմ**, եթե

$$f(ab) = f(a)f(b)$$

Այդ դեպքում ասում են, որ G_1 խումբը **հոմոմորֆ** է G_2-ին:

Ակնհայտ է, որ իզոմորֆ խմբերը նաև հոմոմորֆ են: Իզոմորֆ խմբերը մեկը մյուսի ճշգրիտ պատճեններն են: Հոմոմորֆիզմի դեպքում երկրորդ խումբն առաջինի, ինչ որ իմաստով, "աղավաղված" պատճենն է. սակայն այդ երկրորդ խումբը պարունակում է իր մեջ առաջին խմբին վերաբերող որոշակի ինֆորմացիա:

Օրինակներ

1. $f : G_1 \to G_2$ և $f(x) = e$ բոլոր $x \in G_1$ համար: Ակնհայտ է որ f-ը հոմոմորֆիզմ է:

2. Դիցուք G-ն կամայական խումբ է: Ֆիքսենք որևէ $a \in G$: Դիտարկենք հետևյալ արտապատկերումը՝ $f : (\mathbb{Z},+) \to G$, որտեղ $f(n) = a^n$: Պարզ է, որ $f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$ և f-ը հոմոմորֆիզմ է:

3. Այսուհետև $x = y \, modulo \, n$ գրառումը նշանակի որ x-ը y-ի մնացորդն է, որ ստացվում է y-ը n-ի վրա բաժանելիս: Սահմանենք հետևյալ արտապատկերումը՝ $f : (\mathbb{Z},+) \to (\mathbb{Z}_n,+)$ որպես $f(m) = m \, modulo \, n$: Ակնհայտ է, որ սա հոմոմորֆիզմ է և $f(s+t) = f(s) + f(t)$ (նկատենք, որ առաջին գումարման նշանը դա ամբողջ թվերի սովորական գումարումն է, իսկ երկրորդը՝ մնացքների դասերի ըստ $mod\, n$-ի գումարումը): Բացի դրանից տեղի ունի նաև $f(st) = f(s)f(t)$ բանաձևը, որտեղ առաջին բազմապատկումն ամբողջ թվերի սովորական բազմապատկումն է, իսկ երկրորդը՝ մնացքների դասերի ըստ $mod\, n$-ի բազմապատկումը: Այսինքն հոմոմորֆիզմը պահպանում է n-ի վրա բաժանելիության հետ կապված բոլոր հատկությունները: Պարզ է, որ եթե ամբողջ գործակիցներով $g(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ բազմանդամի փոփոխականի փոխարեն տեղադրենք s և t թվերը, որոնց համար ճիշտ է, որ $s \equiv t\, mod\, n$, ապա $g(s) \equiv g(t)\, mod\, n$: Այս փաստը թույլ է տալիս հեշտությամբ ստանալ հայտնի բաժանելիության հայտանիշները: Դիցուք m ամբողջ թիվը տրված է տասական հիմքով, այսինքն $m = \alpha_0 + \alpha_1 10 + \ldots + \alpha_n 10^n$ տեսքով: Քանի որ $10 \equiv 1\, mod\, 3$ և $10 \equiv 1\, mod\, 9$, ապա $m \equiv \alpha_0 + \alpha_1 + \ldots + \alpha_n\, mod\, 3$ կամ $mod\, 9$: Նույն ձևով օգտվելով $10 \equiv -1\, mod\, 11$-ից ստանում ենք 11-ի համար բաժանելիության շատ լավ հայտնի հայտանիշը՝ $m \equiv \alpha_0 - \alpha_1 + \alpha_2 - \ldots + (-1)^n \alpha_n\, mod\, 11$: Եթե m ամբողջ թիվը տրված է երկուական հիմքով $m = \alpha_0 + \alpha_1 2 + \ldots + \alpha_n 2^n$, ապա, օրինակ 3-ի, բաժանելիության հայտանիշը կստացվի հետևյալ կերպ. քանի որ $2 \equiv -1\, mod\, 3$, ապա

$$m \equiv \alpha_0 - \alpha_1 + \alpha_2 - \ldots + (-1)^n \alpha_n\, mod\, 3:$$

Հարակից դասեր

Սահմանում: Դիցուք H-ը G խմբի ենթախումբն է, այսինքն $H \leq G$ և $a \in G$:

G խմբի ըստ H ենթախմբի a տարրով ծնված **ձախ հարակից դաս** է կոչվում հետևյալ բազմությունը՝

$$aH = \{ah \mid h \in H\}$$

Նման եղանակով սահմանվում է **աջ հարակից դասը**՝ $Ha = \{ha \mid h \in H\}$: Ստորև կուսումնասիրենք ձախ հարակից դասերը: Առանց որևէ դժվարության ստուգվում է, որ բոլոր ստացված արդյունքները ճիշտ են նաև աջ հարակից դասերի համար: Այդ պատճառով, հարմարության համար, ձախ հարակից դասերը կանվանենք ուղղակի հարակից դասեր: Անհրաժեշտության դեպքում դասերի տեսակը հատուկ կնշվի:

Հետազոտենք հարակից դասերի հատկությունները.

1. $a \in aH$

2. **բոլոր հարակից դասերն ունեն միևնույն հզորությունը.** $ah \leftrightarrow h$ օրենքով սահմանված փոխմիարժեք համապատասխանեցումը aH-ի և H-ի միջև ապացուցում է այս պնդումը ($ah_1 = ah_2 \Rightarrow h_1 = h_2$):

3. $aH = bH \Leftrightarrow b^{-1}a \in H$ և $a^{-1}b \in H$ - սա երկու տարրերով ծնված հարակից դասերի համընկման անհրաժեշտ և բավարար պայմանն է (նկատենք, որ $b^{-1}a \in H$ և $a^{-1}b \in H$ պայմանները տեղի ունեն կամ չունեն միաժամանակ և քանի որ H-ը ենթախումբ է, ապա $b^{-1}a \in H \Leftrightarrow (b^{-1}a)^{-1} = a^{-1}b \in H$): Ապացուցենք հատկությունը: Դիցուք $aH = bH$: Որեմն $a = bh,\ h \in H$ և $b^{-1}a = h \in H$: Դիցուք $b^{-1}a \in H$: Որեմն $b^{-1}a = h$ և $a = bh$: Դիցուք $ah_1 \in aH$, ապա $ah_1 = b(hh_1) \in bH$ քանզի $hh_1 \in H$: Ուստի $aH \subseteq bH$: Նման ձևով $a^{-1}b \in H$ պայմանից ստանում ենք որ $bH \subseteq aH$:

4. $aH = H \Leftrightarrow a \in H$ - սա նախորդ հատկության հետևանքն է՝ $b = e$ և $b^{-1}a = a$:

5. $aH \cap bH \neq \varnothing \Rightarrow aH = bH$ - իրոք, եթե $c \in aH \cap bH$, ապա $c = ah_1 = bh_2$ և $b^{-1}a = h_2h_1^{-1} \in H$, ուստի $aH = bH$:

6. $a \in bH \Rightarrow aH = bH$ - սա նշանակում է, որ հարակից դասի կամայական տարր ծնում է այդ նույն դասը:

Սահմանում. G խմբի **կարգ** է կոչվում G բազմության հզորությունը (վերջավոր G-ի դեպքում պարզապես տարրերի քանակը) և այն նշանակվում է $(G : 1)$-ով:

H ենթախմբի **ինդեքսը (դասիչը)** G խմբում դա ըստ H-ի հարակից դասերի բազմության հզորությունն է: Այն նշանակվում է $(G : H)$-ով:

Թեորեմ 2. (Լագրանժի թեորեմը)

Դիցուք $H \leq G$: Ստույգ է հետևյալ բանաձևը.

$$(G : 1) = (G : H)(H : 1) \tag{9}$$

Ապացույց. Քանի որ բոլոր հարակից դասերն ունեն միևնույն հզորությունը, նրանց միավորումը ծածկում է ամբողջ G-ն և հարակից դասերը զույգ առ զույգ չեն հատվում, ապա խմբի կարգը ստանալու համար հարկավոր է հարակից դասերի քանակը *բազմապատիկը H-ի կարգով:*

Լագրանժի թեորեմը ճիշտ է նաև անվերջ կարգ ունեցող խմբերի համար: Ավելի ստույգ, եթե (9)-ում երեք մեծություններից երկուսը վերջավոր են, ապա երրորդ էլ է վերջավոր:

Հետևանք.

Վերջավոր (այսինքն վերջավոր կարգ ունեցող) խմբի ենթախմբի կարգը խմբի կարգի բաժանարար է:

Օրինակ, եթե խմբի կարգը պարզ թիվ է, ապա այն ունի միայն երկու ենթախումբ՝ տրիվիալը և ամբողջ խումբը և չունի ոչ մի սեփական ենթախումբ:

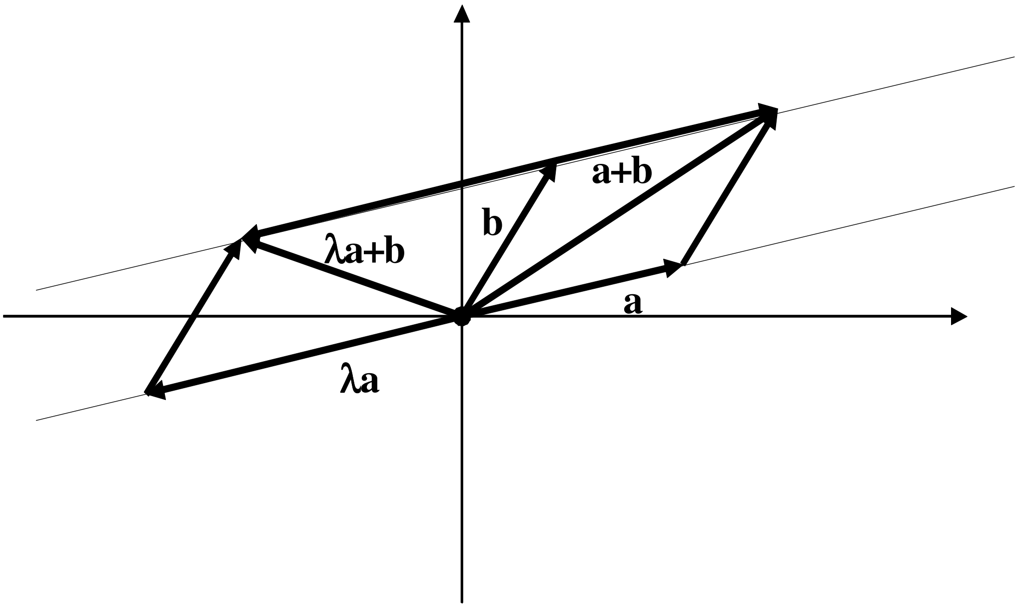
Օրինակներ

1. *Դիցուք $G = S_n$, իսկ $H = A_n$ (հիշեցնենք, որ S_n-ը սիմետրիկ խումբն է, իսկ A_n-ը նշանափոխ խումբն է n տարրանի զույգ տեղադրությունների խումբը): Ունենք, որ $A_n \leq S_n$: Ինչպես գիտենք $(S_n : 1) = n!$ և $(A_n : 1) = \frac{n!}{2}$: Համաձայն հարակից դասերի 3. հատկության (երկու տարրի միևնույն հարակից դասին պատկանելու անհրաժեշտ և բավարար պայմանի) π և σ տեղադրությունները կլինեն ըստ A_n-ի միևնույն հարակից դասից միայն և միայն երբ $\pi^{-1}\sigma \in A_n$, այսինքն $\pi^{-1}\sigma$-ն զույգ տեղադրություն է, իսկ դա հնարավոր է միայն, եթե π-ի և σ-ի զույգությունները նույնն են: Ուստի բոլոր զույգ տեղադրությունները կազմում են հարակից դաս՝ A_n-ը և բոլոր կենտ տեղադրությունները նույնպես հարակից դաս են կազմում, որի տարրերը կարելի է ստանալ վերցնելով կամայական կենտ π տեղադրություն և* *կառուցելով πA_n հարակից դասը: Ակնհայտ է, որ $(S_n : A_n) = 2$ և Լագրանժի թեորեմը ստանում է հետևյալ տեսքը*

$$n! = (S_n : 1) = (S_n : A_n)(A_n : 1)$$

2. *Դիցուք $G = \mathbb{Z}$ և $H = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$: Այստեղ երկու խմբերն էլ դիտարկում ենք ըստ գումարման: Ինչպես գիտենք $n\mathbb{Z} \leq \mathbb{Z}$ և երկու խմբերն էլ անվերջ են: Երկու ամբողջ թվեր p-ն և q-ն կլինեն միևնույն հարակից դասից ըստ $n\mathbb{Z}$-ի միայն և միայն եթե $p - q \in n\mathbb{Z}$: Վերջին պայմանը համարժեք է հետևյալին՝ $p \equiv q mod n$: Ուստի երկու թիվ նույն դասից են միայն եթե դրանք միևնույն ըստ $mod n$-ի մնացքների դասից են: Այսինքն ըստ $n\mathbb{Z}$-ի հարակից դասերը դրանք ըստ $mod n$-ի մնացքների դասերն են: Չնայած $(\mathbb{Z} : 1)$-ը և $(n\mathbb{Z} : 1)$-ն անվերջ են, $n\mathbb{Z}$-ի ինդեքսը $\mathbb{Z}$-ում վերջավոր է՝ $(\mathbb{Z} : n\mathbb{Z}) = n$:*

3. *Դիտարկենք հարթության մեջ գտնվող վեկտորների բազմությունը, որն աբելյան խումբ է կազմում վեկտորների գումարման գործողության նկատմամբ: Ֆիքսած $\mathbf{a}$ վեկտորին կոլինեար վեկտորների բազմությունը կազմում է ենթախումբ: $\mathbf{b}$ և $\mathbf{c}$ վեկտորները կպատկանեն միևնույն հարակից դասին ըստ $\mathbf{a}$-ին կոլինեար վեկտորների ենթախմբի միայն և միայն եթե $\mathbf{b} - \mathbf{c}$ վեկտորը լինի կոլինեար $\mathbf{a}$-ին: Այսինքն հարակից դասը, որ ծնված է $\mathbf{b}$ վեկտորով դա հետևյալ բազմությունն է՝ $\{\mathbf{b} + \boldsymbol{\lambda}\mathbf{a} \mid \boldsymbol{\lambda} \in \mathbb{R}\}$: $\mathbf{a}$-ին կոլինեար բոլոր վեկտորները, որոնց սկզբնակետը կոորդինատային համակարգի սկիզբն է գտնվում են միևնույն ուղղի վրա, որն անցնում է 0 կետով: Ստորև բերված նկարից երևում է, որ $\{\mathbf{b} + \boldsymbol{\lambda}\mathbf{a} \mid \boldsymbol{\lambda} \in \mathbb{R}\}$ բազմության բոլոր վեկտորների ծայրակետերն ընկած են միևնույն ուղղի վրա, որը զուգահեռ է $\mathbf{a}$-ով որոշված ուղղին: Պարզ է, որ կամայական վեկտոր, որի սկզբնակետը 0-ն է, իսկ ծայրակետն ընկած է նշված ուղղի վրա պատկանում է $\{\mathbf{b} + \boldsymbol{\lambda}\mathbf{a} \mid \boldsymbol{\lambda} \in \mathbb{R}\}$ բազմությանը:*



Ուստի, ըստ **a**-ին կոլինեար վեկտորների ենթախմբի հարակից դասերը միարժեքորեն որոշվում են **a**-ին զուգահեռ ուղիղներով, ընդ որում յուրաքանչյուր ուղղին համապատասխանում է մեկ հարակից դաս: Այս դեպքում Լագրանժի թեորեմի բանաձևում մասնակցող բոլոր մեծություններն անվերջ են:

Նորմալ ենթախմբեր

Դիցուք $H \le G$: Դիտարկենք ըստ H-ի հարակից դասերի բազմությունը, որն անվանում են ֆակտոր-բազմություն և նշանակում են հետևյալ կերպ՝ $G \diagdown H$: Փաստորեն $G \diagdown H$-ի հզորությունը հավասար է $(G : H)$-ին: Փորձենք այժմ սահմանել բազմապատկման գործողություն $G \diagdown H$-ի վրա այնպես, որ այն բավարարի խմբի սահմանման պայմաններին: Ամենբնական եղանակը, որով կարելի կլիներ սահմանել հարակից դասերի բազմապատկումը դա

$$(aH)(bH) = (ab)H \tag{10}$$

բանաձևն է: Սակայն, քանի որ (10) բանաձևում դասերի բազմապատկումը սահմանված է տարրերի բազմապատկման միջոցով, ապա անհրաժեշտ է համոզվել որ սահմանումը կոռեկտ է, այսինքն բազմապատկման արդյունքը կախված չէ այն երկու կոնկրետ a և b տարրերից, որոնք վերցվում են բազմապատկվող դասերից: Ավելի ստույգ, հարկավոր է, որ ինչպիսի c և d տարրեր էլ վերցնենք aH-ից և bH-ից համապատասխանաբար, ստանանք $(cd)H = (ab)H$:

Ուրեմն, դիցուք $c \in aH$ և $d \in bH$: Որպեսզի $(cd)H = (ab)H$ անհրաժեշտ է և բավարար, որ

$$(ab)^{-1}(cd) = b^{-1}a^{-1}cd \in H \tag{11}$$

Դիտարկենք (11)-ի մասնավոր դեպքը, երբ $b = d$: Այս դեպքում (11)-ը կարտագրվի որպես $b^{-1}a^{-1}cb \in H$: Նշանակենք $h = a^{-1}c \in H$ (սա անմիջապես հետևում է $c \in aH$ պայմանից) և $b^{-1}a^{-1}cb = b^{-1}hb \in H$, այսինքն որպեսզի հարակից դասերի բազմապատկումը (10) բանաձևով լինի կոռեկտ անհրաժեշտ է, որ

$$\forall b \in G\ \forall h \in H \quad b^{-1}hb \in H \tag{12}$$

Այս պայմանը նաև բավարար է, քանի որ ընդհանուր դեպքում (12)-ից ստանում ենք $b^{-1}h = h_1 b^{-1}$ որոշակի $h_1 \in H$ համար և $d \in bH$-ից ստանում ենք $b^{-1}d \in H$ և, վերջապես, $b^{-1}a^{-1}cd = b^{-1}hd = h_1 b^{-1}d \in H$: Ուստի (12) պայմանը հանդիսանում է այն որոշիչ հանգամանքը, որը թույլ է տալիս (10) բանաձևի օգնությամբ սահմանել հարակից դասերի բազմապատկումը:

Սահմանում: G խմբի H ենթախումբը կոչվում է նորմալ (կամ *ինվարիանտ*) G-ում, եթե

$$x^{-1}Hx \subseteq H,\ \forall x \in G \tag{13}$$

որտեղ $x^{-1}Hx = \{x^{-1}hx \mid h \in H\}$:

$H \lhd G$ գրառումը կնշանակի, որ H-ը նորմալ է G-ում:

Բազմապատկելով (13)-ը ձախից x-ով և աջից x^{-1}-ով կստանանք $H \subseteq xHx^{-1}$: Քանի որ x-ը կամայական է կարող ենք x-ը փոխարինել x^{-1}-ով և ուրեմն $H \subseteq x^{-1}Hx$ և $x^{-1}Hx = H$: Պարզ է, որ համարժեք է նաև $Hx = xH$ պայմանը (ձախ և աջ հարակից դասերի հավասարությունը): Ուստի $\forall x \in G\ \ x^{-1}Hx = H$ և $\forall x \in G\ \ Hx = xH$ պայմանները համարժեք են (13)-ին և կարող են ընդունվել որպես նորմալ ենթախմբի սահմանում:

Վերը կատարված դիտարկումներից հետևում է

որպեսզի (10) բանաձևով սահմանված հարակից դասերի բազմապատկումը լինի կոռեկտ, անհրաժեշտ է և բավարար, որ H ենթախումբը լինի նորմալ G-ում:

Օրինակներ

1. Աբելյան խմբի կամայական ենթախումբ նորմալ է:

2. Դիտարկենք S_n սիմետրիկ խմբի A_n նշանափոխ ենթախումբը: Արդեն տեսել էինք, որ $(S_n : A_n) = 2$, ուստի ըստ A_n-ի ձախ և աջ հարակից դասերը համընկնում են (մի դասը հենց A_n է, իսկ մյուսը՝ կենտ տեղադրությունների բազմությունն է): Ուրեմն A_n-ը նորմալ է S_n-ում և $A_n \triangleleft S_n$:

3. Դիցուք $H \leq G$ և $(G : H) = 2$: Նախորդ օրինակի դիտարկումից պարզ է որ H-ը նորմալ է G-ում:

Ֆակտոր-խումբ

Ստուգենք այժմ, որ (10)-ով սահմանված հարակից դասերի բազմապատկումը նորմալ ենթախմբերի դեպքում բավարարում է խմբի սահմանման պայմաններին:

Ասոցիատիվության պայմանը ստույգ է՝

$$((aH)(bH))(cH) = ((ab)H)(cH) =$$

$$((ab)c)H = (a(bc))H =$$

$$(aH)((bc)H) = (aH)((bH)(cH))$$

ուստի կարելի է գրել ուղղակի abH կամ $abcH$ և այլն:

Միավոր տարրը դա $eH = H$ հարակից դասն է՝ $(aH)(eH) = aeH = aH = eaH = H(aH)$:

Յուրաքանչյուր aH դաս ունի հակադարձ՝ այն է $a^{-1}H$ դասը. $(aH)(a^{-1}H) = aa^{-1}H = H$:

Այսպիսով ապացուցեցինք, որ

$G\setminus H$ ֆակտոր-բազմությունը խումբ է ըստ (10) բանաձևով սահմանված հարակից դասերի բազմապատկման գործողության միայն և միայն այն դեպքում, երբ H ենթախումբը նորմալ է G-ում:

*Այսուհետև, երբ $H \lhd G$ և ֆակտոր-բազմությունը խումբ է այդ խումբը կանվանենք **ֆակտոր-խումբ** (ըստ H **ենթախմբի**) և $G\setminus H$ նշանով կնշանակենք այդ խումբը:*

Հոմոմորֆիզմի կառուցվածքը

Ամեն մի $f : G_1 \to G_2$ հոմոմորֆիզմի հետ կապվում են հետևյալ երկու բազմությունները՝ **միջուկը**

$$\ker f = \{x \in G_1 \mid f(x) = e\}$$

և պատկերը

$$\operatorname{Im} f = \{y \in G_2 \mid \exists x \in G_1\ f(x) = y\}$$

Նկատենք, որ միջուկը չի կարող դատարկ լինել, քանի որ $f(e) = e$ և ուրեմն $e \in \ker f$:

Համոզվենք, որ միջուկը G_1-ի և պատկերը G_2-ի ենթախմբերն են: Դրա համար ստուգենք (1) պայմանի ճշտությունը:

Դիցուք $x_1, x_2 \in \ker f$, ապա

$$f(x_1^{-1}x_2) = f(x_1^{-1})f(x_2) = (f(x_1))^{-1}f(x_2) = e$$

քանի որ $f(x_1) = f(x_2) = e$: (1)-ը ստույգ է:

Միջուկը նորմալ ենթախումբ է G_1-ում: Իրոք, եթե $h \in \ker f$, ապա $f(x^{-1}hx) = f(x^{-1})f(h)f(x) = f(x)^{-1}ef(x) = f(x)^{-1}f(x) = e$ և $x^{-1}hx \in \ker f$:

Դիցուք $y_1, y_2 \in \operatorname{Im} f$: Կգտնվեն $x_1, x_2 \in G_1$, որ $f(x_1) = y_1$ և $f(x_2) = y_2$: Ունենք $f(x_1^{-1}x_2) = (f(x_1))^{-1}f(x_2) = y_1^{-1}y_2$, ուստի $y_1^{-1}y_2 \in \operatorname{Im} f$ և (1)-ը ստույգ է:

Քանի որ պատկերն ենթախումբ է G_2-ում, ապա ակնհայտ է, որ f արտապատկերումը G_1-ից $\operatorname{Im} f$ նույնպես հոմոմորֆիզմ է և սկզբնական $f : G_1 \to G_2$ հոմոմորֆիզմի ուսումնասիրությունը հանգեցվում է $f : G_1 \to \operatorname{Im} f$ հոմոմորֆիզմի ուսումնասիրությանը: Ուստի, առանց ընդհանրությունը խախտելու կարող ենք սահմանափակվել միայն այն դեպքում, երբ $G_2 = \mathrm{Im} f$։

Դիցուք $f : G \to \mathrm{Im} f$ հոմոմորֆիզմ է։ Դյուրին է ստուգել, որ

$$f(a) = f(b) \Leftrightarrow (f(b))^{-1} f(a) = e \Leftrightarrow$$

$$f(b^{-1}) f(a) = e \Leftrightarrow f(b^{-1}a) = e \Leftrightarrow$$

$$b^{-1}a \in \ker f \Leftrightarrow a \ker f = b \ker f\text{։}$$

Այսինքն, երկու տարրերի պատկերները համընկնում են միայն և միայն այն դեպքում, երբ համընկնում են նրանցով ծնված հարակից դասերն ըստ միջուկի։ Ուստի տրված է փոխմիարժեք արտապատկերում $G \setminus \ker f$ ֆակտոր-խմբի և $\mathrm{Im} f$-ի միջև՝

$$\begin{gathered} g : G \setminus \ker f \to \mathrm{Im} f \\ g(a \ker f) = f(a) \end{gathered} \qquad (14)$$

Պարզվում է, որ g-ն իզոմորֆիզմ է։ Իսկապես, քանի որ g-ն փոխմիարժեք է, մնում է ստուգել

$$g((a \ker f)(b \ker f)) = g(a \ker f) g(b \ker f)$$

պայմանի ճշտությունը, բայց

$$g((a \ker f)(b \ker f)) = g(ab \ker f) = f(ab) =$$

$$f(a) f(b) = g(a \ker f) g(b \ker f)\text{։}$$

Թեորեմ 3.(Իզոմորֆիզմի մասին թեորեմը)

Ֆակտոր-խումբն ըստ հոմոմորֆիզմի միջուկի իզոմորֆ է հոմոմորֆիզմի պատկերին։

Կանոնական հոմոմորֆիզմը

Ինչպես գիտենք, հոմոմորֆիզմի միջուկը նորմալ ենթախումբ է: Պարզվում է, որ կամայական նորմալ ենթախմբի համար կարելի է կառուցել խմբերի հոմոմորֆիզմ այնպես, որ այդ ենթախումբը կազմի այդ հոմոմորֆիզմի միջուկը:

Դիցուք $H \lhd G$: Կառուցենք հետևյալ արտապատկերումը.

$$f : G \to G \diagdown H \qquad (15)$$
$$f(a) = aH$$

Փաստորեն f-ը յուրաքանչյուր տարր տանում է այդ տարրով ծնված (և այդ տարրը պարունակող) հարակից դասի մեջ: Համոզվենք, որ f-ը հոմոմորֆիզմ է.

$$f(ab) = abH = (aH)(bH) = f(a)f(b):$$

Գտնենք միջուկը: Դրա համար գտնենք բոլոր $x \in G$, որ $f(x) = eH$: Բայց $f(x) = xH$, իսկ $xH = H \Leftrightarrow x \in H$: Ուստի $\ker f = H$:

Կառուցված հոմոմորֆիզմը կոչվում է **կանոնական հոմոմորֆիզմ** և այն լրիվ որոշվում է G խմբով և նրա H նորմալ ենթախմբով: Այսպիսով պարզվեց, որ

կամայական նորմալ ենթախումբ հանդիսանում է հոմոմորֆիզմի միջուկ և կամայական հոմոմորֆիզմի միջուկ նորմալ ենթախումբ է:

Այսինքն ենթախմբի միջուկ լինելու հատկությունը համարժեք է նորմալ լինելուն և այն կարելի է դիտել որպես նորմալ ենթախմբի համարժեք սահմանում:

Իզոմորֆիզմի մասին թեորեմը հարմար է ձևակերպում նաև կոմուտատիվ դիագրամների լեզվով: Դիտարկենք հետևյալ դիագրամը (պատկերը)

$$\begin{array}{ccc} G & \xrightarrow{f} & \mathrm{Im}f \\ f^*\downarrow & g\nearrow & \\ G\backslash\ker f & & \end{array}$$

որտեղ $f : G \to \mathrm{Im}f$ տրված հոմոմորֆիզմն է, $f^* : G \to G\backslash\ker f$ կանոնական հոմոմորֆիզմն է՝ $f^*(a) = a\ker f$ և $g : G\backslash\ker f \to \mathrm{Im}f$ իզոմորֆիզմն է ֆակտոր-խմբի և պատկերի միջև: Այս դիագրամը հատկանշական է նրանով, որ սկսած G խմբի որևէ a տարրից որ սլաքով էլ շարժվենք, միշտ էլ կհանենք $\mathrm{Im}f$-ի $f(a)$ տարրին: Իրոք, $g(f^*(a)) = g(a\ker f) = f(a)$ համաձայն (14-15) սահմանումների:

Իզոմորֆիզմի մասին թեորեմն ասում է, որ որևէ G խմբի բոլոր հոմոմորֆ պատկերները կարելի է ստանալ վերցնելով նրա բոլոր նորմալ ենթախմբերը և կառուցելով ֆակտոր-խմբերն ըստ այդ նորմալ ենթախմբերի:

Ցիկլիկ խմբեր

Դիցուք G-ն խումբ է և $a \in G$: Նշանակենք $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$: Ակնհայտ է, որ $\langle a \rangle \leq G$:

Հնարավոր է երկու դեպք.

1. a^n տարրերը տարբեր են բոլոր n-ի համար

2. գոյություն ունեն $n \neq m$ որ $a^n = a^m$:

Դիտարկենք առաջին դեպքը: Կառուցենք հետևյալ f արտապատկերումը՝

$$f : \langle a \rangle \to \mathbb{Z}$$
$$f(a^k) = k$$

որտեղ $\mathbb{Z}$-ը վերցված է ըստ գումարման: Ակնհայտ է, որ f-ը փոխմիարժեքորեն արտապատկերում է $\langle a \rangle$-ն $\mathbb{Z}$-ի վրա և $f(a^{n+m}) = f(a^n)f(a^m)$, ուստի այն իզոմորֆիզմ է: Այսպիսով առաջին դեպքում $\langle a \rangle$-ն իզոմորֆ է ամբողջ թվերի խմբին և, ուրեմն, անվերջ է:

Երկրորդ դեպքում գոյություն ունեն ամբողջ $n \neq m$ որ $a^n = a^m$: Դիցուք $n > m$: Բազմապատկելով $a^n = a^m$-ի աջ և ձախ մասերը a^{-m}-ով կստանանք $a^{n-m} = e$: Ուստի երկրորդ դեպքում կգտնվի ամենափոքր դրական ամբողջ n-ը, որ $a^n = e$: Դյուրին է ստուգել, որ $e, a, a^2, \ldots, a^{n-1}$ տարրերը բոլորն էլ տարբեր են: Իսկապես, եթե $a^i = a^j$, $0 \leq j < i \leq n-1$, ապա $a^{i-j} = e$ և $0 < i - j < n$: Վերջին պայմանը հակասում է այն բանին, որ n-ը փոքրագույն դրական ամբողջ թիվն է, որի համար $a^n = e$: Պարզ է, որ $a^n = e$ պայմանի պատճառով $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$ և $(\langle a \rangle : 1) = n$: Կառուցենք հետևյալ f արտապատկերումը՝

$$f : \langle a \rangle \to \mathbb{Z}_n$$
$$f(a^k) = k \,\mathrm{modulo}\, n$$

որտեղ $\mathbb{Z}_n$-ը մնացքների դասն է ըստ $\mathrm{mod}\, n$, որը դիտարկվում է ըստ գումարման: Պարզ է, որ f-ն իզոմորֆիզմ է և երկրորդ դեպքում $\langle a \rangle$ խումբն իզոմորֆ է մնացքների դասերի խմբին:

Սահմանում: $\langle a \rangle$ խումբը կոչվում է **ցիկլիկ** խումբ իսկ $a \in G$ տարրը կոչվում է խմբի **ծնիչ**:

$a \in G$ տարրի **կարգ** է կոչվում այն փոքրագույն դրական ամբողջ n թիվը, որ $a^n = e$:

Դիցուք G-ն վերջավոր ցիկլիկ խումբ է, այսինքն գոյություն ունի $a \in G$ որ $G = \langle a \rangle$: Պարզ է, որ խմբի և a տարրի կարգերը հավասար են միևնույն n թվին: Գտնենք G-ի կամայական տարրի կարգը: Քանի որ $G = \{e, a, a^2, \ldots, a^{n-1}\}$, ապա խմբի կամայական տարր ունի հետևյալ տեսքը՝ a^k, $0 \le k \le n-1$: Գտնենք այն ամենափոքր դրական ամբողջ s-ը, որ $(a^k)^s = e$: Պարզ է, որ $a^{ks} = e$ և քանի որ a-ի կարգը n է, ապա ks-ը պատիկ է n-ին: Ուստի a^k-ի կարգն որոշելու խնդիրը հանգեցվում է հետևյալ թվաբանական խնդրին. տրված n և k բնական թվերի համար գտնել այն ամենափոքր s բնական թիվը, որ ks-ը բաժանվի առանց մնացորդի n-ի վրա: Վերլուծենք n-ը և k-ն պարզ արտադրիչների և պարզենք թե ինչ է հարկավոր ավելացնել k-ի վերլուծությանը, որպեսզի այն իր մեջ պարունակի n-ի վերլուծությունը: Ակնհայտ է, որ n-ի և k-ի վերլուծությունների ընդհանուր մասը դա նրանց ամենափոքր ընդհանուր բաժանարարն է՝ (n, k)-ն: Ուստի k-ի վերլուծության մեջ n-ի վերլուծության չպարունակվող մասը դա $\dfrac{n}{(n, k)}$-ն է: Որեմն

$s = \dfrac{n}{(n,k)}$։ Այսինքն a^k տարրի կարգը հավասար է $\dfrac{n}{(n,k)}$-ի և $(\langle a^k\rangle : 1) = \dfrac{n}{(n,k)}$։ Այստեղից անմիջապես ստանում ենք, որ G խումբը ծնվում է բոլոր a^k տարրերով, որոնց համար $(n,k) = 1$։ Այդպիսի ծնիչների քանակը հավասար է $\varphi(n)$-ի, որտեղ φ-ն Էյլերի ֆունկցիան է՝ n-ից փոքր և n-ի հետ փոխադարձաբար պարզ թվերի քանակը (եթե n-ի վերլուծությունը պարզ արտադրիչների դա $p_1^{\alpha_1}\dots p_q^{\alpha_q}$ է, ապա $\varphi(n) = n(1-\frac{1}{p_1})\dots(1-\frac{1}{p_q})$)։

Օրինակ

Դիտարկենք $\mathbb{Z}/n\mathbb{Z}$ ֆակտոր-խումբը, որն իզոմորֆ է ըստ $\bmod n$-ի մնացքների դասերի խմբին։ Հայտնի է, որ n-ի հետ փոխադարձաբար պարզ a-րի ենթաբազմությունը $\{1,2,\dots,n-1\}$-ից կազմում է մուլտիպլիկատիվ ենթախումբ $\mathbb{Z}/n\mathbb{Z}$-ում, որի կարգը հավասար է $\varphi(n)$-ի, որտեղ φ-ն Էյլերի ֆունկցիան է։ Որեմն $a^{\varphi(n)} \equiv 1 \bmod n$ բոլոր a-րի համար, որ $(n,a) = 1$։ Սա հայտնի Էյլերի թեորեմն է, որի ապացույցը ստացվեց հիմնվելով այն փաստի վրա, որ կամայական տարր բարձրացված խմբի կարգի աստիճան տալիս է խմբի միավոր տարրը։ Մասնավոր դեպքում, երբ n-ը պարզ թիվ է, ստացվում է հայտնի Ֆերմայի "փոքր" թեորեմը՝ $a^{p-1} \equiv 1 \bmod p$ բոլոր $0 < a < p$ համար։

Պարզենք այժմ վերջավոր ցիկլիկ խմբի ենթախմբերի կառուցվածքը։

Թեորեմ 4.

1. Ցիկլիկ խմբի ենթախումբը ցիկլիկ է։

2. ***Եթե*** G***-ն ցիկլիկ խումբ է և*** $(G:1)=n$***, ապա*** n***-ի կամայական*** k ***բաժանարարի համար գոյություն ունի*** k ***կարգի միակ ենթախումբը*** G***-ում:***

Ապացույց. *Ապացուցենք թեորեմի առաջին պնդումը: Դիցուք* $G=\langle a\rangle$ *և* $H\le G$*: Պարզ է, որ* H*-ի տարրերը* a*-ի աստիճաններ են: Եթե* $H=\{e\}$*, ապա ակնհայտորեն* H*-ը ցիկլիկ է: Եթե* $H\neq\{e\}$*, ապա* H*-ում կգտնվի* a*-ի ամենափոքր դրական աստիճանը, այսինքն կգտնվի* $a^m\in H$ *և* $0<p<m\Rightarrow a^p\notin H$*: Քանի որ* H*-ն ենթախումբ է, ապա* $\langle a^m\rangle\subseteq H$*: Դիցուք* $a^n\in H$*: Բաժանենք* n*-ը* m*-ի վրա՝* $n=mq+p,\ 0\le p<m$*: Որտեղ* $a^n=a^{mq+p}=(a^m)^q a^p$ *և քանի որ* $(a^m)^q\in H$ *ստանում ենք՝* $a^p=a^{n-mq}\in H$*: Եթե* $0<p<m$*, ապա* $a^p\notin H$*, ուստի* $p=0$*,* $n=mq$ *և* $a^n=(a^m)^q$*: Իսկ սա նշանակում է, որ* $H\subseteq\langle a^m\rangle$ *և ուրեմն* $H=\langle a^m\rangle$*: Այսպիսով* H*-ը ցիկլիկ է և այն ծնվում է* H*-ում պարունակվող* a*-ի ամենափոքր դրական աստիճանով:*

Ապացուցենք այժմ թեորեմի երկրորդ մասը: Դիցուք $G=\langle a\rangle$*,* $(G:1)=n$ *և* $H\le G$*: Լագրանժի թեորեմից պարզ է, որ* $(H:1)$*-ը* n*-ի բաժանարարն է: Դիցուք* $0<k\le n$ *և* k*-ն* n*-ի բաժանարարն է: Միանգամից պարզ է, որ* $\langle a^{\frac{n}{k}}\rangle$*-ի կարգը հավասար է* $\dfrac{n}{(\frac{n}{k},n)}=k$*: Ապացուցենք, որ դա միակ* k *կարգի ենթախումբն է:*

Դիցուք $H\le G$ *և* $(H:1)=k$*: Ինչպես տեսանք,* $H=\langle a^m\rangle$*, որտեղ* m*-ը* H*-ում պարունակվող* a*-ի ամենափոքր դրական աստիճանն է: Ունենք, որ* $(H:1)=\dfrac{n}{(m,n)}=k$*, ուրեմն* $\dfrac{n}{k}=(m,n)$ *և* m*-ը բաժանվում է* $\dfrac{n}{k}$*-ի վրա առանց մնացորդի: Ուստի* $H=\langle a^m\rangle\le\langle a^{\frac{n}{k}}\rangle$*: Բայց* H*-ը և* $\langle a^{\frac{n}{k}}\rangle$*-ն երկուսն էլ պարունակում են* k

տարր, ուրեմն $H = \langle a^{\frac{n}{k}} \rangle$ և թեորեմն ապացուցված է:

Ուղիղ արտադրյալ

Դիցուք G-ն խումբ է և H-ն ու K-ն G-ի այնպիսի ենթախմբեր են, որ $G = HK = \{hk \mid h \in H, k \in K\}$: Պարզենք, թե ինչպիսի պայմանների դեպքում G խմբի յուրաքանչյուր g տարր միարժեքորեն կներկայացվի $g = hk$, $h \in H, k \in K$ տեսքով, ընդ որում եթե $g_1 = h_1k_1$ և $g_2 = h_2k_2$, ապա $g_1g_2 = (h_1h_2)(k_1k_2)$:

Դյուրին է տեսնել, որ $H \cap K = \{e\}$ պայմանն անհրաժեշտ և բավարար է $g = hk$ ներկայացման միարժեքության համար: Իսկապես, եթե $g = h_1k_1 = h_2k_2$, ապա $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K$: Ուստի $h_2^{-1}h_1 = k_2k_1^{-1} = e$ և $h_1 = h_2, k_1 = k_2$: Մյուս կողմից, եթե $e \neq g \in H \cap K$, ապա g-ն ունի երկու տարբեր ներկայացում՝ ge և eg:

Այժմ, դիցուք $g_1 = h_1k_1$, $g_2 = h_2k_2$ և $g_1g_2 = (h_1h_2)(k_1k_2)$: Ունենք՝ $g_1g_2 = h_1k_1h_2k_2 = h_1h_2k_1k_2$, ուրեմն $k_1h_2 = h_2k_1$, ինչը նշանակում է, որ $\forall h \in H, \forall k \in K$ ստույգ է՝ $hk = kh$, այսինքն H ու K ենթախմբերի տարրերը տեղափոխելի են: Վերջին պայմանը համարժեք է H-ի ու K-ի նորմալությանը G-ում: Համոզվենք դրանում: Դիցուք H ու K ենթախմբերի տարրերը տեղափոխելի են: Դիցուք $g \in G$ և $g = hk$: Դիտարկենք $g^{-1}Hg$ բազմությունը: Պարզ է, որ $g^{-1}Hg = k^{-1}h^{-1}Hhk = k^{-1}Hk = k^{-1}kH = H$ և $H \lhd G$: Նմանապես, $g^{-1}Kg = k^{-1}h^{-1}Khk = h^{-1}k^{-1}Kkh = h^{-1}Kh = h^{-1}hK = K$ և $K \lhd G$: Այժմ ապացուցենք հակառակ պնդումը: Դիցուք $K \lhd G$, $H \lhd G$ և $h \in H, k \in K$: Դիտարկենք $h^{-1}k^{-1}hk$ տարրը: Ունենք $h^{-1}k^{-1}hk = (h^{-1}k^{-1}h)k \in K$, քանի որ $h^{-1}k^{-1}h \in K$: Մյուս կողմից՝ $h^{-1}k^{-1}hk = h^{-1}(k^{-1}hk) \in H$, քանի որ $k^{-1}hk \in H$: Ուստի $h^{-1}k^{-1}hk \in H \cap K = \{e\}$ և $h^{-1}k^{-1}hk = e$, այսինքն՝ $hk = kh$: Այսպիսով հանգում ենք հետևյալ գաղափարին:

Սահմանում: *Ասում են, որ G խումբն իր H և K ենթախմբերի ուղիղ արտադրյալն է, եթե*

1. $G = HK$ *(պարզ է, որ $HK = KH$)*
2. $H \lhd G$ *և* $K \lhd G$
3. $H \cap K = \{e\}$

Ինչպես արդեն գիտենք, յուրաքանչյուր $g \in G$ միարժեքորեն ներկայացվում է որպես $g = hk$ և, եթե $g_1 = h_1k_1,\ g_2 = h_2k_2$, ապա g_1g_2 տարրի ներկայացումը հետևյալն է՝ $(h_1h_2)(k_1k_2)$:

Դիցուք այժմ ունենք երկու խումբ՝ G_1 և G_2: Դիտարկենք $G_1 \times G_2$ դեկարտյան արտադրյալը, որի վրա սահմանենք բազմապատկման գործողություն հետևյալ կերպ: Դիցուք $a_1, b_1 \in G_1$ և $a_2, b_2 \in G_2$: Սահմանենք՝

$$(a_1, a_2)(b_1, b_2) = (a_1b_1, a_2b_2)$$

Դյուրին է ստուգել, որ $G_1 \times G_2$-ն խումբ է վերը նշված ուղղորդված զույգերի բազմապատկման գործողության նկատմամբ: Միավոր տարրը դա (e_1, e_2)-ն է, որտեղ e_1-ը G_1-ի, իսկ e_2-ը G_2-ի միավորներն են: Պարզ է, որ (a,b)-ի հակադարձը (a^{-1}, b^{-1})-ն է: Նկատենք, որ $\{(a, e_2) \mid a \in G_1\}$ և $\{(e_1, b) \mid b \in G_2\}$ բազմությունները ենթախմբեր են $G_1 \times G_2$ խմբում և դրանք համապատասխանաբար իզոմորֆ են G_1-ին ու G_2-ին: Այդ ենթախմբերը նույնացվում են G_1-ին ու G_2-ին: Դյուրին է համոզվել, որ $G_1 \times G_2$-ը, G_1-ն ու G_2-ը բավարարում են ուղիղ արտադրյալի սահմանման 1.-3. պայմաններին, ուստի $G_1 \times G_2$ խումբը G_1 և G_2 խմբերի ուղիղ արտադրյալն է:

$G = HK$ ուղիղ արտադրյալն իզոմորֆ է $H \times K$ խմբին: Իսկապես,

յուրաքանչյուր (h,k) տարրին $H \times K$-ից համապատասխանեցնենք hk տարրը G-ից: Ակնհայտ է, որ այս համապատասխանեցումն հոմոմորֆիզմ է, որը փոխմիարժեք է և պատկերը համընկնում է ամբողջ G-ի հետ: Ուրեմն դա իզոմորֆիզմ է: Այդ պատճառով այն փաստը, որ $G = HK$ ուղիղ արտադրյալ է գրում են հետևյալ կերպ՝ $G = H \times K$:

Բնական ձևով սահմանվում է կամայական վերջավոր քանակությամբ խմբերի ուղիղ արտադրյալը՝ $G_1 \times G_2 \times \ldots \times G_n$ դեկարտյան արտադրյալի տարրերը բազմապատկվում են հետևյալ կերպ՝

$$(a_1,a_2,\ldots,a_n)(b_1,b_2,\ldots,b_n) = (a_1b_1,a_2b_2,\ldots,a_nb_n)$$

G_i խումբը նույնացվում է

$$\{(e_1,\ldots,e_{i-1},a,e_{i+1},\ldots,e_n) \mid a \in G_i\}$$

ենթախմբին:

Դիցուք $H_1,\ldots,H_n$-ը G խմբի ենթախմբեր են և $G = H_1 \ldots H_n$: G խումբը կլինի $H_1,\ldots,H_n$ ենթախմբերի ուղիղ արտադրյալ, եթե $(h_1,\ldots,h_n) \mapsto h_1 \ldots h_n$ արտապատկերումն իզոմորֆիզմ է $H_1 \times H_2 \times \ldots \times H_n$ և $G = H_1 \ldots H_n$ խմբերի միջև: Այդ դեպքում գրում են՝ $G = H_1 \times H_2 \times \ldots \times H_n$ և սա նշանակում է, որ յուրաքանչյուր $g \in G$ համար գոյություն ունի նրա միարժեքորեն որոշված ներկայացումը՝ $g = h_1 \ldots h_n$, որտեղ $h_i \in H_i, i = 1,\ldots,n$, և եթե $g_1 = h_1 \ldots h_n, g_2 = h'_1 \ldots h'_n$, ապա $g_1g_2 = (h_1h'_1)\ldots(h_nh'_n)$: Նաև տարբեր H_i-ի և H_j-ի տարրերը տեղափոխելի են: Ուղիղ արտադրյալի սահմանման 1.-3. պայմանները կգրվեն հետևյալ կերպ.

1. $G = H_1 \ldots H_n$
2. $(\forall i)\ H_i \triangleleft G$

3. $(\forall i)\ H_1 \dots H_i \cap H_{i+1} = \{e\}$

Օրինակներ

1. *Դիցուք* $G = < g >$*-ն ցիկլիկ խումբ է և* $(G:1) = n = pq$*, որտեղ* $(p,q) = 1$*, այսինքն* p*-ն ու* q*-ն փոխադարձաբար պարզ թվեր են: Նշանակենք* $H = < g^p >$ *և* $K = < g^q >$*: Ինչպես գիտենք* $(H:1) = q, (K:1) = p$ *և* H*-ն ու* K*-ն* q *և* p *կարգի միակ ենթախմբերն են* G*-ում: Ապացուցենք, որ* $G = H \times K$*: Համաձայն Էվքլիդեսի ալգորիթմի գոյություն ունեն ամբողջ* x *և* y *այնպիսին, որ* $xp + yq = 1$*: Դիցուք* $g^z \in G$*: Ունենք՝* $g^z = g^{zxp+zyq} = (g^p)^{zx}(g^q)^{zy}$*, սակայն* $(g^p)^{zx} \in H$ *և* $(g^q)^{zy} \in K$*, ուստի* $G = HK$*: Քանի որ ցիկլիկ խումբն աբելյան է (տեղափոխելի), ապա դրա բոլոր ենթախմբերը նորմալ են: Դիցուք* $g^z \in H \cap K$*: Դա նշանակում է, որ* $g^z = g^{ps} = g^{qt}$ *և* $ps \equiv qt \bmod n$*: Որեմն* $ps - qt = nv$ *և* $ps - qt = pqv$*: Այստեղից հետևում է, որ* $ps = q(t + pv)$*: Քանի որ* p*-ն ու* q*-ն փոխադարձաբար պարզ են, ապա* $s \equiv 0 \bmod q$ *և* $t \equiv 0 \bmod p$*: Այսինքն* $ps \equiv 0 \bmod n$ *և* $qt \equiv 0 \bmod n$*, ուստի* $g^{ps} = g^{qt} = e$*: Այսպիսով ուղիղ արտադրյալի սահմանման բոլոր 1.-3. պայմանները բավարարված են և* $G = H \times K$*:*

2. *Ինչպես գիտենք* n *կարգի ցիկլիկ խումբն իզոմորֆ է ըստ* $\bmod n$*-ի մնացքների դասերի խմբին (ըստ գումարման), որն իզոմորֆ է* $\mathbb{Z}/n\mathbb{Z}$ *ֆակտոր-խմբին և որը մենք նշանակել էինք* $\mathbb{Z}_n$*-ով: Վերլուծենք* n*-ը պարզ արտադրիչների՝* $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$*: Համաձայն նախորդ օրինակի ստանում ենք, որ* $\mathbb{Z}_n = \mathbb{Z}_{p_1^{\alpha_1}} \times \dots \times \mathbb{Z}_{p_k^{\alpha_k}}$*:*

3. *Դիցուք* G*-ն ցիկլիկ խումբ է և* $(G:1) = p^\alpha$*, որտեղ* p*-ն պարզ թիվ է: Փոխարինենք* G*-ն նրան իզոմորֆ* $\mathbb{Z}_{p^\alpha}$ *խմբով: Ինչպես գիտենք* $\mathbb{Z}_{p^\alpha}$*-ի կամայական սեփական ենթախումբ ցիկլիկ է և նրա կարգը հավասար է* p^β*,* $0 < \beta < \alpha$*: Որեմն* $\mathbb{Z}_{p^\alpha}$*-ի բոլոր ենթախմբերն են՝*

$\{0\} \subset \mathbb{Z}_p \subset \mathbb{Z}_{p^2} \subset \ldots \subset \mathbb{Z}_{p^{\alpha-1}} \subset \mathbb{Z}_{p^\alpha}$: Ակնհայտ է, որ կամայական երկու սեփական ենթախմբերի հատումը պարունակում է $\mathbb{Z}_p$-ն: Ուստի, $\mathbb{Z}_{p^\alpha}$ (ինչպես և G-ն) հնարավոր չէ ներկայացնել սեփական ենթախմբերի ուղիղ արտադրյալի միջոցով:

Ծնիչ բազմություններ

Սահմանում: G խմբի S ենթաբազմությունը կոչվում է **ծնիչ բազմություն** G-ի համար, եթե G-ի կամայական a տարր կարելի ներկայացնել S-ի տարրերի կամ դրանց հակադարձների արտադրյալով՝ $a = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots x_k^{\varepsilon_k}$, $\varepsilon_i \in \{1,-1\}$, $x_i \in S$, $i = 1,2,\ldots,k$:

Օրինակներ

1. Դիցուք $G = S_n$: Հայտնի է, որ կամայական տեղադրություն կարելի է ներկայացնել տրանսպոզիցիաների արտադրյալով, ուստի բոլոր n տարրանի տրանսպոզիցիաների բազմությունը դա ծնիչ բազմություն է S_n-ի համար: Մեկ այլ ծնիչ բազմություն է S_n-ի համար հետևյալ բազմությունը կազմված երկու տեղադրություններից՝ $\begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 2 & 3 & 4 & \ldots & n & 1 \end{pmatrix}$ և $\begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 1 & 3 & 4 & \ldots & n \end{pmatrix}$, որոնցից առաջինը n երկարության ցիկլ է, իսկ մյուսը՝ տրանսպոզիցիա:

2. Դիցուք $G = A_n$: Ծնիչների բազմություն է բոլոր 3 երկարության ցիկլերի բազմությունը:

3. Դիցուք $G = (\mathbb{Z},+)$: Դիտարկենք հետևյալ բազմությունը $S = \{2^m \mid m \in \mathbb{Z},\ \ m \geq 0\}$: Ակնհայտ է, որ կամայական ամբողջ թիվ ունի երկուական ներկայացում, որը 2-ի աստիճանների գումար է (բացասական թվի համար վերցվում են S բազմության հակադիրները):

4. Դիցուք G-ն հարթության վեկտորների բազմությունն է դիտարկված ըստ գումարման գործողության: Ֆիքսենք *երկու ոչ կոլինեար վեկտորներ $\vec{a}$ և $\vec{b}$: Կառուցենք S բազմությունը՝ $\{\lambda\vec{a} \mid \lambda \in \mathbb{R}\} \cup \{\mu\vec{b} \mid \mu \in \mathbb{R}\}$: Պարզ է, որ կամայական վեկտոր կարելի է ներկայացնել S-ի տարրերի գումարի տեսքով: Ուստի, S-ը ծնիչ բազմություն է:*

Ծնիչների "ուժեղ" բազմություն

Ծնիչ բազմության սահմանումից երևում է, որ խմբի բոլոր տարրերը կարելի է ստանալ կառուցելով ծնիչ բազմության տարրերի բոլոր հնարավոր արտադրյալները: Իհարկե, դա իմաստ ունի անել վերջավոր խմբերի դեպքում: Սակայն ալգորիթմական տեսակետից խմբի ծնիչ բազմության միջոցով տրման եղանակը թերի է, քանի որ ունենալով միայն թեկուզև ծնիչների վերջավոր բազմություն դյուրին չէ բոլոր հնարավոր արտադրյալների կառուցումը: Խմբի տարրի ներկայացումը ծնիչ բազմության տարրերով միարժեք չէ, և ունենալով ծնիչ բազմությունը հնարավոր չէ նույնիսկ հաշվել խմբի կարգը:

Վերը նշված պատճառներով իմաստ ունի դիտարկել ծնիչ բազմության գաղափարի մեկ այլ ավելի նեղ տարբերակ, որը զերծ է վերոհիշյալ թերություններից: Հետագայում ցույց կտանք, որ կամայական ծնիչ բազմությունից կարելի է անցնել համապատասխան նոր "նեղ" տարբերակին:

Այժմ նկարագրենք ծնիչ բազմություն կառուցելու մի եղանակ:

Դիցուք $G \le S_n$: (Ըստ Քելիի թեորեմի (Թեորեմ 1) կարող ենք սահմանափակվել միայն տեղադրությունների խմբերի դիտարկմամբ:) Կառուցենք G-ի ենթախմբերի մի շղթա՝

$$G \ge G_1 \ge G_{12} \ge \ldots \ge G_{123\ldots i} \ge \ldots \ge G_{123\ldots n-1} = G_{123\ldots n} = \{e\} \qquad (16)$$

Այստեղ $G_{123\ldots i}$-ն կազմված է G-ի այն բոլոր տեղադրություններից, որ 1-ը տանում են 1-ի մեջ, 2-ը՝ 2-ի, 3-ը՝ 3-ի..., i-ն՝ i-ի մեջ: Պարզ է, որ $e \in G_{123\ldots i} \neq \varnothing$ և $G_{123\ldots i} \le G$, $i \in \{1,2,\ldots,n\}$: Դիտարկենք (16)-ի երկու հարևան անդամների զույգ՝

$$G_{123\ldots i-1} \geq G_{123\ldots i}$$

և համապատասխան ֆակտոր-բազմությունը՝

$$G_{123\ldots i-1} \diagdown G_{123\ldots i}:$$

Բոլոր տեղադրությունները $G_{123\ldots i-1}$-ից պահպանում են 1-ից $i-1$ տարրերը (այսինքն տանում են 1-ը 1-ի մեջ, ..., $i-1$-ը՝ $i-1$-ի մեջ): Երկու x և y տեղադրություն $G_{123\ldots i-1}$-ից կպատկանեն միևնույն հարակից դասին ըստ $G_{123\ldots i}$-ի $\Leftrightarrow x(i) = y(i)$ (այսինքն միայն երբ x-ը և y-ը i տարրը տանում են միևնույն տարրի մեջ): Իրոք, որպեսզի x-ը և y-ը լինեն միևնույն դասից ըստ $G_{123\ldots i}$-ի անհրաժեշտ է և բավարար, որ $x^{-1}y \in G_{123\ldots i}$: Սա նշանակում է, որ $(x^{-1}y)(i) = i$, բայց $(x^{-1}y)(i) = x^{-1}(y(i)) = i$ և ուրեմն $x(i) = y(i)$: Այստեղից եզրակացնում ենք, որ $G_{123\ldots i-1} \diagdown G_{123\ldots i}$ ֆակտոր-բազմությունը կարող է ունենալ ամենաշատը $n-(i-1) = n-i+1$ տարր (հարակից դաս), այսինքն՝ $(G_{123\ldots i-1} : G_{123\ldots i}) \leq n-i+1$:

Կառուցենք G-ի տարրերի մի բազմություն հետևյալ կերպ:

Դիտարկենք $G \diagdown G_1$-ը: Յուրաքանչյուր հարակից դասից, բացի G_1-ից, կամայական ձևով ընտրենք մի ներկայացուցիչ: G_1-ից որպես ներկայացուցիչ ընտրենք միավոր տարրը՝ e-ն: Նշանակենք այդ ներկայացուցիչները $e, x_1, x_2, \ldots, x_{k_1}$-ով: Պարզ է, որ $k_1 + 1 \leq n$: Դրանից հետո դիտարկենք $G_1 \diagdown G_{12}$-ը: Կրկին յուրաքանչյուր հարակից դասից, բացի G_{12}-ից, կամայական ձևով ընտրենք մի ներկայացուցիչ: G_{12}-ից որպես ներկայացուցիչ ընտրենք միավոր տարրը՝ e-ն: Նշանակենք այդ ներկայացուցիչները $e, y_1, y_2, \ldots, y_{k_2}$-ով: Պարզ է, որ $k_2 + 1 \leq n-1$: Շարունակելով պրոցեսը ամեն մի $G_{123\ldots i-1} \diagdown G_{123\ldots i}$-ի յուրաքանչյուր հարակից դասից ընտրենք ներկայացուցիչներ վերցնելով e-ն որպես $G_{123\ldots i}$-ի ներկայացուցիչ: Վերջում կդիտարկենք $G_{123\ldots n-2} \diagdown G_{123\ldots n-1}$-ը, որն ամենաշատը կարող է ունենալ երկու տարր՝ միավորը և այն *տեղադրությունը, որ պահպանում է* 1*-ից* $n-2$ *տարրերը, իսկ* $n-1$*-ը տանում է* n*-ի մեջ,* n*-ն էլ՝* $n-1$*-ի մեջ:*

Դասավորենք ընտրված ներկայացուցիչներին մի աղյուսակի մեջ տողերում գրելով $G_{123\ldots i-1} \setminus G_{123\ldots i}$*-րի ներկայացուցիչներին: Այդ աղյուսակը կունենա հետևյալ տեսքը.*

$$\begin{array}{ccccc} e & x_1 & x_2 & \cdots & x_{k_1} \\ e & y_1 & y_2 & \cdots & y_{k_2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{array} \qquad (17)$$

Աղյուսակի առաջին տողը պարունակում է k_1+1 *տարր և* $k_1+1 \le n$*, երկրորդ տողը պարունակում է* $k_2+1 \le n-1$ *տարր և այլն: Ապացուցենք, որ* (17) *աղյուսակում ընդգրկված տեղադրությունների բազմությունը ծնիչ բազմություն է* G *խմբի համար:*

Դիցուք $a \in G$*: Դիտարկենք* $G \setminus G_1$*-ը: Պարզ է, որ* a*-ն պատկանում է որևէ հարակից դասի ըստ* G_1*-ի: Դիցուք այդ դասի ներկայացուցիչը* x_1*-ն է: Այդ դեպքում՝* $x_1^{-1}a \in G_1$*, քանի որ արդեն պարզել ենք, որ* a*-ն և* x_1*-ը նույն հարակից դասից են* $\Leftrightarrow x_1(1) = a(1)$*: Դիցուք* $x_1^{-1}a$*-ն պատկանում է* $G_1 \setminus G_{12}$*-ի այն հարակից դասին, որի ներկայացուցիչը* y_2*-ն է: Ուրեմն,* $y_2^{-1}x_1^{-1}a \in G_{12}$*: Դիտարկենք այժմ* $G_{12} \setminus G_{123}$*-ը: Դիցուք* z_3*-ը* $y_2^{-1}x_1^{-1}a$ *տարրը պարունակող* (17) *աղյուսակի երրորդ տողում գտնվող ըստ* G_{123}*-ի հարակից դասի ներկայացուցիչն է: Պարզ է, որ* $z_3^{-1}y_2^{-1}x_1^{-1}a \in G_{123}$*: Շարունակելով այս պրոցեսը կստանանք* (17) *աղյուսակի տարրերի (ամեն տողից մեկական) մի արտադրյալ՝* $\ldots z_3^{-1}y_2^{-1}x_1^{-1}a \in G_{123\ldots n-1} = \{e\}$*, ուստի* $\ldots z_3^{-1}y_2^{-1}x_1^{-1}a = e$ *և* $a = x_1y_2z_3\ldots$*: Այսինքն,* G *խմբի կամայական տեղադրություն ներկայացվում է* (17) *աղյուսակի տարրերի արտադրյալով և այդ բազմությունը ծնիչ բազմություն է:*

Նկատենք, որ վերը նշված արտադրյալում մասնակցում է (17) աղյուսակի յուրաքանչյուր տողից մեկական տարր (որոշ դեպքերում դա կարող է լինել միավորը՝ e-ն), ընդ որում սկզբից վերցվում է առաջին տողից մեկ տարր, հետո երկրորդից՝ և այդպես շարունակ: Նկատենք, որ $a = x_1y_2z_3\ldots$ *ներկայացումը միակն է, քանի որ, եթե այդ ներկայացման որևէ տարր փոխարինվի (17) աղյուսակի նույն տողից մեկ այլ տարրով, ապա դա նշանակում է, որ համապատասխան* $G_{123\ldots i-1} \setminus G_{123\ldots i}$*-ում վերցվում է մեկ այլ հարակից դաս և ուստի հնարավոր չէ ստանալ* a *տարրը: Օրինակ, դիտարկենք* $a = x_1y_2z_3$ *և* $b = x_1y_2z_2$ *տարրերը, ապա* $y_2^{-1}x_1^{-1}a \in G_{12}$ *և* $y_2^{-1}x_1^{-1}b \in G_{12}$*: Քանի որ* $z_3 \neq z_2$*, ապա դրանք ըստ* G_{123}*-ի տարբեր հարակից դասերի ներկայացուցիչներ են և* $z_3(3) \neq z_2(3)$*: Ուստի,* $a(3) \neq b(3)$*:*

Այսպիսով ստացանք, որ (17) աղյուսակով տրվող բազմությունը ծնիչ բազմություն է G *խմբի համար, ընդ որում խմբի տարրերի ներկայացումը (17) աղյուսակի տարրերի միջոցով միակն է եթե ամեն տողից հաջորդաբար վերցված է ճիշտ մեկ տարր: Դյուրին է տեսնել, որ* G *խմբի տարրերի քանակը հավասար է (17) աղյուսակի տարրերի վերը նշված արտադրյալների քանակին, որն իր հերթին հավասար է աղյուսակի տողերում պարունակվող տեղադրությունների քանակների արտադրյալին, այսինքն*

$$(G : 1) = (k_1 + 1)(k_2 + 1)\ldots:$$

Սահմանում *(17) աղյուսակով տրված ծնիչ բազմությունը կոչվում է* "***ուժեղ***" ***ծնիչների բազմություն:***

Սիմսի ալգորիթմը

Դիցուք $G \le S_n$ և խումբը տրված է ծնիչների S բազմության միջոցով: Սիմսի ալգորիթմը ստանալով S բազմությունը կառուցում է G խմբի "ուժեղ" ծնիչների բազմություն:

Ալգորիթմը կառուցում է (17) աղյուսակը: Դրա համար օգտվելու ենք $n \times n$ մի աղյուսակից, որի վանդակների մեջ գրելու ենք տեղադրություններ: Այդ աղյուսակն ունի հետևյալ տեսքը.

	1	2	3	…	n
1	e				
2	■	e			
3	■	■	e		
⋮	■	■	■	⋱	
n	■	■	■	■	e

(18)

Աղյուսակի տողերը և սյուները համարակալված են $1,2,\dots,n$ թվերով: Անկյունագծային վանդակներում գրված է միավոր տեղադրությունը: Անկյունագծից ներքև գտնվող վանդակները չեն օգտագործվում: Վանդակ ասելով մենք այսուհետև կհասկանանք անկյունագծից վերև գտնվող վանդակները: Վանդակներում կարող են տեղադրվել տեղադրություններ՝ մեկ տեղադրություն մեկ վանդակում: Վանդակները նաև կարող են դատարկ լինել: Ալգորիթմի ընթացքում որոշ տեղադրություններ գրվում են դատարկ վանդակների մեջ: Եթե i-րդ տողի j-րդ վանդակում $(i < j)$ գրվել է x տեղադրությունը, ապա պարտադիր պետք է տեղի ունենա $x(i) = j$ պայմանը: Այսինքն այդ վանդակը նախատեսված է միայն այնպիսի տեղադրությունների համար, որոնք i տարրը տանում են j տարրի մեջ: Փաստորեն (18) աղյուսակի վանդակներում ալգորիթմի *աշխատանքի արդյունքում ստացվում են (17) աղյուսակի տարրերը, այսինքն կառուցվում է "ուժեղ" ծնիչների բազմությունը:*

Սիմսի ալգորիթմն աշխատանքի ընթացքում պարբերաբար կատարում է մի գործողություն, որը կոչվում է ***cascade****: Այդ գործողությունը կիրառվում է որևէ տեղադրությանն, երբ (18) աղյուսակը մասամբ լրացված է, այսինքն որոշ վանդակներում արդեն կարող են տեղադրված լինել տեղադրություններ:*

Նկարագրենք ***cascade*** *գործողությունը: Դիցուք տրված է a տեղադրությունը:* ***cascade***(a)*-ով նշանակում են գործողության կիրառումը a տեղադրության նկատմամբ:*

cascade(a)*-ն հաշվում ենք հետևյալ կերպ.*

1. *Նշանակում ենք b-ով ընթացիկ տեղադրությունը և վերցնում ենք $b = a$*

2. *Հաշվում ենք $b(1)$-ը և դիտարկում ենք (18) աղյուսակի առաջին տողը*

3. *Եթե $b(1) = 1$ անցնում ենք* **5**. *կետին*

4. *Եթե $b(1) = i \neq 1$ ստուգում ենք առաջին տողի i-րդ վանդակը. Եթե այն դատարկ է, ապա տեղադրում ենք այդ վանդակում b տեղադրությունը և* ***cascade***(a)*-ն ավարտված է. Եթե այդ վանդակը զբաղեցված է և այդտեղ գրված է x տեղադրությունը, ապա հաշվում ենք $b = x^{-1}b$, վերցնում ենք այդ նոր ընթացիկ տեղադրությունը և անցնում ենք հաջորդ կետին*

5. *Հաշվում ենք $b(2)$-ը և դիտարկում ենք (18) աղյուսակի երկրորդ տողը*

6. *Եթե $b(2) = 2$ անցնում ենք* **8**. *կետին*

7. *Եթե $b(2) = i \neq 2$ ստուգում ենք երկրորդ տողի i-րդ վանդակը. Եթե այն դատարկ է, ապա տեղադրում ենք այդ վանդակում b տեղադրությունը և* ***cascade***(a)*-ն ավարտված* *է. եթե այդ վանդակը զբաղեցված է և այդտեղ գրված է y տեղադրությունը, ապա հաշվում ենք $b = y^{-1}b$, վերցնում ենք այդ նոր ընթացիկ տեղադրությունը և անցնում ենք հաջորդ կետին*

8. *վերը նշված եղանակով շարունակում ենք պրոցեսը մյուս տողերի համար հաջորդաբար:*

Արդյունքում, կամ (18) աղյուսակում լրացվում է մի նոր վանդակ, կամ էլ անցնելով (18) աղյուսակի բոլոր տողերով դուրս ենք գալիս աղյուսակից ստանալով a-ի ներկայացումն աղյուսակի տարրերի միջոցով $a = xy\ldots$ յուրաքանչյուր տողից մեկ տեղադրություն վերցված:

Դիցուք $G \leq S_n$ և խումբը տրված է ծնիչների S բազմության միջոցով: Քանի որ G-ն վերջավոր է կամայական $a \in G$ ունի վերջավոր կարգ, այսինքն գոյություն ունի դրական ամբողջ թիվ m այնպիսի, որ $a^m = e$ (հիշենք, որ m-ը խմբի կարգի բաժանարար է): Ուրեմն $a^{m-1}a = e$ և $a^{m-1} = a^{-1}$: G-ի կամայական a տարր ստացվում է S բազմության տարրերի արտադրյալի միջոցով $a = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots x_k^{\varepsilon_k}$, $\varepsilon_i \in \{1,-1\}$, $x_i \in S$, $i = 1,2,\ldots,k$: Սակայն հաշվի առնելով $a^{m-1} = a^{-1}$ հավասարությունը ստացվում է, որ կամայական a տարրի համար կգտնվի այնպիսի ներկայացում $a = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots x_k^{\varepsilon_k}$, որ $\varepsilon_i = 1$, այսինքն a-ն S բազմության (առանց դրա հակադարձների օգտագործման) տարրերի արտադրյալն է:

Սիմսի ալգորիթմի նկարագրությունը և կոռեկտության ապացույցը

Ալգորիթմի մուտք է հանդիսանում n տարրանի տեղադրություններից կազմված S բազմությունը, որը ծնիչների բազմություն է ինչ-որ մի $G \leq S_n$ ենթախմբի համար: Ալգորիթմի աշխատանքի արդյունքում կառուցվում է G խմբի "ուժեղ" ծնիչների մի բազմություն, որի տարրերը ստացվում են (18) աղյուսակում (որի տողերը համընկնում են համապատասխանաբար "ուժեղ" ծնիչների բազմության (17) աղյուսակի տողերի հետ):

Ալգորիթմի աշխատանքի սկզբում (18) աղյուսակը դատարկ է: Եթե ալգորիթմի որևէ քայլից հետո (18) աղյուսակում լրացվում են բոլոր վանդակները, ապա ալգորիթմը վերջացնում է իր աշխատանքը և այդ դեպքում պարզ է, որ $G = S_n$: Իսկապես, ինչպես արդեն ստուգել ենք $(G:1)$-ը հավասար է (17) աղյուսակի տողերի տարրերի քանակների արտադրյալին, որը համընկնում է (18) աղյուսակի տողերում գրված (հաշվի են առնվում նաև միավոր տարրերը) տեղադրությունների քանակների արտադրյալին: Եթե բոլոր վանդակները զբաղված են, ապա $(G : 1) = n(n-1)\ldots 2 = n!$:

Ալգորիթմի կատարման առաջին փուլում յուրաքանչյուր a-ի համար S բազմությունից կատարում ենք cascade(a) գործողությունը:

Ալգորիթմի կատարման երկրորդ փուլում (18) աղյուսակի տարրերի յուրաքանչյուր a,b զույգի համար (դիտարկվում է նաև $a = b$ դեպքը) կազմվում են a^2, b^2, ab, ba արտադրյալները և դրանց համար կատարվում է cascade գործողությունը: (Հարկ է նշել, որ a,b զույգերի բազմությունը դինամիկ է, այսինքն անընդհատ փոփոխվում է, բայց, քանի որ այն վերջավոր է, ապա ալգորիթմի երկրորդ փուլը կատարվի վերջավոր քանակությամբ քայլերից հետո): Երկրորդ փուլի ավարտով ավարտվում է ալգորիթմի աշխատանքը:

Ապացուցենք այժմ, որ Սիմսի աշխատանքի արդյունքում կառուցված (18) աղյուսակը հանդիսանում է "ուժեղ" ծնիչների բազմություն:

Դիցուք $S = \{t_1, \dots, t_m\}$: Կամայական a տարր G խմբից ներկայացվում է S-ի տարրերի արտադրյալով՝ $a = t_{i_1} t_{i_2} \dots t_{i_k}$: Քանի որ Սիմսի ալգորիթմի առաջին փուլում S-ի բոլոր տարրերն անցել են cascade-ով դրանք բոլորը ներկայացվում են (18) աղյուսակի տարրերի արտադրյալներով, ընդ որում ամեն տողից վերցված է ճիշտ մեկ տեղադրություն (դա կարող է նաև լինել միավորը): Այդպիսի ներկայացում ստանալու համար բավական է կրկին cascade կատարել տվյալ t_{i_j} համար: Այսուհետև (18) աղյուսակի տարրերը կնշանակենք g տառերով: Կօգտագործենք ինդեքսներ՝ ստորին ինդեքսը ցույց կտա թե տվյալ g-ն (18) աղյուսակի որ տողից է վերցված, իսկ վերին ինդեքսը կօգտագործենք ուղղակի հերթականությունը նշելու համար: Այսպիսով $a = t_{i_1} t_{i_2} \dots t_{i_k}$ ներկայացումից (օգտվելով t_{i_j}-րի (18) աղյուսակի տարրերով ներկայացումներից) կստանանք հետևյալը.

$$a = \underbrace{(g_1^1 g_2^1 \dots g_{n-1}^1)}_{t_{i_1}} \underbrace{(g_1^2 g_2^2 \dots g_{n-1}^2)}_{t_{i_2}} \dots \underbrace{(g_1^{k-1} g_2^{k-1} \dots g_{n-1}^{k-1})}_{t_{i_{k-1}}} \underbrace{(g_1^k g_2^k \dots g_{n-1}^k)}_{t_{i_k}} \qquad (19)$$

Այս ներկայացումը թեև պարունակում է միայն (18) աղյուսակի տեղադրություններ, սակայն չի կարող համարվել վավեր ներկայացում, քանի որ ամեն տողից չի վերցված ճիշտ մեկ տեղադրություն (իհարկե, եթե $k = 1$, ապա ներկայացումը վավեր է) և ավելի մեծ համարի տողի տարրը հանդիպում է ավելի շուտ, քան ավելի փոքր համարինը՝ օրինակ $g_{n-1}^{1}g_{1}^{2}$:

Դիտարկենք (19) ներկայացման տարրերը շարժվելով աջից ձախ: Առաջին դեպքը, երբ առաջին տողի տարրը գրված է այլ տողի տարրից հետո դա $g_{n-1}^{k-1}g_{1}^{k}$-ն է: Քանի որ $g_{n-1}^{k-1}g_{1}^{k}$-ը (18) աղյուսակի տարրերի զույգի արտադրյալ է, ապա ալգորիթմի երկրորդ փուլի ժամանակ այս արտադրյալը ենթարկվել է cascade-ի և ուրեմն այն ներկայացվում է (18) աղյուսակի տարրերի արտադրյալով $g_{n-1}^{k-1}g_{1}^{k} = \acute{g}_{1}\acute{g}_{2}\ldots\acute{g}_{n-1}$ (որը հեշտությամբ կարող ենք ստանալ կրկին $g_{n-1}^{k-1}g_{1}^{k}$-ն ենթարկելով cascade-ի): Այսպիսով, (19) ներկայացումը կարտագրվի որպես

$$a = g_{1}^{1}g_{2}^{1}\ldots g_{n-1}^{1}g_{1}^{2}g_{2}^{2}\ldots g_{n-1}^{2}\ldots g_{1}^{k-1}g_{2}^{k-1}\ldots g_{n-2}^{k-1}\acute{g}_{1}\acute{g}_{2}\ldots\acute{g}_{n-1}g_{2}^{k}\ldots g_{n-1}^{k}$$

Այժմ $g_{n-2}^{k-1}\acute{g}_{1}$ դրվագում առաջին տողի տարրը գրված այլ տողի տարրից հետո: Այս դրվագը մեկ տեղով ավելի մոտ է (19) ներկայացման սկզբին: Փոխարինելով $g_{n-2}^{k-1}\acute{g}_{1}$-ը նրա ներկայացումով (18) աղյուսակի տարրերով և շարունակելով այս պրոցեսը կհասնենք այն պահին, երբ աջից ձախ զննելով a-ի ներկայացման առաջին դրվագը, որում առաջին տողի տարրը այլ տողի տարրից հետո է գրված դա $g_{1}^{k-1}g_{1}$ տեսքի դրվագը կլինի: Այս դրվագը մեկ տեղով ավելի մոտ է (19) ներկայացման սկզբին քան նախորդ այդպիսի դրվագը: Քանի որ $g_{1}^{k-1}g_{1}$ արտադրյալն էլ ենթարկվել է cascade-ի ալգորիթմի երկրորդ փուլում, ապա $g_{1}^{k-1}g_{1}$-ն ունի ներկայացում (18) աղյուսակի տարրերով, որով և կփոխարինենք $g_{1}^{k-1}g_{1}$-ն a-ի ներկայացման մեջ: Շարունակելով պրոցեսը կհասնենք a-ի հետևյալ ներկայացմանը՝

$$a = g_{1}g_{j_1}g_{j_2}\ldots g_{j_q}$$

որտեղ միայն g_{1}-ն է (18) աղյուսակի առաջին տողից, իսկ մնացածները երկրորդից սկսած տողերից են: Վերցնելով $g_{j_1}g_{j_2}\dots g_{j_q}$ արտադրյալը վերը դիտարկված եղանակով կարտագրենք այն $g_2g_{i_1}\dots g_{i_p}$ տեսքով, որտեղ միայն g_2-ն է (18) աղյուսակի երկրորդ տողից, իսկ մնացածները երրորդից սկսած տողերից են: Այս պրոցեսի արդյունքում պարզ է, որ կստանանք a-ի մի $a = g_1g_2\dots g_{n-1}$ ներկայացում, որտեղ g_i-ն (18) աղյուսակի i-րդ տողից է: Ալգորիթմի կոռեկտությունն ապացուցված է:

Դյուրին է տեսնել, որ Սիմսի ալգորիթմի առաջին փուլում կատարվող cascade-ների քանակը հավասար է $|S|$-ի , իսկ երկրորդ փուլում այն չի գերազանցում $\binom{n(n-1)/2}{2} = O(n^4)$ թիվը:

Սիմսի ալգորիթմի որոշ կիրառություններ

Սիմսի ալգորիթմը թույլ է տալիս հեշտությամբ լուծել մի շարք կարևոր խնդիրներ: Ստորև բերված են մի քանի օրինակներ:

1. Դիցուք G խումբը $(G \leq S_n)$ տրված է S ծնիչ բազմությունով և հարկավոր է հաշվել G խմբի կարգը: Դրա համար կառուցում ենք Սիմսի ալգորիթմի միջոցով G խմբի "ուժեղ" ծնիչների բազմությունը: Ապա հաշվում ենք (18) աղյուսակի տողերում գրված տեղադրությունների քանակները և այդ քանակներն իրար բազմապատկելով ստանում ենք $(G : 1)$-ը:

2. Դիցուք G խումբը $(G \leq S_n)$ տրված է S ծնիչ բազմությունով: **Խնդիր.** $a \in S_n$ համար ստուգել $a \in G$ պայմանը: Այս խնդիրը լուծվում է հետևյալ կերպ: Կառուցում ենք Սիմսի ալգորիթմի միջոցով G խմբի "ուժեղ" ծնիչների բազմությունը: Այժմ կամայական տրված a տեղադրության համար $a \in G$ պայմանը ստուգելու համար կիրառում ենք cascade(a)-ն (18) աղյուսակի (որը ստացվել է Սիմսի ալգորիթմով) նկատմամբ: Արդյունքում կամ ստանում ենք a-ի ներկայացումն "ուժեղ" ծնիչների բազմության տարրերով և ուստի՝ $a \in G$, կամ էլ cascade(a)-ի արդյունքում փորձ է կատարվում լրացնել (18) աղյուսակի որևէ դատարկ վանդակ, իսկ դա նշանակում է, որ $a \notin G$:

3. Դիցուք G-ն և H-ը S_n-ի ենթախմբեր են և տրված են համապատասխանաբար S^G և S^H ծնիչ բազմություններով: Հարկավոր է ստուգել $H \leq G$ պայմանը: Դրա համար բավական է բոլոր $a \in S^H$ ստուգել $a \in G$ պայմանը: Վերջին խնդիրը լուծված է նախորդ կետում:

4. Դիցուք $H \leq G \leq S_n$ և G-ն ու H-ը տրված են համապատասխանաբար S^G և S^H ծնիչ բազմություններով: Հարկավոր է ստուգել $H \lhd G$ պայմանը: Դրա համար վարվում ենք հետևյալ կերպ: Սիմսի ալգորիթմով կառուցում ենք H-ի և G-ի "ուժեղ" ծնիչների բազմությունները: Յուրաքանչյուր h-ի և g-ի համար համապատասխանաբար վերցված H-ի և G-ի "ուժեղ" ծնիչների բազմություններից ստուգում ենք $ghg^{-1} \in H$ պայմանը: Վերջին պայմանի ստուգումը հեշտությամբ կատարվում է cascade(ghg^{-1})-ը հաշվելով: Եթե բոլոր դեպքերում ստանում ենք, որ $ghg^{-1} \in H$, ապա $H \lhd G$: Եթե գոնե մեկ դեպքում $ghg^{-1} \notin H$, ապա ակնհայտորեն $H \lhd G$ պայմանը տեղի չունի: Ապացուցենք, որ եթե բոլոր h-րի և g-րի համար համապատասխանաբար վերցված H-ի և G-ի "ուժեղ" ծնիչների բազմություններից տեղի ունի $ghg^{-1} \in H$ պայմանը, ապա $H \lhd G$: Փաստորեն հարկավոր է ստուգել, որ $\forall x \in G, \forall y \in H \quad xyx^{-1} \in H$: Դիցուք $x = g_1 \ldots g_{n-1}$ և $y = h_1 \ldots h_{n-1}$ "ուժեղ" ծնիչների բազմությունների տարրերով ներկայացումներն են: Ունենք՝

$$xyx^{-1} = g_1 \ldots g_{n-1} h_1 \ldots h_{n-1} g_{n-1}^{-1} \ldots g_1^{-1}$$

և

$$xyx^{-1} = g_1 \ldots g_{n-2} \underbrace{(g_{n-1} h_1 g_{n-1}^{-1})}_{\in H} \ldots \underbrace{(g_{n-1} h_{n-1} g_{n-1}^{-1})}_{\in H} g_{n-2}^{-1} \ldots g_1^{-1}:$$

Պարզ է, որ $(g_{n-1} h_1 g_{n-1}^{-1})(g_{n-1} h_2 g_{n-1}^{-1}) \ldots (g_{n-1} h_{n-1} g_{n-1}^{-1})$ արտադրյալը պատկանում է H-ը և կարող է փոխարինվել "ուժեղ" ծնիչների ներկայացմամբ՝ (օրինակ cascade-ով) $(g_{n-1} h_1 g_{n-1}^{-1})(g_{n-1} h_2 g_{n-1}^{-1}) \ldots (g_{n-1} h_{n-1} g_{n-1}^{-1}) = h'_1 h'_2 \ldots h'_{n-1}$: Ուստի $xyx^{-1} = g_1 \ldots g_{n-2} h'_1 h'_2 \ldots h'_{n-1} g_{n-2}^{-1} \ldots g_1^{-1}$ և մեզ հաջողվեց վերացնել g_{n-1}-ը xyx^{-1}-ի ներկայացումից: Նման եղանակով կվերացնենք հաջորդաբար g_{n-2}-ը, հետո g_{n-3}-ը և այլն մինչև կմնան միայն H-ի տարրերը: Ուստի $xyx^{-1} \in H$:

Ազատ խմբեր, որոշիչ առնչություններ

Լուծենք հետևյալ խնդիրը: Փորձենք նկարագրել բոլոր 8-րդ կարգի ոչ աբելյան խմբերը:

Դիցուք $(G:1)=8$ և $e \neq a \in G$: Լագրանժի թեորեմից պարզ է, որ a-ի կարգը կարող է միայն 8-ի բաժանարար լինել: Դիցուք G-ում գոյություն ունի a, որի կարգը 8 է, ապա $\langle a\rangle = G$ (հիշենք, որ $\langle a\rangle$-ն դա a-ով ծնված ցիկլիկ խումբն է) և G-ն ցիկլիկ է, ուրեմն աբելյան: Եթե G-ի բոլոր տարրերի կարգը **2** է, ապա $\forall a \in G \quad a^2 = e$: Վերջին պայմանից հետևում է, որ G-ն աբելյան է: Իսկապես, $a^2 = e \Leftrightarrow a = a^{-1}$ և կամայական a և b համար ճիշտ է $ab = (ab)^{-1} = b^{-1}a^{-1} = ba$:

Ուստի G-ի բոլոր տարրերի կարգը կամ 2 է կամ 4 և գոյություն ունի $a \in G$, որի կարգը 4 է՝ $a^4 = e$: Ունենք $\langle a\rangle = \{e, a, a^2, a^3\}$ և տրոհելով G-ն հարակից դասերի ըստ $\langle a\rangle$-ի կստանանք՝ $G = \langle a\rangle \cup b\langle a\rangle$, որտեղ $b \in G\setminus\langle a\rangle$: Պարզ է, որ $b^2 \in \langle a\rangle$, քանի որ եթե $b^2 \in b\langle a\rangle$, ապա $b^2 = ba^k$ և $b = a^k \in \langle a\rangle$, ինչը սխալ է: Դյուրին է ստուգել, որ $b^2 \notin \{a, a^3\}$: Դիցուք $b^2 = a$ կամ $b^2 = a^3$: Պարզ է, որ b-ի կարգը 2 չէ: Այն նաև 4 չէ, քանի որ $b^4 = a^2$ կամ $b^4 = (a^3)^2 = a^4a^2 = a^2$: Եթե b-ի կարգը 8 է այդ դեպքում $\langle b\rangle = G$ և խումբն աբելյան է:

Ուստի $b^2 \in \{e, a^2\}$ և $b^2 = e$ կամ $b^2 = a^2$:

Դիտարկենք այժմ bab^{-1} տարրը: Եթե $bab^{-1} \in b\langle a\rangle$, ապա $bab^{-1} = ba^k$ և $ab^{-1} = a^k$ որից էլ ստանում ենք, որ $b = a^{1-k} \in \langle a\rangle$: Ուստի $bab^{-1} \in \langle a\rangle$: Պարզ է, որ $bab^{-1} \neq e$, քանի որ հակառակ դեպքում $a = e$: Եթե $bab^{-1} = a$, ապա $ba = ab$: Դա նշանակում է որ G-ն աբելյան է, քանի որ G-ի յուրաքանչյուր տարր ներկայացվում է $b^n a^m$ տեսքով, որտեղ $n = 0,1$ և $m = 0,1,2,3$ (դա հետևում է

$G = \langle a \rangle \cup b\langle a \rangle$ հարակից դասերի տրոհումից) և $(b^n a^m)(b^p a^q) = b^{n+p} a^{m+q} = (b^p a^q)(b^n a^m)$։ Եթե $bab^{-1} = a^2$, ապա $ba^2b^{-1} = bab^{-1}bab^{-1} = (bab^{-1})^2 = a^4 = e$ և $a^2 = e$։ Ուստի մնում է եզրակացնել, որ $bab^{-1} = a^3$։

Այսպիսով ստացանք, որ a և b տարրերը կապված են կամ

$$
\begin{aligned}
a^4 &= e \\
b^2 &= e \\
ba &= a^3 b
\end{aligned}
\tag{20}
$$

կամ էլ

$$
\begin{aligned}
a^4 &= e \\
b^2 &= a^2 \\
ba &= a^3 b
\end{aligned}
\tag{21}
$$

առնչություններով։

Վերը նշված (20) և (21) պայմաններին բավարարող 8 տարր պարունակող խմբեր իսկապես գոյություն ունեն։

Դիտարկենք, օրինակ, հետևյալ երկու 4 տարրանի տեղադրությունները. $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$ և $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (24)$, այսինքն a-ն 4 երկարության ցիկլ է, իսկ b-ն տրանսպոզիցիա է։ Դյուրին է ստուգել, որ $a^4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = e = b^2$։ Նաև $ba = (12)(34) = a^3 b$։ Խմբի բոլոր 8 տարրերն են e, a, $a^2 = (13)(24)$, $a^3 = (1432)$, b,

$ab = (14)(23)$, $a^2b = (13)$, $a^3b = (12)(34)$։

(**21**) պայմանների դեպքի համար դիտարկենք հետևյալ 2-չափանի կոմպլեքս մատրիցները. $A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ և $B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, i-ն կեղծ միավորն է։ Դյուրին է ստուգել, որ $A^4 = E$ (E-ն միավոր մատրիցն է), $B^2 = A^2 = -E$, $BA = A^3B = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix}$։ Խմբի բոլոր 8 տարրեր են՝ E, A, $A^2 = -E$, $A^3 = -A, B$, $AB = iE$, $A^2B = -B$, $A^3B = -iE$։ Այս խումբը բավարարում է (**21**) պայմաններին և աբելյան չէ, քանի որ $AB = iE \neq BA = -iE$։ Սա հայտնի, այսպես կոչված, "քվատերնիոնների" խումբն է։

Այժմ ֆիքսենք a և b տառերը և դիտարկենք $\{a,b\}^*$ բազմությունը, որը a և b տառերից կազմված բոլոր վերջավոր բառերի բազմությունն է (այդ բազմության մեջ է մտնում նաև դատարկ բառը, որը տարր չի պարունակում և ունի զրոյական երկարություն)։ $\{a,b\}^*$-ի վրա սահմանենք բազմապատկման գործողությունը հետևյալ կերպ. եթե α և $\beta \in \{a,b\}^*$, ապա α-ի և β-ի արտադրյալը դա $\alpha\beta$ բառն է, որը ստացվում է α և β բառերի կցագրումով։ Պարզ է, որ այս գործողությունն ասոցիատիվ է $(\alpha\beta)\gamma = \alpha(\beta\gamma) = \alpha\beta\gamma$։ Դատարկ բառը նշանակենք Λ-ով։ Ակնհայտ է, որ $\alpha\Lambda = \Lambda\alpha = \alpha$ կամայական α բառի համար և դատարկ բառը խաղում է խմբի միավոր տարրի դերը։

Դիցուք a և b տառերը բավարարում են (**20**) պայմաններին, այսինքն $aaaa = a^4 = \Lambda$, $bb = b^2 = \Lambda$, $ba = aaab = a^3b$։ Դա նշանակում է որ կամայական բառում a^4-ը կարելի է փոխարինել դատարկ բառով և հակառակը՝ դատարկի տեղը (այսինքն բառի կամայական տեղում) գրել a^4 կամ b^2: Նաև կամայական բառում ba հատվածը կարելի է փոխարինել a^3b-ով և հակառակը: Քանի որ $aa^3 = a^3a = \Lambda$ և $bb = \Lambda$, ապա a և b բառերը, և ուրեմն բոլոր բառերը $\{a,b\}^*$-ից, ունեն հակադարձ ըստ բազմապատկման՝ a-ի հակադարձը a^3-ն է, իսկ b-ի հակադարձը հենց b-ն է: Այսպիսով $\{a,b\}^*$ բազմությունը կազմում է խումբ ըստ բառերի կցագրման գործողության եթե a և b տառերը բավարարում են (20) պայմաններին:

Դիտարկենք այժմ $\{a,b\}^*$ խմբի կամայական բառ: Պարզ է, որ կիրառելով $ba = a^3b$ պայմանը (այսինքն կամայական ba հատվածը փոխարինելով a^3b-ով) կարող ենք այդ տրված բառը ձևափոխել այնպես, որ այն ունենա a^nb^m տեսքը: $a^4 = \Lambda$ և $b^2 = \Lambda$ պայմաններից ստանում ենք, որ խմբի կամայական բառ կարող է ներկայացվել a^nb^m տեսքով, որտեղ $n = 0,1,2,3$ և $m = 0,1$: Այսպիսով ստանում ենք 8 տարբեր բառ՝ $\{\Lambda, a, aa, aaa, b, ab, aab, aaab\} = \langle a\rangle \cup \langle a\rangle b$:

Նման եղանակով կարող ենք կառուցել մեկ այլ խումբ, որը բավարարում է (21) պայմաններին: Բոլոր բառերը կներկայացվեն a^nb^m տեսքով, որտեղ $n = 0,1,2,3$ և $m = 0,1,2,3$, քանի որ $b^4 = \Lambda$: Սակայն $b^2 = a^2$ և a^nb^m բառում b^2-ին փոխարինելով a^2-ով կստանանք a^nb^m տեսքի բառ, որում $n = 0,1,2,3$ և $m = 0,1$: Ուստի կրկին խմբի կարգը 8 է և

$$\{\Lambda, a, aa, aaa, b, ab, aab, aaab\} = \langle a\rangle \cup \langle a\rangle b:$$

Խմբի նկարագրման բառերի և որոշիչ առնչությունների ((20) և (21) պայմանների) միջոցով այս վերջին եղանակը կիրառելի է նաև ընդհանուր դեպքում կամայական խմբի համար: Փաստորեն դա խմբի տրման մի եղանակ է, որն ի տարբերություն "ուժեղ" ծնիչների բազմության ալգորիթմական եղանակի կարելի է համարել խմբի "անալիտիկ" նկարագրման եղանակ:

Դիցուք S-ն որևէ բազմություն է, որի տարրերը դիտարկում ենք որպես ֆորմալ տառեր (նիշեր): Ամեն մի a տառի համար սահմանում ենք մի նոր նիշ՝ a^{-1}, որը կանվանենք a-ի հակադարձ: Նշանակենք S^*-ով բոլոր վերջավոր երկարության բառերը, որոնք կազմված են S-ի տարրերից կամ էլ S-ի տարրերի հակադարձներից, այսինքն բոլոր $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots x_k^{\varepsilon_k}$ տեսքի բառերը, որտեղ $k \geq 0$ և $x_i \in S$, $\varepsilon_i \in \{1,-1\}$, $i = 1,2,\ldots,k$: Զրոյական երկարության բառը $k = 0$ կոչվում է դատարկ բառ և նշանակվում է Λ-ով: Երկու բառ S^*-ից համարվում են համարժեք և չեն տարբերվում իրարից եթե մեկը մյուսից կարելի է ստանալ aa^{-1} կամ $a^{-1}a$ տեսքի (${a \in S}$) ենթաբառերը Λ-ով փոխարինելով կամ էլ հակառակը՝ մի բառի հարևան տառերի միջև aa^{-1} կամ $a^{-1}a$ տեսքի ենթաբառեր ավելացնելով: α և β բառերի համարժեքության փաստը կվավերացնենք գրելով $\alpha \approx \beta$: Այլ կերպ ասած կամայական $a \in S$ համար տեղի ունեն հետևյալ առնչությունները

$$aa^{-1} = a^{-1}a = \Lambda \qquad (22)$$

S^* բազմությունը տրոհվում է չհատվող դասերի՝ միևնույն դասի բառերը համարժեք են, իսկ տարբեր դասերինը համարժեք չեն: Իրոք, ամեն մի բառ պատկանում է ինչ որ մի դասի: Եթե $\alpha \approx \beta$, ապա $\beta \approx \alpha$: Եթե $\alpha,\beta,\gamma \in S^*$, ապա $\alpha \approx \beta,\ \beta \approx \gamma \Rightarrow \alpha \approx \gamma$: Այժմ, եթե երկու դաս ունեն ընդհանուր բառ, ապա այդ երկու դասերի կամայական բառեր իրար համարժեք են: $\alpha \in S^*$ բառի համարժեքության դասը կնշանակենք $[\alpha]$-ով:

Նշանակենք $F(S)$-ով S^* բազմության համարժեքության դասերի բազմությունը: $F(S)$-ի վրա սահմանենք բազմապատկման գործողություն՝ $[\alpha][\beta] = [\alpha\beta]$: Ակնհայտ է, որ այսպիսի սահմանումը կոռեկտ է՝ եթե $\alpha_1 \in [\alpha]$ և $\beta_1 \in [\beta]$, ապա $\alpha_1\beta_1 \in [\alpha\beta]$: Դյուրին ստուգվում է, որ $F(S)$-ը խումբ է: Միավոր տարրը Λ-ն է, իսկ $[x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ldots x_k^{\varepsilon_k}]$-ի հակադարձը $[x_k^{-\varepsilon_k}\ldots x_2^{-\varepsilon_2}x_1^{-\varepsilon_1}]$-ն է:

Սահմանում: $F(S)$ խումբը կոչվում է **ազատ** խումբ S բազմության նկատմամբ:

Փաստորեն ազատ խումբը S բազմությամբ ծնված այն խումբն է, որի տարրերի միջև չկա ոչ մի առնչություն բացի (22) տեսքի տրիվիալ առնչություններից: Այդ իմաստով $F(S)$-ն "ազատ" է:

Դիցուք տրված են S ծնիչների բազմությունը և S-ի տարրերի միջև որոշիչ առնչությունների մի բազմություն: Կամայական առնչություն կարելի է գրել այնպես, որ այն ունենա $\alpha = e$ տեսքը: Բոլոր այդ առնչություններից ստանանք առնչություններ $F(S)$ ազատ խմբում վերցնելով $[\alpha] = [\Lambda]$ առնչությունները: Այդ առնչությունների բազմությունը կնշանակենք T-ով: Ազատ խմբի երկու դաս (տարր) կհամարենք հավասար, եթե մի դասի որևէ բառ ստացվում է մյուս դասի որևէ բառից T բազմության առնչությունների հաջորդաբար կիրառմամբ: Այլ կերպ ասած S^*-ի երկու բառ համարժեք են (միևնույն դասից են), եթե մեկը մյուսից ստացվում է (22) տեսքի տրիվիալ և T բազմության առնչությունների վերջավոր անգամ հաջորդաբար կիրառմամբ:

Նշանակենք R-ով T բազմության առնչությունների ձախ մասերից բաղկացած բազմությունը: Պարզ է, որ $R \subseteq F(S)$: Ակնհայտ է, որ բացի T բազմության առնչություններից ազատ խմբում տեղի ունեն նաև հետևյալ առնչությունները՝ $[\beta][\alpha][\beta^{-1}] = [\Lambda]$, որտեղ $[\beta] \in F(S)$ և $[\alpha] \in R$: Ավելացնելով R-ին բոլոր $[\beta][\alpha][\beta^{-1}]$ տեսքի տարրերը կստանանք R-ը պարունակող ամենափոքր նորմալ ենթախումբը $F(S)$ ազատ խմբում, որը կնշանակենք $N(R)$-ով: Դիտարկենք $F(S)/N(R)$ ֆակտոր-խումբը: Երկու տարր $[\alpha]$ և $[\beta]$ կպատկանեն միևնույն հարակից դասին ըստ $N(R)$-ի միայն և միայն, եթե $[\beta^{-1}][\alpha] = [\beta^{-1}\alpha] \in N(R)$, իսկ դա նշանակում է, որ $[\alpha] = [\beta\gamma] = [\beta][\gamma]$, $[\gamma] \in N(R)$: Ուրեմն $[\beta]$-ն ստացվում է $[\alpha]$-ից $N(R)$-ի $[\gamma] = [\Lambda]$ առնչության կիրառմամբ: Դիցուք այժմ $\alpha = \alpha_1\gamma\alpha_2$ և $[\gamma] \in N(R)$: Քանի որ $N(R)$-ը նորմալ է $F(S)$-ում, ապա գոյություն ունի $[\gamma_1] \in N(R)$, որ

$$[\gamma\alpha_2] = [\gamma][\alpha_2] = [\alpha_2][\gamma_1] = [\alpha_2\gamma_1]:$$

Ուստի

$$[\alpha] = [\alpha_1\gamma\alpha_2] = [\alpha_1][\gamma\alpha_2] = [\alpha_1][\alpha_2\gamma_1] = [\alpha_1\alpha_2][\gamma_1] = [\alpha_1\alpha_2]$$

և $[(\alpha_1\alpha_2)^{-1}][\alpha] \in N(R)$: Ստացանք, որ $[\alpha]$-ն և $[\alpha_1\alpha_2]$-ը միևնույն հարակից դասից են ըստ $N(R)$-ի և $[\gamma] = [\Lambda]$, $[\gamma] \in N(R)$, առնչությունների կիրառումը տրված հարակից դասի տարրին դուրս չի բերում արդյունքն այդ դասից:

Այսպիսով ապացուցեցինք, որ $[\alpha]$-ից $[\beta]$-ն կարելի է ստանալ T բազմության առնչությունների հաջորդաբար կիրառմամբ միայն և միայն այն դեպքում, երբ $[\alpha]$-ն ու $[\beta]$-ն միևնույն հարակից դասից են ըստ $N(R)$-ի: Ուստի S ծնիչների բազմությամբ և տրված առնչություններով որոշվում է մի խումբ, որն իզոմորֆ է $F(S)/N(R)$ ֆակտոր-խմբին: Այս դեպքում ասում են, որ խումբը տրված է ծնիչներով և որոշիչ առնչություններով: Վերը նկարագրված 8 կարգի ոչ աբելյան խմբերը տրված են $S = \{a,b\}$ ծնիչներով և (20) կամ (21) որոշիչ առնչություններով:

Վերջավոր ծնված աբելյան խմբեր

*Դիցուք G-ն աբելյան խումբ է, որն ունի ծնիչների վերջավոր բազմություն: Այդպիսի խմբերը կանվանենք **վերջավոր ծնված** աբելյան խմբեր: Դրանց պարզագույն օրինակներն են ցիկլիկ խմբերը, որոնք ծնվում են մեկ ծնիչով: Պարզվում է, որ կամայական վերջավոր ծնված աբելյան խումբ կարելի է ներկայացնել ցիկլիկ խմբերի ուղիղ արտադրյալի տեսքով և դրանով իսկ փաստորեն նկարագրել բոլոր վերջավոր ծնված աբելյան խմբերը:*

Այս մասում կօգտվենք աբելյան խմբերի ադիտիվ ներկայացումից, այսինքն խմբի գործողությունը կնշանակենք գումարման + նշանով: Բոլոր խմբերը այս մասում աբելյան են: $G_1\times\ldots\times G_n$ աբելյան խմբերի ուղիղ արտադրյալը կնշանակենք $G_1\oplus\ldots\oplus G_n$ նշանով (այս արտադրյալը նույնպես անվանում են ուղիղ գումար):

Այն փաստը, որ G խումբը վերջավոր ծնված է, նշանակում է, որ կգտնվեն վերջավոր քանակությամբ տարրեր G-ից՝ $g_1,\ldots,g_n$, որ

$$G=\{\lambda_1 g_1+\ldots+\lambda_n g_n \mid \lambda_i\in\mathbb{Z}, i=1,\ldots,n\}:$$

Նախ և առաջ կուսումնասիրենք

$$\mathbb{Z}^n=\underbrace{\mathbb{Z}\oplus\ldots\oplus\mathbb{Z}}_{n\ \text{հատ}}=\{(\lambda_1,\ldots,\lambda_n) \mid \lambda_i\in\mathbb{Z}, i=1,\ldots,n\}$$

խումբը:

Լեմմ 5. *$\mathbb{Z}^n$ խմբի կամայական ենթախումբ վերջավոր ծնված է և ունի ծնիչների բազմություն, որի հզորությունը $\leq n$:*

Ապացույց. *Ապացույցը կկատարենք ինդուկցիայով ըստ n-ի:*

Ակնհայտ է, որ $n=1$ դեպքում $\mathbb{Z}$-ի կամայական ենթախումբը կազմված է որոշակի ամբողջ թվի բոլոր պատիկներից՝ ուստի վերջավոր ծնված է մեկ ծնիչով: Դիցուք լեմմի պնդումը ճիշտ է $\mathbb{Z}^{n-1}$ համար: Ապացուցենք այն $\mathbb{Z}^n$ համար: Դիցուք $H \leq \mathbb{Z}^n$: Սահմանենք F բազմությունը հետևյալ կերպ՝ $F = \{\mu \mid \exists(\lambda_2, \ldots, \lambda_n)$ $(\mu, \lambda_2, \ldots, \lambda_n) \in H\ \}$: Ակնհայտ է, որ $F \leq \mathbb{Z}$: Եթե $F \neq \{0\}$, ապա նշանակենք μ_1-ով F ենթախմբի փոքրագույն դրական տարրը, եթե $F = \{0\}$, ապա $\mu_1 = 0$: Ֆիքսենք H ենթախմբում որևէ տարր, որի առաջին կոորդինատը μ_1 է՝ $(\mu_1, \mu_2, \ldots, \mu_n)$:

Դիցուք $(\lambda_1, \ldots, \lambda_n) \in H$: Պարզ է, որ $\lambda_1 \in F$: Եթե $F = \{0\}$, ապա $\lambda_1 = 0$: Վերցնենք $\varepsilon = 0$ և $\lambda_1 = \varepsilon\mu_1$: Եթե $F \neq \{0\}$ և $\lambda_1 = 0$, ապա վերցնենք $\varepsilon = 0$ և $\lambda_1 = \varepsilon\mu_1$: Եթե $F \neq \{0\}$ և $\lambda_1 \neq 0$ բաժանենք λ_1-ը μ_1-ի վրա՝ $\lambda_1 = \nu\mu_1 + \delta$, որտեղ $0 \leq \delta < |\mu_1|$: Ստանում ենք՝ $\delta = \lambda_1 - \nu\mu_1 \in F$ և, եթե $\delta > 0$, ապա μ_1-ը F ենթախմբի փոքրագույն դրական տարրը չէ: Ուստի $\lambda_1 = \nu\mu_1$: Այսպիսով բոլոր դեպքերում $(\lambda_1, \ldots, \lambda_n) \in H$ համար գոյություն ունի միարժեքորեն որոշված $\varepsilon \in \mathbb{Z}$, որ $\lambda_1 = \varepsilon\mu_1$ ($\lambda_1 = 0$ դեպքում միշտ $\varepsilon = 0$): Դյուրին է տեսնել, որ

$$(\lambda_1, \lambda_2, \ldots, \lambda_n) = \varepsilon(\mu_1, \mu_2, \ldots, \mu_n) + (0, \lambda_2 - \varepsilon\mu_2, \ldots, \lambda_n - \varepsilon\mu_n) \qquad (23)$$

և յուրաքանչյուր $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in H$ համապատասխանեցված է որոշակի $(\lambda_2 - \varepsilon\mu_2, \ldots, \lambda_n - \varepsilon\mu_n) \in \mathbb{Z}^{n-1}$: Նշանակենք բոլոր $(\lambda_2 - \varepsilon\mu_2, \ldots, \lambda_n - \varepsilon\mu_n)$ տարրերի բազմությունը $\acute{H}$-ով և ցույց տանք, որ $\acute{H} \leq \mathbb{Z}^{n-1}$: Իրոք, դիցուք $(\alpha_1, \ldots, \alpha_n) \in H$ և $(\beta_1, \ldots, \beta_n) \in H$: Համաձայն (23)-ի ստանում ենք՝

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = \varepsilon_\alpha(\mu_1, \mu_2, \ldots, \mu_n) + (0, \alpha_2 - \varepsilon_\alpha\mu_2, \ldots, \alpha_n - \varepsilon_\alpha\mu_n)$$
$$(\beta_1, \beta_2, \ldots, \beta_n) = \varepsilon_\beta(\mu_1, \mu_2, \ldots, \mu_n) + (0, \beta_2 - \varepsilon_\beta\mu_2, \ldots, \beta_n - \varepsilon_\beta\mu_n)$$

Պարզ է, որ $(\alpha_2 - \varepsilon_\alpha\mu_2, \ldots, \alpha_n - \varepsilon_\alpha\mu_n) \in \acute{H}$ և

$(\beta_2 - \varepsilon_\beta\mu_2, \ldots, \beta_n - \varepsilon_\beta\mu_n) \in \acute{H}$: Ակնհայտ է, որ $(\alpha_1 - \beta_1, \ldots, \alpha_n - \beta_n) = (\alpha_1, \ldots, \alpha_n) - (\beta_1, \ldots, \beta_n) \in H$: Ունենք որ $\alpha_1 = \varepsilon_\alpha\mu_1, \beta_1 = \varepsilon_\beta\mu_1$, ուստի

- եթե $\alpha_1 = \beta_1 = 0$, ապա $\varepsilon_\alpha = \varepsilon_\beta = 0$ և $\alpha_1 - \beta_1 = (\varepsilon_\alpha - \varepsilon_\beta)\mu_1$
- եթե $\alpha_1 \neq 0, \beta_1 \neq 0$, $\alpha_1 = \beta_1$, ապա $\varepsilon_\alpha = \varepsilon_\beta$ և $\alpha_1 - \beta_1 = (\varepsilon_\alpha - \varepsilon_\beta)\mu_1$
- եթե $\alpha_1 \neq \beta_1$, ապա $\mu_1 \neq 0$ և $\frac{\alpha_1 - \beta_1}{\mu_1}$-ն որոշված է միարժեքորեն և համընկնում է $\varepsilon_\alpha - \varepsilon_\beta$ հետ

Հետևաբար բոլոր դեպքերում $\alpha_1 - \beta_1 = (\varepsilon_\alpha - \varepsilon_\beta)\mu_1$ և

$$(\alpha_1 - \beta_1, \alpha_2 - \beta_2, \ldots, \alpha_n - \beta_n) = (\varepsilon_\alpha - \varepsilon_\beta)(\mu_1, \mu_2, \ldots, \mu_n) +$$
$$(0, (\alpha_2 - \beta_2) - (\varepsilon_\alpha - \varepsilon_\beta)\mu_2, \ldots, (\alpha_n - \beta_n) - (\varepsilon_\alpha - \varepsilon_\beta)\mu_n)$$

Ուստի

$$(\alpha_2 - \varepsilon_\alpha\mu_2, \ldots, \alpha_n - \varepsilon_\alpha\mu_n) - (\beta_2 - \varepsilon_\beta\mu_2, \ldots, \beta_n - \varepsilon_\beta\mu_n) =$$
$$((\alpha_2 - \beta_2) - (\varepsilon_\alpha - \varepsilon_\beta)\mu_2, \ldots, (\alpha_n - \beta_n) - (\varepsilon_\alpha - \varepsilon_\beta)\mu_n) \in \acute{H}$$

և $\acute{H} \leq \mathbb{Z}^{n-1}$:

Համաձայն ինդուկտիվ ենթադրության $\acute{H}$-ը վերջավոր ծնված է և ունի ծնիչների բազմություն, որ բաղկացած է ոչ ավելի, քան $n-1$ հատ ծնիչներից: $\acute{H}$-ի ծնիչների այդ բազմության վեկտորներին ավելացնենք մեկ նոր զրոյական առաջին կոորդինատ: Այսինքն $(\gamma_1, \gamma_2, \ldots, \gamma_{n-1}) \in \acute{H}$ ծնիչից ստացվում է $(0, \gamma_1, \gamma_2, \ldots, \gamma_{n-1}) \in H$ վեկտորը: Այս զրոյական կոորդինատներով ընդլայնված ծնիչների բազմությունը կանվանենք $\acute{H}$-ի ընդլայնված ծնիչների բազմություն: Այժմ ակնհայտ է, որ (23)-ի $(0, \lambda_2 - \varepsilon\mu_2, \ldots, \lambda_n - \varepsilon\mu_n)$ վեկտորը կստացվի $\acute{H}$-ի ընդլայնված ծնիչների միջոցով, ուստի կամայական $(\lambda_1, \lambda_2, \ldots, \lambda_n) \in H$ կստացվի $(\mu_1, \mu_2, \ldots, \mu_n)$ և $\acute{H}$-ի ընդլայնված ծնիչների միջոցով, որոնք կկազմեն H-ի համար ծնիչների վերջավոր *բազմությունը: Լեմմն ապացուցված է:*

Դիցուք $H \leq \mathbb{Z}^n$ *և* H*-ի ծնիչներն են՝* $\Lambda_1 = (\lambda_{11}, \dots, \lambda_{1n}), \dots, \Lambda_m = (\lambda_{m1}, \dots, \lambda_{mn})$*: Կազմենք հետևյալ մատրիցը*

$$\Lambda = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \end{pmatrix}$$

Այս մատրիցի տողերը կազմում են H*-ի ծնիչների բազմություն: Համաձայն Լեմմ 4ա-ի կարող ենք համարել, որ* $m \leq n$*: Դիտարկենք* Λ *մատրիցի տողերի նկատմամբ հետևյալ գործողությունները՝*

1. *երկու տողերի տեղափոխություն*
2. *տողի բազմապատկում* -1*-ով*
3. *մեկ տողի գումարումը մյուսին*

Այս գործողությունների արդյունքում ստացվում են H*-ի ծնիչների նոր բազմություններ: Առաջին երկու գործողությունների դեպքում դա ակնհայտ է: Դիցուք*

$$\hat{\Lambda} = \begin{pmatrix} \lambda_{11} + \lambda_{21} & \lambda_{12} + \lambda_{22} & \cdots & \lambda_{1n} + \lambda_{2n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \end{pmatrix}$$

Եթե H*-ի որևէ տարր ներկայացվում է* $\varepsilon_1\Lambda_1 + \varepsilon_2\Lambda_2 + \ldots + \varepsilon_m\Lambda_m$ *տեսքով, ապա* $\hat{\Lambda}$ *համակարգով այն կներկայացվի* $\varepsilon_1\hat{\Lambda}_1 + (\varepsilon_2 - \varepsilon_1)\hat{\Lambda}_2 + \varepsilon_3\hat{\Lambda}_3 + \ldots + \varepsilon_m\hat{\Lambda}_m$ *տեսքով:*

Դյուրին է տեսնել, որ եթե $\mathbb{Z}^n$*-ի բոլոր տարրերում միաժամանակ* *տեղերով փոխենք i-րդ և j-րդ կոորդինատները, ապա կստանանք $\mathbb{Z}^n$-ի ավտոմորֆիզմ, որի դեպքում H-ը կանցնի իրեն իզոմորֆ մեկ այլ խմբի մեջ: $\mathbb{Z}^n$-ի ավտոմորֆիզմ է ստացվում նաև, եթե միաժամանակ $\mathbb{Z}^n$-ի բոլոր տարրերում բազմապատկենք i-րդ կոորդինատները -1-ով: Մեկ այլ ավտոմորֆիզմ կստանանք, եթե $\mathbb{Z}^n$-ի բոլոր տարրերում միաժամանակ i-րդ կոորդինատները գումարենք j-րդ կոորդինատներին: Բոլոր դեպքերում H-ը կանցնի իրեն իզոմորֆ մեկ այլ խմբի մեջ: Ուրեմն, եթե Λ մատրիցի սյուներին կիրառենք հետևյալ գործողությունները,*

4. *երկու սյուների տեղափոխություն*

5. *սյան բազմապատկում -1-ով*

6. *մեկ սյան գումարումը մյուսին,*

ապա ձևափոխված Λ մատրիցի տողերը կկազմեն ծնիչների համակարգ H-ին իզոմորֆ խմբի համար:

Պարզ է, որ թե տողերի և թե սյուների դեպքում մեկ տողը/սյունը -1-ով բազմապատկելով և հետո մյուս տողին/սյանը գումարելով իրականացվում է մեկ տողից/սյունից մեկ այլ տող/սյուն հանելու գործողությունը:

*Վերը նշված տողերի 1.-3. և սյուների 4.-6. գործողությունները կանվանենք տողերի և սյուների նկատմամբ **տարրական գործողություններ**:*

Այսպիսով, Λ մատրիցին կիրառելով տողերի և/կամ սյուների տարրական գործողությունները կստանանք H խմբին իզոմորֆ խմբի ծնիչների բազմություն: Տեղի ունի հետևյալ կարևոր փաստը

Թեորեմ 6. (Մատրիցի Սմիթի նորմալ տեսքի մասին)

Կամայական $n \times n$-չափանի մատրից, որի տարրերն ամբողջ թվեր են, տողերի և սյուների տարրարկան գործողություններով կարելի է բերել

$$\begin{pmatrix} n_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & n_r & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

անկյունագծային տեսքի, որտեղ $n_i > 0, i = 1,2,\ldots,r$, ընդ-որում n_{i+1}-ը բաժանվում է առանց մնացորդի n_i-ի վրա, $i = 1,2,\ldots,r-1$:

Ապացույց. Դիցուք տրված է A մատրիցը: Զրոյական A մատրիցի համար թեորեմի պնդումն ակնհայտորեն ճիշտ է, այդ պատճառով կդիտարկենք $A \neq 0$ դեպքը:

Այժմ կնկարագրենք մի ալգորիթմ, որը բերում է տրված մատրիցը Սմիթի նորմալ տեսքին: Մատրիցի առաջին տողում և առաջին սյունում գտնվող տարրը կանվանենք հենքային տարր և կնշանակենք այն α-ով: Սկզբից գտնենք մատրիցի նվազագույն դրական բացարձակ արժեքով տարրը և տողերի ու սյուների տեղափոխություններով և, եթե անհրաժեշտ է, -1-ով բազմապատկելով առաջին սյունը, դարձնենք $|\alpha|$ տարրը հենքային: Վերցնենք այժմ որևէ ոչ հենքային ոչ զրոյական տարր առաջին տողից/սյունից: Դիցուք դա β-ն է: Պարզ է, որ $|\beta| \geq |\alpha|$: Բաժանենք β-ն հենքային տարրի վրա՝ $\beta = \alpha\gamma + \delta$: Ապա $|\gamma|$ անգամ գումարենք (հանենք) առաջին տողը/սյունը β-ն պարունակող տողին(տողից)/սյանը(սյունից): Արդյունքում β-ի տեղում կստանանք δ-ն: Եթե $\delta > 0$, ապա $\delta < |\alpha|$ և տողերի ու սյուների տեղափոխություններով և, եթե անհրաժեշտ է, -1-ով բազմապատկելով առաջին սյունը, դարձնենք δ-ն հենքային տարր: Նշված եղանակով վարվենք մատրիցի բոլոր ոչ հենքային տարրերի հետ, որոնք գտնվում են առաջին տողում/սյունում: Քանի որ հենքային տարրերի բացարձակ արժեքները խիստ նվազում են, ապա այս պրոցեսը կավարտվի վերջավոր քանակությամբ քայլերից հետո և արդյունքում առաջին տողի/սյան բոլոր տարրերը բացի հենքայինից կդառնան զրոյական: Այսինքն մատրիցը կբերվի հետևյալ տեսքի՝

$$A = \left(\begin{array}{c|ccc} \alpha & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & B & \\ 0 & & & \end{array}\right)$$

Դիցուք B մատրիցում գոյություն ունի տարր, որ չի բաժանվում առանց մնացորդի հենքայինի վրա: Նշանակենք այդ տարրը β-ով: Ենթադրենք, որ β-ն գտնվում է A մատրիցի i-րդ տողում և j-րդ սյունում, $i,j > 1$: Բաժանենք β-ն հենքային տարրի վրա՝ $\beta = \alpha\gamma + \delta$, որտեղ $0 < \delta < |\alpha|$: Ապա $|\gamma|$ անգամ գումարենք առաջին սյունը β-ն պարունակող j-րդ սյանը: Արդյունքում A մատրիցի առաջին տողի j-րդ տեղում կստանանք $\pm\alpha\gamma$-ն: Այժմ i-րդ տողն առաջինին գումարելով կամ առաջինից հանելով դարձնենք առաջին տողի j-րդ տարրը հավասար $\pm\delta$: Առաջին տողում ստանում ենք մի տարր, որի բացարձակ արժեքը փոքր է հենքային տարրի բացարձակ արժեքից: Տողերի ու սյուների տեղափոխություններով և, եթե անհրաժեշտ է, -1-ով բազմապատկելով առաջին սյունը, դարձնենք δ տարրը հենքային և կրկնենք վերը շարադրված առաջին տողի և առաջին սյան ոչ հենքային տարրերի զրոյացման պրոցեսը: Քանի որ հենքային տարրերի բացարձակ արժեքները խիստ նվազում են, ապա այս պրոցեսը կավարտվի վերջավոր քանակությամբ քայլերից հետո և B մատրիցի յուրաքանչյուր տարր կբաժանվի հենքայինի վրա առանց մնացորդի: Մնում է ամբողջ պրոցեսը կիրառել B մատրիցին: Թեորեմն ապացուցված է:

Թեորեմ 7.

Մատրիցի Սմիթի նորմալ տեսքը որոշված է միարժեքորեն:

Ապացույց. Դյուրին է նկատել, որ տարրական գործողությունները չեն փոխում մատրիցի մինորների բացարձակ արժեքները: Այստեղից հետևում է, որ չեն փոխվում նաև բոլոր k-չափանի մինորների ամենամեծ ընդհանուր բաժանարարները, $k \leq n$: Հաշվենք k-չափանի մինորների ամենամեծ ընդհանուր բաժանարարները Սմիթի նորմալ տեսքի մատրիցի համար

$$\begin{pmatrix} n_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & n_r & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Ակնհայտ է, որ 1-չափանի մինորների ամենամեծ ընդհանուր բաժանարարը դա n_1-ն է: Դյուրին է համոզվել, որ k-չափանի մինորների ամենամեծ ընդհանուր բաժանարարը դա $n_1 n_2 \ldots n_k$ արտադրյալն է, $k \leq r$: Երբ տեղի ունի $r < k \leq n$ պայմանը k-չափանի մինորները զրոյական են: Ուստի $n_1, n_1n_2, \dots, n_1n_2\dots n_r$ արտադրյալները և դրանց հարաբերությունները՝ $n_1, \frac{n_1n_2}{n_1} = n_2, \frac{n_1n_2n_3}{n_1n_2} = n_3, \dots, \frac{n_1n_2\dots n_r}{n_1n_2\dots n_{r-1}} = n_r$ որոշվում են միարժեքորեն: Թեորեմն ապացուցված է:

Օրինակներ

1. $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ մատրիցի Սմիթի նորմալ տեսքն է

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

2. $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ մատրիցի Սմիթի նորմալ տեսքն է

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Կիրառենք այժմ Սմիթի նորմալ տեսքի մասին թեորեմը $\mathbb{Z}^n$-ի բոլոր ենթախմբերի իզոմորֆիզմի ճշտությամբ նկարագրման համար: Դիցուք $H \leq \mathbb{Z}^n$: Վերցնենք H-ի որևէ ծնիչների բազմություն, որ պարունակում է m ծնիչ ($m \leq n$ համաձայն Թեորեմ 5-ի) և կազմենք ծնիչների մատրիցը, լրացնելով այն $n-m$ հատ զրոյական տողերով՝

$$\Lambda = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ \lambda_{m1} & \lambda_{m2} & \cdots & \lambda_{mn} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

Պարզ է, որ սա նույնպես H-ի ծնիչների բազմություն է: Բերենք Λ մատրիցը Սմիթի նորմալ տեսքի և կստանանք H-ին իզոմորֆ խմբի ծնիչների բազմության $n \times n$ մատրից՝

$$\begin{pmatrix} n_1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & n_r & 0 & \cdots & 0 \\ 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{pmatrix}$$

Դյուրին է տեսնել, որ այս ծնիչներով ծնվում է

$$\left\{ \left(\gamma_1 n_1, \gamma_2 n_2, \ldots, \gamma_r n_r, \underbrace{0, \ldots, 0}_{n-r} \right) \middle| \gamma_i \in \mathbb{Z}, i = 1, 2, \ldots, r \right\}$$

խումբը, որն իր հերթին իզոմորֆ է հետևյալ ուղիղ գումարին՝

$$n_1\mathbb{Z} \oplus n_2\mathbb{Z} \oplus \cdots \oplus n_r\mathbb{Z} \oplus \underbrace{\{0\} \oplus \cdots \oplus \{0\}}_{n-r} ,$$

որտեղ $k\mathbb{Z} = \{kx \mid x \in \mathbb{Z}\}$*: Այսպիսով ապացուցեցինք հետևյալ թեորեմը:*

Թեորեմ 8.

Դիցուք $H \leq \mathbb{Z}^n$**:** H**-ն իզոմորֆ է**

$$n_1\mathbb{Z} \oplus n_2\mathbb{Z} \oplus \cdots \oplus n_r\mathbb{Z} \oplus \underbrace{\{0\} \oplus \cdots \oplus \{0\}}_{n-r}$$

ուղիղ գումարին միարժեքորեն որոշված $n_1, n_2, \ldots, n_r$ **այնպիսի դրական ամբողջ թվերի համար, որ** n_{i+1}**-ը բաժանվում է առանց մնացորդի** n_i**-ի վրա,** $i = 1, 2, \ldots, r-1$**:**

Այստեղից էլ ստացվում է վերջավոր ծնված աբելյան խմբերի նկարագրությունը՝

Թեորեմ 9.

Դիցուք G**-ն վերջավոր ծնված աբելյան խումբ է և ծնված է** n **հատ ծնիչ պարունակող ծնիչների բազմությամբ: Գոյություն ունեն միարժեքորեն որոշված այնպիսի դրական ամբողջ** $n_1, n_2, \ldots, n_r$ **թվեր, որ** n_{i+1}**-ը բաժանվում է առանց մնացորդի** n_i**-ի վրա,** $i = 1, 2, \ldots, r-1$**, որ** G**-ն իզոմորֆ է**

$$\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r} \oplus \mathbb{Z}^{n-r}$$

ուղիղ գումարին, որտեղ $\mathbb{Z}_k = \mathbb{Z}/k\mathbb{Z}$**:**

Ապացույց. Դիցուք G-ի ծնիչներն են՝ $g_1, \ldots, g_n$ տարրերը, ուստի

$$G = \{\lambda_1 g_1 + \ldots + \lambda_n g_n \mid \lambda_i \in \mathbb{Z}, i = 1, \ldots, n\}:$$

Դյուրին է տեսնել, որ $(\lambda_1,\ldots,\lambda_n) \mapsto \lambda_1 g_1 + \ldots + \lambda_n g_n$ արտապատկերումը դա հոմոմորֆիզմ է $\mathbb{Z}^n$-ից G-ի վրա: Համաձայն իզոմորֆիզմի մասին թեորեմի G-ն իզոմորֆ է $\mathbb{Z}^n$-ի ըստ նշված հոմոմորֆիզմի միջուկի ֆակտոր-խմբին: Բայց միջուկը լինելով $\mathbb{Z}^n$-ի ենթախումբ ըստ Թեորեմ 8-ի իզոմորֆ է

$$n_1\mathbb{Z} \oplus n_2\mathbb{Z} \oplus \cdots \oplus n_r\mathbb{Z} \oplus \underbrace{\{0\} \oplus \cdots \oplus \{0\}}_{n-r}$$

ուղիղ գումարին: Դյուրին է տեսնել, որ

$$\mathbb{Z}^n / n_1\mathbb{Z} \oplus n_2\mathbb{Z} \oplus \cdots \oplus n_r\mathbb{Z} \oplus \underbrace{\{0\} \oplus \cdots \oplus \{0\}}_{n-r} =$$

$$\mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z} \oplus \underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n-r}$$

Իսկապես՝ $(\lambda_1,\ldots,\lambda_n)$ և $(\mu_1,\ldots,\mu_n)$ տարրերը $\mathbb{Z}^n$-ից կպատկանեն միևնույն հարակից դասին ըստ

$$n_1\mathbb{Z} \oplus n_2\mathbb{Z} \oplus \cdots \oplus n_r\mathbb{Z} \oplus \underbrace{\{0\} \oplus \cdots \oplus \{0\}}_{n-r}$$

խմբի, միայն և միայն, եթե դրանց տարբերությունը պատկանի

$$n_1\mathbb{Z} \oplus n_2\mathbb{Z} \oplus \cdots \oplus n_r\mathbb{Z} \oplus \underbrace{\{0\} \oplus \cdots \oplus \{0\}}_{n-r}$$

խմբին, իսկ դա համարժեք է հետևյալին՝

1. $\lambda_i - \mu_i \equiv mod\, n_i,\ i = 1,2,\ldots,r$
2. $\lambda_i = \mu_i,\ i = r+1,\ldots,n$

Թեորեմն ապացուցված է:

Նկատենք, որ վերջավոր ծնված աբելյան խումբը կլինի վերջավոր, միայն երբ $r = n$:

Այժմ ստանանք վերջավոր աբելյան խմբերի ուղիղ գումարի ավելի

"Նուրբ" վերլուծությունը:

Դիցուք G-ն վերջավոր աբելյան խումբ է և իզոմորֆ է $\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ ուղիղ գումարին: **Վերցնենք** n_r-ի վերլուծությունը պարզ արտադրիչների՝ $n_r = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$: **Քանի** որ n_{i+1}-ը բաժանվում է առանց մնացորդի n_i-ի վրա, $i = 1, 2, \dots, r-1$, ապա կարող ենք գրել՝

$$\begin{aligned} n_r &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \\ n_{r-1} &= p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} \\ &\vdots \\ n_1 &= p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_k^{\varepsilon_k} \end{aligned}$$

որտեղ $\alpha_i \geq \beta_i \geq \dots \geq \varepsilon_i \geq 0,\ i = 1, 2, \dots, k$: **Ինչպես** գիտենք՝ (տեսեք ուղիղ արտադրյալներին վերաբերվող մասի օրինակները)

$$\begin{aligned} \mathbb{Z}_{n_r} &= \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}} \\ \mathbb{Z}_{n_{r-1}} &= \mathbb{Z}_{p_1^{\beta_1}} \oplus \mathbb{Z}_{p_2^{\beta_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\beta_k}} \\ &\vdots \\ \mathbb{Z}_{n_1} &= \mathbb{Z}_{p_1^{\varepsilon_1}} \oplus \mathbb{Z}_{p_2^{\varepsilon_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\varepsilon_k}} \end{aligned}$$

և G-ն իզոմորֆ է

$$\mathbb{Z}_{p_1^{\alpha_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}} \oplus \mathbb{Z}_{p_1^{\beta_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\beta_k}} \oplus \dots \oplus \mathbb{Z}_{p_1^{\varepsilon_1}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\varepsilon_k}}$$

ուղիղ գումարին: **Նկատենք**, որ ավելի "նուրբ" վերլուծություն ցիկլիկ խմբերի ուղիղ գումար ստանալու համար հնարավոր չէ, քանի որ, ինչպես գիտենք (տեսեք ուղիղ արտադրյալներին վերաբերվող մասի օրինակները), ցիկլիկ խումբը, որի կարգը պարզ թվի աստիճան է, հնարավոր չէ ոչ տրիվիալ ձևով ներկայացնել ուղիղ գումարի տեսքով:

Թեորեմ 10.

Վերջավոր աբելյան խումբն իզոմորֆ է ցիկլիկ խմբերի ուղիղ գումարին, ընդ որում ցիկլիկ խմբերի կարգերը պարզ թվերի աստիճաններ են: Ուղիղ գումարը որոշված է միարժեքորեն գումարելիների տեղափոխության ճշտությամբ:

Ապացույց. Մնում է ապացուցել միակությունը: Բայց դա դառնում է ակնհայտ, եթե նկատենք, որ

$$\mathbb{Z}_{p_1^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\alpha_k}} \oplus \mathbb{Z}_{p_1^{\beta_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\beta_k}} \oplus \ldots \oplus \mathbb{Z}_{p_1^{\varepsilon_1}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{\varepsilon_k}}$$

ուղիղ գումարով $n_1, \ldots, n_r$ թվերն որոշվում են միարժեքորեն: Թեորեմն ապացուցված է:

Նպատակահար է բերել Թեորեմ 10-ի միակության վերաբերյալ պնդման մեկ այլ ապացույց, որը հիմնված չէ ծնիչների մատրիցի մինորների ամենամեծ ընդհանուր բաժանարարների ինվարիանտության վրա:

Դիցուք G-ն աբելյան խումբ է և $n \in \mathbb{Z}$: Նշանակենք՝ $nG = \{ng \mid g \in G\}$: Ակնհայտ է, որ $nG \leq G$ և, եթե n-ը բաժանվում է m-ի վրա, ապա $nG \leq mG$:

Ապացուցենք այժմ, որ $n\mathbb{Z}_m$-ն իզոմորֆ է $\mathbb{Z}_{\frac{m}{(m,n)}}$-ին: Իսկապես, ունենք, որ $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, ուստի $n\mathbb{Z}_m = \{0, n \bmod m, 2n \bmod m, \ldots, (m-1)n \bmod m\}$: Դյուրին է տեսնել, որ նվազագույն դրական x-ը, որի համար $nx \equiv 0 \bmod m$ դա $\frac{m}{(m,n)}$ թիվն է: Ուստի $n\mathbb{Z}_m$-ն իզոմորֆ է $\mathbb{Z}_{\frac{m}{(m,n)}}$-ին:

Մասնավորապես, եթե n-ը բաժանվում է m-ի վրա, ապա

$n\mathbb{Z}_m = \{0\}$, *խսկ եթե* m*-ը և* n*-ը փոխադարձաբար պարզ են, ապա* $n\mathbb{Z}_m$*-ն իզոմորֆ է* $\mathbb{Z}_m$*-ին:*

Դյուրին է համոզվել, որ

$$n(G_1 \oplus G_2 \oplus \ldots \oplus G_k) = nG_1 \oplus nG_2 \oplus \ldots \oplus nG_k:$$

Այժմ, դիցուք, G*-ն վերջավոր աբելյան խումբ է և ունի ցիկլիկ խմբերի գումարների երկու տարբեր վերլուծություն: Առանձնացնենք* p *պարզ թվի աստիճաններին համապատասխան գումարելիները՝*

$$G = \mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k}} \oplus \ldots = \mathbb{Z}_{p^{\beta_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\beta_s}} \oplus \ldots$$

որտեղ $\alpha_1 \leq \ldots \leq \alpha_k$ *և* $\beta_1 \leq \ldots \leq \beta_s$*: Նշանակենք* t*-ով* G*-ի այս երկու ներկայացումների մեջ մասնակցող մնացած պարզ թվերի աստիճանների ամենափոքր ընդհանուր բազմապատիկը: Համաձայն վերն ապացուցվածի՝*

$$tG = t\mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus t\mathbb{Z}_{p^{\alpha_k}} \oplus \{0\} \oplus \ldots = t\mathbb{Z}_{p^{\beta_1}} \oplus \ldots \oplus t\mathbb{Z}_{p^{\beta_s}} \oplus \{0\} \ldots$$

և

$$tG = \mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k}} \oplus \{0\} \oplus \ldots = \mathbb{Z}_{p^{\beta_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\beta_s}} \oplus \{0\} \ldots$$

Ուստի

$$tG = \mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k}} = \mathbb{Z}_{p^{\beta_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\beta_s}}$$

Դիցուք $\alpha_1 \leq \ldots \leq \alpha_k$ *և* $\beta_1 \leq \ldots \leq \beta_s$ *հաջորդականությունները տարբեր են: Ուրեմն կգտնվի* i *այնպիսին, որ* $\alpha_{k-j} = \beta_{s-j}$ *բոլոր* $j = 0, 1, \ldots, i-1$ *համար և* $\alpha_{k-i} \neq \beta_{s-i}$*: Որոշակիության համար ենթադրենք, որ* $\alpha_{k-i} > \beta_{s-i}$ *և, ուրեմն,* $\alpha_{k-i} - 1 \geq \beta_{s-i}$*: Կստանանք՝*

$$p^{\alpha_{k-i}-1}tG = \ldots \oplus \mathbb{Z}_p \oplus \mathbb{Z}_{p^{\alpha_{k-i+1}-\alpha_{k-i}+1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\alpha_k-\alpha_{k-i}+1}} =$$
$$\{0\} \oplus \ldots \oplus \{0\} \oplus \mathbb{Z}_{p^{\beta_{s-i+1}-\alpha_{k-i}+1}} \oplus \ldots \oplus \mathbb{Z}_{p^{\beta_s-\alpha_{k-i}+1}}$$

Ուրեմն $p^{\alpha_{k-i}-1}tG$ *խմբի կարգը մի կողմից*

$p^{1+(\alpha_{k-i+1}-\alpha_{k-i}+1)+\ldots+(\alpha_k-\alpha_{k-i}+1)}$-*ից փոքր չէ, մյուս կողմից էլ հավասար է* $p^{(\beta_{s-i+1}-\alpha_{k-i}+1)+\ldots+(\beta_s-\alpha_{k-i}+1)}$-*ի:*

Ո*ւստի* $p^{1+(\alpha_{k-i+1}-\alpha_{k-i}+1)+\ldots+(\alpha_k-\alpha_{k-i}+1)} \leq p^{(\beta_{s-i+1}-\alpha_{k-i}+1)+\ldots+(\beta_s-\alpha_{k-i}+1)}$*:*

Ս*ակայն*

$$(\alpha_{k-i+1}-\alpha_{k-i}+1)+\ldots+(\alpha_k-\alpha_{k-i}+1) =$$

$$(\beta_{s-i+1}-\alpha_{k-i}+1)+\ldots+(\beta_s-\alpha_{k-i}+1)$$

և հանգում ենք հակասության:

Օրինակ

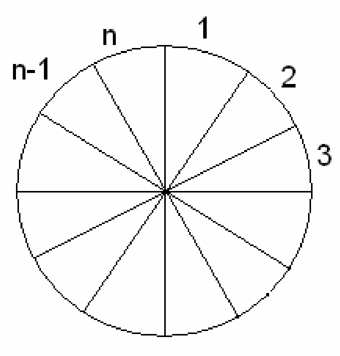
Համաձայն Թեորեմ 10*-ի ստորև բերված են բոլոր իրար ոչ իզոմորֆ* $1800 = 2^3 3^2 5^2$ *կարգի աբելյան խմբերը.*

$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$$
$$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}$$

Խմբի գործողությունը բազմության վրա

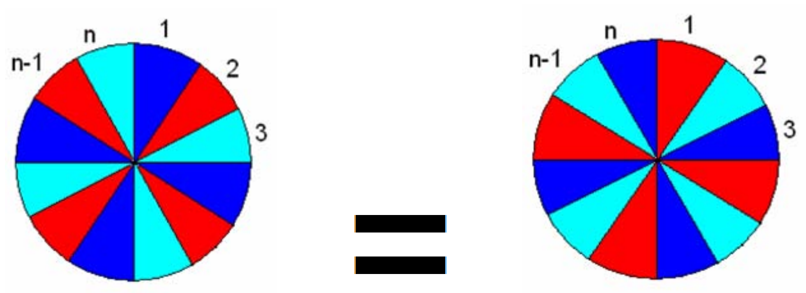
Դիտարկենք հետևյալ խնդիրը:

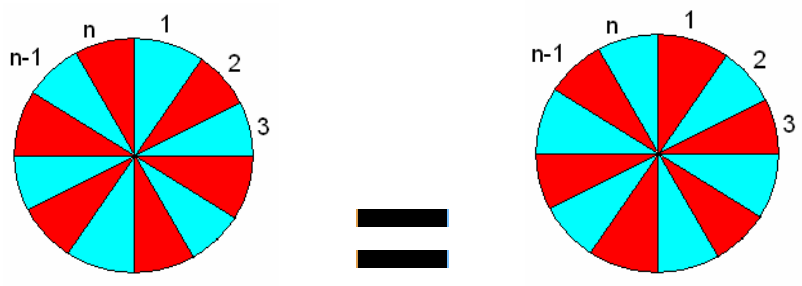
Դիցուք տրված է մի անիվ, որը բաժանված է n հատ հավասար սեկտորների, որոնք պայմանականորեն համարակալված են $1, 2, \ldots, n$ թվերով, ինչպես ցույց է տրված ստորև բերված նկարում:



Անիվը կարելի է պտտել կենտրոնի նկատմամբ: Պտույտի միավոր քայլը մեկ սեկտորի չափով է: Այսինքն մեկ քայլով առաջին սեկտորը գրավում է երկրորդի տեղը, երկրորդը՝ երրորդի և այլն, $n-1$-ը՝ n-ի տեղը, իսկ n-ը՝ առաջինի:

Տրված են նաև r տարբեր գույնի ներկեր: Յուրաքանչյուր սեկտոր ներկելով որևէ գույնով ստանում ենք անիվի ներկում: Երկու ներկում համարում ենք նույնը, եթե մեկը մյուսից ստացվում է անիվի պտույտով: Օրինակ, ստորև բերված ներկումները նույնն են





Պահանջվում է հաշվել տարբեր (իրարից պտույտով չստացվող) ներկումների քանակը:

Փորձենք խնդրին տալ մաթեմատիկական ձևակերպում: Նշանակենք՝ $N = \{1, 2, \ldots, n\}$ և $R = \{1, 2, \ldots, r\}$:

Ամեն մի ներկման եղանակ տրվում է $f : N \to R$ ֆունկցիայի միջոցով: Այսպիսի ֆունկցիայով որոշված ներկման եղանակով i-րդ սեկտորը ներկվում է $f(i)$ գույնով: Բոլոր $f : N \to R$ ֆունկցիաների բազմությունն ընդունված է նշանակել R^N-ով:

Անիվի պտույտները կարելի է նկարագրել

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}$$

տեղադրության աստիճաններով: Դյուրին է տեսնել, որ π-ն նկարագրում է անիվի միավոր պտույտը, քանի որ i-րդ սեկտորը գրավում է $i+1$-ի տեղը $i \in \{1, 2, \ldots, n-1\}$ համար, իսկ n-րդ սեկտորը գրավում է առաջինի տեղը: Պարզ է, որ π^k տեղադրությունը (π-ի k անգամ հաջորդաբար կիրառումը) համարժեք է k հատ միավոր պտույտներին: Այսինքն անիվի բոլոր պտույտները նկարագրվում են π-ով ծնված ցիկլիկ խմբով $\langle \pi \rangle = \{e, \pi, \pi^2, \pi^3, \ldots, \pi^{n-1}\}$ և $(\langle \pi \rangle : 1) = n$: Նաև π տեղադրության կարգը հավասար է n-ի, այսինքն π-ի ամենափոքր դրական աստիճանը, որ հավասար է միավորի դա n-ն է (որովհետև n միավոր պտույտից հետո ամեն մի սեկտոր վերադառնում է իր սկզբնական տեղին):

Դիցուք ունենք երկու ներկման եղանակ $f, g \in R^N$ և դրանք ստացվում են իրարից պտույտով, որը տրվում է π^k-ով: Այդ փաստը համարժեք է $f(i) = g(\pi^k(i)),\ i \in N$: Եթե օգտագործենք $g\pi^k$ նշանը π^k տեղադրության և g ֆունկցիայի հաջորդաբար կիրառման արդյունքում ստացվող ֆունկցիայի նշանակման համար, ապա f և g ներկումների իրարից պտույտով ստացվելու փաստը կարող ենք գրել նաև հետևյալ կերպ՝ $f = g\pi^k$: Վերջին պայմանը համարժեք է $f\pi^{n-k} = g$ պայմանին: Իսկապես, եթե $f(i) = g(\pi^k(i))$ բոլոր i-րի համար N-ից, ապա $\pi^k(i) = j$ ընդունում է մեկական անգամ բոլոր արժեքները N-ից և $\pi^{n-k}(j) = i$, ուստի $f(\pi^{n-k}(j)) = g(j)$ բոլոր $j \in N$: Այն փաստը, որ $f, g \in R^N$ ներկման եղանակներն իրարից պտույտով են ստացվում կնշանակենք $f \sim g$ նշանով: Այսինքն՝

$$f \sim g \Leftrightarrow (\exists k)\, f = g\pi^k \tag{24}$$

Տեղի ունեն հետևյալ հատկությունները.

1. $f \sim f$
2. $f \sim g \Leftrightarrow g \sim f$
3. $f \sim g$ և $g \sim h \Rightarrow f \sim h$

Իսկապես, (24)-ի աջ մասը կարելի է գրել նաև որպես $(\exists k)$ $f\pi^{n-k} = g$, ուստի $g \sim f$ և 2. հատկությունը ստույգ է:

Եթե $f \sim g$ և $g \sim h$, ապա գոյություն ունեն k և m որ $f = g\pi^k$ և $g = h\pi^m$, որտեղից ստանում ենք $f = h\pi^m\pi^k = h\pi^{m+k} \Rightarrow f \sim h$ և 3. հատկությունը ստույգ է:

Այս երեք հատկություններից հետևում է, որ R^N-ը տրոհված է համարժեքության դասերի՝ $f, g \in R^N$ միևնույն դասից են $\Leftrightarrow f \sim g$: Պարզ է, որ յուրաքանչյուր $f \in R^N$ պատկանում է ինչ-որ դասի:

Երկու դասեր կամ չեն հատվում կամ էլ համընկնում են: Իրոք, եթե f-ը պատկանում է A և B դասերին, ապա $g \in A \Rightarrow f \sim g$ և $h \in B \Rightarrow f \sim h$: Համաձայն 2. և 3. հատկությունների $g \sim f$ և $f \sim h \Rightarrow g \sim h$, այսինքն A դասի ֆունկցիաները պատկանում են B դասին և հակառակը՝ B դասի ֆունկցիաները պատկանում են A դասին: Ուստի $A = B$:

Քանի որ միևնույն դասին պատկանող ֆունկցիաներով տրվող ներկումները համընկնում են, իսկ տարբեր դասերի ֆունկցիաներով տրվող ներկումները չեն համընկնում, ապա տարբեր ներկումների քանակը հավասար է տարբեր դասերի քանակին: Այսպիսով տարբեր ներկումների քանակի հաշվման խնդիրը հանգեցվեց ֆունկցիաների համարժեքության դասերի քանակի հաշվման խնդրին:

Այս և այլ նման խնդիրների լուծման համար հարմար է օգտագործել հետևյալ գաղափարը:

Սահմանում: Դիցուք տրված են G խումբը և S բազմությունը: Ասում են, որ G խումբը **գործում է S բազմության վրա**, եթե սահմանված է մի $G \times S \to S$ արտապատկերում (ամեն (g, s) զույգին համապատասխանող տարրը S-ից նշանակվում է gs-ով), որ բավարարում է հետևյալ պայմաններին.

1. $es = s$
2. $g_1(g_2 s) = (g_1 g_2)s$

Այս սահմանման բովանդակալից իմաստը հետևյալն է: Խմբի տարրերը մեկնաբանվում են որպես S բազմության տարրերի "ձևափոխությունների" խումբ: Այսինքն խմբի g տարրը ազդելով S բազմության s տարրի վրա "ձևափոխում" է այն $gs \in S$ տարրի: Սահմանման առաջին պայմանը նշանակում է, որ միավոր կամ նույնաբար "ձևափոխությունը" ազդելով տարրի վրա այն չի փոխում: Երկու "ձևափոխությունների" հաջորդաբար կիրառումը համարժեք է նրանց արտադրյալով ստացվող մեկ "ձևափոխության" ազդեցությանը:

Օրինակներ

1. Դիցուք $G = S_n$ և $S = N = \{1, 2, \ldots, n\}$: Ամեն մի α տեղադրությունը $i \in N$ թիվը տանում է $\alpha(i)$ թվի մեջ, այսինքն $\alpha i = \alpha(i)$: Ակնհայտ է, որ S_n-ը գործում է N բազմության վրա:

2. Դիցուք $G = S_n$, $N = \{1, 2, \ldots, n\}$, $R = \{1, 2, \ldots, r\}$ և $S = R^N$: S_n-ի գործողությունը R^N-ի վրա սահմանում ենք հետևյալ կերպ ՝ $\alpha \in S_n$, $f \in R^N$ համար $\alpha f = f \bullet \alpha$, այսինքն $(\alpha f)(x) = f(\alpha(x))$:

3. Խորանարդի գագաթների (կողերի, նիստերի) տեղադրությունների բազմությունը, որ ստացվում են խորանարդի պտույտներով խումբ են կազմում: Այդ խումբը գործում է խորանարդի գագաթների բազմության վրա: Այդպիսի պտույտները 24-ն են.

a. միավոր պտույտ (փաստացի պտույտ չի կատարվում) - 1 հատ

b. 90^o պտույտ խորանարդի երկու հանդիպակաց նիստերի կենտրոններով անցնող առանցքի շուրջ - 3 հատ

c. 180^o պտույտ խորանարդի երկու հանդիպակաց նիստերի կենտրոններով անցնող առանցքի շուրջ - 3 հատ

d. 270^o պտույտ խորանարդի երկու հանդիպակաց նիստերի կենտրոններով անցնող առանցքի շուրջ - 3 հատ

ե. 120^o պտույտ խորանարդի անկյունագծի շուրջ - 4 հատ

զ. 240^o պտույտ խորանարդի անկյունագծի շուրջ - 4 հատ

գ. 180^o պտույտ խորանարդի երկու հանդիպակաց կողերի կենտրոններով անցնող առանցքի շուրջ - 6 հատ

4. G խումբը գործում է ինքն իր վրա $(S = G)$ հետևյալ կերպ. $g \in G$, $s \in G$ զույգին համապատասխանում է $gs \in S$

5. G խումբը գործում է ինքն իր վրա $(S = G)$ հետևյալ կերպ. $g \in G$, $s \in G$ համար $gs = g^{-1}sg$: Իրոք, $e^{-1}se = s$ և $g_1^{-1}(g_2^{-1}sg_2)g_1 = (g_2g_1)^{-1}s(g_2g_1)$:

Դիցուք G խումբը գործում է S բազմության վրա: Ֆիքսենք որևէ $g \in G$: Այդ g-ով որոշվում է S բազմության փոխմիարժեք արտապատկերում S-ի վրա՝ $T_g : S \to S$, $T_g(s) = gs$: Եթե $T_g(s_1) = T_g(s_2)$, ապա $gs_1 = gs_2$ և $s_1 = s_2$: Եթե $s \in S$, ապա $T_g(g^{-1}s) = s$, ուստի T_g արտապատկերումը S բազմության $g^{-1}s$ տարրը տանում է s-ի մեջ:

T_g արտապատկերումների բազմությունը փակ է հաջորդաբար կիրառման գործողության նկատմամբ: Իսկապես, $T_{g_2}(T_{g_1}(s)) = T_{g_2}(g_1s) = g_2(g_1s) = (g_2g_1)s = T_{g_2g_1}(s)$: Ուստի

$$T_{g_2} \cdot T_{g_1} = T_{g_2g_1}$$
$$T_gT_{g^{-1}} = T_e$$

Վերջին երկու հատկությունները նշանակում են, որ T_g արտապատկերումների բազմությունը խումբ է *արտապատկերումների Համընդգրկող կիրառման գործողության նկատմամբ:*

Եթե S *բազմությունը վերջավոր է, ապա* T_g *արտապատկերումները տեղափոխություններ են* S_n *սիմետրիկ խմբից, որտեղ* $n = |S|$*: Պարզ է, որ* $g \mapsto T_g$ *արտապատկերումը* G*-ից* S_n *հոմոմորֆիզմ է և* G*-ի գործողության փոխարեն կարելի է սահմանափակվել* T_g *տեղափոխությունների* S*-ի վրա գործողության հետազոտմամբ: Այսուհետև վերջավոր* S*-ի դեպքում միշտ կհամարենք, որ* G*-ն տեղափոխությունների խումբ է:*

Սահմանում. *Դիցուք* G *խումբը գործում է* S *բազմության վրա:* $s \in S$ *տարրի* ***ստաբիլ խումբ*** *(կամ պարզապես* ***ստաբիլիզատոր****) է կոչվում հետևյալ բազմությունը.*

$$G_s = \{g \in G \mid gs = s\},$$

$s \in S$ *տարրի* ***ուղեծիր*** *է կոչվում* $Gs = \{s' \mid \exists g \in G, gs = s'\} = \{gs \mid g \in G\}$ *բազմությունը: Ուղեծրի* ***երկարությունը*** *ուղեծրի տարրերի քանակն է:*

Համոզվենք, որ $G_s \leq G$*: Եթե* $g_1, g_2 \in G_s$*, ապա* $g_1 s = s$*,* $g_2 s = s$ *և* $g_2^{-1} s = s$*: Որտեղ* $(g_2^{-1} g_1)s = g_2^{-1}(g_1 s) = g_2^{-1} s = s$ *և* $g_2^{-1} g_1 \in G_s$*, ուստի`* $G_s \leq G$*: Նկատենք, որ* $e \in G_s$ *և* $G_s \neq \varnothing$*:*

Դիցուք $g \in G$*,* $s, t \in S$ *և* $gs = t$*: Այս դեպքում* $G_s = g^{-1} G_t g$*: Ապացուցենք դա: Եթե* $g_1 \in g^{-1} G_t g$*, ապա* $\exists h \in G_t$ $g_1 = g^{-1} h g$ *և*

$$g_1 s = (g^{-1} h g)s = (g^{-1} h) gs = (g^{-1} h)t = g^{-1}(ht) = g^{-1} t = s:$$

Այսինքն $g_1 \in G_s$ *և* $G_s \supseteq g^{-1} G_t g$*: Քանի որ* $g^{-1} t = s$*, ապա, ըստ ապացուցածի,* $G_t \supseteq (g^{-1})^{-1} G_s g^{-1} = g G_s g^{-1}$ *և* $g^{-1} G_t g \supseteq G_s$*:*

Ուսումնասիրենք այժմ ուղեծրերը: Դիցուք $s_1 \in Gs$ և $gs = s_1$: Պարզ է, որ $g^{-1}s_1 = s$ և ուրեմն $s \in Gs_1$: Հետևաբար՝ $Gs = Gs_1$: Այսինքն իրար մեջ որևէ "ձևափոխությամբ" անցնող բոլոր s-րի ուղեծրերը նույնն են:

Դիցուք $s \in Gs_1 \cap Gs_1$: Ուրեմն $Gs = Gs_1$ և $Gs = Gs_2$, այսինքն՝ $Gs_1 = Gs_2$:

Այսպիսով S բազմությունը տրոհվում է չհատվող ուղեծրերի: Փորձենք հաշվել այդ տարբեր ուղեծրերի քանակը վերջավոր S բազմության դեպքում: Եթե բոլոր ուղեծրերի երկարությունները համընկնեին, ապա ուղեծրերի քանակը պարզապես հավասար կլիներ S-ի հզորության և ուղեծրի երկարության քանորդին (հարակից դասերի դեպքի նման): Սակայն տարբեր ուղեծրեր կարող են ունենալ տարբեր երկարություններ և ուղեծրերի քանակի հաշվարկն ավելի նուրբ մեթոդների կրառում է պահանջում:

Նախ պարզենք, թե որ դեպքում խմբի տարբեր "ձևափոխությունները" կիրառած s-ին տալիս են միևնույն տարրը: Ստույգ է համարժեքությունների հետևյալ շղթան.

$$g_1 s = g_2 s \Leftrightarrow (g_2^{-1} g_1)s = s \Leftrightarrow g_2^{-1} g_1 \in G_s \Leftrightarrow g_1 G_s = g_2 G_s$$

Սա նշանակում է, որ $g_1 s = g_2 s$ միայն և միայն այն դեպքում, երբ համընկնում են g_1-ի և g_2-ի ըստ G_s-ի կառուցված հարակից դասերը: Ուրեմն տարբեր gs-րի քանակը տրված s-ի համար հավասար է հարակից դասերի քանակին ըստ G_s ենթախմբի՝ G_s-ի ինդեքսին: Այսինքն՝

$$|Gs| = (G : G_s) \tag{25}$$

Սորև կօգտագործենք հետևյալ նշանակումը՝ $\psi(g) = |\{s \in S \mid gs = s\}|$, այսինքն կամայական $g \in G$ համար

$\psi(g)$-ն դա այն s-րի քանակն է S-ից, որ $gs = s$: Նշանակենք նաև $\mathfrak{M}(G,S)$-ով բոլոր ուղեծրերի քանակը:

Թեորեմ 11. (Բեռնսայդի լեմմ)

Դիցուք G խումբը գործում է S վերջավոր բազմության վրա: Ստույգ է հետևյալ բանաձևը

$$\mathfrak{M}(G,S) = \frac{1}{(G:1)} \sum_{g \in G} \psi(g)$$

Ապացույց. Հաշվենք բոլոր (g,s) զույգերի քանակը, որոնց համար $gs = s$: Ֆիքսած $g \in G$ համար բոլոր s-րի քանակը, որ $gs = s$ հավասար է $\psi(g)$-ի, ուստի գումարելով ըստ բոլոր g-րի կստանանք՝ $\sum_{g \in G} \psi(g) = |\{(g,s) \mid gs = s\}|$: Մյուս կողմից, եթե ֆիքսենք $s \in S$, ապա բոլոր g-րի քանակը, որ $gs = s$ հավասար է $(G_s : 1)$-ին: Գումարելով ըստ բոլոր s-րի ստանում ենք՝ $\sum_{s \in S}(G_s : 1) = |\{(g,s) \mid gs = s\}|$: Հետևաբար ստույգ է $\sum_{g \in G} \psi(g) = \sum_{s \in S}(G_s : 1)$: Օգտվելով Լագրանժի թեորեմից և (25) բանաձևից կստանանք

$$\sum_{g \in G} \psi(g) = \sum_{s \in S} \frac{(G:1)}{(G:G_s)} = (G:1) \sum_{s \in S} \frac{1}{(G:G_s)} = (G:1) \sum_{s \in S} \frac{1}{|Gs|}: \qquad (26)$$

Ավելի ուշադիր դիտարկենք $\sum_{s \in S} \frac{1}{|Gs|}$ գումարը: Դիցուք բոլոր տարբեր ուղեծրերը հետևյալն են՝ $Gs_1, \ldots, Gs_k$ (այսինքն՝ $\mathfrak{M}(G,S) = k$): Ուրեմն, $\sum_{s \in S} \frac{1}{|Gs|} = \sum_{i=1}^{k} \sum_{s \in Gs_i} \frac{1}{|Gs|}$: Բոլոր $s \in Gs_i$

Համար $Gs = Gs_i$ և բնականաբար $\frac{1}{|Gs|} = \frac{1}{|Gs_i|}$: Այսպիսով,

$$\sum_{s\in S}\frac{1}{|Gs|} = \sum_{i=1}^{k}\sum_{s\in Gs_i}\frac{1}{|Gs|} = \sum_{i=1}^{k}|Gs_i|\frac{1}{|Gs_i|} = \sum_{i=1}^{k}1 = k:$$

Այժմ (26)-ից հետևում է, որ

$$\frac{1}{(G:1)}\sum_{g\in G}\psi(g) = \sum_{s\in S}\frac{1}{|Gs|} = k = \mathfrak{M}(G,S)$$

և թեորեմն ապացուցված է:

Անիվի խնդրի լուծումը

Կիրառենք Թեորեմ 11-ի բանաձևը վերը դիտարկված "անիվի" խնդրին: Պարզ է, որ $\langle \pi \rangle = \{e, \pi, \pi^2, \pi^3, \ldots, \pi^{n-1}\}$ խումբը գործում է R^N-ի վրա (տես օրինակ 2.-ը): Նաև դյուրին է տեսնել, որ ներկման ֆունկցիաների համարժեքության դասերը համընկնում են այդ ֆունկցիաների ուղեծրերի հետ: Հետևաբար իրարից պտույտով չստացվող ներկումների քանակը հավասար է ֆունկցիաների ուցեծրերի քանակին, որն ըստ Բեռնսայդի լեմի տրվում է հետևյալ բանաձևով

$$\mathfrak{M}(\langle \pi \rangle, R^N) = \frac{1}{n} \sum_{k=0}^{n-1} \psi(\pi^k)$$

Այսպիսով խնդիրը հանգեցվեց $\psi(\pi^k)$-ի հաշվմանը: Ըստ սահմանման $\psi(\pi^k) = |\{f \in R^N \mid f\pi^k = f\}|$:

Դիցուք α-ն որևէ տեղադրություն է S_n-ից: Նկարագրենք բոլոր $f \in R^N$, որ $f\alpha = f$: Տրոհենք α-ն ցիկլերի: Հիշեցնենք որ յուրաքանչյուր ցիկլ ունի հետևյալ տեսքը՝

$$\{i, \alpha(i), \alpha^2(i), \ldots, \alpha^m(i)\},$$

որտեղ բոլոր $i, \alpha(i), \alpha^2(i), \ldots, \alpha^m(i)$ տարրերը տարբեր են և $\alpha^{m+1}(i) = i$: $f\alpha = f$ պայմանը նշանակում է, որ

$$f(i) = f(\alpha(i)) = f(\alpha^2(i)) = \ldots = f(\alpha^m(i))$$

բոլոր $i \in N$ համար, այսինքն f ֆունկցիան հաստատուն է α տեղադրության ցիկլերի վրա: Ուստի, եթե α-ի ցիկլերի քանակը հավասար է q-ի, ապա $f\alpha = f$ պայմանին բավարարող ֆունկցիաները թվարկելու համար պետք է ընտրել ֆունկցիայի արժեքը յուրաքանչյուր ցիկլի համար: Քանի որ ֆունկցիաների արժեքների տիրույթը $R = \{1, 2, \ldots, r\}$-ն է և ցիկլերի վրա արժեքներն ընտրվում են իրարից անկախ, ապա $f\alpha = f$ պայմանին բավարարող ֆունկցիաների քանակը կլինի հավասար r^q։

Այժմ պարզ է դառնում, որ $\psi(\pi^k)$-ն հաշվելու համար անհրաժեշտ է հաշվել π^k-ի ցիկլերի քանակը։ Հիշենք, որ π^k-ով նկարագրվում է անիվի պտույտը k սեկտորների չափով։ Դիտարկենք 1 համարի սեկտորի ցիկլը։ π^k-ին համապատասխանող պտույտով 1 համարի սեկտորը անցնում է $k+1$ համարի սեկտորի մեջ, վերջինս՝ $2k+1$ համարի սեկտորի մեջ և այլն մինչև որ վերադառնանք համար 1 սեկտորին։ Բայց, եթե վերադարձել ենք համար 1 սեկտորին, ապա նույն պտույտներով 2 համարի սեկտորը կվերադառնա իր տեղը և մյուս բոլոր սեկտորները նույնպես կվերադառնան իրենց տեղերը։ Ուստի π^k-ի բոլոր ցիկլերն ունեն միևնույն երկարությունը։ Ակնհայտ է, որ այդ երկարությունը ամենափոքր դրական l թիվն է, որ $(\pi^k)^l = e$։ Այսինքն, ցիկլի երկարությունը համընկնում է π^k-ի կարգի հետ, որն ինչպես գիտենք հավասար է $\dfrac{n}{(n,k)}$։ Քանի որ ցիկլերի միավորումը համընկնում է $N = \{1, 2, \ldots, n\}$ բազմության հետ, ապա ցիկլերի քանակը հավասար է (n,k)-ին։ Հետևաբար $\psi(\pi^k) = r^{(n,k)}$ և

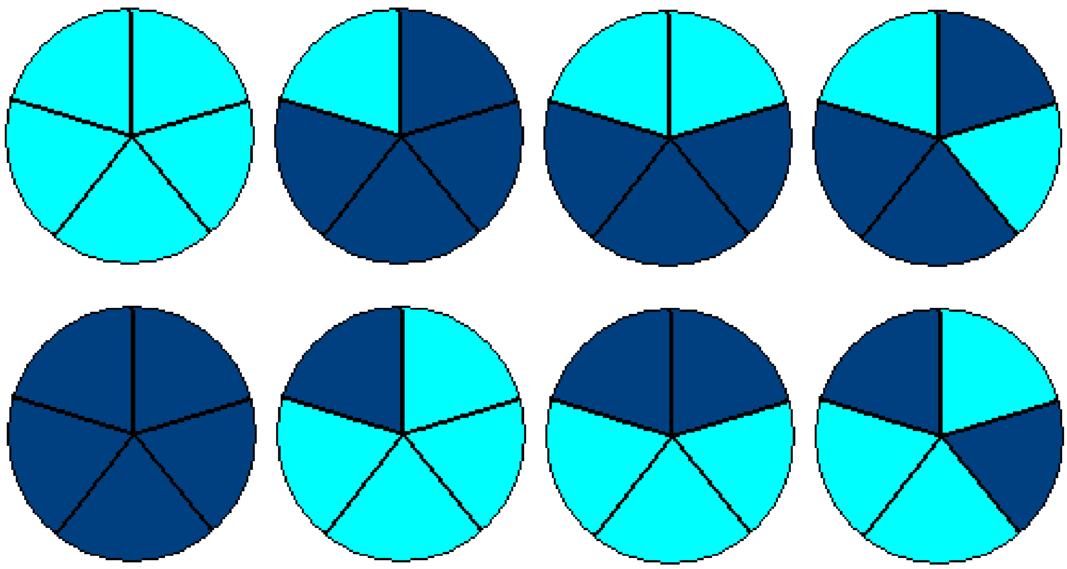
$$\mathfrak{M}(\langle\pi\rangle, R^N) = \frac{1}{n}\sum_{k=0}^{n-1} r^{(n,k)}$$

Վերջին բանաձևը կարելի է ավելի պարզեցնել։ Ակնհայտ է, որ (n,k)-ն n-ի բաժանարարն է և n-ի կամայական m բաժանարարի համար կարելի է ընտրել $k \in \{0, 1, \ldots, n-1\}$, որի համար $(n,k) = m$ (օրինակ $k = m$)։ Հաշվենք թե քանի անգամ է կրկնվում r^m-ը $\sum_{k=0}^{n-1} r^{(n,k)}$ գումարում։ Եթե $(n,k) = m$, ապա m-ը և n-ի և k-ի բաժանարարն է, ուստի $\left(\frac{n}{m}, \frac{k}{m}\right) = 1$։ Ուրեմն k-երի քանակը, որոնց համար $(n,k) = m$ հավասար է $\frac{n}{m}$-ից փոքր $\frac{n}{m}$-ի հետ փոխադարձաբար *պարզ թվերի քանակին: Այդ թիվը տրվում է հայտնի $\varphi(\frac{n}{m})$ Էյլերի ֆունկցիայի միջոցով: (Էյլերի ֆունկցիան $\varphi(n)$-ը հավասար է n-ից փոքր և n-ի հետ փոխադարձաբար պարզ թվերի քանակին: Եթե $n = p_1^{\alpha_1}\ldots p_s^{\alpha_s}$-ը n-ի վերլուծությունն է պարզ թվերի արտադրյալի միջոցով, ապա $\varphi(n) = n(1-\frac{1}{p_1})\ldots(1-\frac{1}{p_s})$:*

Այսպիսով "անիվի" խնդրի վերջնական լուծումը տրվում է հետևյալ բանաձևով

$$\mathfrak{M}(\langle\pi\rangle, R^N) = \frac{1}{n}\sum_{m|n}\varphi(\frac{n}{m})r^m$$

Դիտարկենք "անիվի" խնդիրը $n = 5$ և $k = 2$ դեպքում: Դյուրին է թվարկել բոլոր ներկումները, որ պտույտներով իրարից չեն ստացվում: Դրանք ութն են՝



Համաձայն ստացված բանաձևի՝

$$\frac{1}{5}(\varphi(1)2^5 + \varphi(5)2^1) = \frac{1}{5}(1\cdot 2^5 + 4\cdot 2^1) = \frac{40}{5} = 8:$$

Խմբի գործողության մեկ այլ կիրառության օրինակ

Օգտվելով խմբի գործողության գաղափարից և վերը ստացված արդյունքներից, ապացուցենք, որ եթե վերջավոր խմբի ենթախմբի դասիչը (ինդեքսը) խմբի կարգի ամենափոքր պարզ բաժանարարն է, ապա այդ ենթախումբը նորմալ է։ Այս պնդումը մենք արդեն ապացուցել ենք, երբ դասիչը հավասար է 2-ի։

Սահմանում։ Դիցուք $H \leq G$։ H ենթախմբի **նորմալիզատոր** է կոչվում

$$N_H = \{g \in G \mid g^{-1}Hg = H\}$$

բազմությունը։

Դյուրին է տեսնել, որ նորմալիզատորը ենթախումբ է G-ում։ Իսկապես, դիցուք $g_1, g_2 \in N_H$ և $g_1^{-1}Hg_1 = H, g_2Hg_2^{-1} = H$։ Ուստի,

$$(g_2^{-1}g_1)^{-1}H(g_2^{-1}g_1) = g_1^{-1}(g_2Hg_2^{-1})g_1 = g_1^{-1}Hg_1 = H$$

և $g_2^{-1}g_1 \in N_H$, այսինքն N_H-ն ենթախումբ է։

Ակնհայտ է, որ $H \leq N_H \leq G$ և N_H-ն ամենամեծ ենթախումբն է G-ում, որի համար H-ը նորմալ է։ Եթե $N_H = G$, ապա H-ը նորմալ է G-ում։

Դիցուք $S = \{a^{-1}Ha \mid a \in G\}$։ G խումբը գործում է S բազմության վրա՝ $g \in G$ խմբի տարրը գործելով $a^{-1}Ha$ վրա այն տանում է $g^{-1}(a^{-1}Ha)g = (ag)^{-1}H(ag)$-ի մեջ։ Պարզ է, որ $H \in S$ և H-ի ուղեծիրը համընկնում է ամբողջ S-ի հետ, իսկ ստաբիլ խումբը դա N_H-ն է։ Ուրեմն ուղեծրի երկարությունը հավասար է

$(G : N_H)$-ին:

Թեորեմ 12.

Դիցուք $H \leq G$: Եթե $(G : 1) = n$, p-ն n-ի ամենափոքր պարզ բաժանարարն է և $(G : H) = p$, ապա $H \lhd G$:

Ապացույց. Քանի որ $H \leq N_H \leq G$, ապա թեորեմն ապացուցված է, եթե $N_H = G$:

Դիցուք $N_H \subset G$: Պարզ է, որ $(H : 1) \leq (N_H : 1)$ և ուրեմն $1 < (G : N_H) \leq (G : H) = p$: Ուստի, $(G : N_H) = (G : H) = p$, $H = N_H$ և $|S| = p$: Սա նշանակում է, որ գոյություն ունի հոմոմորֆիզմ G խմբից S_p սիմետրիկ խմբի մեջ (տես վերը նկարագրված T_g արտապատկերումները): Նշանակենք այդ հոմոմորֆիզմը f-ով: Համաձայն իզոմորֆիզմի մասին թեորեմի ստանում ենք, որ $G/\ker f$-ը իզոմորֆ է $\mathrm{Im} f$-ին: Ուրեմն $(G : \ker f) = (\mathrm{Im} f : 1)$: Քանի որ $\mathrm{Im} f$-ը S_p սիմետրիկ խմբի ենթախումբ է, ապա $(\mathrm{Im} f : 1)$-ը $(S_p : 1) = p!$-ի բաժանարարն է: Ստանում ենք, որ $(G : \ker f)$-ը $p!$-ի բաժանարարն է:

Մյուս կողմից, եթե $g \in \ker f$, ապա g-ն իրացնում է S բազմության վրա նույնաբար տեղադրությունը, ուստի՝ $g^{-1}Hg = H$: Այստեղից բխում է, որ $g \in N_H = H$ և $\ker f \subseteq H$: Հետևաբար, $p = (G : H) \leq (G : \ker f)$:

Ստացանք, որ $p \leq (G : \ker f)$ և $(G : \ker f)$-ը $p!$-ի բաժանարարն է: Քանի որ համաձայն Լագրանժի թեորեմի $(G : 1) = (G : \ker f)(\ker f : 1)$, ապա $(G : \ker f)$-ը չի կարող ունենալ p-ից փոքր պարզ բաժ անարար: Ուրեմն $(G : \ker f)$-ի ամենափոքր պարզ բաժանարարը p-ն է և $(G : \ker f) = p$։ Ուստի, $(G : H) = (G : \ker f)$ և $\ker f \subseteq H$։ Հետևաբար, $H = \ker f$ և $H \triangleleft G$, քանի որ հոմոմորֆիզմի միջուկը նորմալ է G-ում։

Խմբի ցիկլիկ ինդեքսը

Դիտարկենք n տարրանի տեղադրությունները: Ֆիքսենք զույգ առ զույգ տեղափոխելի $t_1,t_2,\ldots,t_n$ անկախ փոփոխականները՝ $t_it_j = t_jt_i$: Կամայական n տարրանի տեղադրության համար սահմանենք նրա ցիկլիկ տեսակը որպես $t_1^{b_1}t_2^{b_2}\ldots t_n^{b_n}$, որտեղ b_i-ն դա տեղադրության i երկարության ցիկլերի քանակն է: Դյուրին է նկատել, որ $\sum_{i=1}^{n} ib_i = n$: Իսկապես, ib_i-ն i երկարության ցիկլերում պարունակվող $\{1,2,\ldots,n\}$ բազմության տարրերի քանակն է:

$\alpha \in S_n$ տեղադրության ցիկլիկ տեսակը կնշանակենք հետևյալ կերպ. $t_1^{b_1(\alpha)}t_2^{b_2(\alpha)}\ldots t_n^{b_n(\alpha)}$:

Սահմանում: Տեղադրությունների $G \leq S_n$ խմբի **ցիկլիկ ինդեքս** է կոչվում հետևյալ բազմանդամը

$$P_G(t_1,t_2,\ldots,t_n) = \frac{1}{(G:1)} \sum_{\alpha\in G} t_1^{b_1(\alpha)}t_2^{b_2(\alpha)}\ldots t_n^{b_n(\alpha)}$$

Օրինակներ

1. Դիցուք $G = \langle\pi\rangle = \{e,\pi,\pi^2,\pi^3,\ldots,\pi^{n-1}\}$, որտեղ

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix}:$$

Ինչպես տեսանք "անիվի" խնդրի լուծման ժամանակ π^k-ի ցիկլիկ տեսակը դա $t_{\frac{n}{(n,k)}}^{(n,k)}$-ն է, ուստի ցիկլիկ խմբի համար

$$P_{\langle\pi\rangle}(t_1,t_2,\ldots,t_n) = \frac{1}{n}\sum_{k=0}^{n} t_{\frac{n}{(n,k)}}^{(n,k)} = \frac{1}{n}\sum_{m|n}\varphi(\frac{n}{m})t_{\frac{n}{m}}^{m}$$

2. *Դիցուք* $G = S_n$ *և* $b_1, b_2, \ldots, b_n$ *թվերը բավարարում են* $\sum_{i=1}^{n} i b_i = n$ *պայմանին: Հաշվենք* $t_1^{b_1} t_2^{b_2} \ldots t_n^{b_n}$ *ցիկլիկ տեսակի տեղադրությունների քանակը: Յուրաքանչյուր* α *տեղադրություն ներկայացնենք ցիկլերի արտադրյալով, որը գրված է հետևյալ կերպ՝*

$$\alpha = (i_1)\ldots(i_{b_1})(j_1 k_1)\ldots(j_{b_2} k_{b_2})(p_1 q_1 s_1)\ldots(p_{b_3} q_{b_3} s_{b_3})\ldots \qquad (27)$$

որտեղ $(i_1)\ldots(i_{b_1})$*-ը* 1 *երկարության ցիկլերն են,* $(j_1 k_1)\ldots(j_{b_2} k_{b_2})$*-ը* 2 *երկարության ցիկլերն են,* $(p_1 q_1 s_1)\ldots(p_{b_3} q_{b_3} s_{b_3})$*-ը* 3 *երկարության ցիկլերն են և այլն: Փաստորեն (27)-ում որոշակի հերթականությամբ գրված են բոլոր* $1, 2, \ldots, n$ *թվերը՝ ամեն մեկը ճիշտ մեկ անգամ, այսինքն (27)-ով որոշվում է* $1, 2, \ldots, n$ *թվերի մի տեղափոխություն: (27)-ի յուրաքանչյուր ցիկլի թվերի ցիկլիկ տեղափոխությունը ցիկլի մեջ չի փոխում տեղադրությունը, քանի որ այդ ցիկլը չի փոխվում և փոխվում է միայն ցիկլի գրառումը: Նաև տեղադրությունը չի փոխվի, եթե տեղերով փոխենք միևնույն երկարության երկու ցիկլ: Ամեն մի այդպիսի ցիկլիկ տեղաշարժ և ցիկլերի տեղափոխություն (27)-ում չեն փոխում* α*-ն, սակայն փոխում են* $1, 2, \ldots, n$ *թվերի տեղափոխությունը: Ցիկլիկ տեղաշարժերի և ցիկլերի տեղափոխությունների քանակը հավասար է* $\prod_{i=1}^{n} b_i! i^{b_i}$*: Ուրեմն* α*-ին համապատասխանում է* $\prod_{i=1}^{n} b_i! i^{b_i}$ *հատ* $1, 2, \ldots, n$ *թվերի տեղափոխություն և քանի որ բոլոր տեղափոխությունների քանակը* $n!$ *է, ապա (27) ցիկլիկ տեսակի* α *տեղադրությունների քանակը*

$$\frac{n!}{\prod_{i=1}^{n} b_i! i^{b_i}}$$

է: Ուստի S_n-ի ցիկլիկ ինդեքսն է հետևյալ բազմանդամը՝

$$P_{S_n}(t_1, t_2, \ldots, t_n) = \frac{1}{n!} \sum_{(b_1, b_2, \ldots, b_n)} \frac{n!}{\prod_{i=1}^{n} b_i! i^{b_i}} t_1^{b_1} t_2^{b_2} \ldots t_n^{b_n},$$

որտեղ գումարը վերցվում է ըստ բոլոր $(b_1, b_2, \ldots, b_n)$ հավաքածուների, որ $\sum_{i=1}^{n} i b_i = n$:

3. Դիցուք $G = A_n$: Կամայական $\alpha \in S_n$ տեղադրության համար, որի ցիկլիկ տեսակը $t_1^{b_1} t_2^{b_2} \ldots t_n^{b_n}$ է կնշանակենք $d(\alpha)$-ով α տեղադրության դեկրեմենտը՝

$$d(\alpha) = \sum_{i=1}^{n} (i-1) b_i = n - \sum_{i=1}^{n} b_i:$$

Հայտնի է, որ դեկրեմենտը զույգ թիվ է միայն և միայն, երբ α տեղադրությունը զույգ է: Ուստի, A_n-ի ցիկլիկ ինդեքսը կարելի է ստանալ հետևյալ կերպ՝

$$P_{S_n}(t_1, t_2, \ldots, t_n) = \frac{1}{n!} \sum_{(b_1, b_2, \ldots, b_n)} \frac{n!\left(1 + (-1)^{n - \sum_{i=1}^{n} b_i}\right)}{\prod_{i=1}^{n} b_i! i^{b_i}} t_1^{b_1} t_2^{b_2} \ldots t_n^{b_n},$$

որտեղ գումարը վերցվում է ըստ բոլոր $(b_1, b_2, \ldots, b_n)$ հավաքածուների, որ $\sum_{i=1}^{n} i b_i = n$:

4. Դիցուք G-ն վերը դիտարկված խորանարդի գագաթների բազմության պտույտներով ստացվող տեղադրությունների խումբն է: Պարզենք այդ տեղադրությունների ցիկլիկ տեսակները.

a. միավոր պտույտ (փաստացի պտույտ չի կատարվում) - 1 Հատ - ցիկլիկ տեսակը t_1^8 է

b. 90^o պտույտ խորանարդի երկու Հանդիպակաց նիստերի կենտրոններով անցնող առանցքի շուրջը - 3 Հատ - ամեն մի Հանդիպակաց նիստի գագաթները կազմում են մի ցիկլ - ցիկլիկ տեսակը t_4^2 է

c. 180^o պտույտ խորանարդի երկու Հանդիպակաց նիստերի կենտրոններով անցնող առանցքի շուրջը - 3 Հատ - առանցքի վրա գագաթ չկա՝ բոլոր ցիկլերը 2 երկարության են - ցիկլիկ տեսակը t_2^4 է

d. 270^o պտույտ խորանարդի երկու Հանդիպակաց նիստերի կենտրոններով անցնող առանցքի շուրջը - 3 Հատ - նույնն է ինչ 90^o պտույտի Համար - t_4^2

e. 120^o պտույտ խորանարդի անկյունագծի շուրջը - 4 Հատ - առանցքի վրայի երկու գագաթները 1 երկարության ցիկլեր են կազմում, այդ գագաթներից յուրաքանչյուրին կից 3 գագաթները ցիկլ են կազմում - ցիկլիկ տեսակը $t_1^2t_3^2$ է

f. 240^o պտույտ խորանարդի անկյունագծի շուրջը - 4 Հատ - նույնն է ինչ 120^o պտույտի Համար - $t_1^2t_3^2$

g. 180^o պտույտ խորանարդի երկու Հանդիպակաց կողերի կենտրոններով անցնող առանցքի շուրջը - 6 Հատ - առանցքի վրա գագաթ չկա՝ բոլոր ցիկլերը 2 երկարության են - ցիկլիկ տեսակը t_2^4 է

Ցիկլիկ ինդեքսը Հետևյալն է.

$$P_{\text{գագաթների}}(t_1,\ldots,t_8) = \frac{1}{24}(t_1^8 + 6t_4^2 + 8t_1^2t_3^2 + 9t_2^4)$$

Պոյայի թեորեմը

Դիցուք $N = \{1,2,\dots,n\}$, $R = \{1,2,\dots,r\}$ և $G \le S_n$ խումբը գործում է R^N-ի վրա՝ $(\forall\alpha \in G \ \ \forall f \in R^N)$ $(\alpha,f) \mapsto f \cdot \alpha$: Ստաբիլ խումբը դա $G_f = \{\alpha \in G \mid f = f\alpha\}$-ն է, իսկ ուղեծիրը դա $Gf = \{f\alpha \mid \alpha \in G\}$-ն է: Ինչպես գիտենք R^N-ը տրոհվում է չհատվող ուղեծրերի:

Ընտրենք $x_1,x_2,\dots,x_r$ անկախ փոփոխականների բազմությունը՝ $x_ix_j = x_jx_i$: Յուրաքանչյուր $f \in R^N$ համար սահմանենք ֆունկցիայի կշիռը հետևյալ բանաձևով՝ $\omega(f) = \prod_{i=1}^{n} x_{f(i)}$: Փաստորեն ֆունկցիայի կշիռը թույլ է տալիս իմանալ, թե ֆունկցիան քանի անգամ է ընդունում տրված արժեքը R բազմությունից:

Դիցուք $g \in Gf$, այսինքն $\exists\alpha \in G$ որ $f = g\alpha$: Պարզ է, որ $\omega(f) = \prod_{i=1}^{n} x_{f(i)} = \prod_{i=1}^{n} x_{g(\alpha(i))}$: Քանի որ α-ն տեղադրություն է, ապա երբ i-ն ընդունում է 1-ից n արժեքները $\alpha(i)$-ն նույնպես ընդունում է 1-ից n արժեքներն (ընդհանուր դեպքում մեկ այլ հաջորդականությամբ): Օգտվելով $x_1,x_2,\dots,x_r$ փոփոխականների տեղափոխելի լինելու հանգամանքից ստանում ենք՝

$$\omega(f) = \prod_{i=1}^{n} x_{f(i)} = \prod_{i=1}^{n} x_{g(\alpha(i))} = \prod_{j=1}^{n} x_{g(j)} = \omega(g):$$

Այսպիսով ապացուցեցինք, որ միևնույն ուղեծրի ֆունկցիաների կշիռները հավասար են: Հակառակը միշտ չէ որ ճիշտ է: Դիցուք $n = 4$, $r = 2$ և $f(1) = f(3) = 1 = g(1) = g(2)$, $f(2) = f(4) = 2 = g(3) = g(4)$ և $G = \{e,\pi\}$, որտեղ

$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$: Ակնհայտ է, որ $\omega(f) = x_1^2 x_2^2 = \omega(g)$ սակայն f-ը և g-ն տարբեր ուղեծրերից են, քանի որ $g = g\pi$:

Յուրաքանչյուր ուղեծրի համար սահմանենք կշիռը որպես այդ ուղեծրի ֆունկցիայի կշիռը: Քանի որ այդ ուղեծրի բոլոր ֆունկցիաներն ունեն միևնույն կշիռն, այս սահմանումը կոռեկտ է: Փորձենք այժմ հաշվել բոլոր ուղեծրերի կշիռների գումարը՝ $\sum\limits_{\substack{\text{ըստ բոլոր } Gf \\ \text{ուղեծրերի}}} \omega(Gf)$, որը կնշանակենք $\Omega(N,R)$-ով: Այսպիսով

$\Omega(N,R) = \sum\limits_{f \in R^N} \frac{\omega(f)}{|Gf|}$ և օգտվելով (25) բանաձևից ստանում ենք՝

$$\Omega(N,R) = \sum_{f \in R^N} \frac{\omega(f)}{(G : G_f)} = \sum_{f \in R^N} \frac{\omega(f)}{(G : 1)} (G_f : 1) =$$

$$\frac{1}{(G : 1)} \sum_{f \in R^N} \omega(f)(G_f : 1)$$

(այստեղ օգտվեցինք Լագրանժի թեորեմից): Ձևափոխելով վերջին գումարը ստանում ենք՝

$$\sum_{f \in R^N} \omega(f)(G_f : 1) = \sum_{f \in R^N} \omega(f) |\{\alpha \in G \mid f = f\alpha\}| =$$

$$\sum_{f \in R^N} \omega(f) \sum_{\substack{\alpha \in G \\ f = f\alpha}} 1 = \sum_{\alpha \in G} \sum_{\substack{f \in R^N \\ f = f\alpha}} \omega(f) :$$

Ուստի,

$$\Omega(N,R) = \frac{1}{(G : 1)} \sum_{\alpha \in G} \sum_{\substack{f \in R^N \\ f = f\alpha}} \omega(f) \qquad (28)$$

Ներմուծենք հետևյալ բազմանդամները (տարրական սիմետրիկ բազմանդամները)՝

$$
\begin{aligned}
s_1 &= x_1 + \ldots + x_r \\
s_2 &= x_1^2 + \ldots + x_r^2 \\
s_3 &= x_1^3 + \ldots + x_r^3 \\
&\ldots \\
s_k &= x_1^k + \ldots + x_r^k \\
&\ldots
\end{aligned}
$$

Տեղադրենք $s_1, s_2, \ldots, s_n$ բազմանդամները G խմբի ցիկլիկ ինդեքսի մեջ $t_1, t_2, \ldots, t_n$ փոփոխականների փոխարեն և կստանանք

$$P_G(s_1, s_2, \ldots, s_n) = \frac{1}{(G:1)} \sum_{\alpha \in G} s_1^{b_1(\alpha)} s_2^{b_2(\alpha)} \ldots s_n^{b_n(\alpha)},$$

որտեղ $(b_1(\alpha), \ldots, b_n(\alpha))$-ն α տեղադրության տեսակն է: Համադրելով (28)-ը և $P_G(s_1, s_2, \ldots, s_n)$-ը տեսնում ենք, որ եթե $\sum\limits_{\substack{f \in R^N \\ f = f\alpha}} \omega(f) = s_1^{b_1(\alpha)} s_2^{b_2(\alpha)} \ldots s_n^{b_n(\alpha)}$, ապա $\Omega(N, R) = P_G(s_1, s_2, \ldots, s_n)$:

Դիտարկենք $s_1^{b_1(\alpha)} s_2^{b_2(\alpha)} \ldots s_n^{b_n(\alpha)}$ արտադրյալը: Այն կարելի է վերարտադրել հետևյալ կերպ.

$$(x_1 + \ldots + x_r)^{b_1(\alpha)} (x_1^2 + \ldots + x_r^2)^{b_2(\alpha)} \ldots (x_1^n + \ldots + x_r^n)^{b_n(\alpha)} \tag{29}$$

Այս արտադրյալի փակագծերը բացելուց հետո ստացվում է մի բազմանդամ, որի յուրաքանչյուր անդամ կարելի է նաև ստանալ (29)-ի փակագծերից յուրաքանչյուրից մեկական գումարելի ընտրելով: Նշանակենք α տեղադրության ցիկլերը (դիտարկելով դրանք որպես N-ի ենթաբազմություններ) հետևյալ կերպ.

$A_1, A_2, \ldots, A_{b_1(\alpha)}$ - 1 երկարության ցիկլերը

$B_1, B_2, \ldots, B_{b_2(\alpha)}$ - 2 երկարության ցիկլերը

$C_1, C_2, \ldots, C_{b_3(\alpha)}$ - 3 երկարության ցիկլերը

$\ldots$

Ինչպես արդեն պարզել էինք, տրված α տեղադրության համար $f \in R^N$ ֆունկցիան բավարարում է $f = f\alpha$ պայմանին միայն և միայն այն դեպքում, երբ f ֆունկցիան հաստատուն է α տեղադրության ցիկլերի վրա: Ուստի, կարելի է խոսել f ֆունկցիայի ցիկլի վրա արժեքի մասին, այսինքն գրելով $f(A_1)$ հասկանում ենք $f(i)$, $i \in A_1$:

Եթե $f \in R^N$ և $f = f\alpha$, ապա

$$\omega(f) = x_{f(A_1)} \ldots x_{f(A_{b_1(\alpha)})} x^2_{f(B_1)} \ldots x^2_{f(B_{b_2(\alpha)})} x^3_{f(C_1)} \ldots x^3_{f(C_{b_3(\alpha)})} \cdots \quad (30)$$

որտեղ $x_{f(A_1)} \ldots x_{f(A_{b_1(\alpha)})}$-ն դա 1 երկարության ցիկլերում պարունակվող թվերի վրա f ֆունկցիայի արժեքներին համապատասխանող կշռի մասն է, $x^2_{f(B_1)} \ldots x^2_{f(B_{b_2(\alpha)})}$-ը՝ 2 երկարության ցիկլերում պարունակվող թվերի վրա f ֆունկցիայի արժեքներին համապատասխանող կշռի մասն է (քանի որ B_i-ն երկու թվից է բաղկացած, ուստի այդ մասի կշիռն է $x_{f(B_i)} x_{f(B_i)} = x^2_{f(B_i)}$) և այլն: Այժմ ցույց տանք, որ գոյություն ունի (29)-ի փակագծերից անդամների ընտրման մի եղանակ, որի արդյունքում ստացվում է (30)-ը: (29)-ում ունենք $b_1(\alpha)$ հատ $(x_1 + \ldots + x_r)$ փակագիծ, առաջինից ընտրենք $x_{f(A_1)}$-ն, երկրորդից՝ $x_{f(A_2)}$-ը, և այլն և վերջինից՝ $x_{f(A_{b_1(\alpha)})}$-ն: Այնուհետև, $b_2(\alpha)$ հատ $(x_1^2 + \ldots + x_r^2)$ փակագծերից սկզբից կընտրենք առաջին փակագծից $x^2_{f(B_1)}$-ը, երկրորդից՝ $x^2_{f(B_2)}$-ը և այլն և վերջինից՝ $x^2_{f(B_{b_2(\alpha)})}$: Նման ձևով կստանանք ամբողջ (30)-ը: Այսպիսով, յուրաքանչյուր $f \in R^N$ $(f = f\alpha)$ համար, (29)-ի փակագծերը բացելով կստանանք $\omega(f)$-ը: Մյուս կողմից պարզ է, որ (29)-ի փակագծերից անդամների ընտրման կամայական եղանակ համադեյնում է որևէ $f \in R^N$ $(f = f\alpha)$ ֆունկցիայի կշռի ստացմանը: Իսկապես, դիցուք առաջին $b_1(\alpha)$ հատ $(x_1 + \ldots + x_r)$ փակագծերից ընտրվել են $x_{i_1}, \ldots, x_{i_{b_1(\alpha)}}$, հաջորդ $b_2(\alpha)$ հատ $(x_1^2 + \ldots + x_r^2)$ փակագծերից ընտրվել են $x_{j_1}^2, \ldots, x_{j_{b_2(\alpha)}}^2$ և այլն: Դա նշանակում է, որ համապատասխան ֆունկցիայի համար

$$f(A_1) = i_1, \ldots, f(A_{b_1(\alpha)}) = i_{b_1(\alpha)}, f(B_1) = j_1, \ldots, f(B_{b_2(\alpha)}) = j_{b_2(\alpha)}$$

և այլն: Եթե գոնե մեկ փակագծից ընտրենք մեկ այլ անդամ, ապա ակնհայտորեն կստանանք մեկ այլ ֆունկցիա, քանի որ կփոխվի ֆունկցիայի արժեքը համապատասխան ցիկլի վրա: Այսպիսով ապացուցվեց որ

$$\sum_{\substack{f \in R^N \\ f = f\alpha}} \omega(f) = s_1^{b_1(\alpha)} s_2^{b_2(\alpha)} \ldots s_n^{b_n(\alpha)}$$

և հետևաբար՝

$$\Omega(N,R) = P_G(s_1, s_2, \ldots, s_n)$$

Վերջին բանաձևը հայտնի է որպես Պոյայի թեորեմ:

Թեորեմ 13. (Պոյա)

Դիցուք $N = \{1,2,\ldots,n\}$, $R = \{1,2,\ldots,r\}$ **և** $G \leq S_n$ **խումբը գործում է** R^N**-ի վրա:** R^N**-ի բոլոր ֆունկցիաների կշիռների գումարը՝** $\Omega(N,R)$**-ը հավասար է** $P_G(s_1, s_2, \ldots, s_n)$**-ին:**

Դյուրին է նկատել, որ տեղադրելով $x_i = 1$ բոլոր $i \in R$ համար ստացվում է $\omega(f) = 1$, ուստի

$$\Omega(N,R) = \sum_{\substack{\text{ըստ բոլոր } Gf \\ \text{ուղեծրերի}}} \omega(Gf)$$

հավասար է դառնում ուղեծրերի քանակին:

Դիցուք հարկավոր է գտնել ուղեծրերի քանակը, որոնց կշիռը հավասար է $x_1^{m_1}x_2^{m_2}\ldots x_r^{m_r}$, որտեղ $\sum_{i=1}^{r} m_i = n$: Պարզ է, որ այդ քանակը հավասար է $P_G(s_1,s_2,\ldots,s_n)$ բազմանդամում $x_1^{m_1}x_2^{m_2}\ldots x_r^{m_r}$ անդամի գործակցին:

Օրինակներ

1. Դիցուք հարկավոր է գտնել խորանարդի գագաթների իրարից պտույտով չստացվող երեք գույներով ներկումների քանակը: Պարզ է, որ ներկումները տրվում են $f : N \to R$ ֆունկցիաներով, որտեղ $N = \{1,2,\ldots,8\}$, $R = \{1,2,3\}$: Պտույտները նկարագրված են նախորդ օրինակներից մեկում, որտեղ կառուցված է համապատասխան 24 տարր պարունակող խմբի ցիկլիկ ինդեքսը՝ $P(t_1,\ldots,t_8) = \frac{1}{24}(t_1^8 + 6t_4^2 + 8t_1^2t_3^2 + 9t_2^4)$: Այդ խումբը գործում է R^N-ի վրա և համաձայն Պոյայի թեորեմի իրարից պտույտով չստացվող ներկումների (ֆունկցիաների տարբեր ուղեծիրների) քանակը կստացվի եթե

$$\frac{1}{24}\Big((x_1+x_2+x_3)^8 + 6(x_1^4+x_2^4+x_3^4)^2 +$$

$$8(x_1+x_2+x_3)^2(x_1^3+x_2^3+x_3^3)^2 + 9(x_1^2+x_2^2+x_3^2)^4\Big)$$

բազմանդամում տեղադրենք մեկեր փոփոխականների փոխարեն: Այդ քանակը կլինի հավասար

$\frac{1}{24}(3^8 + 6 \times 3^2 + 8 \times 3^2 \times 3^2 + 9 \times 3^4) = 333$:

2. *Դիցուք հարկավոր է գտնել խորանարդի գագաթների իրարից պտույտով չստացվող երեք գույներով այնպիսի ներկումների քանակը, որ առաջին գույնով ներկված է երկու գագաթ, երկրորդով՝ ևս երկու գագաթ, իսկ մնացած չորս գագաթները ներկված են երրորդ գույնով: Պարզ է, որ հարկավոր է գտնել* $x_1^2x_2^2x_3^4$ *անդամի գործակիցը*

$$\frac{1}{24}\Big((x_1 + x_2 + x_3)^8 + 6(x_1^4 + x_2^4 + x_3^4)^2 +$$

$$8(x_1 + x_2 + x_3)^2(x_1^3 + x_2^3 + x_3^3)^2 + 9(x_1^2 + x_2^2 + x_3^2)^4\Big)$$

բազմանդամում: $(x_1 + x_2 + x_3)^8$*-ում* $x_1^2x_2^2x_3^4$ *անդամի գործակիցը հավասար է* $\binom{8}{2}\binom{6}{2} = 420$: $6(x_1^4 + x_2^4 + x_3^4)^2 + 8(x_1 + x_2 + x_3)^2(x_1^3 + x_2^3 + x_3^3)^2$*-ում* $x_1^2x_2^2x_3^4$ *անդամի գործակիցը զրո է, իսկ* $9(x_1^2 + x_2^2 + x_3^2)^4$*-ում՝* $9 \times \binom{4}{1}\binom{3}{1} = 108$: *Ուստի խնդրի պատասխանն է* $\frac{420+108}{24} = 22$:

Սիլովյան խմբեր

Ինչպես գիտենք Լագրանժի թեորեմից, վերջավոր խմբում կամայական ենթախմբի կարգը խմբի կարգի բաժանարարն է: Այս մասում մենք կապացուցենք ինչ որ իմաստով հակադարձ պնդում՝ եթե խմբի կարգը բաժանվում է p^n-ի վրա, որտեղ p-ն պարզ թիվ է, ապա կամայական $s \leq n$ համար խմբում կգտնվի p^s կարգի ենթախումբ:

Նախ ապացուցենք մի քանի էլեմենտար պնդում:

Լեմմ 14.

Դիցուք H-ը և K-ն G վերջավոր խմբի ենթախմբեր են և $HK = \{hk \mid h \in H,\ k \in K\}$: HK բազմության տարրերի քանակի՝ $|HK|$-ի համար ստույգ է՝

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Ապացույց. Դիցուք $h \in H,\ k \in K$: Որոշենք այն $(h_1,k_1) \in H \times K$ զույգերի քանակը, որ $hk = h_1k_1$: Դյուրին է տեսնել, որ $hk = h_1k_1 \Rightarrow h_1^{-1}h = k_1k^{-1} \in H \cap K$: Նշանակենք $t = h_1^{-1}h = k_1k^{-1}$: Ստանում ենք՝ $h_1 = ht^{-1}$ և $k_1 = tk$: Այսինքն յուրաքանչյուր $t \in H \cap K$ տարրին համապատասխանում է մի $(h_1,k_1) \in H \times K$ զույգ, որ $hk = h_1k_1$: Ուստի, HK-ի տարրերի քանակը հավասար է

$$\frac{|H \times K|}{|H \cap K|}$$

և լեմմն ապացուցված է:

Նկատենք, որ այս լեմմի պնդումից հետևում է, որ եթե

$H \cap K = \{e\}$, ապա $|HK| = |H||K|$ և HK-ի տարրերի ներկայացումը hk տեսքով, որտեղ $h \in H$, $k \in K$, միակն է: Սա մենք պարզել էինք ուղիղ արտադրյալի ուսումնասիրման ժամանակ:

Լեմմ 15.

Դիցուք m-ը ամբողջ դրական թիվ է, իսկ p^α-ն պարզ թվի ոչ բացասական ամբողջ աստիճան է:

$\binom{mp^\alpha - 1}{p^\alpha - 1}$ բինոմիալ գործակիցը լինելով ամբողջ թիվ չի բաժանվում p-ի վրա:

Ապացույց. Ըստ սահմանման ունենք՝

$$\binom{mp^\alpha - 1}{p^\alpha - 1} = \frac{(mp^\alpha - 1)(mp^\alpha - 2)\ldots(mp^\alpha - (p^\alpha - 1))}{(p^\alpha - (p^\alpha - 1))(p^\alpha - (p^\alpha - 2))\ldots(p^\alpha - 1)} = \prod_{k=1}^{p^\alpha - 1} \frac{mp^\alpha - k}{k}$$

Ապացուցենք, որ բոլոր $1 \le k \le p^\alpha - 1$ համար k և $mp^\alpha - k$ թվերը միաժամանակ կամ բաժանվում կամ էլ չեն բաժանվում p^s-ի վրա:

Դիցուք k-ն բաժանվում է p^s-ի վրա: Ակնհայտ է, որ $p^s < p^\alpha$ և $s < \alpha$: Ուստի $k = np^s$ և $mp^\alpha - k = mp^\alpha - np^s = p^s(mp^{\alpha - s} - n)$:

Դիցուք $mp^\alpha - k$-ն բաժանվում է p^s-ի վրա և $mp^\alpha - k = np^s$: Եթե $s \ge \alpha$, ապա $p^\alpha(m - np^{s-\alpha}) = k \ge p^\alpha$ քանի որ $m - np^{s-\alpha} \ge 1$: Ուստի, $s < \alpha$ և $k = p^s(mp^{\alpha-s} - n)$:

Այսպիսով, $\prod_{k=1}^{p^\alpha - 1} \frac{mp^\alpha - k}{k}$ արտադրյալում յուրաքանչյուր $\frac{mp^\alpha - k}{k}$ կոտորակի համարիչի և հայտարարի p^s տեսքի բաժանարարները միմյանց չեզոքացնում են և ուրեմն $\binom{mp^\alpha - 1}{p^\alpha - 1}$-ը չի բաժանվում p-ի վրա: Լեմմն ապացուցված է:

Լեմմ 16․

Եթե H**-ը և** K**-ն** G **խմբի ենթախմբեր են և բոլոր** $h \in H$ **համար տեղի ունի** $h^{-1}Kh = K$ **պայմանը, ապա** $HK = \{hk \mid h \in H,\ k \in K\}$**-ն նույնպես** G **խմբի ենթախումբ է։**

Ապացույց. Բավական է ստուգել, որ $(h_2k_2)^{-1}(h_1k_1) \in HK$։ Պարզ է, որ $h_2^{-1}h_1 = h_3 \in H$ և $h_3^{-1}k_2^{-1}h_3 = k_3 \in K$։ Ուստի, $k_2^{-1}h_3 = h_3k_3$ և

$$(h_2k_2)^{-1}(h_1k_1) = k_2^{-1}h_2^{-1}h_1k_1 = k_2^{-1}h_3k_1 = h_3(k_3k_1) \in HK\text{։}$$

Լեմմն ապացուցված է։

Սահմանում։ Դիցուք G-ն վերջավոր խումբ է և p^α-ն p պարզ թվի ամենամեծ աստիճանն է, որի վրա առանց մնացորդի բաժանվում է խմբի $(G:1)$ կարգը։ G խմբի H ենթախումբը կոչվում է p-**ենթախումբ,** եթե $(H:1) = p^\beta$, $\beta \le \alpha$։

p^α կարգի p-ենթախումբը կոչվում է **Սիլովյան** p-**ենթախումբ** G-ում։

G խմբի H_1 և H_2 ենթախմբերը կանվանենք **համալուծ,** եթե կգտնվի $g \in G$, որ $g^{-1}H_1g = H_2$։ Հեշտությամբ ստուգվում է, որ համալուծ ենթախմբերն իզոմորֆ են։

Թեորեմ 17․ (Սիլովի թեորեմը)

Դիցուք G**-ն վերջավոր խումբ է,** p**-ն պարզ թիվ է,** $(G:1) = mp^\alpha$ **և** $(m,p) = 1$**, այսինքն՝** $(G:1)$**-ը չի**

բաժանվում $p^{\alpha+1}$-ի վրա, ապա

1. կամայական β-ի համար, որ $1 \leq \beta \leq \alpha$, G-ում գոյություն ունի p^{β} կարգի p-ենթախումբ

2. Սիլովյան p-ենթախմբերի n_p քանակը բավարարում է $n_p \equiv 1 \, mod p$ բաղդատմանը

3. կամայական երկու Սիլովյան p-ենթախմբեր իրար համալուծ են

4. յուրաքանչյուր p-ենթախումբ պարունակվում է Սիլովյան p-ենթախմբի մեջ:

Ապացույց. Դիցուք $S = \{s \subseteq G \mid |s| = p^{\beta}\}$ (ինչպես միշտ $|s|$-ը բազմության տարրերի քանակն է): G խումբը գործում է S բազմության վրա հետևյալ կերպ՝ $g \in G$ և $s \in S$ համար $gs = \{gx \mid x \in s\}$: Ակնհայտ է, որ $|gs| = |s|$ և $es = s$, $g_1(g_2s) = (g_1g_2)s$: Նշանակենք $\tilde{m} = mp^{\alpha-\beta}$ և $(G:1) = \tilde{m}p^{\beta}$: Դյուրին է տեսնել, որ $|S| = \binom{\tilde{m}p^{\beta}}{p^{\beta}} = \tilde{m}\binom{\tilde{m}p^{\beta}-1}{p^{\beta}-1}$: Համաձայն Լեմմ 15-ի p թվի ամենամեծ աստիճանը, որի վրա բաժանվում է $|S|$-ը, համընկնում է p թվի ամենամեծ աստիճանին, որի վրա բաժանվում է $\tilde{m}$-ը: Պարզ է, որ p-ի այդպիսի աստիճանը $p^{\alpha-\beta}$-ն է: G խմբի գործողությունը S բազմության վրա տրոհում է վերջինս չհատվող ուղեծրերի: Եթե բոլոր ուղեծրերի երկարությունները բաժանվում են p թվի ավելի մեծ քան $p^{\alpha-\beta}$-ն աստիճանի վրա, ապա $|S|$-ն էլ կբաժանվի p-ի այդ աստիճանի վրա, ինչն անհնար է: Ուստի կգտնվի մի ուղեծիր, որի երկարությունը չի բաժանվում $p^{\alpha-\beta}$-ից մեծ p-ի աստիճանի վրա: Ֆիքսենք որևէ s էլեմենտ այդ ուղեծրից (այդ ուղեծիրը կնշանակենք սովորաբար Gs նշանով) և դիտարկենք դրա ստաբիլ խումբը՝ $G_s = \{g \in G \mid gs = s\}$: Համաձայն (**25**)-ի $|Gs| = (G : G_s)$ և Լագրանժի թեորեմի՝

$$mp^{\alpha} = (G : 1) = (G : G_s)(G_s : 1) = |Gs|(G_s : 1)$$

Քանի որ $|Gs|$-ը չի բաժանվում $p^{\alpha-\beta}$-ից մեծ p-ի աստիճանի վրա, ստանում ենք, որ $(G_s : 1)$-ը բաժանվում է p^{β}-ի վրա և ուրեմն $p^{\beta} \leq (G_s : 1)$:

Մյուս կողմից ունենք, որ $(G_s : 1) \leq p^{\beta}$: Իսկապես, վերցնենք որևէ $\tilde{x}$ տարր s բազմությունից: Պարզ է, որ $g\tilde{x} \in s$ բոլոր $g \in G_s$ համար, քանի որ $gs = \{gx \mid x \in s\} = s$: Եթե $g_1\tilde{x} = g_2\tilde{x}$ որևէ $g_1, g_2 \in G_s$ համար, ապա բազմապատկելով $g_1\tilde{x} = g_2\tilde{x}$ առնչությունն աջից $\tilde{x}^{-1}$-ով ստանում ենք՝ $g_1 = g_2$: Ուրեմն բոլոր $g\tilde{x}$ արտադրյալները, որտեղ $g \in G_s$, տարբեր են և պատկանում են s բազմությանը: Ուստի $p^{\beta} = |s| \geq (G_s : 1)$:

Այսպիսով G_s ենթախումբը p^{β} կարգի p-ենթախումբ է G-ում և թեորեմի **1**. պնդումն ապացուցված է:

Դիցուք H-ը Սիլովյան p-ենթախումբ է G-ում: Նշանակենք $\mathfrak{H}$-ով H-ն համալուծ բոլոր ենթախմբերի բազմությունը՝ $\mathfrak{H} = \{g^{-1}Hg \mid g \in G\}$: H-ը գործում է $\mathfrak{H}$-ի վրա հետևյալ կերպ՝ $h \in H$ տարրը տանում է $\tilde{H} \in \mathfrak{H}$ ենթախումբը $h^{-1}\tilde{H}h = h^{-1}g^{-1}Hgh = (gh)^{-1}H(gh) \in \mathfrak{H}$ ենթախմբի մեջ: Տրիվիալ ստուգվում է, որ դա գործողություն է: Յուրաքանչյուր ուղեծրի երկարությունը p-ի աստիճան է, քանի որ այն հավասար է համապատասխան ստաբիլ խմբի ինդեքսին H-ում: Համաձայն Լագրանժի թեորեմի, p-ենթախմբի ենթախմբերի թե կարգերը, թե ինդեքսները, լինելով p-ենթախմբի կարգի բաժանարարներ, p-ի աստիճաններ են:

Պարզ է, որ $H \in \mathfrak{H}$: Դիտարկենք H-ի ուղեծիրը՝ $\{h^{-1}Hh \mid h \in H\} = H$: Ապացուցենք, որ միայն H-ի ուղեծիրն է կազմված մեկ տարրից, այսինքն ունի 1 երկարություն: Դիցուք կգտնվի մեկ այլ $K \in \mathfrak{H}$, որ $\{h^{-1}Kh \mid h \in H\} = K$, այսինքն $h^{-1}Kh = K$ բոլոր $h \in H$: Համաձայն Լեմմ 16-ի $HK = \{hk \mid h \in H, k \in K\}$-ն ենթախումբ է G-ում: Համաձայն Լեմմ 14-ի $(HK : 1) = \dfrac{(H : 1)(K : 1)}{(H \cap K : 1)}$: Սակայն ունենք, որ $(H : 1) = p^{\alpha}$ և քանի որ K-ն H-ի համալուծն է, ապա $(K : 1) = p^{\alpha}$: Ենթախմբերի հատումը նորից ենթախումբ է: Ուստի՝ $H \cap K \leq H$ և $(H \cap K : 1) = p^{\beta}$, որտեղ $0 \leq \beta \leq \alpha$: Որեմն, HK-ն նույնպես p-ենթախումբ է G-ում, $(HK : 1) = p^{2\alpha-\beta}$: Քանի որ $HK \leq G$, ապա $(HK : 1)$-ն p^{α}-ի բաժանարարն է և $p^{2\alpha-\beta} \leq p^{\alpha}$: Հետևաբար, $p^{\alpha} \leq p^{\beta}$ և $\alpha = \beta$: Ստանում ենք, որ $(H \cap K : 1) = p^{\alpha} = (H : 1) = (K : 1)$ և $H = K$:

Այսպիսով բոլոր ուղեծրերի երկարությունները, բացի մեկից, p-ի դրական աստիճաններ են: Հետևաբար ուղեծրերի երկարությունների գումարը՝ $|\mathfrak{H}|$-ը $1 + pq$ տեսքի թիվ է, այսինքն՝ $|\mathfrak{H}| \equiv 1 \bmod p$:

Դիցուք կամայական p-ենթախումբ պարունակվում է $\mathfrak{H}$-ի ենթախմբերից մեկում: Այստեղից Սիլովյան p-ենթախմբի դեպքում կբխի, որ բոլոր Սիլովյան p-ենթախմբերը համալուծ են H-ին և ուստի միմյանց (թեորեմի 3. պնդումը): Նաև կստացվի, որ $\mathfrak{H}$-ը դա բոլոր Սիլովյան p-ենթախմբերի բազմությունն է և $|\mathfrak{H}| = n_p \equiv 1 \bmod p$ (թեորեմի 2. պնդումը): Վերջապես կապացուցվի նաև թեորեմի 4. պնդումը:

Ապացուցենք այժմ, որ կամայական p-ենթախումբ պարունակվում է $\mathfrak{H}$-ի ենթախմբերից մեկում: Դիցուք K-ն p-ենթախումբ է, որը չի պարունակվում $\mathfrak{H}$-ի ենթախմբերից ոչ մեկում: K-ն գործում է $\mathfrak{H}$-ի *վրա ճիշտ այնպես, ինչպես H-ը՝ $k \in K$ տարրը տանում է $\tilde{H} \in \mathfrak{H}$ ենթախումբը*

$$k^{-1}\tilde{H}k = k^{-1}g^{-1}Hgk = (gk)^{-1}H(gk) \in \mathfrak{H}$$

ենթախմբի մեջ: Դիցուք գոյություն ունի 1 երկարության ուղեծիր, այսինքն $\tilde{H} \in \mathfrak{H}$, որ $k^{-1}\tilde{H}k = \tilde{H}$ բոլոր $k \in K$: Ինչպես վերը բերված դատողություններում $K\tilde{H}$-ն ենթախումբ է,

$$(K\tilde{H} : 1) = \frac{(K : 1)(\tilde{H} : 1)}{(\tilde{H} \cap K : 1)}$$

և $K\tilde{H}$-ը p-ենթախումբ է: Սակայն $(\tilde{H} : 1) = p^{\alpha}$ և

$$\frac{(K : 1)}{(\tilde{H} \cap K : 1)} \geq 1,$$

հետևաբար $(K\tilde{H} : 1) \geq p^{\alpha}$: Ուրեմն, $(K\tilde{H} : 1) = p^{\alpha}$ և $(K : 1) = (\tilde{H} \cap K : 1)$: Վերջին հավասարությունից բխում է, որ $K \subseteq \tilde{H}$, ինչն անհնար է: Այսպիսով, բոլոր ուղեծրերի երկարությունները p-ի դրական աստիճաններ են և $|\mathfrak{H}| \equiv 0 \bmod p$, ինչը նույնպես անհնար է: Հետևաբար, բոլոր p-ենթախմբերը պարունակվում են $\mathfrak{H}$-ի ենթախմբերից մեկում:

Թեորեմն ապացուցված է:

Օրինակներ

1. *Ապացուցենք, որ Թեորեմ* 17*-ում սահմանված n_p թիվը m-ի բաժանարարն է: Դիցուք G խումբը գործում է իր ենթախմբերի վրա հետևյալ կերպ՝ $g \in G$ տարրը տանում է H ենթախումբը $g^{-1}Hg$ ենթախմբի մեջ: Թեորեմ* 17*-ից անմիջապես բխում է, որ բոլոր Սիլովյան p-ենթախմբերը կազմում են մեկ ուղեծիր, իսկ կամայական H Սիլովյան p-ենթախմբի ստաբիլ խումբը դա նրա նորմալիզատորն է $N_H = \{g \in G \mid g^{-1}Hg = H\}$: Ուրեմն համաձայն* (25)*-ի*

$n_p = (G : N_H)$։ Դյուրին է ստուգել, որ $m = (G : H) = (G : N_H)(N_H : H)$ և, հետևաբար, m-ը բաժանվում է n_p-ի վրա։

2. Ապացուցենք, որ եթե $(G : 1) = 15$, ապա G խումբը ցիկլիկ է։ Դիցուք G խումբը գործում է իր ենթախմբերի վրա այնպես, ինչպես **1**. օրինակում։ Դիցուք H-ը Սիլովյան 5-ենթախումբն է, իսկ K-ն Սիլովյան 3-ենթախումբը։ Հետևաբար $(K : 1) = 3$, $(H : 1) = 5$ և H-ն ու K-ն ցիկլիկ են։ Համաձայն թեորեմ **12**-ի H-ը նորմալ է G-ում, ուստի $N_H = G$ և $(G : N_H) = 1$, այսինքն Սիլովյան 5-ենթախմբերի ուղեծիրը բաղկացած է միայն H-ից և H-ը միակ 5-ենթախումբն է։ Սիլովյան 3-ենթախմբերի ուղեծրի երկարությունը հավասար է $(G : N_K)$-ին։ Պարզ է, որ $(G : N_K) \in \{1, 3, 5, 15\}$ և թեորեմ **17**-ի համաձայն $(G : N_K) \equiv 1 \bmod 3$, ուստի $(G : N_K) \notin \{3, 5, 15\}$։ Հետևաբար K-ն միակ 3-ենթախումբն է։ Դիցուք k-ն K-ի ծնիչն է, իսկ h-ը H-ի։ Դիտարկենք kh-ով ծնված $\langle kh \rangle$ ցիկլիկ ենթախումբը G-ում։ Ակնհայտ է, որ $kh \notin H \cup K$, ուստի kh-ը չի պատկանում G-ի և ոչ մի սեփական ենթախմբի, ուրեմն $\langle kh \rangle = G$։

ՕՂԱԿՆԵՐ ԵՎ ԴԱՇՏԵՐ

Սահմանումներ

Դիցուք A բազմության վրա տրված են երկու գործողություն, որոնցից առաջինը կանվանենք "գումարում ", իսկ երկրորդը՝ "բազմապատկում ": Համապատասխանաբար կօգտվենք $+$ և $\cdot$ նշաններից:

Սահմանում. $(A,+,\cdot)$ համակարգը կոչվում է **օղակ**, եթե

1. $(A,+)$ համակարգը տեղափոխելի խումբ է (միավոր տարրը նշանակվում է 0-ով)

2. $(ab)c = a(bc)$

3. A-ում գոյություն ունի տարր, որը նշանակվում 1-ով, այնպիսին, որ $\forall a \in A$ համար $a1 = 1a = a$

4. $(a+b)c = ac+bc$ և $a(b+c) = ab+ac$

Եթե տեղի ունի նաև $ab = ba$ պայմանը A-ի բոլոր տարրերի համար, ապա օղակը կոչվում է **տեղափոխելի**:

Տեղափոխելի օղակը կոչվում է **դաշտ**, եթե յուրաքանչյուր ոչ զրոյական տարր ունի հակադարձ ըստ բազմապատկման, այսինքն՝ $(\forall a \neq 0\ \exists b)\ ab = ba = 1$:

Նշենք օղակների մի քանի տարրական, բայց կարևոր հատկություն.

ա) $a0 = 0a = 0$

իսկապես, $a + a0 = a1 + a0 \underbrace{=}_{\text{համաձայն } 4} a(1+0) = a1 = a,$ ուստի

$a0 = 0$

բ) $(-1)a = -a$

$a + (-1)a = 1a + (-1)a \underbrace{=}_{\text{համաձայն } 4} (1 + (-1))a = 0a = 0,$ ուստի

$(-1)a = -a$

Այսուհետև միշտ կհամարենք, որ $0 \neq 1$, քանի որ հակառակ դեպքում $a = a1 = a0 = 0$ և օղակի բոլոր տարրերը հավասար են 0-ի, այսինքն՝ $A = \{0\}$։

Ամփոփելով վերը նշվածը կարելի է ասել, որ օղակը դա այն հանրահաշվական համակարգն է, որում կարելի է գումարել, հանել և բազմապատկել, իսկ դաշտում նաև բաժանել։

Օրինակներ

1. Դյուրին է ստուգել, որ $(\mathbb{Z}, +, \cdot)$-ը տեղափոխելի օղակ է (դաշտ չէ), իսկ $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ և $(\mathbb{C}, +, \cdot)$-ը դաշտեր են։

2. Դիտարկենք $(\mathbb{Z}_n, +, \cdot)$-ը, որտեղ $\mathbb{Z}_n$-ն ինչպես միշտ ըստ $mod\, n$-ի մնացքների դասերի բազմությունն է։ Ակնհայտ է, որ $(\mathbb{Z}_n, +, \cdot)$-ը տեղափոխելի օղակ է։ Ինչպես գիտենք, $\mathbb{Z}_n$-ում ըստ բազմապատկման հակադարձ ունեն միայն այն ոչ զրոյական տարրերը, որոնք փոխադարձաբար պարզ են մոդուլի հետ։

3. Ուրեմն $(\mathbb{Z}_n, +, \cdot)$-ը դաշտ է միայն, երբ n-ը պարզ թիվ է։ Նշենք $(\mathbb{Z}_n, +, \cdot)$ օղակի մի կարևոր հատկություն ևս։ Դիցուք $n = 6$, ապա $2 \cdot 3 \equiv 0 mod 6$։ Սակայն ոչ $2 \equiv 0 mod 6$ ոչ էլ $3 \equiv 0 mod 6$, այսինքն այն բանից, որ տարրերի արտադրյալը հավասար է զրոյի չի հետևում, որ արտադրիչներից որևէ մեկը զրոյական է:

4. Նշանակենք $A[x]$-ով x փոփոխականի A տեղափոխելի օղակից գործակիցներով բոլոր բազմանդամների բազմությունը: $A[x]$-ը տեղափոխելի օղակ է բազմանդամների սովորական գումարման և բազմապատկման նկատմամբ:

5. $n \times n$ չափանի մատրիցների բազմությունը, որոնց տարրերը A օղակից են, օղակ է (ոչ տեղափոխելի) մատրիցների գումարման և բազմապատկման նկատմամբ:

6. Դիտարկենք $a + b\sqrt{2}$ տեսքի բոլոր թվերի բազմությունը, որտեղ a-ն և b-ն ռացիոնալ թվեր են: Դյուրին է համոզվել, որ այս բազմությունը դաշտ է, եթե գումարումը և բազմապատկումը սահմանենք հետևյալ կերպ.

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$
$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

7. Դիտարկենք $(0,1)$ հատվածի վրա բոլոր անընդհատ ֆունկցիաների բազմությունը: Այս բազմությունը տեղափոխելի օղակ է ֆունկցիաների գումարման և բազմապատկման նկատմամբ:

Ենթաօղակներ և օղակային հոմոմորֆիզմներ

Սահմանում: A օղակի B ենթաբազմությունը կոչվում է **ենթաօղակ**, եթե՝

1. $(B,+) \le (A,+)$ - այսինքն, ըստ գումարման B-ն A-ի ենթախումբն է
2. $1 \in B$
3. $a,b \in B \Rightarrow ab \in B$ - այսինքն, B-ն փակ է բազմապատկման նկատմամբ:

Այլ կերպ ասած, օղակի որևէ ենթաբազմություն ենթաօղակ է, եթե օղակի գործողությունների սահմանափակումը տվյալ ենթաբազմության վրա այն դարձնում է օղակ:

Սահմանում: Դիցուք A_1-ը և A_2-ն օղակներ են: $f : A_1 \to A_2$ արտապատկերումը կոչվում է **օղակային հոմոմորֆիզմ** (կամ ուղղակի **հոմոմորֆիզմ**) եթե

1. $f(0) = 0, f(1) = 1$
2. $f(a+b) = f(a)+f(b)$
3. $f(ab) = f(a)f(b)$

Եթե վերը նշված f արտապատկերումը փոխմիարժեքորեն արտապատկերում է A_1-ը A_2-ի վրա, ապա ասում են, որ օղակներն իրար **իզոմորֆ** են և f-ը կոչվում է **օղակային իզոմորֆիզմ:**

Փաստորեն, եթե դիտարկենք միայն գումարման գործողությունը, օղակային հոմոմորֆիզմը կվերածվի խմբերի հոմոմորֆիզմի:

Ինչպես և խմբերի դեպքում այսուհետև մենք իրարից չենք *տարրերի իզոմորֆ օղակները:*

Յուրաքանչյուր հոմոմորֆիզմի հետ կապվում են հետևյալ երկու բազմությունները միջուկը՝

$$\ker f = \{a \in A_1 \mid f(a) = 0\}$$

և պատկերը՝

$$\mathrm{Im} f = \{b \in A_2 \mid (\exists a \in A_1) f(a) = b\}:$$

Դյուրին է ստուգել, որ պատկերը ենթաօղակ է: Իսկապես, քանի որ հոմոմորֆիզմը խմբերի հոմոմորֆիզմ է գումարման գործողության նկատմամբ, ապա պատկերը նաև խմբերի հոմոմորֆիզմի պատկեր է, ուստի և այն ենթախումբ է և $(\mathrm{Im} f, +) \le (A_2, +)$*: Ակնհայտ է, որ* $f(1) = 1 \in \mathrm{Im} f$*: Եթե* $b_1, b_2 \in \mathrm{Im} f$*, ապա կգտնվեն* a_1 *և* a_2 *այնպիսին, որ* $b_1 = f(a_1)$, $b_2 = f(a_2)$*: Պարզ է, որ* $f(a_1 a_2) = f(a_1) f(a_2) = b_1 b_2$*, ուրեմն* $b_1 b_2 \in \mathrm{Im} f$ *և պատկերը ենթաօղակ է: Ինչպես և խմբերի դեպքում, առանց ընդհանրությունը խախտելու, հարմարության համար կարող ենք համարել, որ* $\mathrm{Im} f = A_2$*:*

Միջուկը չի կարող լինել ենթաօղակ A_1*-ում, որովհետև* $f(1) = 1$ *և* $1 \notin \ker f$*: Սակայն* $(\ker f, +) \le (A_1, +)$*, քանի որ միջուկը նաև խմբերի հոմոմորֆիզմի միջուկն է և ենթախումբ է* A_1*-ում: Միջուկի համար տեղի ունի մի շատ կարևոր պայման, որն ավելի ուժեղ է քան ենթաօղակի սահմանման 3-րդ պայմանը (փակ լինելն ըստ բազմապատկման).*

$$a \in \ker f,\ x \in A_1 \Rightarrow ax \in \ker f,\ xa \in \ker f \qquad (31)$$

Իսկապես, $f(ax) = f(a) f(x) = 0 \cdot f(x) = 0$*: Այլ կերպ ասած,* միջուկը պարունակում է իր տարրերի բոլոր պատիկները:

Անդրադառնանք հոմոմորֆիզմի կառուցվածքին:

Դիցուք $f : A \to \mathrm{Im}f$ արտապատկերումն օղակային հոմոմորֆիզմ է: Քանի որ այն նաև խմբային հոմոմորֆիզմ է գումարման գործողության նկատմամբ, ապա համաձայն իզոմորֆիզմի մասին թեորեմի ստանում ենք, որ $(A/\ker f, +)$ ֆակտոր-խումբն իզոմորֆ է $(\mathrm{Im}f, +)$ պատկերին: Ինչպես գիտենք, $A/\ker f$ ֆակտոր-խմբի տարրերն ըստ $\ker f$-ի հարակից դասերն են, այսինքն՝

$$a + \ker f = \{a + x \mid x \in \ker f\}$$

բազմությունները: Ցույց տանք, որ այդ դասերը ոչ միայն կարելի է գումարել, այլ նաև կարելի է բազմապատկել:

Սահմանենք հարակից դասերի արտադրյալը հետևյալ բնական եղանակով. $(a + \ker f)(b + \ker f) \equiv ab + \ker f$: Ստուգենք այս սահմանման կոռեկտությունը: Դիցուք $a_1 \in a + \ker f$, $b_1 \in b + \ker f$: Ապացուցենք, որ $a_1 b_1 \in ab + \ker f$: Ունենք, որ $a_1 - a \in \ker f$ և $b_1 - b \in \ker f$: Հետևաբար,

$$a_1 b_1 - ab = a_1 b_1 - a_1 b + a_1 b - ab = a_1(b_1 - b) + (a_1 - a)b$$

և համաձայն (31)-ի $a_1(b_1 - b) \in \ker f$, $(a_1 - a)b \in \ker f$: Ուստի՝

$$a_1 b_1 - ab = a_1(b_1 - b) + (a_1 - a)b \in \ker f$$

և

$$a_1 b_1 \in ab + \ker f:$$

Այսպիսով (31) պայմանը թույլ տվեց սահմանել հարակից դասերի բազմապատկումը: Հասարակ վարժություն է ստուգել, որ $A/\ker f$ ֆակտոր-խումբը հանդիսանում է օղակ հարակից դասերի գումարման և բազմապատկման նկատմամբ: Այդ օղակը կանվանենք **ֆակտոր-օղակ** և պարզ է, որ զրոյական տարրը դա

$0+\ker f = \ker f$-ն է, իսկ մեկը՝ $1+\ker f$-ն է:

Հիշենք, որ $(A/\ker f,+)$ *ֆակտոր-խմբի և* $(\mathrm{Im} f,+)$ *պատկերի իզոմորֆիզմն իրականացվում է մի* g *արտապատկերմամբ, որը սահմանվում է հետևյալ կերպ.* $g(a+\ker f) = f(a)$*: Քանի որ սա խմբերի իզոմորֆիզմ է, ապա*

$$g((a_1+\ker f)+(a_2+\ker f)) = g(a_1+\ker f)+g(a_2+\ker f),$$

$$g(0+\ker f) = g(\ker f) = f(0) = 0:$$

Համոզվենք այժմ, որ g*-ն նաև օղակային իզոմորֆիզմ է՝* $g(1+\ker f) = f(1) = 1$ *և*

$$g((a_1+\ker f)(a_2+\ker f)) = g(a_1a_2+\ker f) =$$

$$f(a_1a_2) = f(a_1)f(a_2) = g(a_1+\ker f)g(a_2+\ker f):$$

Այսպիսով ապացուցեցինք հետևյալ պնդումը.

Թեորեմ 18.

$f: A_1 \to A_2$ օղակային հոմոմորֆիզմի դեպքում $A_1/\ker f$ ֆակտոր-օղակն իզոմորֆ է $\mathrm{Im} f$ պատկերին:

Իդեալներ

Սահմանում. A օղակի B ենթաբազմությունը կոչվում է **ձախ իդեալ**, եթե

1. $(B,+) \le (A,+)$ - այսինքն, ըստ գումարման B-ն A-ի ենթախումբն է

2. $BA \subseteq B$, որտեղ $BA \equiv \{ax \mid a \in B,\ x \in A\}$

Նման եղանակով սահմանվում են աջ և երկկողմանի իդեալները: Ոչ էական մանրամասների մեջ չխորանալու համար այսուհետև կդիտարկենք միայն տեղափոխելի օղակները և **օղակ** անվանումը կնշանակի **տեղափոխելի օղակ**: Դա մեզ թույլ կտա միավորել ձախ, աջ և երկկողմանի իդեալների դեպքերը, քանի որ տեղափոխելի օղակների համար այդ երեք գաղափարները համընկնում են: Այդ պատճառով այսուհետև կօգտագործենք **իդեալ** անվանումը:

Կամայական A օղակ ունի առնվազն երկու իդեալ՝ A-ն և $\{0\}$-ն: Այս իդեալները կոչվում են **տրիվիալ** իդեալներ, մնացած բոլորը՝ **ոչ տրիվիալ**:

Պնդում 19.

Դիցուք B-ն A օղակի իդեալն է և գոյություն ունի $a \in B$, որն ունի հակադարձ ըստ բազմապատկման: Այդ դեպքում $B = A$:

Իրոք, $1 = aa^{-1} \in B$ համաձայն իդեալի սահմանման 2. կետի, ուրեմն, համաձայն նույն 2. կետի, B-ին է պատկանում նաև 1-ի *կամայական պատիկը, այսինքն կամայական $x \in A$ համար $x = 1 \cdot x \in B$, ուստի և $B = A$:*

Հետևանք.

Դաշտն ունի միայն տրիվիալ իդեալներ:

Օրինակներ

1. ***Դիտարկենք ամբողջ թվերի $\mathbb{Z}$ օղակը: Ինչպես գիտենք, ըստ գումարման ենթախմբերն են բոլոր $m\mathbb{Z} \equiv \{mx \mid x \in \mathbb{Z}\}$ տեսքի բազմությունները: Եթե $mx \in m\mathbb{Z}$ և $n \in \mathbb{Z}$, ապա $(mx)n = m(xn)$, որտեղ $xn \in \mathbb{Z}$: Ուրեմն, $m\mathbb{Z}$-ը իդեալ է:***

2. *Դիցուք A-ն դաշտ է: Նշանակենք $A[x]$-ով x փոփոխականի այն բազմանդամների օղակը, որոնց գործակիցները A-ից են: Դիցուք $\alpha \in A$: Նշանակենք $F(\alpha) \equiv \{f \in A[x] \mid f(\alpha) = 0\}$: Այսինքն, $F(\alpha)$-ն բոլոր բազմանդամների բազմությունն է, որոնց համար α-ն արմատ է: Դյուրին է ստուգել, որ $F(\alpha)$-ն իդեալ է $A[x]$-ում:*

3. *Դիցուք A-ն օղակ է և $a_1, a_2, \ldots, a_n \in A$: Նշանակենք $(a_1, a_2, \ldots, a_n)$-ով հետևյալ բազմությունը՝*

$$\{a_1x_1 + a_2x_2 + \ldots + a_nx_n \mid x_1, x_2, \ldots, x_n \in A\}:$$

$(a_1, a_2, \ldots, a_n)$-ը իդեալ է A-ում:

Ինչպես տեսանք նախորդ բաժնում՝ օղակային հոմոմորֆիզմի միջուկն իդեալ է: Փաստորեն իդեալ լինելը համարժեք է հոմոմորֆիզմի միջուկ լինելուն (այսինքն իդեալները խաղում են նորմալ ենթախմբերի դերն օղակների դեպքում):

Դիցուք B-ն A օղակի իդեալն է: Դիտարկենք $(A/B,+)$ ֆակտոր-խումբը (դիտարկելով միայն գումարման գործողությունը): Ճիշտ այնպես, ինչպես վարվեցինք միջուկի ուսումնասիրման դեպքում նախորդ բաժնում սահմանվում է հարակից դասերի արտադրյալը՝ $(a+B)(b+B) \equiv ab+B$ և ստուգվում է այդ սահմանման կոռեկտությունը: Ակնհայտ է, որ A/B-ն դառնում է օղակ (տեղափոխելի): Այսպիսով տեսնում ենք, որ եթե B-ն A օղակի իդեալն է, ապա A/B-ն օղակ է, այսինքն $(a+B)(b+B) \equiv ab+B$ բանաձևով սահմանվում է բազմապատկումը A/B-ում: Տեղի ունի նաև հակառակ պնդումը. եթե A օղակի որևէ B ենթաբազմության համար (որը հանդիսանում է ենթախումբ ըստ բազմապատկման) $(a+B)(b+B) \equiv ab+B$ բանաձևը սահմանում է հարակից դասերի արտադրյալ և A/B-ն օղակ է, ապա B-ն A օղակի իդեալն է: Բավական է ստուգել իդեալի սահմանման 2. կետը: Դիցուք $a \in B$ և $x \in A$: Ունենք, որ $(a+B)(x+B) \equiv ax+B$: Սակայն $a+B = B$ դասը A/B օղակի զրոն է, հետևաբար $ax+B$-ն էլ հավասար է զրոյի, այսինքն՝ $ax+B = B$: Քանի որ $ax+B = B \Leftrightarrow ax \in B$ ստանում ենք, որ $a \in B$ և $x \in A \Rightarrow ax \in B$ և իդեալի սահմանման 2. կետը ստույգ է:

Դիցուք այժմ B-ն A օղակի իդեալն է: Խմբերի դեպքի նման կառուցենք հետևյալ **կանոնական հոմոմորֆիզմը**.

$$f : A \to A/B$$
$$f(a) = a+B$$

Գտնենք f-ի միջուկը.

$$a \in \ker f \Leftrightarrow f(a) = 0+B \Leftrightarrow a+B = B \Leftrightarrow a \in B:$$

Այսպիսով, $\ker f = B$ և յուրաքանչյուր իդեալ հանդիսանում է օղակային հոմոմորֆիզմի միջուկ:

Մաքսիմալ և պարզ իդեալներ

Սահմանում. A օղակի B իդեալը կոչվում է **մաքսիմալ**, եթե այն բանից, որ C-ն նույնպես իդեալ է A-ում և $B \subset C$ հետևում է, որ $C = A$:

A օղակի B իդեալը կոչվում է **պարզ**, եթե տեղի ունի հետևյալը՝ $ab \in B \Rightarrow a \in B$ կամ $b \in B$:

Փաստորեն մաքսիմալ իդեալը դա այնպիսի իդեալ է, որը հնարավոր չէ ընդգրկել մեկ այլ ոչ տրիվիալ իդեալի մեջ:

Պարզ իդեալի գաղափարը բացահայտելու համար ներմուծենք մի նոր և շատ կարևոր օղակների դաս:

Սահմանում. A օղակը կոչվում է **ամբողջ**, եթե $ab = 0 \Rightarrow a = 0$ կամ $b = 0$:

Կամայական դաշտ ամբողջ օղակ է: Ամբողջ թվերի և որևէ դաշտից գործակիցներով բազմանդամների օղակներն ամբողջ են: Ամբողջ չեն մնացքների դասերի օղակները բաղադրյալ մոդուլի դեպքում(տեսեք օրինակ 2-ը օղակների սահմանումից հետո բերված օրինակներում): Ամբողջ չեն նաև մատրիցների օղակները՝

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Արտագրենք այժմ պարզ իդեալի սահմանման պայմանը հետևյալ կերպ.

$$ab + B = B \Rightarrow a + B = B \text{ կամ } b + B = B$$

Սա իր հերթին համարժեք է

$$(a+B)(b+B) = 0+B \Rightarrow a+B = 0+B \text{ կամ } b+B = 0+B$$

պայմանին: Անցնելով A/B ֆակտոր-օղակին ստանում ենք, որ B-ն պարզ իդեալ է միայն և միայն այն դեպքում երբ A/B-ն ամբողջ է:

Թեորեմ 20.

Մաքսիմալ իդեալը պարզ է:

Ապացույց. Դիցուք B-ն A օղակի մաքսիմալ իդեալն է և $ab \in B$: Եթե $a \in B$, ուրեմն B-ն պարզ է: Դիցուք $a \notin B$: Ցույց տանք, որ այդ դեպքում $b \in B$:

Կառուցենք $\{a\} \cup B$ բազմությունը պարունակող փոքրագույն իդեալը A-ում: Այդ իդեալը պետք է առնվազն պարունակի բոլոր ax տեսքի տարրերը կամայական $x \in A$ համար: Նաև այն պետք է պարունակի բոլոր $ax+y$ տեսքի տարրերը, որտեղ $y \in B$: Դիտարկենք $\{ax+y \mid x \in A, \quad y \in B\}$ բազմությունը, որը կնշանակենք C-ով: Ստուգենք, որ C-ն իդեալ է A-ում: Նախ ստուգենք, որ C-ն ենթախումբ է ըստ գումարման՝

$$(ax_1+y_1)-(ax_2+y_2) = a(x_1-x_2)+(y_1-y_2) \in C,$$

քանի որ $y_1-y_2 \in B$ (B-ն իդեալ է): Իդեալի սահմանման երկրորդ պայմանը ստուգելու համար դիտարկենք $(ax+y)z$, որտեղ $ax+y \in C$ իսկ $z \in A$: Ունենք՝ $(ax+y)z = a(xz)+yz$: Սակայն ակնհայտ է, որ $xz \in A$ և $yz \in B$, քանի որ B-ն իդեալ է և $y \in B$: Ուստի, $(ax+y)z \in C$ և C-ն իդեալ է A-ում:

Պարզ է, որ $B \subseteq C$, քանի որ B-ի բոլոր տարրերը ստացվում են, եթե $ax+y$-ի մեջ տեղադրենք $x=0$ բոլոր $y \in B$ համար: Նաև պարզ է, որ $a \in C$, քանզի $a \cdot 1+0 \in C$: Ըստ ենթադրության $a \notin B$, ուրեմն $B \subset C$: Բայց B-ն մաքսիմալ իդեալ է, հետևաբար $C = A$ և $1 \in C$: Կգտնվեն $x_0 \in A$ և $y_0 \in B$ այնպիսին, որ $1 = ax_0+y_0$:

Բազմապատկենք վերջին հավասարությունը b-ով՝ $b = abx_0 + by_0$: Ունենք, որ $ab \in B$, ուրեմն $abx_0 \in B$, քանի որ B-ն իդեալ է: Նույն պատճառով էլ $by_0 \in B$ և $b = abx_0 + by_0 \in B$: Ստացանք, որ $b \in B$ և թեորեմն ապացուցված է:

Թեորեմ 21.

Որպեսզի A օղակի B իդեալը լինի մաքսիմալ, անհրաժեշտ է և բավարար, որ A/B ֆակտոր-օղակը լինի դաշտ:

Ապացույց. Նախ ճշտենք, թե ինչ է նշանակում A/B-ի դաշտ լինելը: A/B-ն տեղափոխելի օղակ է, ուստի այն դաշտ է միայն եթե ամեն մի ոչ զրոյական տարր ունի հակադարձ ըստ բազմապատկման: A/B-ի ոչ զրոյական տարրերն են $a + B$ տեսքի այն հարակից տարրերը, որոնց համար $a \notin B$: Այն, որ $a + B$-ն ունի հակադարձ, նշանակում է, որ կգտնվի մեկ այլ $b + B$ հարակից դաս, որ $(a + B)(b + B) = 1 + B$: Սակայն $(a + B)(b + B) = ab + B$, ուրեմն $ab + B = 1 + B$ և սա համարժեք է հետևյալ պայմանին՝

$$(\forall a \notin B)(\exists b)\ ab - 1 \in B:$$

Այսպիսով թեորեմի պնդումը համարժեք է հետևյալին.

$$B \text{ իդեալը մաքսիմալ է} \Leftrightarrow (\forall a \notin B)(\exists b)\ ab - 1 \in B$$

Սկզբից ապացուցենք առաջին մասը՝ B իդեալը մաքսիմալ է $\Rightarrow (\forall a \notin B)(\exists b)\ ab - 1 \in B$:

Դիցուք $a \notin B$: Կառուցենք հետևյալ իդեալը՝

$$C = \{ax + y \mid x \in A, y \in B\}:$$

Թեորեմ 20-ում ապացուցել ենք, որ C-ն իդեալ է և $B \subset C$: Քանի որ B-ն մաքսիմալ է, ապա $C = A$ և կգտնվեն $x_0 \in A$, $y_0 \in B$, այնպես որ $1 = ax_0 + y_0$ ։ Հետևաբար, $ax_0 - 1 = -y_0 \in B$ և վերցնելով $b = x_0$ ապացուցում ենք թեորեմի պնդման առաջին մասը։

Այժմ ապացուցենք թեորեմի պնդման երկրորդ մասը՝

$(\forall a \notin B)(\exists b)\ ab - 1 \in B \Rightarrow B$ իդեալը մաքսիմալ է։

Դիցուք գոյություն ունի այնպիսի C իդեալ, որ $B \subset C$ և $a \in C \setminus B$։ Քանի որ $a \notin B$ գոյություն ունի b, որ $ab - 1 \in B$։ Սակայն $B \subset C$, ուստի $ab - 1 \in C$։ C-ն իդեալ է և $a \in C$, ուրեմն $ab \in C$ և վերջապես, $1 \in C$։ Համաձայն Պնդում 19-ի $C = A$ և B-ն մաքսիմալ իդեալ է։

Դիտարկենք Թեորեմ 21-ի մի շատ կարևոր մասնավոր դեպք։

Նախ պարզենք բազմանդամների օղակների իդեալների կառուցվածքը։

Դիցուք K-ն դաշտ է։ Նշանակենք $K[x]$-ով x փոփոխականի բոլոր բազմանդամների բազմությունը, որոնց գործակիցները K դաշտից են։ Ակնհայտ է, որ $K[x]$-ը տեղափոխելի օղակ է։ $f(x)$ բազմանդամի աստիճանը կնշանակենք ինչպես միշտ $\deg f(x)$-ով։ Եթե M-ն իդեալ է $K[x]$-ում և պարունակում է գոնե մեկ հաստ զրո աստիճանի բազմանդամ, ապա, հաշվի առնելով, որ ըստ բազմապատկման հակադարձ ունեն միայն զրոյական աստիճանի բազմանդամները, համաձայն Պնդում 19-ի ստացվում է, որ $M = K[x]$։ Մյուս ծայրահեղ դեպքն է, երբ $M = \{0\}$։ Դիցուք $M \neq K[x]$ և $M \neq \{0\}$։ Այս դեպքում M-ում կգտնվի դրական աստիճանի բազմանդամ և, հետևաբար, ամենափոքր դրական աստիճանի բազմանդամ։ Ամենափոքր դրական աստիճանի բազմանդամը միակը չէ, այն որոշված է համապատասխան գործակցի ճշտությամբ: Իսկապես իդեալի սահմանումից հետևում է, որ $f(x) \in M \Leftrightarrow \lambda f(x) \in M$, $\lambda \neq 0$: Որպեսզի որոշակի դարձնենք ամենափոքր դրական աստիճանի բազմանդամի ընտրությունը, կպայմանավորվենք վերցնել նորմավորված բազմանդամը, այսինքն այն բազմանդամը, որի x փոփոխականի ամենաբարձր աստիճանի գործակիցը 1 է: Նշանակենք $f(x)$-ով M իդեալի ամենափոքր դրական աստիճանի նորմավորված բազմանդամը: Եթե $0 \neq g(x) \in M$, ապա $\deg g(x) \geq \deg f(x)$: Բաժանենք $g(x)$-ը $f(x)$-ի վրա՝ $g(x) = f(x)h(x) + r(x)$: Դյուրին է տեսնել, որ համաձայն իդեալի սահմանման 2-րդ պայմանի $f(x)h(x) \in M$ և համաձայն 1-ին պայմանի $r(x) = g(x) - f(x)h(x) \in M$: Եթե $\deg r(x) > 0$, ապա $\deg r(x) < \deg f(x)$ և M-ը կպարունակի $f(x)$-ի աստիճանից փոքր դրական աստիճանի բազմանդամ, ինչն անհնար է: Ուստի, $r(x) = 0$ և $g(x)$-ը բաժանվում է $f(x)$-ի վրա առանց մնացորդի: Որեմն,

$$M = \{f(x)h(x) \mid h(x) \in K[x]\},$$

այսինքն իդեալը բաղկացած է ամենափոքր դրական աստիճանի նորմավորված բազմանդամի պատիկներից: Այսպիսի իդեալները (երբ բոլոր տարրերը մեկ տարրի պատիկներն են) կոչվում են **գլխավոր** իդեալներ, իսկ $f(x)$ բազմանդամը կոչվում է իդեալի **ծնորդ** կամ **ծնիչ**: Այն դեպքերում երբ $M = K[x]$ կամ $M = \{0\}$, իդեալները նույնպես գլխավոր են, քանի որ ծնված են համապատասխանաբար 1 և 0 բազմանդամներով:

Վերադառնանք Թեորեմ 21-ի մասնավոր դեպքին: Դիցուք $f(x)$-ն անվերածելի բազմանդամ է (այսինքն՝ $f(x) = g(x)h(x) \Rightarrow \deg g(x) = 0$ կամ $\deg h(x) = 0$) $K[x]$-ից: Դյուրին է տեսնել, որ հետևյալ բազմությունը՝ $(f) \equiv \{f(x)g(x) \mid g(x) \in K[x]\}$ մաքսիմալ իդեալ է $K[x]$-ում: Իսկապես տրիվիալ է, որ (f)-ը իդեալ է: Դիցուք այն պարունակվում է մեկ այլ իդեալի մեջ $(f) \subset M \subseteq K[x]$: Նշանակենք $g(x)$-ով M իդեալի ծնորդը՝ $M = (g)$: Պարզ է, որ $f(x) \in (g) = M$, ուրեմն $f(x) = g(x)h(x)$: Սակայն $f(x)$-ն անվերածելի է և կամ $\deg g(x) = 0$ կամ $\deg h(x) = 0$: Եթե $\deg h(x) = 0$, ապա $g(x) = f(x)h^{-1}(x) \in (f)$ և $g(x)$-ին պատիկ բազմանդամը կլինի պատիկ նաև $f(x)$-ին, իսկ դա կնշանակի, որ $(f) = M$, ինչն անհնար է: Ուրեմն, $\deg g(x) = 0$: Համաձայն պնդում 12-ի $(g) = M = K[x]$ և (f) իդեալը մաքսիմալ է: Կիրառենք այժմ Թեորեմ 14-ը (f) մաքսիմալ իդեալին՝ $K[x]/(f)$ ֆակտոր-օղակը դաշտ է: Ավելի մանրամասն ուսումնասիրենք $K[x]/(f)$ դաշտը: Ամեն մի հարակից դաս $K[x]/(f)$-ից ունի հետևյալ տեսքը

$$g(x) + (f) = \{g(x) + f(x)h(x) \mid h(x) \in K[x]\}:$$

Պարզ է, որ եթե $r(x)$-ը $g(x)$-ի $f(x)$-ի վրա բաժանելուց ստացված մնացորդն է, ապա $g(x) = f(x)s(x) + r(x)$ և

$$g(x) + f(x)h(x) = f(x)s(x) + r(x) + f(x)h(x) =$$

$$r(x) + f(x)(s(x) + h(x)):$$

Ուրեմն, $g(x) + (f) = r(x) + (f)$ և $K[x]/(f)$-ից յուրաքանչյուր հարակից դասում կարելի է ընտրել այնպիսի ներկայացուցիչ, որը կամ 0-ն է ((f)-ի դեպքում), կամ էլ մի բազմանդամ է, որի աստիճանը $f(x)$-ի աստիճանից փոքր է: Այսպիսով $K[x]/(f)$ դաշտի տարրերն են $r(x) + (f)$ հարակից դասերը, որտեղ $r(x)$-ը կամ 0-ն է կամ էլ $K[x]$-ի $f(x)$-ի աստիճանից փոքր աստիճան ունեցող կամայական բազմանդամ է: Այդ դաշտն ակնհայտորեն իզոմորֆ է հետևյալ ավելի մատչելի նկարագրություն ունեցող դաշտին: Դիցուք $n = \deg f(x)$: Նշանակենք $K_n[x]$-ով $K[x]$-ի բազմանդամների բազմությունը, որոնց աստիճանները փոքր են n-ից: Ակնհայտ է, որ $K[x]/(f)$ դաշտի տարրերի և $K_n[x]$-ի միջև կարելի է իրականացնել փոխմիարժեք համապատասխանեցում նույնացնելով $r(x)+(f)$ հարակից դասերը $r(x)$ բազմանդամներին: $K_n[x]$-ի վրա բնականորեն որոշվում են բազմանդամների ըստ $\mathrm{mod} f(x)$-ի գումարման և բազմապատկման գործողությունները, որոնք օղակի կառուցվածք են սահմանում $K_n[x]$-ի վրա: Վերը նշված փոխմիարժեք համապատասխանեցումն իրականացնում է իզոմորֆիզմ $K[x]/(f)$-ի և $K_n[x]$-ի միջև: Ուստի, $K_n[x]$-ը դաշտ է:

Կոնկրետացնելով Թեորեմ 21-ի վերը նկարագրված մասնավոր դեպքի գլխավոր իդեալի ծնորդի՝ $f(x)$ անվերածելի բազմանդամի տեսքը կարելի է լուծել մի շարք կարևորագույն խնդիրներ: Ստորև կդիտարկենք այդպիսի երեք օրինակ:

Օրինակ 1

Ինչպես հայտնի է $f(x) = x^2 + 1 \in \mathbb{R}[x]$ բազմանդամը (հիշենք, որ $\mathbb{R}$-ով նշանակել ենք իրական թվերի իսկ $\mathbb{C}$-ով կոմպլեքս թվերի դաշտերը) չունի իրական արմատ: Փորձենք Թեորեմ 21-ի օգնությամբ կառուցել իրական թվերի դաշտի այնպիսի ընդլայնում, որում x^2+1 բազմանդամը կունենա արմատ: Այդ նպատակով կառուցենք $K[x]/(f)$ և $K_n[x]$ դաշտերը, որոնք տվյալ դեպքում կլինեն $\mathbb{R}[x]/(x^2+1)$ և $\mathbb{R}_2[x]$ դաշտերը: Դյուրին է նկարագրել $\mathbb{R}_2[x]$-ի տարրերը: $\mathbb{R}_2[x] = \{a + bx \mid a, b \in \mathbb{R}\}$ և հաշվի առնելով $x^2 \equiv -1 \,\mathrm{mod}(x^2+1)$ առնչությունը օղակային գործողություններն ըստ $\mathrm{mod}(x^2+1)$-ի կատարվում են հետևյալ կերպ.

$$\begin{aligned}(a_1 + b_1x) + (a_2 + b_2x) &= (a_1 + a_2) + (b_1 + b_2)x \\ (a_1 + b_1x)(a_2 + b_2x) &= (a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)x\end{aligned} \tag{32}$$

Մյուս կողմից պարզ է, որ $\mathbb{R}$-ն իզոմորֆ է $\mathbb{R}_2[x]$-ի $a + 0x$ տեսքի բազմանդամների ենթադաշտին: Այսինքն $\mathbb{R}_2[x]$ դաշտը կարելի է դիտարկել որպես իրական թվերի դաշտի ընդլայնում և $y^2 + 1 \in \mathbb{R}_2[x][y]$: Այս նոր դաշտում $y^2 + 1$ բազմանդամն ունի երկու արմատ (պարզ է, որ ավելի շատ արմատ լինել չի կարող): Իսկապես, դիտարկենք $\mathbb{R}_2[x]$-ի հետևյալ տարրը՝ $0 + 1x$: Ճիշտ է, որ

$$(0 + 1x)^2 = (0 + 1x)(0 + 1x) \underbrace{=}_{\text{համաձայն } (31)} -1$$

և $(0 + 1x)^2 + 1 = 0$, այսինքն $0 + 1x$-ը $y^2 + 1$ (պարզ է որ նաև $x^2 + 1$) բազմանդամի արմատն է: Մյուս արմատը դա $0 - 1x$-ն է: Փաստորեն մենք կառուցեցինք կոմպլեքս թվերի $\mathbb{C}$ դաշտը, քանի որ ակնհայտ է, որ $a + bi \mapsto a + bx$ համապատասխանեցումը սահմանում է իզոմորֆիզմ $\mathbb{C}$-ի և $\mathbb{R}_2[x]$-ի միջև: Փոխարինելով x նշանը կեղծ միավորի i նշանով (32)-ը վերածվում է կոմպլեքս թվերի գումարման և բազմապատկման բանաձևերին: Այս օրինակը շատ ուսանելի է այն առումով, որ մեզ հաջողվեց բնական ձևով (առանց կեղծ միավորի որևէ վերացական գաղափար ներմուծելու և որպես դրա հիմնավորում բովանդակալից մեկնաբանություն փնտրելու) ընդլայնել իրական թվերի դաշտը, ստանալով կոմպլեքս թվերի դաշտը: Այսպիսով, մենք ստացանք միալար եղանակ թվային դաշտի այնպիսի ընդլայնման կառուցման համար, որում տվյալ արմատ չունեցող բազմանդամն ունի արմատներ:

Օրինակ 2

Այս օրինակում $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ (այստեղ $\mathbb{Q}$-ն ռացիոնալ թվերի դաշտն է): Պարզ է, որ $x^2 - 2$-ը չունի ռացիոնալ արմատ: Կիրառելով Թեորեմ 21-ը ստանում ենք $\mathbb{Q}$-ի $\mathbb{Q}_2[x] = \{a + bx \mid a, b \in \mathbb{Q}\}$ ընդլայնումը: Այս դաշտում գործողությունները կատարվում են հետևյալ կերպ (հաշվի առնելով $x^2 \equiv 2 \bmod (x^2-2)$ առնչությունը).

$$(a_1+b_1x)+(a_2+b_2x) = (a_1+a_2)+(b_1+b_2)x \tag{33}$$
$$(a_1+b_1x)(a_2+b_2x) = (a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)x$$

Դիտարկենք y^2-2 բազմանդամը: Այն ունի արմատ $\mathbb{Q}_2[x]$-ում $0+1x$ տարրը: **Ի**սկապես

$$(0+1x)(0+1x) \underbrace{=}_{\text{համաձայն (33)}} 2$$

և $(0+1x)^2-2=0$:

Փաստորեն, մենք կառուցեցինք $a+b\sqrt{2}$, $a,b \in \mathbb{Q}$ թվերի քառակուսային դաշտը (x-ը համապատասխանում է $\sqrt{2}$ նշանին): Այս օրինակում ևս, օգտվելով միալար եղանակից, կարողացանք ընդլայնել ռացիոնալ թվերի դաշտն այնպես, որ x^2-2 բազմանդամն ունենա արմատ և ելնելով ռացիոնալ թվերից ներմուծեցինք $\sqrt{2}$ իռացիոնալ թիվը:

Օրինակ 3

Թեորեմ 21-ի մեկ այլ կարևոր կիրառության օրինակ կտեսնենք վերջավոր դաշտերի կառուցման ժամանակ:

Քանորդների օղակներ և դաշտեր

Նախորդ օրինակներում տեսանք, թե ինչպես ենելով տրված օղակից կամ դաշտից Թեորեմ 21-ի օգնությամբ կարելի է կառուցել վերջիններիս ընդլայնումները: Դիտարկենք նման մի իրավիճակ: Դիցուք տրված է $2x-3 \in \mathbb{Z}[x]$ բազմանդամը: Ակնհայտ է, որ այդ բազմանդամը չունի արմատ $\mathbb{Z}$-ում: Սակայն այն ունի ռացիոնալ արմատ՝ $\frac{3}{2}$: Այժմ տեսնենք, թե ինչպես կարելի է ստանդարտ եղանակով կառուցել տրված օղակի ընդլայնումը մինչև դաշտ, մասնավորապես կառուցել ռացիոնալ թվերի դաշտը:

Դիցուք A-ն տեղափոխելի օղակ է և S-ն օղակի այնպիսի ենթաբազմություն է, որի համար $0 \notin S$, $1 \in S$ և

$$a,b \in S \Rightarrow ab \in S$$

պայմանը, այսինքն S-ը փակ է բազմապատկման նկատմամբ (այդպիսի բազմությունները ընդունված է անվանել **մոնոիդներ** կամ **կիսախմբեր**): $A \times S$ դեկարտյան արտադրյալի վրա ներմուծենք հետևյալ $\simeq$ համարժեքության հարաբերությունը.

$$(a,s) \simeq (b,t) \Leftrightarrow \exists p \in S, \text{ որ } p(at-bs) = 0$$

Սա իսկապես համարժեքության հարաբերություն է, քանի որ

1. $(a,s) \simeq (a,s)$
2. $(a,s) \simeq (b,t) \Rightarrow (b,t) \simeq (a,s)$
3. $(a,s) \simeq (b,t)$ և $(b,t) \simeq (c,r) \Rightarrow (a,s) \simeq (c,r)$

Առաջին երկու հատկությունները ակնհայտ են: Ապացուցենք երրորդը, ունենք $(a,s) \simeq (b,t)$ և $(b,t) \simeq (c,r) \Rightarrow \exists p,q \in S$, որ $p(at-bs) = 0$ և $q(br-ct) = 0$: Այստեղից բխում է, որ

$prq(at-bs)=0$ և $qsp(br-ct)=0$: Գումարելով վերջին երկու հավասարությունները ստանում ենք՝

$$pqt(ar-cs)=0 \Rightarrow (a,s)\simeq(c,r):$$

Նշանակենք $\frac{a}{s}$-ով (a,s)-ի համարժեքության դասը, իսկ $S^{-1}A$-ով համարժեքության դասերի բազմությունը:

$S^{-1}A$ բազմությունը կարելի է դարձնել օղակ, սահմանելով գումարման և բազմապատկման գործողություններ:

Սահմանենք գումարումը և բազմապատկումը հետևյալ բնական բանաձևերով.

$$\frac{a}{s}+\frac{b}{t}=\frac{at+bs}{st}$$
$$\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st}$$

Քանի որ գործ ունենք համարժեքության դասերի հետ, անհրաժեշտ է ստուգել գործողությունների կոռեկտությունը: Սկսենք գումարումից: Դիցուք $\frac{a}{s}=\frac{a_1}{s_1}$ և $\frac{b}{t}=\frac{b_1}{t_1}$: Ապացուցենք, որ $\frac{a}{s}+\frac{b}{t}=\frac{a_1}{s_1}+\frac{b_1}{t_1}$, այսինքն $\frac{at+bs}{st}=\frac{a_1t_1+b_1s_1}{s_1t_1}$: Ունենք, որ $\exists p,q\in S$ որ $p(as_1-a_1s)=0$ և $q(bt_1-b_1t)=0$: Հետևաբար, $pqtt_1(as_1-a_1s)=0$ և $pqss_1(bt_1-b_1t)=0$: Գումարելով վերջին հավասարումների աջ և ձախ մասերը կստանանք՝

$$0=pqtt_1as_1-pqtt_1a_1s+pqss_1bt_1-pqss_1b_1t=$$
$$pq((at+bs)s_1t_1-(a_1t_1+b_1s_1)st)\Rightarrow\frac{at+bs}{st}=\frac{a_1t_1+b_1s_1}{s_1t_1}$$

Բազմապատկման համար՝ $\frac{a}{s}=\frac{a_1}{s_1}$ և $\frac{b}{t}=\frac{b_1}{t_1}$ պայմաններից ստանում ենք, որ

$$\exists p,q\in S,\text{որ } p(as_1-a_1s)=0 \text{ և } q(bt_1-b_1t)=0:$$

Հետևաբար $pqbt_1(as_1 - a_1s) = 0$ և $pqa_1s(bt_1 - b_1t) = 0$: Գումարելով վերջին հավասարումների աջ և ձախ մասերը ստանում ենք՝

$$0 = pqabs_1t_1 - pqa_1bst_1 + pqa_1bst_1 - pqa_1b_1st =$$

$$pq(abs_1t_1 - a_1b_1st) \Rightarrow \frac{a}{s}\frac{b}{t} = \frac{a_1}{s_1}\frac{b_1}{t_1}:$$

Դյուրին է ստուգել, որ բազմապատկման համար ստույգ է $\frac{at}{st} = \frac{a}{s}$ կոտորակների կրճատման բանաձևը:

Վերցնելով $\frac{0}{1}$ և $\frac{1}{1}$ դասերը համապատասխանաբար որպես զրո և մեկ, դյուրին է համոզվել, որ $S^{-1}A$-ն տեղափոխելի օղակ է: Այն

կոչվում է **քանորդների օղակ**:

Դիտարկենք $\frac{a}{1}$ տեսքի տարրերից կազմված ենթաօղակը $S^{-1}A$-ում: Սահմանենք φ հոմոմորֆիզմը A-ից դեպի այդ ենթաօղակը որպես $\varphi(a) = \frac{a}{1}$: Այն դեպքում, երբ A օղակն ամբողջ է $\varphi(a) = \varphi(b) \Rightarrow \frac{a}{1} = \frac{b}{1} \Rightarrow a = b$ և φ հոմոմորֆիզմը փոխմիարժեքորեն ներդնում է A-ն $S^{-1}A$-ի մեջ: Այսինքն ամբողջ օղակի դեպքում A-ն կարելի է նույնացնել $S^{-1}A$-ում $\frac{a}{1}$ տեսքի տարրերից կազմված ենթաօղակի հետ և փաստորեն $S^{-1}A$-ն հանդիսանում է A օղակի ընդլայնում:

Եթե A ամբողջ օղակում վերցնենք $S = A \setminus \{0\}$, ապա $S^{-1}A$-ի բոլոր ոչ զրոյական տարրերը կունենան հակադարձներ ըստ բազմապատկման՝ $\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = \frac{1}{1}$: Ստանում ենք, որ այս դեպքում $S^{-1}A$-ն դաշտ է՝ **քանորդների դաշտ**, որը A օղակի ընդլայնում է: Մասնավոր դեպքում, երբ $A = \mathbb{Z}$ քանորդների դաշտը ռացիոնալ թվերի դաշտն է:

Գործողություններ իդեալների նկատմամբ

Դիցուք A-ն տեղափոխելի օղակ է իսկ B_1-ը և B_2-ը իդեալներ են A-ում:

Դյուրին է ստուգել, որ $B_1 \cap B_2$-ը իդեալ է A-ում: Ավելին, իդեալների կամայական B_i, $i \in I$ ընտանիքի համար $\bigcap_{i \in I} B_i$-ն իդեալ է:

Իդեալների արտադրյալ է կոչվում հետևյալ բազմությունը՝

$$B_1B_2 = \{x_1y_1 + \ldots + x_ny_n \mid n \in \mathbb{N},\ x_i \in B_1,\ y_i \in B_2,\ i = 1, \ldots, n\},$$

որտեղ $\mathbb{N}$-ը բնական թվերի բազմությունն է: Ստուգենք, որ B_1B_2-ը իդեալ է: Եթե $x_1y_1 + \ldots + x_ny_n \in B_1B_2$ և $z_1w_1 + \ldots + z_mw_m \in B_1B_2$, ապա նշանակելով

$$\bar{x}_i = \begin{cases} x_i, & i = 1, \ldots, n \\ -z_{i-n}, & i = n+1, \ldots, n+m \end{cases}$$

և

$$\bar{y}_i = \begin{cases} y_i, & i = 1, \ldots, n \\ -w_{i-n}, & i = n+1, \ldots, n+m \end{cases}$$

ստանում ենք՝

$$x_1y_1 + \ldots + x_ny_n - (z_1w_1 + \ldots + z_mw_m) = \bar{x}_1\bar{y}_1 + \ldots + \bar{x}_{n+m}\bar{y}_{n+m},$$

որտեղ $\bar{x}_i \in B_1$, $\bar{y}_i \in B_2$, $i = 1, \ldots, n+m$: Ուստի՝

$$x_1y_1 + \ldots + x_ny_n - (z_1w_1 + \ldots + z_mw_m) \in B_1B_2:$$

Մյուս կողմից, եթե

$$x_1y_1 + \ldots + x_ny_n \in B_1B_2$$

և $z \in A$, ապա

$$z(x_1y_1 + \ldots + x_ny_n) = (zx_1)y_1 + \ldots + (zx_n)y_n:$$

Քանի որ B_1-ը իդեալ է՝ $zx_i \in B_1,\ i = 1,,\ldots,n$: Ուրեմն՝

$$z(x_1y_1+\ldots+x_ny_n) = (zx_1)y_1+\ldots+(zx_n)y_n \in B_1B_2:$$

Իդեալների արտադրյալը միշտ ընկած է հատման մեջ.

$$B_1B_2 \subseteq B_1 \cap B_2 \tag{34}$$

Իսկապես, եթե $x_1y_1+\ldots+x_ny_n \in B_1B_2$ և $x_i \in B_1$, $y_i \in B_2$, $i = 1,\ldots,n$, ապա յուրաքանչյուր x_iy_i արտադրյալը պատկանում է թե B_1-ն և թե B_2-ն: Ուստի $x_1y_1+\ldots+x_ny_n$-ը պատկանում է և B_1-ն և B_2-ն, ուրեմն և $B_1 \cap B_2$-ն: Ակնհայտ է, որ (34) բանաձևը տեղի ունի նաև իդեալների կամայական վերջավոր ընտանիքի համար:

Իդեալների գումար է կոչվում հետևյալ բազմությունը՝

$$B_1+B_2 = \{x+y \mid x \in B_1,\ y \in B_2\}$$

որն իդեալ է: Իսկապես, եթե x_1+y_1-ը և x_2+y_2-ը պատկանում են B_1+B_2-ին, ապա

$$(x_1+y_1)-(x_2+y_2) =$$

$$\underbrace{(x_1-x_2)}_{\in B_1} + \underbrace{(y_1-y_2)}_{\in B_2} \in B_1+B_2:$$

Նաև եթե $x+y \in B_1+B_2$, ապա $z(x+y) = \underbrace{zx}_{\in B_1} + \underbrace{zy}_{\in B_2} \in B_1+B_2:$

Մնացքների մասին "չինական" թեորեմը

Թեորեմ 22.

Դիցուք A-ն տեղափոխելի օղակ է և $B_1, \dots, B_m$ իդեալները փոխադարձաբար պարզ են՝ այսինքն $i \neq j \Rightarrow B_i + B_j = A$: Նախապես ընտրված կամայական m հատ $y_1, \dots, y_m \in A$ տարրերից կազմված հավաքածուի համար գոյություն ունի $x \in A$ այնպիսին, որ $x - y_i \in B_i, i = 1, 2, \dots, m$:

Ապացույց. Թեորեմը կապացուցենք ինդուկցիայով ըստ m-ի:

Դիցուք $m = 2$: Քանի որ $B_1 + B_2 = A$ գոյություն ունեն $x_1 \in B_1$ և $x_2 \in B_2$ որ $x_1 + x_2 = 1$: Կառուցենք $x = x_1 y_2 + x_2 y_1$ տարրը և համոզվենք, որ x-ը բավարարում է թեորեմի պնդմանը: Իսկապես,

$$x - y_1 = x_1 y_2 + (x_2 - 1) y_1 = x_1 (y_2 - y_1) \in B_1:$$

Սիմետրիկությունից բխում է, որ $x - y_2 \in B_2$:

Դիցուք թեորեմի պնդումը ճիշտ է, եթե իդեալների քանակը փոքր է m-ից $(m > 2)$: Ապացուցենք թեորեմը m հատ իդեալների դեպքում:

Համաձայն թեորեմի պայմանների ունենք՝

$$\begin{cases} B_1 + B_2 = A \\ B_1 + B_3 = A \\ \quad \vdots \\ B_1 + B_m = A \end{cases}$$

և կգտնվեն $a_1, \dots, a_{m-1} \in B_1$, $b_1 \in B_2$, $b_2 \in B_3, \dots, b_{m-1} \in B_m$ այնպիսին, որ

$$\begin{cases} a_1+b_1 = 1 \\ a_2+b_2 = 1 \\ \vdots \\ a_{m-1}+b_{m-1} = 1 \end{cases}$$

Բազմապատկելով վերջին հավասարությունների աջ և ձախ մասերը ստանում ենք՝ $1=\prod_{i=1}^{m-1}(a_i+b_i)$: Վերջին արտադրյալի փակագծերը բացելով կստանանք a_i և b_j տարրերի արտադրյալների գումար, ընդ որում բոլոր արտադրյալները, բացի մեկից՝ $b_1b_2\dots b_{m-1}$-ից կպարունակեն առնվազն մեկ հատ a_i: Ակնհայտ է, որ բոլոր արտադրյալները, որ պարունակում են որևէ a_i տարր և, հետևաբար, դրանց գումարը պատկանում է B_1 իդեալին: Նշանակենք այդ գումարը a-ով: Մյուս կողմից $b_1b_2\dots b_{m-1}$ արտադրյալը պատկանում է $B_2B_3\dots B_m$ իդեալին, համաձայն իդեալների արտադրյալի սահմանման: Համաձայն (34) բանաձևի

$$B_2B_3\dots B_m \subseteq B_2\cap B_3\cap\dots\cap B_m$$

և

$$b_1b_2\dots b_{m-1}\in B_2\cap B_3\cap\dots\cap B_m:$$

Նշանակենք $b_1b_2\dots b_{m-1}$ արտադրյալը b-ով: Վերը շարադրվածից ստանում ենք, որ $1=a+b$, $a\in B_1$, $b\in B_2\cap B_3\cap\dots\cap B_m$: Սրանից բխում է, որ $B_1+B_2\cap B_3\cap\dots\cap B_m=A$ և թեորեմի պնդումը կիրառելի է B_1 և $B_2\cap B_3\cap\dots\cap B_m$ իդեալների դեպքում, քանի որ ինդուկտիվ ենթադրությամբ թեորեմը ճիշտ է, եթե փոխադարձաբար պարզ իդեալների քանակը՝ տվյալ դեպքում 2-ը փոքր է m-ից: Ընտրենք $y_1=1$ և $y_2=0$ տարրերը և կիրառենք թեորեմը 2 փոխադարձաբար պարզ B_1 և $B_2\cap B_3\cap\dots\cap B_m$ իդեալների *դեպքում կգտնվի x_1 այնպիսին, որ $x_1 - 1 \in B_1$ և $x_1 - 0 = x_1 \in B_2 \cap B_3 \cap \ldots \cap B_m$: Այսպիսով, մենք կառուցեցինք այնպիսի x_1 տարր, որ*

$$
\begin{cases}
x_1 - 1 \in B_1 \\
x_1 \in B_2 \\
x_1 \in B_3 \\
\vdots \\
x_1 \in B_m
\end{cases}
$$

Փոխարինելով հաջորդաբար B_1-ը B_2-ով, B_3-ով … վերը կիրառված եղանակով կկառուցենք $x_2, x_3, \ldots, x_m$ տարրերը, այնպես որ յուրաքանչյուր $i = 1, 2, \ldots, m$ համար տեղի ունի.

$$
\begin{cases}
x_i - 1 \in B_i \\
\forall j \neq i \quad x_i \in B_j
\end{cases}
\tag{35}
$$

Վերադառնանք թեորեմի ապացուցմանը m հատ իդեալների դեպքում: Օգտվելով կառուցված $x_1, x_2, x_3, \ldots, x_m$ և թեորեմի պայմաններում տրված $y_1, y_2, y_3, \ldots, y_m$ տարրերից կառուցենք $x = x_1 y_1 + x_2 y_2 + \ldots + x_m y_m$ տարրը և հաշվենք

$$
x - y_i = x_1 y_1 + x_2 y_2 + \ldots + x_m y_m - y_i = \sum_{\substack{j=1 \\ j \neq i}}^{m} x_j y_j + (x_i - 1) y_i
$$

Համաձայն (35)-ի $x_j \in B_i$, $\forall j \neq i$ և ուրեմն $\sum\limits_{\substack{j=1 \\ j \neq i}}^{m} x_j y_j \in B_i$: Նաև համաձայն (35)-ի $x_i - 1 \in B_i$ և $(x_i - 1) y_i \in B_i$: Այսինքն $x - y_i \in B_i$ յուրաքանչյուր $i \in \{1, 2, \ldots, m\}$ համար և թեորեմն ապացուցված է:

Հետևանք 1.

Նկատենք որ $\underbrace{A\times A\times\cdots\times A}_{m} = A^m$ դեկարտյան արտադրյալը հեշտությամբ կարելի է դարձնել տեղափոխելի օղակ, սահմանելով դրա տարրերի՝ $(y_1,y_2,\ldots,y_m)$ հավաքածուների նկատմամբ կորդինատ առ կորդինատ գումարման և բազմապատկման գործողությունները.

$$(y_1,y_2,\ldots,y_m)+(z_1,z_2,\ldots,z_m) = (y_1+z_1,y_2+z_2,\ldots,y_m+z_m)$$
$$(y_1,y_2,\ldots,y_m)\cdot(z_1,z_2,\ldots,z_m) = (y_1z_1,y_2z_2,\ldots,y_mz_m)$$

Դյուրին է ստուգել, որ բավարարված են օղակի սահմանման բոլոր պայմանները և A^m օղակի մեկն ու զրոն համապատասխանաբար $(1,1,\ldots,1)$ և $(0,0,\ldots,0)$ հավաքածուներն են:

Դիտարկենք այժմ $A\Big/\bigcap\limits_{i=1}^{m}B_i$ ֆակտոր-օղակը: Դիցուք տրված $(y_1,y_2,\ldots,y_m)$ հավաքածուին համապատասխանում են երկու տարրեր x_1 և x_2, որ բավարարում են թեորեմի պնդմանը.

$$x_1-y_i\in B_i,\ i=1,2,\ldots,m$$
$$x_2-y_i\in B_i,\ i=1,2,\ldots,m$$

Անմիջապես պարզ է, որ $x_1-x_2\in B_i,\ \ i=1,2,\ldots,m$ և ուրեմն՝ $x_1-x_2\in\bigcap\limits_{i=1}^{m}B_i$: Այսինքն, x_1-ը և x_2-ը համապատասխանում են տրված $(y_1,y_2,\ldots,y_m)$-ին, միայն և միայն այն դեպքում, երբ x_1-ը և x_2-ը պատկանում են միևնույն հարակից դասին ըստ $\bigcap\limits_{i=1}^{m}B_i$-ի: Մյուս կողմից

$$x-y_i\in B_i,\ i=1,2,\ldots,m \Leftrightarrow x-z_i\in B_i,\ i=1,2,\ldots,m,$$

որտեղ $y_i - z_i \in B_i, i = 1,2,\ldots,m$, այսինքն y_i-ն և z_i-ն միևնույն հարակից դասից են ըստ B_i:

Այսպիսով, ստանում ենք փոխմիարժեք համապատասխանեցում $A/\bigcap_{i=1}^{m} B_i$ և

$$(A/B_1)\times\ldots\times(A/B_m) = \prod_{i=1}^{m} A/B_i$$

օղակների միջև: Այդ համապատասխանումն իզոմորֆիզմ է: Իսկապես, դիցուք

$$f : A/\bigcap_{i=1}^{m} B_i \to \prod_{i=1}^{m} A/B_i,$$

որտեղ

$$f(x + \bigcap_{i=1}^{m} B_i) = (x + B_1,\ldots,x + B_m):$$

Կամայական

$$(y_1 + B_1,\ldots,y_m + B_m) \in \prod_{i=1}^{m} A/B_i$$

համար համաձայն Թեորեմ 22-ի գոյություն ունի $x \in A$ այնպիսին, որ $x + B_i = y_i + B_i$, $i = 1,2,\ldots,m$: Հետևաբար,

$$f(x + \bigcap_{i=1}^{m} B_i) = (x + B_1,\ldots,x + B_m) = (y_1 + B_1,\ldots,y_m + B_m):$$

Այսպիսով, կամայական տարր $\prod_{i=1}^{m} A/B_i$-ից ունի նախապատկեր (այդպիսի դեպքերում ասում են, որ f արտապատկերումը սուրյեկտիվ է):

Դիցուք $f(x + \bigcap_{i=1}^{m} B_i) = (B_1,\ldots,B_m)$: Պարզ է, որ

$$(x+B_1,\dots,x+B_m) = (B_1,\dots,B_m)$$

և $x+B_i = B_i,\ \ i=1,2,\dots,m$: Որտեղ, $x\in B_i,\ \ i=1,2,\dots,m$ և $x\in\bigcap_{i=1}^{m}B_i$: Հետևաբար, $\ker f=\bigcap_{i=1}^{m}B_i$ և f արտապատկերումը փոխմիարժեք է (ինյեկտիվ է): Ապացուցեցինք, որ f-ը փոխմիարժեքորեն արտապատկերում է $A/\bigcap_{i=1}^{m}B_i$-ը $\prod_{i=1}^{m}A/B_i$-ի վրա: Դյուրին է ստուգել, որ

$$f((x_1+\bigcap_{i=1}^{m}B_i)+(x_2+\bigcap_{i=1}^{m}B_i)) \ =f((x_1+x_2)+\bigcap_{i=1}^{m}B_i) =$$
$$((x_1+x_2)+B_1,\dots,(x_1+x_2)+B_m) =$$

$$((x_1+B_1)+(x_2+B_1),\dots,(x_1+B_m)+(x_2+B_m)) \ =$$
$$(x_1+B_1,\dots,x_1+B_m)+(x_2+B_1,\dots,x_2+B_m) =$$

$$f(x_1+\bigcap_{i=1}^{m}B_i)+f(x_2+\bigcap_{i=1}^{m}B_i)$$

և նմանապես՝

$$f((x_1+\bigcap_{i=1}^{m}B_i)(x_2+\bigcap_{i=1}^{m}B_i)) \ =f(x_1+\bigcap_{i=1}^{m}B_i)f(x_2+\bigcap_{i=1}^{m}B_i):$$

Այսպիսով ապացուցեցինք, որ վերը նշված f արտապատկերումը $A/\bigcap_{i=1}^{m}B_i$ և $\prod_{i=1}^{m}A/B_i$ օղակների իզոմորֆիզմ է:

Հետևանք 2.

Նախորդ հետևանքում սահմանված f արտապատկերումը կիրառենք $x^k+\bigcap_{i=1}^{m}B_i$ տարրին.

$$f(x^k + \bigcap_{i=1}^{m} B_i) = f((x + \bigcap_{i=1}^{m} B_i)^k) = (f(x + \bigcap_{i=1}^{m} B_i))^k =$$
$$(x + B_1, \dots, x + B_m)^k = (x^k + B_1, \dots, x^k + B_m):$$

Այսինքն, եթե $(y_1, y_2, \dots, y_m)$ հավաքածուին, ըստ Թեորեմ 22-ի, համապատասխանում է x տարրը, ապա $(y_1^k, y_2^k, \dots, y_m^k)$ հավաքածուին համապատասխանում է x^k-ն: Այս փաստն ունի նաև ուղղակի ապացույց: Ունենք $x - y_i \in B_i$, $i = 1, 2, \dots, m$: Օգտվենք հայտնի բանաձևից՝

$$x^k - y_i^k = (x - y_i) \sum_{j=1}^{k-1} x^{k-j} y_i^{j-1}$$

Քանի որ $x - y_i \in B_i$, ապա իդեալների սահմանումից հետևում է, որ

$$x^k - y_i^k = (x - y_i) \sum_{j=1}^{k-1} x^{k-j} y_i^{j-1} \in B_i, i = 1, 2, \dots, m:$$

Մնացքների մասին "չինական" թեորեմի որոշ մասնավոր դեպքեր

Թեորեմ 22-ի մասնավոր դեպքերն են ամբողջ թվերի և բազմանդամների համար հայտնի թեորեմները:

Դիցուք A օղակը դա ամբողջ թվերի $\mathbb{Z}$ օղակն է: Ինչպես գիտենք յուրաքանչյուր իդեալ $\mathbb{Z}$-ում ծնված է մեկ տարրով, այսինքն բաղկացած է որոշակի ամբողջ թվի բոլոր պատիկներից: Երկու իդեալների փոխադարձաբար պարզ լինելը համարժեք է իդեալների ծնիչների փոխադարձաբար պարզ լինելուն: Հետևաբար, եթե $B_i = \{k_i x \mid x \in \mathbb{Z}\}$, $i = 1,2,\dots,m$, ապա Թեորեմ 22-ի $i \neq j \Rightarrow B_i + B_j = A$ պայմանն ընդունում է $i \neq j \Rightarrow (\exists x_1, x_2 \in \mathbb{Z})$ $k_i x_i + k_j x_j = 1$ տեսքը, որն իր հերթին համարժեք է $i \neq j \Rightarrow (k_i, k_j) = 1$ պայմանին (այստեղ (k_i, k_j)-ն ամենամեծ ընդհանուր բաժանարարն է): Ուստի, ամբողջ թվերի դեպքում Թեորեմ 22-ն ընդունում է հետևյալ տեսքը.

Դիցուք $k_1, k_2, \dots, k_m$ թվերը փոխադարձաբար պարզ են: Կամայական $y_1, y_2, \dots, y_m$ թվերի հավաքածուի համար գոյություն ունի այնպիսի x թիվ, որ $x \equiv y_i \mod k_i$, $i = 1,2,\dots,m$:

Քանի որ բազմանդամների (որոնց գործակիցներն K դաշտից են) $K[x]$ օղակում իդեալները ծնվում են մեկ տարրի միջոցով (իդեալի ամենափոքր դրական աստիճանի բազմանդամով), ապա իդեալների փոխադարձաբար պարզ լինելը այս դեպքում ևս համարժեք է *իդեալների ծնիչների փոխադարձաբար պարզ լինելուն: Թեորեմ 22-ը շարադրվում է հետևյալ կերպ.*

Դիցուք $f_1(x), f_2(x), \dots, f_m(x)$ ***փոխադարձաբար պարզ բազմանդամներ են*** $K[x]$ ***օղակում: Կամայական*** $h_1(x), h_2(x), \dots, h_m(x) \in K[x]$ ***բազմանդամների համար գոյություն ունի այնպիսի*** $g(x) \in K[x]$ ***բազմանդամ, որ*** $g(x) \equiv h_i(x) \bmod f_i(x)$, $i = 1, 2, \dots, m$:

Դիտարկենք Թեորեմ 22-ի մեկ այլ ուշագրավ մասնավոր դեպք $K[x]$ *օղակի համար: Ֆիքսենք իրարից տարբեր* m *հատ* K *դաշտի տարրեր՝* $a_1, a_2, \dots, a_n$: *Նշանակենք* $f_i(x) = x - a_i$, $i = 1, 2, \dots, m$ *և* $f(x) = \prod_{i=1}^{m}(x - a_i)$: *Ակնհայտ է, որ բոլոր* $f_i(x)$ *բազմանդամները փոխադարձաբար պարզ են: Ֆիքսենք այժմ* K *դաշտի որևէ* $b_1, b_2, \dots, b_m$ *տարրեր, որոնց կդիտարկենք որպես բազմանդամներ: Համաձայն Թեորեմ 22-ի գոյություն ունի* $g(x) \in K[x]$, *որ* $g(x) \equiv b_i \bmod (x - a_i)$, $i = 1, 2, \dots, m$: *Սակայն պարզ է նաև (Բեզուի թեորեմից), որ* $g(x) \equiv g(a_i) \bmod (x - a_i)$, *ուստի*

$$g(a_i) = b_i,\ i = 1, 2, \dots, m \tag{36}$$

Այս դեպքում հետևանք 1-ում դիտարկված $\bigcap_{i=1}^{m} B_i$ *իդեալը դա* $f(x) = \prod_{i=1}^{m}(x - a_i)$ *բազմանդամով ծնված իդեալն է, այսինքն*

$$\bigcap_{i=1}^{m} B_i = \{f(x)q(x) \mid q(x) \in K[x]\}$$

և համաձայն Հետևանք 1-ի $g(x)$-ը միակն է $\bigcap_{i=1}^{m} B_i$ ճշտությամբ, այսինքն բոլոր բազմանդամները, որոնք բավարարում են (36) պայմանին հետևյալ տեսքի են՝ $g(x)+f(x)q(x)$ և պատկանում են $g(x)$-ի հարակից դասին ըստ $f(x)$-ի $K[x]$ օղակում: Վերցնելով այդ հարակից դասի կամայական բազմանդամ և բաժանելով այն $f(x)$-ի վրա մնացորդում կստանանք նույն հարակից դասի մեկ այլ բազմանդամ, որի աստիճանը փոքր է $f(x)$-ի աստիճանից՝ m-ից: Այդ բազմանդամը բավարարում է (36) պայմանին և $g(x)$-ի հարակից դասի միակ m-ից փոքր աստիճանի բազմանդամն է (եթե լինեին այդպիսի երկու տարբեր բազմանդամներ, ապա $f(x)$-ի վրա բաժանելուց ստացված դրանց մնացորդները պետք է իրար համընկնեին, բայց այդ մնացորդները համընկնում են հենց դրանց հետ, քանի որ դրանց աստիճանները փոքր են $f(x)$-ի աստիճանից): Ուստի (36) պայմանին բավարարող m-ից փոքր աստիճանի բազմանդամը միակն է: Դա նշանակում է, որ m տարբեր կետերում տրված արժեքները ընդունող m-ից փոքր աստիճանի բազմանդամը միակն է:

Մնացքների մասին "չինական" թեորեմի մի կիրառության մասին

Դիցուք $K[x]$-ը x փոփոխականից կախված K դաշտից գործակիցներով բազմանդամների օղակն է: Դիցուք x^m-1 բազմանդամն ունի K դաշտում m հատ տարբեր արմատներ: Հայտնի է, որ այդ դեպքում բոլոր այդ արմատների բազմությունը կազմում է ցիկլիկ խումբ ըստ բազմապատկման, այսինքն գոյություն ունի մեկ ω արմատ, որ x^m-1 բազմանդամի բոլոր տարբեր արմատները դա ω-ի աստիճաններն են՝ $1,\omega,\omega^2,\ldots,\omega^{m-1}$ և $x^m-1=\prod_{i=0}^{m-1}(x-\omega^i)$: Նշանակենք $K_m[x]$-ով $K[x]$-ի այն բազմանդամների ենթաբազմությունը, որոնց աստիճանը փոքր է m թվից: Սահմանենք $\mathcal{F}$ արտապատկերումը $K_m[x]$-ից $K^m=K\times K\times\ldots\times K$ դեկարտյան արտադրյալի վրա հետևյալ կերպ.

$$\mathcal{F}(f(x)) = (f(1),f(\omega),\ldots,f(\omega^{m-1})) \tag{37}$$

Վերը նկարագրված Թեորեմ 22-ի բազմանդամների համար մասնավոր դեպքից հետևում է, որ $\mathcal{F}$ արտապատկերումը փոխմիարժեք է: Սա թույլ է տալիս դիտարկել հակադարձ արտապատկերումը՝ $\mathcal{F}^{-1}$-ը:

Դիցուք $f(x),g(x)\in K_m[x]$: Պարզ է, որ

$$\mathcal{F}(f(x)) = (f(1),f(\omega),\ldots,f(\omega^{m-1}))$$

և

$$\mathcal{F}(g(x)) = (g(1),g(\omega),\ldots,g(\omega^{m-1})):$$

Հետևանք 1-ից ստանում ենք, որ

$$\mathcal{F}^{-1}((f(1)g(1),f(\omega)g(\omega),\ldots,f(\omega^{m-1})g(\omega^{m-1}))) =$$

$$f(x)g(x)\bmod(x^m-1)\text{։}$$

Դիցուք $f(x)=\sum_{i=0}^{m-1}a_ix^i$ և $g(x)=\sum_{i=0}^{m-1}b_ix^i$։ Դյուրին է ստուգել, որ ըստ բազմանդամների բազմապատկման սահմանման

$$f(x)g(x)=\sum_{i=0}^{m-1}(\sum_{j=0}^{i}a_jb_{i-j})x^i+\sum_{i=0}^{m-1}(\sum_{j=i+1}^{m-1}a_jb_{m+i-j})x^{i+m},\tag{38}$$

որտեղ $b_m=0$։

Քանի որ $x^m\equiv 1\bmod(x^m-1)$, ապա (37)-ում փոխարինելով x^m-ը 1-ով կստանանք

$$f(x)g(x)\bmod(x^m-1)=\sum_{i=0}^{m-1}(\sum_{j=0}^{i}a_jb_{i-j}+\sum_{j=i+1}^{m-1}a_jb_{m+i-j})x^i\tag{39}$$

Նման եղանակով ստացվում է.

$$f(x)g(x)\bmod(x^m+1)=\sum_{i=0}^{m-1}(\sum_{j=0}^{i}a_jb_{i-j}-\sum_{j=i+1}^{m-1}a_jb_{m+i-j})x^i\tag{40}$$

Դիցուք գոյություն ունի $\psi\in K$ որ $\psi^2=\omega$ և $\psi^m=-1$։ Պարզ է, որ $\psi^{2m}=\omega^m=1$ և $\psi^{-1}=\psi^{2m-1}$։

Սահմանենք $f_\psi(x)=\sum_{i=0}^{m-1}(\psi^ia_i)x^i$ և $g_\psi(x)=\sum_{i=0}^{m-1}(\psi^ib_i)x^i$։

Համաձայն (38)-ի

$$f_\psi(x)g_\psi(x)=\sum_{i=0}^{m-1}(\sum_{j=0}^{i}\psi^ja_j\psi^{i-j}b_{i-j})x^i+\sum_{i=0}^{m-1}(\sum_{j=i+1}^{m-1}\psi^ja_j\psi^{m+i-j}b_{m+i-j})x^{i+m}$$

և

$$f_\psi(x)g_\psi(x)=\sum_{i=0}^{m-1}\psi^i(\sum_{j=0}^{i}a_jb_{i-j})x^i+\sum_{i=0}^{m-1}\psi^{m+i}(\sum_{j=i+1}^{m-1}a_jb_{m+i-j})x^{i+m},$$

ապա

$$f_\psi(x)g_\psi(x)\,\mathrm{mod}(x^m-1) = \sum_{i=0}^{m-1}\psi^i(\sum_{j=0}^{i}a_jb_{i-j}-\sum_{j=i+1}^{m-1}a_jb_{m+i-j})x^i \qquad (41)$$

Նկատենք, որ $\deg f(x) = \deg g(x) = m-1$ դեպքում բազմանդամների (38) բանաձևով $f(x)g(x)$ արտադրյալի գործակիցները հաշվելու համար K դաշտում անհրաժեշտ գործողությունների (գումարումների և բազմապատկումների) քանակը $O(m^2)$ կարգի է:

Նշանակենք $F(m)$-ով $\mathcal{F}$ արտապատկերումը և դրա հակադարձը հաշվելու համար K դաշտում կատարվելիք գործողությունների քանակը: Վերը ստացված (38)-(41) բանաձևերը թույլ են տալիս հաշվել $f(x)g(x)$ արտադրյալը կիրառելով $\mathcal{F}$ և $\mathcal{F}^{-1}$ արտապատկերումները: Իսկապես, սկզբից կհաշվենք

$$\mathcal{F}(f(x)) = (f(1), f(\omega), \dots, f(\omega^{m-1}))$$

և

$$\mathcal{F}(g(x)) = (g(1), g(\omega), \dots, g(\omega^{m-1}))$$

կատարելով $2F(m)$ գործողություն: Ապա կատարելով m հատ բազմապատկում կհաշվենք

$$(f(1)g(1), f(\omega)g(\omega), \dots, f(\omega^{m-1})g(\omega^{m-1}))$$

վեկտորը: Հետո կհաշվենք

$$\mathcal{F}^{-1}((f(1)g(1), \dots, f(\omega^{m-1})g(\omega^{m-1}))) = f(x)g(x)\,\mathrm{mod}(x^m-1)$$

կատարելով $F(m)$ գործողություն:

Կատարելով ոչ ավելի քան $2m$ բազմապատկում կկառուցենք $1, \psi, \psi^2, \dots, \psi^{2m-1}$ տարրերը (այսինքն բոլոր $1, \psi, \psi^2, \dots, \psi^{m-1}$ տարրերը և դրանց հակադարձները): Դրանից հետո կկառուցենք $f_\psi(x)$ և $g_\psi(x)$ բազմանդամները կատարելով ոչ ավելի քան $2m$ բազմապատկում: Կիրառելով $\mathcal{F}$-ը կստանանք $\mathcal{F}(f_\psi(x))$ և $\mathcal{F}(g_\psi(x))$ վեկտորները կատարելով $2F(m)$ գործողություն: Կորդինատ առ կորդինատ կբազմապատկենք այդ վեկտորները և կկիրառենք $\mathcal{F}^{-1}$-ը, ստանալով $f_\psi(x)g_\psi(x)\bmod(x^m-1)$-ը: Դրա համար կկատարվի $m+F(m)$ գործողություն:

Համանման (40) և (41) բանաձևերի $f(x)g(x)\bmod(x^m+1)$-ը տարբերվում է $f_\psi(x)g_\psi(x)\bmod(x^m-1)$-ից միայն ψ^i գործակիցներով: Բազմապատկենք $f_\psi(x)g_\psi(x)\bmod(x^m-1)$-ի գործակիցները ψ^{2m-i} տարրերով, որ նախապես հաշվել էինք, և կստանանք $f(x)g(x)\bmod(x^m+1)$-ը: Դրա համար կծախսենք m բազմապատկում: Հիմնվելով (38), (39) և (40) բանաձևերի վրա, դյուրին է տեսնել, որ $f(x)g(x)$ բազմանդամի առաջին m գործակիցները համընկնում են

$$\frac{1}{2}\left(f(x)g(x)\bmod(x^m-1)+f(x)g(x)\bmod(x^m+1)\right)$$

բազմանդամի գործակիցների հետ, իսկ մնացած գործակիցները

$$\frac{1}{2}\left(f(x)g(x)\bmod(x^m-1)-f(x)g(x)\bmod(x^m+1)\right)$$

բազմանդամի գործակիցների հետ: Ուստի, կատարելով ևս ոչ ավելի քան $2(m+1)$ գործողություն, իվերջո, կստանանք $f(x)g(x)$ բազմանդամի բոլոր գործակիցները: Ընդհանուր գործողությունների քանակը կլինի $O(F(m)+m)$: Սակայն ակնհայտ է, որ $F(m)\geq m$ և, ուրեմն, $f(x)g(x)$-ը հաշվելու համար կկատարենք $O(F(m))$ գործողություն:

Օգտվելով x^m-1 բազմանդամի արմատների հատուկ հատկություններից, կառուցվել է հատուկ ալգորիթմ, որի օգնությամբ $\mathcal{F}$ և $\mathcal{F}^{-1}$ արտապատկերումները հաշվարկվում են կատարելով $O(m\ln m)$ գործողություն: Դա թույլ է տալիս հաշվել $f(x)g(x)$ արտադրյալը շատ ավելի արագ, քան համանման բազմանդամների արտադրյալի սահմանման բանաձևի, երբ ծախսվում է $O(m^2)$ գործողություն:

$\mathcal{F}$ և $\mathcal{F}^{-1}$ արտապատկերումները հայտնի են որպես Ֆուրյեի դիսկրետ ուղիղ և հակադարձ ձևափոխություններ, իսկ դրանց հաշվման ալգորիթմը՝ Ֆուրյեի արագ ձևափոխություն: Ֆուրյեի արագ ձևափոխությունը նաև ընկած է մեծ թվերի բազմապատկման մինչ օրս հայտնի լավագույն ալգորիթմի հիմքում(Շյոնհագեի և Շտրասենի ալգորիթմ):

Գլխավոր իդեալների օղակներ

Սահմանում: A տեղափոխելի օղակի տարրը կոչվում է **միավոր**, եթե այն ունի հակադարձ ըստ բազմապատկման գործողության: Միավորների բազմությունը նշանակվում է A^*-ով:

Ամբողջ թվերի օղակում միակ միվորները դրանք ± 1 տարրերն են: $\mathbb{R}[x]$ բազմանդամների օղակի միավորներն են բացառապես բոլոր զրո աստիճանի բազմանդամները, այսինքն ոչ զրոյական հաստատունները:

Սահմանում: A տեղափոխելի օղակի B իդեալը կոչվում է **գլխավոր**, եթե այն ծնված է մեկ տարրով

$$B = (a) = \{ax \mid x \in A\}$$

իսկ a տարրը կոչվում է **իդեալի ծնիչ**:

Սահմանում: A տեղափոխելի օղակը, որի բոլոր իդեալները գլխավոր են կոչվում է **գլխավոր իդեալների օղակ**:

Սահմանում: A տեղափոխելի օղակի $p \neq 0$ տարրը կոչվում է **անվերածելի**, եթե $p \notin A^*$ և տեղի ունի

$$p = ab \Rightarrow \text{կամ } a \in A^* \text{ կամ } b \in A^*$$

Պնդում 23.

- **Եթե p-ն անվերածելի է, ապա անվերածելի է նաև εp-ն կամայական $\varepsilon \in A^*$ համար:**

Իսկապես, ակնհայտ է, որ $\varepsilon p \notin A^*$: Եթե $\varepsilon p = ab$, ապա

$p = a(b\varepsilon^{-1})$ և կամ $a \in A^*$ կամ $b\varepsilon^{-1} \in A^*$։ Սակայն $b\varepsilon^{-1} \in A^*$ պայմանը համարժեք է $b \in A^*$ պայմանին, ուստի εp-ն անվերածելի է։

- **Եթե ամբողջ օղակում $p \notin A^*$, $p \neq 0$ տարրով ծնված (p) իդեալը պարզ է, ապա p-ն անվերածելի է։**

Եթե $p = ab$, ապա $ab \in (p)$ և a և b տարրերից առնվազն մեկը պատկանում է (p) իդեալին։ Դիցուք դա a-ն է՝ $a = px$ որոշակի $x \in A$ համար։ Որեմն, $p = pxb$ և $p(1 - xb) = 0$։ Օղակն ամբողջ է, որեմն, $1 - xb = 0$ և $b \in A^*$։

- **Եթե p-ն անվերածելի է գլխավոր իդեալների օղակում, ապա (p) իդեալը մաքսիմալ է (նաև պարզ)։**

Դիցուք (p) իդեալը պարունակվում է մեկ այլ (q) իդեալում և $(p) \neq (q)$։ Որեմն $\exists x$, որ $p = qx$։ Քանի որ p-ն անվերածելի է, ապա կամ $q \in A^*$ կամ $x \in A^*$։ Եթե $x \in A^*$, ապա $q = px^{-1}$ և $(p) = (q)$ ինչն անհնար է։ Եթե $q \in A^*$, ապա $(q) = A$ և (p) իդեալը մաքսիմալ է։

Երկու p և q տարրերը կանվանենք **ասոցիացված**, եթե $\exists(\varepsilon \in A^*)$, որ $p = \varepsilon q$։ Պարզ է, որ ասոցիացվածության հարաբերությունը սահմանում է համարժեքության հարաբերություն օղակի անվերածելի տարրերի բազմության վրա, տրոհելով այն չհատվող համարժեքության դասերի՝ երկու անվերածելի տարր մեկ դասից են միայն և միայն, եթե դրանք ասոցիացված են։ Ակնհայտ է, որ ասոցիացված տարրերը ծնում են միևնույն իդեալը։

Ամբողջ թվերի օղակում միակ անվերածելի տարրերը պարզ թվերն են, ընդ որում p և $-p$ պարզ թվերն ասոցիացված են։

Բազմանդամների $\mathbb{R}[x]$ օղակում անվերածելի տարրերը դրանք անվերածելի բազմանդամներն են:

Ասում են, որ տեղափոխելի օղակի B իդեալը ծնված է a և b տարրերով, եթե $B = \{ax + by \mid x, y \in A\}$: Դյուրին է ստուգել, որ $\{ax + by \mid x, y \in A\}$ բազմությունն իդեալ է: Մենք կօգտագործենք (a, b) նշանակումը $\{ax + by \mid x, y \in A\}$ իդեալի համար:

Նաև կասենք, որ ամբողջ օղակի a տարրը բաժանվում է b տարրի վրա, եթե կգտնվի այնպիսի c, որ $a = bc$: Այդ փաստը կարձանագրենք հետևյալ կերպ՝ $b \vdots a$: Սահմանենք **ամենամեծ ընդհանուր բաժանարարի** գաղափարը. a և b տարրերի ամենամեծ ընդհանուր բաժանարար է կոչվում այդ տարրերի այն ընդհանուր բաժանարարը, որն բաժանվում է դրանց կամայական այլ ընդհանուր բաժանարարի վրա:

Պնդում 24.

Դիցուք A-ն գլխավոր իդեալների օղակ է: a և b տարրերով ծնված իդեալը գլխավոր է և գոյություն ունի $c \in A$, որ $(c) = (a, b)$: c-ն a և b տարրերի ամենամեծ ընդհանուր բաժանարարն է:

Ապացույց. Ակնհայտ է, որ կգտնվի $c \in A$, որ $(c) = (a, b) = \{ax + by \mid x, y \in A\}$: Տեղադրելով $x = 1$, $y = 0$ կստանանք որ $a \in (c)$: Նմանապես՝ $b \in (c)$: Ուստի $c \vdots a$ և $c \vdots b$ և c-ն a և b տարրերի ընդհանուր բաժանարարն է:

Դիցուք $d \vdots a$ և $d \vdots b$: Այսինքն, կգտնվեն e և f այնպիսին, որ $a = de$ և $b = df$: Քանի որ $c \in (a, b)$, ապա գոյություն ունեն x_0 և y_0, որ

$c = ax_0 + by_0$: Այստեղից անմիջապես ստացվում է $c = ax_0 + by_0 = d(ex_0 + fy_0)$ և $d \vdots c$: Պնդումն ապացուցված է:

Օրինակներ

1. Դիցուք $\mathbb{Z}$-ն ամբողջ թվերի օղակն է: Ինչպես գիտենք, $\mathbb{Z}$-ի կամայական ոչ տրիվիալ ենթախումբ ըստ գումարման կազմված է որոշակի տարրի (ամենափոքր դրական տարրի) բոլոր պատիկներից: Ուստի յուրաքանչյուր իդեալ լինելով ենթախումբ ըստ գումարման գլխավոր է:

2. Դիցուք $K[x]$-ը K դաշտից գործակիցներով բազմանդամների օղակն է: Դիցուք B-ն իդեալ է $K[x]$-ում: Եթե $B = K[x]$ կամ էլ $B = \{0\}$, ապա ակնհայտորեն B-ն գլխավոր է: Դիցուք B-ն պարունակում է առնվազն մեկ դրական աստիճանի բազմանդամ (հակառակ դեպքում կամ $B = K[x]$ կամ էլ $B = \{0\}$): Նշանակենք $f(x)$-ով B-ում պարունակվող ամենափոքր դրական աստիճանի բազմանդամներից որևէ մեկը: Դիցուք $g(x) \in B$: Բաժանենք $g(x)$-ը $f(x)$-ի վրա՝ $g(x) = f(x)h(x) + r(x)$: Պարզ է, որ $r(x) = g(x) - f(x)h(x) \in B$: Եթե $r(x) \neq 0$, ապա $0 \leq deg\, r(x) < deg f(x)$: Սակայն $deg\, r(x) > 0$, քանի որ եթե $deg\, r(x) = 0$, ապա $B = K[x]$: Ուրեմն $0 < deg\, r(x) < deg f(x)$: Բայց իդեալում չկա դրական աստիճանի բազմանդամ, որի աստիճանը փոքր է $deg f(x)$-ից: Ուստի $r(x) = 0$ և $g(x) = f(x)h(x)$: Ակնհայտ է, որ $B = (f(x)) = \{f(x)h(x) \mid h(x) \in K[x]\}$ գլխավոր իդեալ է:

3. Դիտարկենք

$$\mathbb{Z}[\sqrt{-1}\,] = \{x + y\sqrt{-1} \mid x, y \in \mathbb{Z}\}$$

բազմությունը: Դյուրին է ստուգել, որ այն ամբողջ տեղափոխելի օղակ է կոմպլեքս թվերի գումարման ու բազմապատկման նկատմամբ: Այդ օղակը կոչվում է

Գաուսյան ամբողջ թվերի օղակ: Ապացուցենք, որ այն գլխավոր իդեալների օղակ է: Նախ ցույց տանք, որ $\mathbb{Z}[\sqrt{-1}]$-ում հնարավոր է սահմանել մնացորդով բաժանում: Նշանակենք $|\alpha|$-ով $\alpha = x + y\sqrt{-1}$ թվի նորմը՝ $|\alpha| = x^2 + y^2$: Դյուրին է ստուգել, որ $\|\alpha\beta\| = \|\alpha\|\|\beta\|$ և $\|\alpha\| = 0 \Leftrightarrow \alpha = 0$: Դիցուք $\alpha, \beta \in \mathbb{Z}[\sqrt{-1}]$ և $\beta \neq 0$: Բաժանենք α-ն β-ի վրա որպես հասարակ կոմպլեքս թվեր՝ $\alpha = \beta\gamma$: Եթե $\gamma \notin \mathbb{Z}[\sqrt{-1}]$, ապա վերցնենք $\in \mathbb{Z}[\sqrt{-1}]$, որի իրական և կեղծ մասերը γ-ի իրական և կեղծ մասերի մոտակա ամբողջ թվերն են: Պարզ է, որ $\|\gamma - \hat{\gamma}\| \leq \frac{1}{4}$: Վերցնենք $\delta = \alpha - \beta\hat{\gamma} \in \mathbb{Z}[\sqrt{-1}]$: Ունենք

$$\delta = \alpha - \beta\hat{\gamma} = \beta\gamma - \beta\hat{\gamma} = \beta(\gamma - \hat{\gamma})$$

և $\|\delta\| = \|\beta\|\|\gamma - \hat{\gamma}\| < \|\beta\|$: Այսպիսով ստացանք մնացորդով բաժանում $\mathbb{Z}[\sqrt{-1}]$-ում՝ $\alpha = \beta\hat{\gamma} + \delta$, որտեղ կամ $\delta = 0$ կամ էլ $0 \leq \|\delta\| < \|\beta\|$: Դիցուք այժմ B-ն իդեալ է $\mathbb{Z}[\sqrt{-1}]$-ում և $B \neq \{0\}$: Նշանակենք β-ով B-ի ամենափոքր դրական նորմ ունեցող տարրերից մեկը: Դիցուք $\alpha \in B$: Բաժանենք մնացորդով α-ն β-ի վրա՝ $\alpha = \beta\hat{\gamma} + \delta$: Պարզ է, որ $\delta = \alpha - \beta\hat{\gamma} \in B$: Եթե $\delta \neq 0$, ապա $0 < \|\delta\| < \|\beta\|$ և ստացվում է, որ B-ն պարունակում է մի տարր, որի նորմը դրական է և փոքր է $\|\beta\|$-ից: Ուստի $\delta = 0$, $\alpha = \beta\hat{\gamma}$ և $B = (\beta) = \{\beta\gamma \mid \gamma \in \mathbb{Z}[\sqrt{-1}]\}$ գլխավոր իդեալ է:

4. Դիտարկենք

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{\frac{a}{2} + \frac{b}{2}\sqrt{-19} \mid a, b \in \mathbb{Z}, a \equiv b \bmod 2\right\}$$

բազմությունը: $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ն ամբողջ տեղափոխելի օղակ է կոմպլեքս թվերի գումարման և բազմապատկման նկատմամբ: Իրոք,

$$\left(\frac{a}{2} + \frac{b}{2}\sqrt{-19}\right)\left(\frac{c}{2} + \frac{d}{2}\sqrt{-19}\right) \stackrel{def}{=}$$

$$\frac{1}{4}(ac - 19bd) + \frac{1}{4}(ad + bc)\sqrt{-19} =$$

$$\frac{(ac-19bd)/2}{2} + \frac{(ad+bc)/2}{2}\sqrt{-19},$$

այստեղ $(ac-19bd)/2$ և $(ad+bc)/2$ ամբողջ թվեր են, քանի որ $a \equiv b \bmod 2$, $c \equiv d \bmod 2$ պայմաններից բխում է՝

$$ac \equiv 19bd \bmod 2, ad \equiv bc \bmod 2,$$

և $ac-19bd$ ու $ad+bc$ թվերը զույգ են: Նաև $\frac{ac-19bd}{2} \equiv \frac{ad+bc}{2} \bmod 2$: Իսկապես, դա համարժեք է $ac-19bd-ad-bc \equiv 0 \bmod 4$ պայմանին, որի ճշտությունը դառնում է ակնհայտ, եթե ձախ մասը վերարտագրենք որպես

$$ac-20bd+bd-ad-bc = (a-b)(c-d)-20bd:$$

Եթե $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, ապա դրա կոմպլեքս համալուծը՝ $\bar{\alpha}$-ն նույնպես պատկանում է $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ին, քանի որ $a \equiv b \bmod 2 \Leftrightarrow a \equiv (-b) \bmod 2$:

Սահմանենք $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ տարրի նորմը ստանդարտ եղանակով որպես $\|\alpha\| = \alpha\bar{\alpha} = \frac{a^2}{4} + 19\frac{b^2}{4}$: Դյուրին է ստուգել, որ $\|\alpha\beta\| = \|\alpha\|\|\beta\|$: Նաև $\|\alpha\| \in \mathbb{Z}$: Քանի որ a-ն ու b-ն միևնույն զույգության են, ապա

$$a^2 \equiv b^2 \equiv \begin{cases} 0 \bmod 4, & a\text{-ն ու } b\text{-ն զույգ են} \\ 1 \bmod 4, & a\text{-ն ու } b\text{-ն կենտ են} \end{cases}$$

և ամեն դեպքում $a^2 + 19b^2 \equiv 0 \bmod 4$, ուստի $\|\alpha\| \in \mathbb{Z}$:

Ցույց տանք այժմ, որ

$$\forall \alpha, \beta \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right], \beta \neq 0 \text{ համար, եթե } \alpha\text{-ն չի}$$
$$\text{բաժանվում } \beta\text{-ի վրա և } \|\beta\| \leq \|\alpha\|, \text{ ապա} \qquad (42)$$
$$\exists \gamma, \delta \text{ այնպիսի, որ } 0 < \|\alpha\gamma - \beta\delta\| < \|\beta\|:$$

Հիմնվելով (42)-ի վրա դյուրին է համոզվել, որ

$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ը գլխավոր իդեալների օղակ է: Իսկապես, դիցուք ոչ տրիվիալ իդեալ է և $0 \neq \beta \in B$ տարրն ունի նվազագույն դրական նորմը B-ում: Դիցուք $\alpha \in B$ և չի բաժանվում β-ի վրա: Ակնհայտ է, որ $\alpha \neq 0$ և $\|\beta\| \leq \|\alpha\|$: Կգտնվեն γ, δ այնպիսի, որ $0 < \|\alpha\gamma - \beta\delta\| < \|\beta\|$: Քանի որ $\alpha, \beta \in B$, ապա $\alpha\gamma - \beta\delta \in B$: Նաև քանի որ $0 < \|\alpha\gamma - \beta\delta\|$, ապա $\alpha\gamma - \beta\delta \neq 0$: Ուստի B-ում գտանք ոչ զրոյական տարր $\alpha\gamma - \beta\delta$, որի նորմը փոքր է β-ի նորմից, ինչն անհնար է:

Այժմ ապացուցենք (42) պնդումը: Դիցուք $\alpha, \beta \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, $\beta \neq 0$, α-ն չի բաժանվում β-ի վրա և $\|\beta\| \leq \|\alpha\|$: Քանի որ β-ն միավոր չէ ստանում ենք՝ $\|\beta\| > 1$ (եթե β-ն միավոր է, ապա $\beta\beta^{-1} = 1$ և $\|\beta\|\|\beta^{-1}\| = 1$, ուստի $\|\beta\| = 1$): Նշանակենք՝ $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{-19}$ և $\beta = \frac{c}{2} + \frac{d}{2}\sqrt{-19}$: Դյուրին է հաշվել β-ի սովորական կոմպլեքս հակադարձը: Ունենք $\|\beta\| = \beta\bar{\beta}$ և

$$\beta^{-1} = \frac{1}{\|\beta\|}\bar{\beta} = \frac{1}{\|\beta\|}\left(\frac{c}{2} - \frac{d}{2}\sqrt{-19}\right):$$

Այժմ

$$\frac{\alpha}{\beta} = \frac{1}{\|\beta\|}\left(\frac{a}{2} + \frac{b}{2}\sqrt{-19}\right)\left(\frac{c}{2} - \frac{d}{2}\sqrt{-19}\right) =$$

$$\frac{1}{\|\beta\|}\left(\frac{m}{2} + \frac{n}{2}\sqrt{-19}\right),$$

որտեղ

$$\frac{m}{2} + \frac{n}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

(այսինքն՝ $m \equiv n \bmod 2$) և

$$\frac{1}{\|\beta\|}\left(\frac{m}{2} + \frac{n}{2}\sqrt{-19}\right) \notin \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]:$$

Նշանակենք՝ $x = \frac{m}{2\|\beta\|}$, $y = \frac{n}{2\|\beta\|}$: Ստանում ենք՝ $\frac{\alpha}{\beta} = \frac{x}{2} + \frac{y}{2}\sqrt{-19} \notin \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$: Սա նշանակում է, որ կամ x-ը կամ y-ը ամբողջ չեն, կամ էլ դրանք ամբողջ են, բայց

$x \equiv y \bmod 2$ բաղդատումը սխալ է, ինչ համարժեք է $\frac{x-y}{2} \notin \mathbb{Z}$ պայմանին: Ապացուցենք, որ կգտնվեն $\gamma, \delta \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$, որ $0 < \left\| \frac{\alpha}{\beta}\gamma - \delta \right\| < 1$, հետևաբար՝

$$0 < \|\alpha\gamma - \beta\delta\| < \|\beta\|:$$

Նշանակենք $\{a\}$-ով a իրական թվին մոտակա ամբողջ թիվը, ընդ որում, եթե $a = m + \frac{1}{2}$, ապա $\{a\} = m$:

Դեպք 1: $y \in \mathbb{Z}$, $\frac{x-y}{2} \notin \mathbb{Z}$

Ունենք

$$\frac{\alpha}{\beta} = \frac{x}{2} + \frac{y}{2}\sqrt{-19} = \frac{x-y}{2} + \frac{y}{2} + \frac{y}{2}\sqrt{-19}:$$

Վերցնենք $\gamma = 1$ և $\delta = \frac{2\left\{\frac{x-y}{2}\right\}+y}{2} + \frac{y}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$: Ստանում ենք, որ $\frac{\alpha}{\beta}\gamma - \delta = \frac{x-y}{2} - \left\{\frac{x-y}{2}\right\} \neq 0$ և

$$\left\| \frac{\alpha}{\beta}\gamma - \delta \right\| \leq \left(\frac{x-y}{2} - \left\{ \frac{x-y}{2} \right\} \right)^2 \leq \frac{1}{4} < 1$$

Դեպք 2: $y \notin \mathbb{Z}$, $\frac{x-y}{2} \in \mathbb{Z}$

Ենթադեպք 2.1: $5y \in \mathbb{Z}$

Պարզ է, որ $y = m + \frac{i}{5}$, $i = 1,2,3,4$ և

$$\{y\} = \begin{cases} m, & i = 1,2 \\ m+1, & i = 3,4 \end{cases}:$$

Ուստի՝ $|y - \{y\}| \in \left\{\frac{1}{5}, \frac{2}{5}\right\}$: Պարզ է նաև, որ $x - y$-ը զույգ թիվ է: Վերցնենք $\gamma = 1$ և

$$\delta = \frac{x - y + \{y\}}{2} + \frac{\{y\}}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]:$$

Ստանում ենք՝

$$\frac{\alpha}{\beta}\gamma - \delta = \frac{y - \{y\}}{2} + \frac{y - \{y\}}{2}\sqrt{-19} \neq 0$$

և

$$\left\| \frac{\alpha}{\beta}\gamma - \delta \right\| = \frac{(y - \{y\})^2}{4} + \frac{(y - \{y\})^2}{4}19 =$$

$$5(y-\{y\})^2 \leq 5 \times \frac{4}{25} < 1:$$

Ենթադեպք 2.2: $5y \notin \mathbb{Z}$

Վերցնենք $\gamma = \frac{1}{2} - \frac{1}{2}\sqrt{-19}$ *: Կստանանք՝*

$$\frac{\alpha}{\beta}\gamma = \left(\frac{x}{2} + \frac{y}{2}\sqrt{-19}\right)\left(\frac{1}{2} - \frac{1}{2}\sqrt{-19}\right) =$$

$$\frac{\frac{x-y}{2} + 10y}{2} - \frac{\frac{x-y}{2}}{2}\sqrt{-19}:$$

Վերցնենք

$$\delta = \frac{\frac{x-y}{2} + 2\{5y\}}{2} - \frac{\frac{x-y}{2}}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

և $\frac{\alpha}{\beta}\gamma - \delta = 5y - \{5y\} \neq 0$*: Ուրեմն՝*

$$\left\|\frac{\alpha}{\beta}\gamma - \delta\right\| = (5y - \{5y\})^2 \leq \frac{1}{4} < 1$$

Դեպք 3: $y \notin \mathbb{Z}$, $\frac{x-y}{2} \notin \mathbb{Z}$

Ենթադեպք 3.1: $2y \in \mathbb{Z}$, $x - y \in \mathbb{Z}$

Ունենք՝ $2y \in \mathbb{Z} \Rightarrow y = m + \frac{1}{2} \Rightarrow 5y = 5m + \frac{5}{2} \notin \mathbb{Z}$ *և* $5y - \{5y\} = \frac{1}{2}$*: Պարզ է, որ* $x - y$*-ը կենտ է: Դիցուք* $x - y = 2k + 1$*: Ստանում ենք՝*

$$x + y = 2k + 1 + 2\left(m + \frac{1}{2}\right) = 2(k + m + 1)$$

և $x + y$*-ը զույգ է: Վերցնենք* $\gamma = \frac{1}{2} + \frac{1}{2}\sqrt{-19}$*, ապա*

$$\frac{\alpha}{\beta}\gamma = \left(\frac{x}{2} + \frac{y}{2}\sqrt{-19}\right)\left(\frac{1}{2} + \frac{1}{2}\sqrt{-19}\right) =$$

$$\frac{\frac{x+y}{2} - 10y}{2} + \frac{\frac{x+y}{2}}{2}\sqrt{-19}$$

և

$$\delta = \frac{\frac{x+y}{2} - 2\{5y\}}{2} + \frac{\frac{x+y}{2}}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

Ստանում ենք՝

$$\frac{\alpha}{\beta}\gamma - \delta = \{5y\} - 5y = -\frac{1}{2} \neq 0$$

և վերջապես՝

$$\left\| \frac{\alpha}{\beta}\gamma - \delta \right\| = (\{5y\} - 5y)^2 = \frac{1}{4} < 1$$

Ենթադեպք 3.2: $2y \in \mathbb{Z}, x - y \notin \mathbb{Z}$

Ունենք

$$2y \in \mathbb{Z} \Rightarrow y = m + \frac{1}{2} \Rightarrow 2y = 2m + 1:$$

Վերցնենք $\gamma = 2$, ապա $\frac{\alpha}{\beta}\gamma = \frac{2x}{2} + \frac{2y}{2}\sqrt{-19}$:

Կգտնվի ամբողջ p, որ $p \leq x \leq p + 1$, ուստի $2p \leq 2x \leq 2p + 2$ և $|2x - (2p+1)| \leq 1$:

Վերցնենք

$$\delta = \frac{2p+1}{2} + \frac{2y}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$$

Պարզ է, որ $\frac{\alpha}{\beta}\gamma - \delta = \frac{2x-(2p+1)}{2} \neq 0$, քանի որ, եթե $2x = 2p + 1$, ապա $x - y = p - m \in \mathbb{Z}$ ինչն անհնար է:

Վերջապես ստանում ենք՝

$$\left\| \frac{\alpha}{\beta}\gamma - \delta \right\| = \frac{(2x - (2p+1))^2}{4} \leq \frac{1}{4} < 1$$

Ենթադեպք 3.3: $2y \notin \mathbb{Z}$

Ունենք $y \notin \mathbb{Z}$ և $y \neq m + \frac{1}{2}$: Կգտնվի ամբողջ p, որ $p < y < p + 1$: Եթե $p < y \leq p + \frac{1}{3}$ կամ $p + \frac{2}{3} \leq y < p + 1$, ապա $|y - \{y\}| \leq \frac{1}{3}$: Եթե $p + \frac{1}{3} < y < p + \frac{2}{3}$, ապա

$$2p + \frac{2}{3} < 2y < 2p + 1 + \frac{1}{3}, \{2y\} = 2p + 1$$

և $|2y - \{2y\}| \leq \frac{1}{3}$:

Դիտարկենք տեղի ունի $p < y \leq p + \frac{1}{3}$ կամ $p + \frac{2}{3} \leq y < p + 1$ դեպքը: Կգտնվի ամբողջ k որ $k \leq x < k + 1$: Սահմանենք՝

$$z = \begin{cases} k, & k \equiv \{y\} \bmod 2 \\ k+1, & k+1 \equiv \{y\} \bmod 2 \end{cases}$$

Պարզ է, որ $|z - x| \le 1$: Վերցնենք $\gamma = 1$ և

$$\delta = \frac{z}{2} + \frac{\{y\}}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]:$$

Ստանում ենք՝

$$\frac{\alpha}{\beta}\gamma - \delta = \frac{x-z}{2} + \frac{y-\{y\}}{2}\sqrt{-19} \neq 0$$

քանի որ $y \notin \mathbb{Z}$: Վերջապես

$$\left\| \frac{\alpha}{\beta}\gamma - \delta \right\| = \frac{(x-z)^2}{4} + \frac{19(y-\{y\})^2}{4} \le$$

$$\frac{1}{4} + \frac{1}{9} \times \frac{19}{4} = \frac{7}{9} < 1:$$

Այժմ դիտարկենք $p + \frac{1}{3} < y < p + \frac{2}{3}$ դեպքը: Կգտնվի ամբողջ k որ $k \le x < k+1$: Սահմանենք z-ը հետևյալ կերպ: Եթե $\{2y\}$-ը զույգ է, ապա

$$z = \begin{cases} 2k, & 2k \le 2x \le 2k+1 \\ 2k+2, & 2k+1 < 2x < 2k+2 \end{cases}$$

Եթե $\{2y\}$-ը կենտ է, ապա $z = 2k+1$: Բոլոր դեպքերում ՝ $|z - 2x| \le 1$:

Վերցնենք $\gamma = 2$ և

$$\delta = \frac{z}{2} + \frac{\{2y\}}{2}\sqrt{-19} \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]:$$

Ստանում ենք՝

$$\frac{\alpha}{\beta}\gamma - \delta = \frac{2x-z}{2} + \frac{2y-\{2y\}}{2}\sqrt{-19} \neq 0$$

քանի որ $2y \notin \mathbb{Z}$: Վերջապես՝

$$\left\| \frac{\alpha}{\beta}\gamma - \delta \right\| = \frac{(2x-z)^2}{4} + \frac{19(2y-\{2y\})^2}{4} \le$$

$$\frac{1}{4} + \frac{1}{9} \times \frac{19}{4} = \frac{7}{9} < 1։$$

5. *Դիցուք $\mathbb{Z}[x]$-ն ամբողջ գործակիցներով բազմանդամների օղակն է։ Դիտարկենք 2 և x բազմանդամներով ծնված իդեալը՝*

$$(2,x) = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}։$$

Դյուրին է ստուգել, որ սա իսկապես իդեալ է։ Այն գլխավոր իդեալ չէ։ Ապացուցենք դա։ Պարզ է, որ $2f(x) + xg(x)$ տեսքի բազմանդամի ազատ անդամը զույգ թիվ է, ուստի $(2,x)$ իդեալը չի պարունակում 1 կամ -1 հաստատուն բազմանդամները։ Եթե գտնվի մի $\in \mathbb{Z}[x]$, որ ծնում է $(2,x)$ իդեալը, ապա $2 = h(x)p(x)$ և $x = h(x)q(x)$, որոշակի $p(x)$ և $q(x)$ բազմանդամների համար $\mathbb{Z}[x]$-ից։ Ակնհայտ է, որ $deg\, h(x) + deg\, p(x) = 0$ և $h(x) \neq \pm 1$։ Հետևաբար՝ $h(x) = \pm 2$։ Սակայն գոյություն չունի ամբողջ գործակիցներով մի $q(x)$ բազմանդամ, որ բավարարի $x = \pm 2q(x)$ պայմանին։

6. *Դիցուք $\mathbb{C}[x,y]$-ը կոմպլեքս գործակիցներով x,y փոփոխականներից կախված բազմանդամների օղակն է։ Դյուրին է տեսնել, որ*

$$(x,y) = \{xf(x,y) + yg(x,y) \mid f(x), g(x) \in \mathbb{C}[x,y]\}$$

իդեալը գլխավոր չէ։ Իսկապես, $xf(x,y) + yg(x,y)$ տեսքի բազմանդամի ազատ անդամը զրոյական է։ Եթե գտնվեր $h(x,y)$ ծնիչ այդ իդեալի համար, ապա $x = h(x,y)p(x,y)$ և $y = h(x,y)q(x,y)$։ Պարզ է, որ $h(x,y)$-ը չի կարող լինել հաստատուն (ոչ զրոյական)։ Մյուս կողմից, եթե $deg\, h = 1$, ապա $q(x,y)$-ը հաստատուն է։ Ակնհայտ է, որ $h(x,y)$-ի առաջին աստիճանի անդամը կպարունակի կամ միայն x փոփոխականը կամ էլ միայն y փոփոխականը։ Ուստի $x = h(x,y)p(x,y)$ և $y = h(x,y)q(x,y)$ պայմանները միաժամանակ բավարարվել չեն կարող։

Ֆակտորիալ օղակներ

Սահմանում: *A ամբողջ տեղափոխելի օղակը կոչվում է* ***ֆակտորիալ օղակ,*** *եթե բոլոր ոչ զրոյական տարրերն այդ օղակից միարժեքորեն ներկայացվում է անվերածելի տարրերի արտադրյալներով, այսինքն՝ կամայական $0 \neq a \in A$ տարրի համար կգտնվեն անվերածելի $p_1, \ldots, p_n$ և միավոր $\varepsilon \in A^*$ այնպիսին, որ $a = \varepsilon p_1 \ldots p_n$:*

Անվերածելի տարրերի արտադրյալի միակությունը հասկացվում է հետևյալ կերպ: Միևնույն տարրի երկու $a = \varepsilon p_1 \ldots p_n$ և $a = \delta q_1 \ldots q_m$ ներկայացումները համարվում են հավասար, եթե կամայական p_i համար կգտնվի նրան ասոցիացված q_j և հակառակը՝ կամայական q_i համար կգտնվի նրան ասոցիացված p_j: Խմբավորենք ասոցիացված տարրերը $a = \varepsilon p_1 \ldots p_n$ ներկայացման մեջ, կստանանք՝ $a = \mu p_{i_1}^{s_1} p_{i_2}^{s_2} \ldots p_{i_k}^{s_k}$, որտեղ $\mu \in A^*$ և $r \neq t \Rightarrow p_r$ և p_t անվերածելի տարրերն ասոցիացված չեն: Երկու $a = \varepsilon p_1^{s_1} \ldots p_n^{s_n}$ և $a = \delta q_1^{t_1} \ldots q_m^{t_m}$ ներկայացումները հավասար են, եթե $n = m$ և յուրաքանչյուր p_i համար կգտնվի նրան ասոցիացված q_j, որ $s_i = t_j$, իսկ յուրաքանչյուր q_j համար կգտնվի նրան ասոցիացված p_i, որ $s_i = t_j$: Պարզ է, որ $p_i^{s_i} = \lambda_i q_{j_i}^{t_{j_i}}, \lambda_i \in A^*$ և $\varepsilon = \delta \lambda_1 \ldots \lambda_n$:

Դյուրին է նկատել, որ ֆակտորիալ օղակում անվերածելի տարրով ծնված իդեալը պարզ է: Իսկապես, դիցուք p-ն անվերածելի է: Դիտարկենք դրանով ծնված (p) իդեալը և ստուգենք այդ իդեալի պարզությունը: Դիցուք $ab \in (p)$: Կգտնվի c, որ $ab = pc$: Քանի որ օղակը ֆակտորիալ է, ապա ab-ն ունի միակ ներկայացում անվերածելի տարրերի արտադրյալի միջոցով, որը կհամընկնի pc-ն նման ներկայացման հետ, որը պարունակում է p-ին ասոցիացված տարր: Ուստի p-ին ասոցիացված տարր կպարունակի անհրաժեշտորեն կամ a-ի ներկայացումն անվերածելի տարրերով կամ էլ b-ի ներկայացումը: Հետևաբար, կամ $a \in (p)$ կամ էլ $b \in (p)$ և (p) իդեալը պարզ է: Այս պատճառով պարզ իդեալ ծնող տարրերը կոչվում են օղակի **պարզ տարրեր**:

Ֆակտորիալ օղակում սահմանված եղանակով, օգտվելով պարզ տարրերի վերլուծությունից, կարելի է սահմանել տարրերի ամենամեծ ընդհանուր բաժանարարի և ամենափոքր ընդհանուր բազմապատիկի գաղափարները:

Օրինակ

Դիտարկենք $R[x]$ իրական գործակիցներով բազմանդամների օղակը: Դյուրին է ստուգել, որ

$$18x^4 - 12x^3 + 20x^2 - 12x + 2 = f^2(x)g(x),$$

որտեղ $f(x) = 3x - 1,\ g(x) = 2x^2 + 2$ բազմանդամներն անվերածելի են: Պարզ է, որ $f(x)$-ն ասոցիացված է $x - \frac{1}{3}$, իսկ $g(x)$-ը՝ $x^2 + 1$ բազմանդամին, ուստի

$$18x^4 - 12x^3 + 20x^2 - 12x + 2$$

բազմանդամի անվերածելի արտադրիչների $(3x - 1)^2(2x^2 + 2)$ և $18(x^2 + 1)(x - \frac{1}{3})^2$ վերլուծությունները համասար են:

Թեորեմ 25.

Ամբողջ գլխավոր իդեալների օղակը ֆակտորիալ է:

Ապացույց. Սկզբից կապացուցենք, որ կամայական ոչ զրոյական տարր ներկայացվում է անվերածելի տարրերի արտադրյալով, իսկ հետո կապացուցենք այդ ներկայացման միակությունը:

Նշանակենք S-ով այն (a) գլխավոր իդեալների բազմությունը, որ a-ն չի ներկայացվում անվերածելի տարրերի արտադրյալով: Պարզ է, որ եթե $(a) \in S$, ապա a-ն ոչ անվերածելի է, ոչ էլ միավոր:

Ցույց տանք, որ եթե $(a) \in S$, ապա գոյություն ունի մեկ այլ $(a_1) \in S$, որ $(a) \subset (a_1)$:

Նկատենք, որ եթե $(a) \in S$, ապա $a = bc$, որտեղ $b, c \notin A^*$: Ակնհայտ է, որ $(a) \subseteq (b)$ և $(a) \subseteq (c)$: Համոզվենք, որ $(a) \subset (b)$ և $(a) \subset (c)$: Իսկապես, դիցուք $(a) = (b)$: Նշանակում է, որ $b = ad$: Սատի $a = bc = adc$ և $a(1 - dc) = 0$: Քանի որ $a \neq 0$ և օղակն ամբողջ է, ապա $1 - dc = 0$ և $c \in A^*$: Նմանապես ստուգում ենք, որ $(a) \neq (c)$:

Պարզ է, որ b և c տարրերից առնվազն մեկը չունի ներկայացում անվերածելի արտադրիչներով և կամ $(b) \in S$ կամ էլ $(c) \in S$, քանի որ հակառակ դեպքում իրար կցագրելով b-ի և c-ի ներկայացումներն անվերածելի տարրերի արտադրյալներով կստանանք a-ի համապատասխան ներկայացումը: Այսպիսով ստացանք մեկ նոր տարր S-ից ((b)-ն կամ (c)-ն, որը նշանակենք (a_1)-ով), որի համար $(a) \subset (a_1)$:

Վերը նշվածից հետևում է, որ եթե $S \neq \varnothing$, ապա S-ում գոյություն ունի իդեալների անվերջ շղթա՝

$$(a_0) \subset (a_1) \subset \ldots \subset (a_n) \subset \ldots$$

Դիտարկենք $\bigcup_{i=0}^{\infty} (a_i)$ բազմությունը: Դա իդեալ է: Իսկապես, եթե $x, y \in \bigcup_{i=0}^{\infty} (a_i)$, ապա $x \in (a_{i_1})$ և $y \in (a_{i_2})$ որոշակի i_1 և i_2 համար: Ակնհայտ է, որ $x, y \in (a_{\max(i_1, i_2)})$ և

$$x - y \in (a_{\max(i_1,i_2)}) \subseteq \bigcup_{i=0}^{\infty}(a_i):$$

Նմանապես՝

$$x \in \bigcup_{i=0}^{\infty}(a_i) \Rightarrow x \in (a_{i_1}) \Rightarrow xy \in (a_{i_1}) \subseteq \bigcup_{i=0}^{\infty}(a_i)$$

Քանի որ A օղակը գլխավոր իդեալների օղակ է, ապա գոյություն ունի $b \in A$, որ $(b) = \bigcup_{i=0}^{\infty}(a_i)$: Ուստի $b \in (a_k)$, որոշակի k-ի համար: Պարզ է, որ $(b) \subseteq (a_k)$: Մյուս կողմից $(a_k) \subseteq \bigcup_{i=0}^{\infty}(a_i) = (b)$ և $(b) = (a_k)$: Ստացանք հակասություն, քանի որ $\exists x \in (a_{k+1}) \setminus (a_k)$ և $\bigcup_{i=0}^{\infty}(a_i) = (a_k) \subset \bigcup_{i=0}^{\infty}(a_i)$: Ուրեմն $S = \varnothing$ և օղակի յուրաքանչյուր տարր ունի ներկայացում անվերածելի տարրերի արտադրյալով: Ապացուցենք այժմ, որ այդ ներկայացումը միակն է:

Սկզբից ապացուցենք մի օժանդակ պնդում՝ եթե $p \vdots ab$ և p-ն անվերածելի է, ապա կամ $p \vdots a$, կամ $p \vdots b$: Իսկապես, դիցուք a-ն չի բաժանվում p-ի վրա: Դիցուք d-ն a-ի և p-ի ամենամեծ ընդհանուր բաժանարարն է, այսինքն՝ $a = dx$ և $p = dy$: Քանի որ p-ն անվերածելի է, ապա կամ $d \in A^*$ կամ $y \in A^*$: Դիցուք $y \in A^*$: Այս դեպքում $d = py^{-1}$ և $a = py^{-1}x$ ինչն անհնար է: Ուրեմն՝ $d \in A^*$ և $(d) = A$: Սակայն, ինչպես գիտենք (Պնդում 24), $A = (d) = (a,p)$ և գոյություն ունեն $x_0, y_0 \in A$, որ $1 = ax_0 + py_0$: Բազմապատկելով վերջին հավասարության աջ և ձախ մասերը b-ով կստանանք՝ $b = abx_0 + bpy_0$ և b-ն բաժանվում է p-ի վրա:

Եթե $p \vdots a^k$ և a-ն չի բաժանվում p-ի վրա, ապա ինչպես ցույց տվեցինք վերը՝ $1 = ax_0 + py_0$: Ուստի $a^{k-1} = a^k x_0 + a^{k-1} p y_0$ և $p \vdots a^{k-1}$: Շարունակելով պրոցեսը կստանանք, որ $p \vdots a$ ինչը հակասում է այն *բանին, որ a-ն չի բաժանվում p-ի վրա: Ուրեմն եթե $p\dot{:}a^k$, ապա $p\dot{:}a$:*

Այսպիսով ապացուցել ենք, որ եթե օղակի վերջավոր քանակությամբ տարրերի արտադրյալը բաժանվում է անվերածելի տարրի վրա, ապա արտադրիչներից առնվազն մեկը կբաժանվի այդ անվերածելի տարրի վրա:

Դիցուք տրված են միևնույն տարրի երկու ներկայացումներ անվերածելի արտադրյալների միջոցով

$$\varepsilon_1 p_1^{s_1}\dots p_n^{s_n} = \varepsilon_2 q_1^{t_1}\dots q_m^{t_m}$$

Ակնհայտ է, որ $\varepsilon_2 q_1^{t_1}\dots q_m^{t_m}$ տարրը բաժանվում է p_1-ի վրա: Միավոր ε_2-ը չի բաժանվում p_1-ի վրա: Հակառակ դեպքում $\varepsilon_2 = p_1 x \Rightarrow 1 = p_1 x \varepsilon_2^{-1}$ և անվերածելի p_1-ը միավոր է: Ուրեմն $q_1,\dots,q_m$ տարրերից ճիշտ մեկը (հիշենք, որ $q_1,\dots,q_m$ տարրերից ոչ մի զույգ ասոցիացված չէ) բաժանվում է p_1-ի վրա: Պարզության համար ենթադրենք, որ դա q_1-ն է $q_1 = p_1\delta_1$ և ակնհայտորեն $\delta_1 \in A^*$: Ստանում ենք, որ $\varepsilon_1 p_1^{s_1}\dots p_n^{s_n} = \varepsilon_2 p_1^{t_1}\dots q_m^{t_m}$: Եթե $s_1 \neq t_1$, ասենք $s_1 > t_1$, ապա $\varepsilon_1 p_1^{s_1}\dots p_n^{s_n} - \varepsilon_2\delta_1 p_1^{t_1}\dots q_m^{t_m} = 0$ և

$$p_1^{t_1}(\varepsilon_1 p_1^{s_1-t_1}p_2^{s_2}\dots p_n^{s_n} - \varepsilon_2\delta_1 q_2^{t_2}\dots q_m^{t_m}) = 0:$$

Օղակի ամբողջությունից ստանում ենք՝

$$\varepsilon_1 p_1^{s_1-t_1}p_2^{s_2}\dots p_n^{s_n} = \varepsilon_2\delta_1 q_2^{t_2}\dots q_m^{t_m}$$

և ձախ մասը բաժանվում է p_1-ի վրա, իսկ աջ մասը՝ ոչ (քանի որ $q_2,\dots,q_m$ տարրերն ասոցիացված չեն p_1-ի հետ): Ուստի $s_1 = t_1$ և օգտվելով օղակի ամբողջությունից՝

$$\varepsilon_1 p_2^{s_2}\dots p_n^{s_n} = \varepsilon_2\delta_1 q_2^{t_2}\dots q_m^{t_m}$$

Կրկնելով վերը շարադրված դատողությունները կստանանք, որ կգտնվի $\delta_2 \in A^*$, որ

$$\varepsilon_1 p_3^{s_3}\dots p_n^{s_n} = \varepsilon_2\delta_1\delta_2 q_3^{t_3}\dots q_m^{t_m}$$

Շարունակելով պրոցեսը կբացառենք բոլոր p_i տարրերը ձախ մասում: Որևէ քայլում q_j-ներն չեն կարող սպառվել p_i-ներից շուտ և նույնպես p_i-ները չեն կարող սպառվել q_j-ներից շուտ, ուստի $n = m$ և թեորեմն ամբողջությամբ ապացուցված է:

Ինչպես գիտենք որևէ դաշտից գործակիցներով բազմանդամների օղակը գլխավոր իդեալների օղակ է, ուստի ստանում ենք՝

Հետևանք

Եթե K-ն դաշտ է, ապա K դաշտից գործակիցներով բազմանդամների $K[x]$ օղակը ֆակտորիալ է:

Օրինակ

Դիտարկենք $\mathbb{Z}[\sqrt{-3}\,] = \{m + n\sqrt{-3} \mid m,n \in \mathbb{Z}\}$ օղակը: Այս օղակում նորմը սահմանվում է բնական եղանակով $\| m + n\sqrt{-3} \| = (m + n\sqrt{-3}\,)(m - n\sqrt{-3}\,) = m^2 + 3n^2$: Այս օղակը ֆակտորիալ չէ, քանի որ $2 \cdot 2 = (1 + \sqrt{-3}\,)(1 - \sqrt{-3}\,)$: Դյուրին է համոզվել, որ 2-ը և $1 \pm \sqrt{-3}$ անվերածելի են և ասոցիացված չեն: Իսկապես, դիցուք $2 = (m + n\sqrt{-3}\,)(p + q\sqrt{-3}\,)$: Ունենք $\|2\| = 4 = (m^2 + 3n^2)(p^2 + 3q^2)$: Ակնհայտ է, որ $p^2 + 3q^2 \neq 2$, հետևաբար $m^2 + 3n^2 = 4$ և $p^2 + 3q^2 = 1$: Այստեղից բխում է, որ $q = 0, p = \pm 1$ և $p + q\sqrt{-3}$-ը միավոր է: Ակնհայտ է նաև, որ օղակի միակ միավորներն են ± 1 տարրերը, ուստի 2-ը և $1 \pm \sqrt{-3}$ ասոցիացված չեն:

Դիտարկենք $\mathbb{Z}[\sqrt{-3}\,]$-ի ընդլայնումը՝

$$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right] = \left\{\frac{x}{2}+\frac{y}{2}\sqrt{-3} \;\middle|\; x,y\in\mathbb{Z}, x\equiv y \bmod 2\right\}:$$

Դյուրին է ստուգել, որ տեղափոխելի օղակ է (տեսեք վերը դիտարկված $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ օղակի օրինակը)։ $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$-ը գլխավոր իդեալների օղակ է։ Համոզվենք դրանում։ Դիցուք $\alpha,\beta\in\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ և $\beta\neq 0$։ Բաժանենք α-ն β-ի վրա որպես սովորական կոմպլեքս թվեր՝ $\alpha=\beta\gamma$ և գրենք γ-ն $\frac{\hat{x}}{2}+\frac{\hat{y}}{2}\sqrt{-3}$ տեսքով։ Նշանակենք $\gamma_1=\frac{\{\hat{x}\}}{2}+\frac{\{\hat{y}\}}{2}\sqrt{-3}$։ Եթե $\{\hat{x}\}\equiv\{\hat{y}\}\bmod 2$ բաղդատումը սխալ է, ապա γ_1-ում փոխարինենք $\{\hat{x}\}$-ը մյուս մոտակա ամբողջ թվով այնպես, որ $\{\hat{x}\}\equiv\{\hat{y}\}\bmod 2$ բաղդատումը լինի ստույգ։ Պարզ է, որ $\|\gamma-\gamma_1\|\leq\frac{1}{4}+3\times\frac{1}{4^2}=\frac{7}{16}<1$։ Այժմ նշանակենք $\delta=\alpha-\beta\gamma_1$։ Ստանում ենք, որ

$$\|\delta\|=\|\alpha-\beta\gamma_1\|=\|\alpha-\beta\gamma+\beta\gamma-\beta\gamma_1\|=$$

$$\|\beta\gamma-\beta\gamma_1\|=\|\beta\|\|\gamma-\gamma_1\|<\|\beta\|:$$

Այսինքն մենք սահմանեցինք $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$-ում մնացորդով բաժանում։

Մնում է կրկնել այն դատողությունը, որ կատարել էինք Գաուսյան ամբողջ թվերի օղակի համար։

$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ օղակում 2-ը և $1\pm\sqrt{-3}$-ն ասոցիացված են։ Իսկապես, $2\times\frac{1\pm\sqrt{-3}}{2}=1\pm\sqrt{-3}$ և $\frac{1\pm\sqrt{-3}}{2}$ տարրերը միավորներ են, քանի որ $\frac{1+\sqrt{-3}}{2}\times\frac{1-\sqrt{-3}}{2}=1$։ Այսինքն 4-ի $2\cdot 2$ և $(1+\sqrt{-3})(1-\sqrt{-3})$ ներկայացումները նույնն են։

Ամբողջ գործակիցներով բազմանդամների օղակի ֆակտորիալությունը

Ապացուցենք այժմ, որ $\mathbb{Z}[x]$ ամբողջ գործակիցներով բազմանդամների օղակը (որն ինչպես գիտենք գլխավոր իդեալների օղակ չէ) ֆակտորիալ է: Այսինքն ֆակտորիալ օղակների դաս ավելի լայն է, քան գլխավոր իդեալների օղակների դասը:

Սահմանում. $f(x) \in \mathbb{Z}[x]$ բազմանդամի գործակիցների ամենամեծ ընդհանուր բաժանարարը կոչվում է բազմանդամի **պարունակություն** և նշանակվում է $cont(f)$-ով:

Լեմմ 26. (Գաուսի Լեմմը)

Դիցուք $f(x), g(x) \in \mathbb{Z}[x]$: Ստույգ է հետևյալ բանաձևը՝

$$cont(fg) = cont(f)cont(g)$$

Ապացույց. Ակնհայտ է, որ $f(x) = cont(f)f_1(x)$ և $g(x) = cont(g)g_1(x)$, որտեղ $cont(f_1) = cont(g_1) = 1$: Պարզ է նաև, որ $f(x)g(x) = cont(f)cont(g)f_1(x)g_1(x)$ և $cont(fg) = cont(f)cont(g)cont(f_1g_1)$: Ուստի բավական է ապացուցել, որ $cont(f_1) = cont(g_1) = 1 \Rightarrow cont(f_1g_1) = 1$:

Դիցուք $f_1(x) = \alpha_0 + \ldots + \alpha_n x^n$, $\alpha_n \neq 0$ և $g_1(x) = \beta_0 + \ldots + \beta_m x^m$, $\beta_m \neq 0$: Ցույց տանք, որ $cont(f_1g_1)$-ը չի բաժանվում և ոչ մի p պարզ թվի վրա: Դիցուք α_r-ը և β_s-ը համապատասխանաբար $f_1(x)$-ի և $g_1(x)$-ի ամենամեծ համարի գործակիցներն են, որ չեն բաժանվում

p-ի վրա: Դյուրին է ստուգել, որ $f_1(x)g_1(x)$-ում x^{r+s}-ի գործակիցը հավասար է

$$\alpha_r\beta_s + \alpha_{r+1}\beta_{s-1} + \ldots + \alpha_{r-1}\beta_{s+1} + \ldots$$

Պարզ է, որ $\alpha_r\beta_s$-ը չի բաժանվում p-ի վրա, իսկ բոլոր մնացած գումարելիները (եթե դրանք կան) բաժանվում են p-ի վրա, քանի որ պարունակում են կամ r-ից մեծ համարի $f_1(x)$-ի գործակիցներ կամ էլ s-ից մեծ համարի $g_1(x)$-ի գործակիցներ: Ուստի լեմմն ապացուցված է:

Պնդում 27.

Դիցուք $\mathbb{Q}[x]$-ը ռացիոնալ գործակիցներով բազմանդամների օղակն է: Յուրաքանչյուր $f(x) \in \mathbb{Q}[x]$ միարժեքորեն ներկայացվում է $f(x) = \frac{m}{n}f_1(x)$ տեսքով, որտեղ $f_1(x) \in \mathbb{Z}[x]$, $cont(f_1) = 1$ և $\frac{m}{n} \in \mathbb{Q}$ դրական հայտարարով անկրճատելի կոտորակ է:

Ապացույց. $f(x) = \frac{m}{n}f_1(x)$ ներկայացման գոյությունն ակնհայտ է՝ բավական է ընդհանուր հայտարարի բերել $f(x)$-ի գործակիցները և դուրս բերել փակագծից այդ ընդհանուր հայտարարը, ապա դուրս բերել գործակիցների ամենամեծ ընդհանուր բաժանարարը:

Ապացուցենք միակությունը: Դիցուք $f(x) = \frac{m}{n}f_1(x) = \frac{r}{s}f_2(x)$: Բազմապատկենք երկու կողմերը ns-ով՝ $msf_1(x) = nrf_2(x)$: Ուստի $ms = cont(msf_1) = cont(nrf_2) = nr$: Քանի որ $(m,n) = (r,s) = 1$, այսինքն $\frac{m}{n}$-ը և $\frac{r}{s}$-ն անկրճատելի են, ապա n-ը բաժանվում է s-ի վրա և ընդհակառակը՝ s-ը բաժանվում է n-ի վրա, ուրեմն՝ $n = s$: Նմանապես ստանում ենք, որ $m = r$: Այստեղից էլ բխում է, որ

$f_1(x) = f_2(x)$։

Պնդում 28.

Եթե $f(x) \in \mathbb{Z}[x]$ **և** $f(x) = g(x)h(x)$, **որտեղ** $g(x), h(x) \in \mathbb{Q}[x]$, **ապա** $f(x) = kg_1(x)h_1(x)$, **որտեղ** $k \in \mathbb{Z}$, $g_1(x), h_1(x) \in \mathbb{Z}[x]$, $cont(g_1) = cont(h_1) = 1$**։**

Ապացույց. *Համաձայն* *Պնդում 27-ի ունենք՝* $f(x) = mf_1(x)$, $g(x) = \frac{p}{q}g_1(x)$, $h(x) = \frac{r}{s}h_1(x)$, *ընդ որում*

$$cont(f_1) = cont(g_1) = cont(h_1) = (p,q) = (r,s) = 1։$$

Ուրեմն

$$mf_1(x) = f(x) = g(x)h(x) = \frac{p}{q}\frac{r}{s}g_1(x)h_1(x)$$

և

$$qsmf_1(x) = prg_1(x)h_1(x)։$$

Համաձայն Գաուսի լեմմի՝

$$qsm \times cont(f_1) = pr \times cont(g_1)cont(h_1)$$

և $qsm = pr$։ *Քանի որ* $(p,q) = (r,s) = 1$, *ստանում ենք, որ* p*-ն բաժանվում է* s*-ի վրա իսկ* r*-ը՝* q*-ի վրա։ Հետևաբար* $\frac{pr}{qs}$*-ն ամբողջ թիվ է և* $f(x) = kg_1(x)h_1(x)$, *որտեղ* $k = \frac{pr}{qs}$։

Այստեղից անմիջապես բխում է՝

Պնդում 29.

Եթե $f(x) \in \mathbb{Z}[x]$ **անվերածելի է** $\mathbb{Z}[x]$**-ում, ապա այն անվերածելի է նաև** $\mathbb{Q}[x]$**-ում։** $\mathbb{Z}[x]$ **օղակի անվերածելի**

բազմանդամներն են պարզ թիվ հանդիսացող հաստատուն բազմանդամները և $\mathbb{Q}[x]$-ում անվերածելի 1 պարունակությամբ բազմանդամները:

Թեորեմ 30.

$\mathbb{Z}[x]$ օղակը ֆակտորիալ է:

Ապացույց. Ակնհայտ է, որ $\mathbb{Z}[x]$-ն ամբողջ է: Դիցուք $f(x) \neq 0$: Քանի որ $\mathbb{Q}$-ն դաշտ է, ապա համաձայն Թեորեմ 25-ի հետևանքի $\mathbb{Q}[x]$-ը ֆակտորիալ է և գոյություն ունի $f(x)$-ի վերլուծությունն անվերածելի բազմանդամների $\mathbb{Q}[x]$-ում: Համաձայն Պնդում 28-ի փոխարինելով $\mathbb{Q}[x]$-ի անվերածելի բազմանդամներն 1 պարունակությամբ ասոցիացվածներով $\mathbb{Z}[x]$-ից կստանանք $f(x)$-ի հետևյալ ներկայացումը՝ $f(x) = mg_1(x)\dots g_r(x)$, որտեղ $m \in \mathbb{Z}$, $g_i(x) \in \mathbb{Z}[x]$ և $cont(g_i) = 1$, $i = 1,\dots,r$:

Դիցուք տրված է $f(x)$-ի մեկ այլ վերլուծություն անվերածելի բազմանդամների $\mathbb{Z}[x]$-ում՝ $f(x) = nh_1(x)\dots h_s(x)$, որտեղ $n \in \mathbb{Z}$, $h_i(x) \in \mathbb{Z}[x]$ և $cont(h_i) = 1$, $i = 1,\dots,s$: $\mathbb{Q}[x]$ օղակի ֆակտորիալությունից հետևում է, որ $r = s$ և արտադրիչների վերադասավորումից հետո $g_i(x) = \frac{p_i}{q_i}h_i(x)$: Որեմն՝ $q_ig_i(x) = p_ih_i(x)$ և անցնելով պարունակություններին ստանում ենք $q_i = p_i$, այսինքն՝ $g_i(x) = h_i(x)$: Թեորեմն ապացուցված է:

Փոխարինելով $\mathbb{Z}$-ը կամայական ֆակտորիալ օղակով և $\mathbb{Q}$-ն այդ օղակի քանորդների դաշտով և կրկնելով վերը շարադրված դատողությունները դյուրին է ապացուցել հետևյալ թեորեմը:

Թեորեմ 31.

Եթե A-ն ֆակտորիալ օղակ է, ապա $A[x]$-ը նույնպես ֆակտորիալ է: Ֆակտորիալ է նաև $A[x_1, \ldots, x_n]$ օղակը, $x_1, \ldots, x_n$ փոփոխականների A-ից գործակիցներով բազմանդամների օղակը:

Էվքլիդեսյան (Էվքլիդյան) օղակներ

Ֆակտորիալ օղակների կարևոր ենթադաս են կազմում Էվքլիդեսյան օղակները: Մասնավորապես դրանց դասին են պատկանում ամբողջ թվերի օղակը, դաշտից գործակիցներով բազմանդամների օղակները, Գաուսյան ամբողջ թվերի օղակը:

Էվքլիդեսյան օղակներն ամբողջ և գլխավոր իդեալների օղակներ են, ուստի դրանք ֆակտորիալ են:

Սահմանում: A ամբողջ օղակը կոչվում է **Էվքլիդեսյան օղակ**, եթե նրա յուրաքանչյուր ոչ զրոյական a տարրին կարելի է համապատասխանեցնել որոշակի ամբողջ թիվ՝ $|a|$ (որը կանվանենք **Էվքլիդեսյան նորմ**) այնպես, որ տեղի ունեն հետևյալ պայմանները.

1. $|a| \geq 0$
2. $a = bc \Rightarrow |b| \leq |a|$
3. $(\forall a, b \in A,\ b \neq 0)(\exists q, r \in A)\ a = bq + r$ և $|r| < |b|$ եթե $r \neq 0$ (Էվքլիդեսյան բաժանման հնարավորությունը)

Օրինակներ

1. Ամբողջ թվերի $\mathbb{Z}$ օղակի համար նորմը դա թվի բացարձակ արժեքն է:

2. Որևէ K դաշտից գործակիցներով բազմանդամների $K[x]$ օղակի համար նորմը դա բազմանդամի աստիճանն է:

3. $\mathbb{Z}[i]$ Գաուսյան ամբողջ թվերի օղակի դեպքում $m + in$ թվի նորմը դա $(m + in)(m - in) = m^2 + n^2$ թիվն է:

4. Դյուրին է ստուգել, որ K դաշտից գործակիցներով

աստիճանային շարքերը կազմում են ամբողջ օղակ, որը նշանակվում է $K[[x]]$-ով: Շարքի նորմը դա x-ի ամենափոքր աստիճանի ցուցիչն է:

5. $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ օղակում $\frac{x}{2}+\frac{y}{2}\sqrt{-3}$ տարրի նորմը դա $\left\| \frac{x}{2}+\frac{y}{2}\sqrt{-3} \right\| = \frac{x^2}{4}+3\frac{y^2}{4}$ է:

Պնդում 32.

Էվքլիդեսյան օղակը գլխավոր իդեալների օղակ է:

Ապացույց. Դիցուք A օղակը Էվքլիդեսյան է և B-ն իդեալ է A-ում: Դիցուք $B \neq \{0\}$ և $B \neq A$ (ակնհայտ է, որ բավական է դիտարկել այս դեպքը): Դիցուք $0 \neq b \in B$ և $|b|$-ն փոքրագույնն է B-ի տարրերի համար: Վերցնենք այժմ B-ի կամայական a տարր և բաժանենք այն b-ի վրա համաձայն Էվքլիդեսյան օղակի սահմանման 3. պայմանի: Կստանանք $a = bq + r$ և, հետևաբար, $r = a - bq \in B$:

Դիցուք $|b| = 0$: Եթե $r \neq 0$, ապա $|r| < |b| = 0$, ինչն անհնար է: Ուրեմն $r = 0$ և իդեալի բոլոր տարրերը պատիկ են b-ին, վերջինս էլ իդեալի ծնիչն է՝ $B = (b)$:

Դիցուք $|b| > 0$: Եթե $r \neq 0$, ապա $|r| < |b|$ և $|b|$-ն փոքրագույնը չէ, ինչն անհնար է: Ուրեմն $r = 0$ և $B = (b)$:

Հետևանք

Էվքլիդեսյան օղակը ֆակտորիալ է:

Ինչպես տեսել էինք, $\mathbb{Z}[x]$ օղակը ֆակտորիալ է, բայց գլխավոր իդեալների օղակ չէ: Այսինքն, գլխավոր իդեալների օղակները ֆակտորիալ օղակների իսկական ենթադաս է: Ցույց տանք, որ Էվքլիդեսյան օղակներն էլ գլխավոր իդեալների օղակների իսկական ենթադասն են: Դրա համար բավական է նշել մի գլխավոր իդեալների օղակ, որն Էվքլիդեսյան չէ: Այդպիսի օղակ է

$$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right] = \left\{\frac{a}{2} + \frac{b}{2}\sqrt{-19} \mid a, b \in \mathbb{Z}, a \equiv b \bmod 2\right\}$$

օղակը: Արդեն համոզվել ենք, որ սա գլխավոր իդեալների օղակ է: Ապացուցենք, որ այն Էվքլիդեսյան չէ:

Դիցուք $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ն Էվքլիդեսյան է և $\alpha \in \mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ էվքլիդեսյան նորմը նշանակենք $|\alpha|$-ով: Հիշենք, որ $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ օղակի կոմպլեքս նորմը սահմանել էինք որպես $\left\| \frac{a}{2} + \frac{b}{2}\sqrt{-19} \right\| = \frac{a^2}{4} + 19\frac{b^2}{4}$:

Դիցուք U-ն $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ի բոլոր ոչ զրոյական տարրերի բազմությունն է, որոնց Էվքլիդեսյան նորմը մինիմալն է: Եթե α (ոնի հակադարձ ըստ բազմապատկման), ապա կամայական ոչ զրոյական տարր բաժանվում է α-ի վրա առանց մնացորդի: Ուստի համաձայն Էվքլիդեսյան նորմի 2. հատկության ստանում ենք, որ $|\alpha|$ չի գերազանցում U-ի տարրերի նորմին և ուրեմն $\alpha \in U$: Մյուս կողմից, եթե $\beta \in U$, ապա համաձայն Էվքլիդեսյան նորմի 3. հատկության $1 = \beta\gamma + \delta$: Եթե $\delta \neq 0$, ապա $|\delta| < |\beta|$ և ստացանք ոչ զրոյական տարր, որի էվքլիդեսյան նորմը փոքր է $|\beta|$-ից, ինչն անհնար է: Ուստի՝ $\delta = 0$ և $1 = \beta\gamma$, այսինքն β-ն միավոր է: Այսպիսով ստանում ենք, որ U-ն համընկնում է $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ի միավորների բազմության հետ:

Ապացուցենք այժմ, որ $U = \{1, -1\}$:

Դիցուք $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{-19}$ տարրը միավոր է՝ $\alpha\alpha^{-1} = 1$ և $\|\alpha\|\|\alpha^{-1}\| = 1$: Քանի որ կոմպլեքս նորմը ամբողջ ոչ բացասական թիվ է, ապա $\|\alpha\| = \frac{a^2}{4} + 19\frac{b^2}{4} = 1$: Որեմն $a^2 + 19b^2 = 4$ ինչն հնարավոր է միայն, երբ $b = 0$ և $a = \pm 2$: Հետևաբար, $\alpha = \frac{a}{2} + \frac{b}{2}\sqrt{-19} = \pm 1$:

Դիցուք $\alpha \notin \{0, 1, -1\}$ և ունի նվազագույն հնարավոր էվքլիդեսյան նորմը: Էվքլիդեսյան նորմի 3. հատկության համաձայն $2 = \alpha\beta + \delta$ և կամ $\delta = 0$ կամ էլ $|\delta| < |\alpha|$: Հետևաբար, $\delta \in \{0, 1, -1\}$: Եթե $\delta = 1$, ապա $1 = \alpha\beta$ և α-ն միավոր է, այսինքն $\alpha \in U = \{1, -1\}$, ինչն անհնար է: Որեմն՝ $\delta \in \{0, -1\}$ և կամ $2 = \alpha\beta$ կամ էլ $3 = \alpha\beta$: Այստեղից բխում է, որ կամ $\alpha = \pm 2$ կամ $\alpha = \pm 3$: Ապացուցենք դա: Ստուգենք, որ 2-ը պարզ թիվ է $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ում (հիշենք, որ $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$-ը ֆակտորիալ օղակ է): Դիցուք $2 = \left(\frac{a}{2} + \frac{b}{2}\sqrt{-19}\right)\left(\frac{c}{2} + \frac{d}{2}\sqrt{-19}\right)$: Անցնելով կոմպլեքս նորմերին ստանում ենք՝

$$\|2\| = 4 = \left\|\frac{a}{2} + \frac{b}{2}\sqrt{-19}\right\|\left\|\frac{c}{2} + \frac{d}{2}\sqrt{-19}\right\|:$$

Եթե ոչ $\frac{a}{2} + \frac{b}{2}\sqrt{-19}$-ը, ոչ էլ $\frac{c}{2} + \frac{d}{2}\sqrt{-19}$-ը միավոր չեն, ապա

$$\left\|\frac{a}{2} + \frac{b}{2}\sqrt{-19}\right\| = \left\|\frac{c}{2} + \frac{d}{2}\sqrt{-19}\right\| = 2:$$

Հետևաբար, $a^2 + 19b^2 = c^2 + 19d^2 = 8$, որտեղից ստանում ենք $b = d = 0$ և $a^2 = c^2 = 8$, ինչն անհնար է: Նմանապես վարվելով ապացուցվում է, որ 3-ն էլ պարզ է: Իսկապես $\|3\| = 9$ և $a^2 + 19b^2 = c^2 + 19d^2 = 12$, ինչն անհնար է: Քանի որ α-ն միավոր չէ և 2-ն ու 3-ը պարզ թվեր են, $2 = \alpha\beta$ և $3 = \alpha\beta$ պայմաններից հետևում է, որ կամ $\alpha = \pm 2$, կամ $\alpha = \pm 3$:

Այժմ, համաձայն Էվքլիդեսյան նորմի 3. հատկության, բաժանենք $\frac{1+\sqrt{-19}}{2}$-ը α-ի վրա՝ $\frac{1+\sqrt{-19}}{2} = \alpha\beta + \delta$ և կամ $\delta = 0$, կամ էլ $|\delta| < |\alpha|$:

Ուստի՝ $\delta \in \{0, 1, -1\}$ և $\frac{1+\sqrt{-19}}{2}$, $\frac{1+\sqrt{-19}}{2} - 1$, $\frac{1+\sqrt{-19}}{2} + 1$ թվերից մեկը բաժանվում է α-ի վրա, այսինքն կամ ± 2-ի, կամ էլ ± 3-ի վրա: Ունենք $\|\pm 2\| = 4$ և $\|\pm 3\| = 9$: Հաշվենք $\frac{1+\sqrt{-19}}{2}$, $\frac{1+\sqrt{-19}}{2} - 1$, $\frac{1+\sqrt{-19}}{2} + 1$ թվերի կոմպլեքս նորմերը.

$$\left\| \frac{1+\sqrt{-19}}{2} \right\| = \left\| \frac{1+\sqrt{-19}}{2} - 1 \right\| = \frac{1}{4} + 19 \times \frac{1}{4} = 5$$

$$\left\| \frac{1+\sqrt{-19}}{2} + 1 \right\| = \left\| \frac{3+\sqrt{-19}}{2} \right\| = \frac{9}{4} + 19 \times \frac{1}{4} = 7:$$

Դիցուք $x \in \left\{ \frac{1+\sqrt{-19}}{2}, \frac{1+\sqrt{-19}}{2} - 1, \frac{1+\sqrt{-19}}{2} + 1 \right\}$: Ունենք՝ $x = \alpha\beta$ և $\|x\| = \|\alpha\|\|\beta\|$, հետևաբար $\|x\|$-ը բաժանվում է առանց մնացորդի $\|\alpha\|$-ի վրա: Սակայն $\|x\| \in \{5, 7\}$ և $\|\alpha\| = \{4, 9\}$ և $\|x\|$-ը չի կարող բաժանվել առանց մնացորդի $\|\alpha\|$-ի վրա: Ուրեմն օղակը չի կարող լինել Էվքլիդեսյան:

Դաշտի բնութագրիչը

Դիցուք F-ը դաշտ է: Բնական է **ենթադաշտ** անվանել F-ի այն K ենթաօղակները, որոնք փակ են հակադարձի հաշվման գործողության նկատմամբ, այսինքն՝ եթե $\alpha \in K$, ապա $\alpha^{-1} \in K$:

Յուրաքանչյուր $n \in \mathbb{Z}$ համար $\bar{n}$-ով նշանակենք F-ի հետևյալ տարրը՝

$$\bar{n} = \begin{cases} \underbrace{1 + 1 + \ldots + 1}_{|n| \text{ հատ}}, & \text{եթե } n > 0 \\ -(\underbrace{1 + 1 + \ldots + 1}_{|n| \text{ հատ}}), & \text{եթե } n < 0 \end{cases}$$

Համարում ենք, որ $\bar{0} = 0$:

Դիտարկենք F-ի հետևյալ ենթաօղակը՝ $F_0 = \{\bar{n} \mid n \in \mathbb{Z}\}$: Դյուրին է ստուգել, որ F_0-ն իսկապես ենթաօղակ է: Պարզ է նաև, որ կամայական դաշտ (նաև կամայական տեղափոխելի օղակ) պարունակում F_0 ենթաօղակը: Պարզ է նաև, որ $p = nm \Rightarrow \bar{p} = \bar{n}\bar{m}$:

Պարզ է, որ կամ F_0-ի բոլոր տարրերը տարբեր են, կամ էլ կգտնվեն երկու հավասար տարրեր: Երկու հավասար տարրերի գոյությունը համարժեք է այնպիսի $\bar{n}$-ի գոյությանը, որ $\bar{n} = 0$ և $n > 0$:

Դիցուք F_0-ի բոլոր տարրերը տարբեր են: Այդ դեպքում ակնհայտ է, որ F_0-ն իզոմորֆ է որպես օղակ ամբողջ թվերի $\mathbb{Z}$ օղակին: Այդ իզոմորֆիզմը տրվում է յուրաքանչյուր $n \in \mathbb{Z}$ ամբողջ թվին համապատասխանեցնելով $\bar{n}$ տարրը: Քանի որ F-ը դաշտ է, ապա այն պարունակում է F_0-ի հետ մեկտեղ F_0-ի ոչ զրոյական տարրերի հակադարձները, որոնք կազմում են F_0-ի քանորդների դաշտը, որն իր Հերթին իզոմորֆ է ամբողջ թվերի օղակի քանորդների դաշտին, այսինքն ռացիոնալ թվերի դաշտին: Այսպիսով ստացանք, որ եթե F_0-ի բոլոր տարրերը տարբեր են, ապա դաշտը պարունակում է ռացիոնալ թվերի դաշտին իզոմորֆ ենթադաշտ:

Դիտարկենք մյուս դեպքը: Դիցուք այժմ կգտնվի $p > 0$, որ $\bar{p} = 0$: Կհամարենք, որ p-ն նվազագույնն է: Եթե p-ն բաղադրյալ է ` $p = nm$, ապա $\bar{p} = \bar{n}\bar{m}$: Քանի որ F-ը դաշտ է և ուրեմն ամբողջ օղակ է, ստանում ենք՝ կամ $\bar{n} = 0$ կամ $\bar{m} = 0$: Որտեղից p-ն նվազագույնը չէ: Հետևաբար նվազագույն p-ն, որ $p > 0$ և $\bar{p} = 0$ պարտադիր պարզ թիվ է: Այս դեպքում F_0-ն իզոմորֆ է ըստ $\mathrm{mod}\, p$-ի $\mathbb{Z}_p$ մնացքների օղակին՝ $\bar{n} = \bar{m} \Leftrightarrow n \equiv m \,\mathrm{mod}\, p$: Ստացվում է, որ $F_0 = \{0, \bar{1}, \bar{2}, \ldots, \overline{p-1}\}$: Քանի որ p պարզ մոդուլի դեպքում $\mathbb{Z}_p$-ն դաշտ է (բոլոր ոչ զրոյական տարրերը կունենան հակադարձներ ըստ բազմապատկման), ուրեմն F_0-ն դաշտ է և այն նույնացվում է $\mathbb{Z}_p$-ն: Այսպիսով այս դեպքում դաշտը պարունակում է $\mathbb{Z}_p$-ն իզոմորֆ ենթադաշտ:

Ամփոփելով վերը ստացվածը՝

յուրաքանչյուր դաշտ կամ պարունակում է ռացիոնալ թվերի դաշտին իզոմորֆ ենթադաշտ և անվերջ է, կամ էլ պարունակում է պարզ մոդուլով մնացքների դասերին իզոմորֆ ենթադաշտ:

Նշված F_0 ենթադաշտը կոչվում F դաշտի ***պարզ ենթադաշտ***:

Առաջին դեպքում ասում են, որ դաշտի ***բնութագրիչը*** 0 է, իսկ երկրորդ դեպքում p է: F դաշտի բնութագրիչը նշանակում են $char(F)$ նշանով:

Այսուհետև $\underbrace{\alpha + \alpha + \ldots + \alpha}_{n \text{ հատ}}$ տարրը կնշանակենք $n\alpha$-ով: Պարզ է, որ

$$n\alpha = \underbrace{\alpha + \alpha + \ldots + \alpha}_{n \text{ հատ}} = (1 + 1 + \ldots + 1)\alpha = \bar{n}\alpha$$

և, եթե $char(F) = p > 0$, ապա $n\alpha = 0 \Leftrightarrow \alpha = 0$ կամ $n \equiv 0 \bmod p$: Մասնավորապես, եթե $n \equiv 0 \bmod p$, ապա $n\alpha = 0$:

Դիցուք $char(F) = p > 0$: Ինչպես գիտենք, $(\alpha + \beta)^p = \sum_{k=0}^{p} \binom{p}{k} \alpha^k \beta^{p-k}$ և $\binom{p}{k} = \frac{p!}{k!(p-k)!}$: Ստանում ենք, որ $k!(p-k)!\binom{p}{k} = p!$: Եթե $0 < k < p$, ապա $k!(p-k)!$ թիվը չի բաժանվում p-ի վրա, քանի որ դա p-ից փոքր թվերի արտադրյալ է: Որեմն $\binom{p}{k}$-ն բաժանվում է p-ի վրա առանց մնացորդի և $\binom{p}{k} \equiv 0 \bmod p$: Հետևաբար $(\alpha + \beta)^p = \alpha^p + \beta^p$: Նմանապես՝

$$(\alpha + \beta)^{p^2} = ((\alpha + \beta)^p)^p = (\alpha^p + \beta^p)^p = \alpha^{p^2} + \beta^{p^2}$$

և

$$(\alpha + \beta)^{p^m} = \alpha^{p^m} + \beta^{p^m} \tag{43}$$

Վերջավոր դաշտեր

Այսուհետև կդիտարկենք միայն վերջավոր քանակությամբ տարր պարունակող դաշտեր և դաշտ ասելով ի նկատի ենք ունենալու վերջավոր դաշտ: Այդ դաշտերը նաև կոչվում են Գալուայի դաշտեր: Ինչպես տեսանք, p բնութագրիչ ունեցող վերջավոր դաշտը պարունակում է իր մեջ $\mathbb{Z}_p$ պարզ դաշտը: Դիցուք K-ն F դաշտի ենթադաշտն է: Դյուրին է նկատել, որ F-ը գծային տարածություն է K-ի նկատմամբ: Իսկապես, եթե $\lambda \in K$ և $\alpha \in F$, ապա $\lambda\alpha \in F$: Որպես գումարման գործողություն վերցնում ենք F-ի գումարումը: Գծային տարածության սահմանման բոլոր պայմաններն ակնհայտորեն բավարարված են: Քանի որ դաշտը վերջավոր է, ապա F-ը վերջավոր չափանի գծային տարածություն է և ունի վերջավոր բազիս: Դիցուք F-ը m-չափանի է և K-ի տարրերի քանակը հավասար է q-ի: Ուրեմն, այն իզոմորֆ է (որպես գծային տարածություն) $V_m(K) = \{(\lambda_1,\dots,\lambda_m) \mid \lambda_i \in K, \quad i = 1,2,\dots,m\}$ m-չափանի վեկտորական տարածությանը և F-ի տարրերի քանակը հավասար է $V_m(K)$-ի տարրերի քանակին, որը հավասար է q^m: Կիրառելով այս դատողությունները $K = \mathbb{Z}_p$ դեպքին անմիջապես ստանում ենք՝

Պնդում 33.

Վերջավոր դաշտի տարրերի քանակը պարզ թվի (դաշտի բնութագրիչի) աստիճան է:

Այսուհետև q տարր պարունակող դաշտը կնշանակենք F_q նշանով:

Ինչպես արդեն տեսել էինք մաքսիմալ իդեալների ուսումնասիրության ժամանակ (Թեորեմ 14-ի մասնավոր դեպքում), անվերածելի բազմանդամով ծնված գլխավոր իդեալի նկատմամբ կառուցված ֆակտոր-օղակը դաշտ է: Կիրառենք Թեորեմ 14-ի մասնավոր դեպքի դատողությունները p պարզ թվի համար F_{p^n} վերջավոր դաշտի կառուցման համար:

Դիցուք $n \geq 2$ և $f(x)$-ն անվերածելի բազմանդամ է F_p պարզ դաշտում և $\deg f = n$: Համաձայն Թեորեմ 21-ի $F_p[x]/(f(x))$ ֆակտոր օղակը դաշտ է: Ինչպես ցույց էինք տվել Թեորեմ 21-ի մասնավոր դեպքի ուսումնասիրության ժամանակ $F_p[x]/(f(x))$ դաշտի յուրաքանչյուր տարր (հարակից դաս ըստ $(f(x)) = \{f(x)g(x) \mid g(x) \in F_p[x]\}$ իդեալի) պարունակում է միարժեքորեն որոշված $h(x) \in F_p[x]$ մի բազմանդամ, որի համար $\deg h < \deg f$: Ավելի ստույգ, հարակից դասի յուրաքանչյուր բազմանդամ տալիս է միևնույն $h(x)$ մնացորդը: Քանի որ $\deg h < \deg f = n$, ապա $h(x) = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1} x^{n-1}$ և այդպիսի $h(x)$ բազմանդամների քանակը հավասար է p^n (քանի որ $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ գործակիցների ընտրության եղանակների քանակը p^n է): Ակնհայտ է նաև, որ յուրաքանչյուր հարակից դաս պարունակում է ճիշտ մեկ հատ բազմանդամ, որի աստիճանը փոքր է n-ից (քանի որ դրանց մնացորդները $f(x)$-ի վրա բաժանելիս համընկնում են հենց այդ բազմանդամների հետ): Այսպիսով ստացանք, որ $F_p[x]/(f(x))$ տարրերի քանակը հավասար է p^n-ի: Պարզ է որ, եթե որպես $F_p[x]/(f(x))$ դաշտի տարրերի՝ հարակից դասերի ներկայացուցիչներ վերցնենք համապատասխան $h(x)$ բազմանդամները, ապա հարակից դասերի նկատմամբ գումարումը և բազմապատկումը կհամապատասխանեն ըստ $\operatorname{mod} f(x)$-ի $h(x)$

բազմանդամների գումարումը և բազմապատկումը: Նշանակենք θ-ով $h(x)=x$ բազմանդամին համապատասխանող հարակից դասը: Դիցուք $f(x)=\beta_0+\beta_1x+\ldots+\beta_nx^n$: Դիտարկենք $\beta_0+\beta_1\theta+\ldots+\beta_n\theta^n$ հարակից դասը: Պարզ է, որ դրա համապատասխան $h(x)$ բազմանդամը դա $(\beta_0+\beta_1x+\ldots+\beta_nx^n)\,\mathrm{mod}f(x)$ բազմանդամն է, որն հավասար է 0-ի: Այսինքն, θ-ն $f(x)$ բազմանդամի արմատն է $F_p[x]/(f(x))$ դաշտում: Այսպիսով կառուցեցինք F_{p^n} վերջավոր դաշտը: Ասում են, որ այս դեպքում F_{p^n} դաշտը ստացվում է F_p-ից վերջինին θ արմատը միացնելով:

Դյուրին է նկատել, որ որպես բազիս (հիշենք, որ դաշտը գծային տարածություն է F_p-ի նկատմամբ) կարող ենք վերցնել $1,x,x^2,\ldots,x^{n-1}$ բազմանդամներին համապատասխանող հարակից դասերը, այսինքն F_{p^n} դաշտի $1,\theta,\theta^2,\ldots,\theta^{n-1}$ տարրերը: Իսկապես, $h(x)=\alpha_0+\alpha_1x+\ldots+\alpha_{n-1}x^{n-1}$ բազմանդամին համապատասխանող հարակից դասը դա $\alpha_0+\alpha_1\theta+\ldots+\alpha_{n-1}\theta^{n-1}$ դասն է: Ուստի, F_{p^n} դաշտի յուրաքանչյուր տարր ներկայացվում է $1,\theta,\theta^2,\ldots,\theta^{n-1}$ տարրերի գծային կոմբինացիայով: Պարզ է, որ $1,\theta,\theta^2,\ldots,\theta^{n-1}$ տարրերը գծորեն անկախ են F_p-ի նկատմամբ: Իսկապես, դիցուք

$$\gamma_0,\gamma_1,\ldots,\gamma_{n-1}\in F_p \text{ և } \gamma_0+\gamma_1\theta+\ldots+\gamma_{n-1}\theta^{n-1}=0:$$

Սա նշանակում է, որ $\gamma_0+\gamma_1\theta+\ldots+\gamma_{n-1}\theta^{n-1}$ տարրին համապատասխանող $h(x)$ բազմանդամը դա $\gamma_0+\gamma_1x+\ldots+\gamma_{n-1}x^{n-1}$ բազմանդամն է, որը $f(x)$-ի վրա բաժանելիս պետք է տա զրոյական մնացորդ, ինչը հնարավոր է միայն $\gamma_0=\gamma_1=\ldots=\gamma_{n-1}=0$ դեպքում: Ուստի, դաշտի կամայական տարր միարժեքորեն ներկայացվում է $1,\theta,\theta^2,\ldots,\theta^{n-1}$ տարրերի գծային կոմբինացիայով:

Նկատենք, որ մենք ապացուցեցինք նաև, որ կամայական բազմանդամ $F_p[x]$-ից, որի համար θ-ն արմատ է, առանց մնացորդի բաժանվում է $f(x)$-ի վրա (քանի որ θ-ն արմատ է այդպիսի բազմանդամի $f(x)$-ի վրա բաժանելուց ստացված մնացորդի՝ $h(x)$-ի համար)։ Այսինքն, $(f(x))$ իդեալը կազմված է բոլոր այն բազմանդամներից, որոնց համար θ-ն արմատ է և $f(x)$-ը ամենափոքր աստիճանի այդպիսի բազմանդամներից մեկն է։

Այսպիսով տեսանք, որ F_{p^n} դաշտը կառուցելու համար բավական է ունենալ n-րդ աստիճանի F_p-ի նկատմամբ որևէ անվերածելի բազմանդամ։ Սորև կապացուցենք, որ կամայական F_p-ի դեպքում բոլոր $n \geq 1$ համար գոյություն ունեն n-րդ աստիճանի անվերածելի բազմանդամներ։ Այսինքն, բոլոր պարզ p թվերի և բոլոր $n \geq 1$ համար գոյություն ունի F_{p^n} դաշտը։

Օրինակ

Կառուցենք F_{3^2} դաշտը։ Դրա համար վերցնենք $f(x) = 2 + x + x^2$ բազմանդամը, որն անվերածելի է $F_3[x]$-ում։ Այժմ F_{3^2} դաշտը դա $F_3[x] / (2 + x + x^2)$ դաշտն է, որի տարրերը 1 և θ տարրերի բոլոր գծային կոմբինացիաներից են բաղկացած (այստեղ θ միացվող արմատն է՝ $h(x) = x$ բազմանդամին համապատասխանող հարակից դասն է $F_3[x] / (2 + x + x^2)$-ում)։ Թվարկենք F_{3^2}-ի տարրերը՝

$$F_{3^2} = \{0, 1, 2, \theta, 1 + \theta, 2 + \theta, 2\theta, 1 + 2\theta, 2 + 2\theta\}$$

Կառուցենք գումարման և բազմապատկման աղյուսակները կատարելով գումարում և բազմապատկում ըստ $\mathrm{mod}(2 + x + x^2)$-ի, այսինքն օգտվելով այն բանից, որ $2 + \theta + \theta^2 = 0$։ Օրինակ՝ $\theta \times \theta = \theta^2 = -2 - \theta = 1 + 2\theta$։

Գումարման աղյուսակ՝

$+$	0	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
0	0	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
1	■	2	0	$1+\theta$	$2+\theta$	θ	$1+2\theta$	$2+2\theta$	2θ
2	■	■	1	$2+\theta$	θ	$1+\theta$	$2+2\theta$	2θ	$1+2\theta$
θ	■	■	■	2θ	$1+2\theta$	$2+2\theta$	0	1	2
$1+\theta$	■	■	■	■	$2+2\theta$	2θ	1	2	0
$2+\theta$	■	■	■	■	■	$1+2\theta$	2	0	1
2θ	■	■	■	■	■	■	θ	$1+\theta$	$2+\theta$
$1+2\theta$	■	■	■	■	■	■	■	$2+\theta$	θ
$2+2\theta$	■	■	■	■	■	■	■	■	$1+\theta$

Բազմապատկման աղյուսակ՝

$\times$	0	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
0	0	0	0	0	0	0	0	0	0
1	■	1	2	θ	$1+\theta$	$2+\theta$	2θ	$1+2\theta$	$2+2\theta$
2	■	■	1	2θ	$2+2\theta$	$1+2\theta$	θ	$2+\theta$	$1+\theta$
θ	■	■	■	$1+2\theta$	1	$1+\theta$	$2+\theta$	$2+2\theta$	2
$1+\theta$	■	■	■	■	$2+\theta$	2θ	2	θ	$1+2\theta$
$2+\theta$	■	■	■	■	■	2	$2+2\theta$	1	θ
2θ	■	■	■	■	■	■	$1+2\theta$	$1+\theta$	1
$1+2\theta$	■	■	■	■	■	■	■	2	2θ
$2+2\theta$	■	■	■	■	■	■	■	■	$2+\theta$

Հաշվենք θ-ի աստիճանները՝

$$
\begin{aligned}
\theta^0 &= 1\\
\theta^1 &= \theta\\
\theta^2 &= 1 + 2\theta\\
\theta^3 &= \theta(1 + 2\theta) = \theta + 2\theta^2 = \theta + 2(1 + 2\theta) = 2 + 2\theta\\
\theta^4 &= \theta(2 + 2\theta) = 2\theta + 2\theta^2 = 2\theta + 2 + 4\theta = 2\\
\theta^5 &= 2\theta\\
\theta^6 &= 2\theta^2 = 2 + \theta\\
\theta^7 &= \theta(2 + \theta) = 2\theta + \theta^2 = 2\theta + 1 + 2\theta = 1 + \theta\\
\theta^8 &= \theta(1 + \theta) = \theta + \theta^2 = \theta + 1 + 2\theta = 1
\end{aligned}
$$

Ստացվում է, որ θ-ի աստիճաններով ներկայացվում են F_{3^2} դաշտի բոլոր ոչ զրոյական տարրերը, այսինքն ոչ զրոյական տարրերը կազմում են ցիկլիկ խումբ ըստ բազմապատկման: Ստորև կապացուցենք, որ դա տեղի ունի բոլոր վերջավոր դաշտերի համար:

Այսուհետև F_q^*-ով կնշանակենք F_q դաշտի ոչ զրոյական տարրերի բազմությունը, որն ակնհայտորեն կազմում է $q-1$ կարգի խումբ ըստ բազմապատկման գործողության: F_q^*-ը կոչվում է դաշտի **մուլտիպլիկատիվ խումբ**: Ուրեմն, յուրաքանչյուր $\alpha \in F_q^*$ բավարարում է $x^{q-1} = 1$ հավասարմանը, իսկ յուրաքանչյուր տարր F_q-ից՝ $x^q = x$ հավասարմանը: Քանի որ $x^q - x$ բազմանդամն ունի ոչ ավել, քան q հատ արմատ, ապա ստույգ է, որ

$$x^q - x = \prod_{\alpha \in F_q} (x - \alpha) \tag{44}$$

Պնդում 34.

Դիցուք $F_q \subset K$, որտեղ K-ն մեկ այլ վերջավոր դաշտ է: Որպեսզի K դաշտի α տարրը պատկանի F_q դաշտին անհրաժեշտ է և բավարար, որ $\alpha^q = \alpha$:

Ապացույց. $\alpha^q = \alpha$ պայմանը տեղի ունի միայն և միայն այն ժամանակ, երբ α-ն $x^q - x$ բազմանդամի արմատն է: Համաձայն (44) բանաձևի $x^q - x$ բազմանդամի արմատները F_q դաշտի բոլոր տարրերն են:

Թեորեմ 35.

F_q դաշտի մուլտիպլիկատիվ խումբը ցիկլիկ է:

Ապացույց. Ունենք, որ F_q^*-ի կարգը (տարրերի քանակը) հավասար է $q-1$: Դիտարկենք $q-1$-ի վերլուծությունը պարզ թվերի արտադրյալի՝ $q-1 = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$: Նշանակենք $h_i = p_i^{k_i}$, $i = 1, 2, \ldots, s$: Ինչպես գիտենք (Բեզուի թեորեմից) $x^{\frac{q-1}{p_i}} - 1$ բազմանդամի արմատների քանակը F_q^*-ում չի գերազանցում $\frac{q-1}{p_i}$ թիվը, ուստի կգտնվի $\alpha_i \in F_q^*$, որի համար $\alpha_i^{\frac{q-1}{p_i}} \neq 1$, $i = 1, 2, \ldots, s$: Նշանակենք $\beta_i = \alpha_i^{\frac{q-1}{h_i}}$, $i = 1, 2, \ldots, s$: Պարզ է, որ $\beta_i^{h_i} = \alpha_i^{q-1} = 1$, ուստի β_i-ի կարգը h_i-ի բաժանարար է, այսինքն p_i^m տեսքի թիվ է, որտեղ $m \leq k_i$: Եթե $m < k_i$, ապա $1 = \beta_i^{p_i^m}$ և

$$1 = \left(\beta_i^{p_i^m}\right)^{p_i^{k_i-m-1}} = \beta_i^{p_i^{k_i-1}} = \left(\alpha_i^{\frac{q-1}{h_i}}\right)^{p_i^{k_i-1}} = \alpha_i^{\frac{q-1}{p_i}} \neq 1 :$$

Ուստի՝ $m = k_i$ և β_i-ի կարգը հավասար է h_i-ի:

Նշանակենք՝ $\beta = \beta_1\beta_2\ldots\beta_s$: Ստուգենք, որ β-ի կարգը հավասար է $q-1$-ի, այսինքն β-ն F_q^*-ի ծնիչն է, ուստի F_q^*-ը ցիկլիկ խումբ է: Ակնհայտ է, որ $\beta^{q-1} = 1$: Դիցուք β-ի կարգը $q-1$-ի բաժանարար է, որը տարբեր է $q-1$-ից: Այդ դեպքում β-ի կարգը կլինի $\frac{q-1}{p_1}, \frac{q-1}{p_2}, \ldots, \frac{q-1}{p_s}$ թվերից մեկի բաժանարարը: Որոշակիության համար ենթադրենք, որ β-ի կարգը $\frac{q-1}{p_1}$-ի բաժանարարն է: Այդ դեպքում $\beta^{\frac{q-1}{p_1}} = 1$ և $\beta_i^{\frac{q-1}{p_1}} = \left(\beta_i^{h_i}\right)^{p_1^{k_1-1}h_1\ldots h_{i-1}h_{i+1}\ldots h_s} = 1$ բոլոր $i \in \{2,\ldots,s\}$: Որեմն՝ $\beta_1^{\frac{q-1}{p_1}} = 1$ և $\frac{q-1}{p_1}$-ը պետք է լինի պատիկ β_1-ի կարգին՝ $h_1 = p_1^{k_1}$-ին, սակայն դա այդպես չէ: Հետևաբար β-ի կարգը $q-1$ է: Թեորեմն ապացուցված է:

Վերջավոր դաշտի ենթադաշտերը

Այժմ նկարագրենք վերջավոր դաշտի բոլոր ենթադաշտերը:

Պնդում 36.

1. $x^m - 1$ բազմանդամն առանց մնացորդի բաժանվում է $x^k - 1$ բազմանդամի վրա միայն և միայն այն դեպքում, երբ m-ը առանց մնացորդի բաժանվում է k-ի վրա

2. a դրական թվի համար $a^m - 1$-ը առանց մնացորդի բաժանվում է $a^k - 1$-ի վրա միայն և միայն այն դեպքում, երբ m-ը առանց մնացորդի բաժանվում է k-ի վրա

Ապացույց. Ապացուցենք 1.-ը: Ակնհայտ է, որ $m \geq k$: Բաժանենք մնացորդով m-ը k-ի վրա՝ $m = kt + r,\ 0 \leq r < k$, ապա

$$\frac{x^m - 1}{x^k - 1} = x^r \frac{x^{kt} - 1}{x^k - 1} + \frac{x^r - 1}{x^k - 1}$$

Քանի որ $\frac{x^{kt} - 1}{x^k - 1} = (x^k)^{t-1} + (x^k)^{t-2} + \ldots + x^k + 1$, ապա $\frac{x^m - 1}{x^k - 1}$-ը բազմանդամ է միայն և միայն այն դեպքում, երբ $\frac{x^r - 1}{x^k - 1}$-ն է բազմանդամ: Սակայն ակնհայտ է, որ $\frac{x^r - 1}{x^k - 1}$-ը բազմանդամ է միայն երբ $r = 0$:

Պնդման 2. կետն ապացուցվում է նմանապես:

Թեորեմ 37.

Դիցուք տրված է F_{p^n} դաշտը։ n-ի յուրաքանչյուր d բաժանարարի համար գոյություն ունի F_{p^n} դաշտի միակ F_{p^d} ենթադաշտը։ F_{p^n} դաշտը այլ ենթադաշտեր չունի։

Ապացույց. Ակնհայտ է, որ F_{p^n} դաշտի բոլոր ենթադաշտերն ունեն միևնույն բնութագրիչը, որն հավասար է p-ի։ Դիցուք $F_{p^d} \subset F_{p^n}$։ Ապացուցենք, որ d-ն n-ի բաժանարարն է։ $F_{p^d}^*$-ի տարրերը $p^d - 1$ հատ են և բավարարում են $x^{p^d-1} - 1 = 0$ հավասարմանը, սակայն դրանք նաև $F_{p^n}^*$-ից են և բավարարում են $x^{p^n-1} - 1 = 0$ հավասարմանը, ուստի համաձայն (44) բանաձևի ստանում ենք, որ $x^{p^n-1} - 1$ բազմանդամը բաժանվում է $x^{p^d-1} - 1$ բազմանդամի վրա առանց մնացորդի։ Համաձայն Պնդում 36-ի 1. կետի $p^n - 1$-ը բաժանվում է $p^d - 1$-ի վրա, իսկ համաձայն նույն պնդման 2. կետի n-ը բաժանվում է d-ի վրա։

Դիցուք այժմ d-ն n-ի բաժանարարն է։ Ապացուցենք, որ F_{p^n} դաշտը պարունակում է F_{p^d} ենթադաշտը և այն միակն է։ Նշանակենք՝ $E = \{\alpha \in F_{p^n} \mid \alpha^{p^d} = \alpha\}$։ Այս բազմությունը դաշտ է։ Իսկապես, եթե $\alpha, \beta \in E$, ապա

$$(\alpha+\beta)^{p^d} \underbrace{=}_{\text{համաձայն } (43)} \alpha^{p^d} + \beta^{p^d} = \alpha + \beta$$

$$(\alpha\beta)^{p^d} = \alpha^{p^d}\beta^{p^d} = \alpha\beta$$

$$(\alpha^{-1})^{p^d} = \left(\alpha^{p^d}\right)^{-1} = \alpha^{-1} \text{ կամայական } \alpha \neq 0 \text{ համար}$$

Այսպիսով, $0, 1 \in E$, նաև $\alpha, \beta \in E \Rightarrow \alpha + \beta, \alpha\beta \in E$ և, վերջապես, $0 \neq \alpha \in E \Rightarrow \alpha^{-1} \in E$։ Ուստի, E-ն դաշտ է։

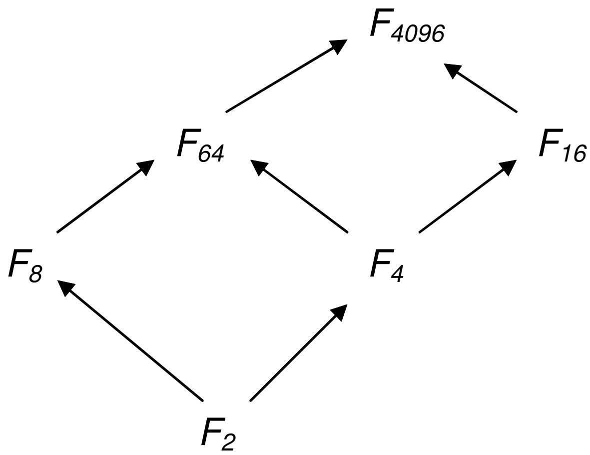
Ունենք, որ E^*-ի տարրերը $x^{p^d-1} - 1$ բազմանդամի արմատներն են F_{p^n} դաշտում։ Քանի որ d-ն n-ի բաժանարարն է, ապա համաձայն

Պնդում 36-ի p^n-1-ը բաժանվում է p^d-1-ի վրա և $x^{p^n-1}-1$ բազմանդամը բաժանվում է $x^{p^d-1}-1$ բազմանդամի վրա: Որեմն, $x^{p^n}-x$ բազմանդամը բաժանվում է $x^{p^d}-x$ բազմանդամի վրա և կգտնվի մի $g(x)$ բազմանդամ, որ $x^{p^n}-x=\left(x^{p^d}-x\right)g(x)$ և $\deg g(x)=p^n-p^d$: Ինչպես գիտենք, $x^{p^n}-x$ բազմանդամն ունի ճիշտ p^n հատ տարբեր պարզ (ոչ պատիկ) արմատ, որոնք կազմում են F_{p^n} դաշտը: Քանի որ $x^{p^d}-x$ և $g(x)$ բազմանդամները $x^{p^n}-x$-ի բաժանարարներն են, ապա դրանց արմատները նույնպես պարզ են (պատիկ չեն): Ակնհայտ է, որ $\left(x^{p^d}-x\right)g(x)$-ի արմատների քանակը դա $x^{p^d}-x$-ի և $g(x)$-ի արմատների քանակների գումարն է: Եթե $x^{p^d}-x$ բազմանդամի արմատների քանակը p^d-ից փոքր է, ապա $x^{p^n}-x=\left(x^{p^d}-x\right)g(x)$-ի արմատների քանակը կլինի փոքր $p^d+(p^n-p^d)=p^n$-ից, ինչն անհնար է: Հետևաբար $x^{p^d}-x$ բազմանդամն ունի ճիշտ p^d հատ տարբեր պարզ արմատ, որոնք էլ կազմում են F_{p^d} դաշտը: Այսինքն՝ $E=F_{p^d}$:

Եթե H-ը մեկ այլ ենթադաշտ է F_{p^n}-ում և ունի p^d հատ տարր, ապա համաձայն Պնդում 34-ի այդ տարրերը պետք է բավարարեն $x^{p^d}-x=0$ հավասարմանը, այսինքն $H=E$: Թեորեմն ապացուցված է:

Օրինակ

Նկարագրենք $F_{4096}=F_{2^{12}}$ դաշտի բոլոր ենթադաշտերը: Համաձայն Թեորեմ 37-ի ստանում ենք ենթադաշտերի ներդրվածության հետևյալ պատկերը՝


F_{4096}
F_{64}
F_{16}
F_8
F_4
F_2

Վերջավոր դաշտերի գոյությունը

Պնդում 38.

Դիցուք $f(x) \in F_p[x]$ անվերածելի բազմանդամ է: $x^{p^k} - x$ բազմանդամը բաժանվում է առանց մնացորդի $f(x)$-ի վրա միայն և միայն այն դեպքում, երբ k-ն բաժանվում է առանց մնացորդի $\deg f(x)$-ի վրա:

Ապացույց. Դիցուք $\deg f(x) = n$ և $x^{p^k} - x$-ը բաժանվում է $f(x)$-ի վրա: Ինչպես գիտենք, F_{p^n} դաշտը ստացվում է որպես $F_p[x] \diagup (f(x))$ և θ-ն դա x բազմանդամի հարակից դասն է: Գիտենք նաև, որ F_{p^n} դաշտի կամայական տարր ներկայացվում է $1, \theta, \theta^2, \ldots, \theta^{n-1}$ տարրերի գծային կոմբինացիայով: Վերցնենք F_{p^n} դաշտի կամայական տարր՝ $\gamma_0 + \gamma_1\theta + \ldots + \gamma_{n-1}\theta^{n-1}$, $\gamma_i \in F_p$, $i = 0, 1, \ldots, n-1$: Քանի որ $\gamma_i \in F_p$ ստանում ենք՝ $\gamma_i^{p^k} = \gamma_i$ բոլոր $i = 0, 1, \ldots, n-1$ համար: Բարձրացնենք $\gamma_0 + \gamma_1\theta + \ldots + \gamma_{n-1}\theta^{n-1}$ տարրը p^k աստիճան՝

$$(\gamma_0 + \gamma_1\theta + \ldots + \gamma_{n-1}\theta^{n-1})^{p^k} = \gamma_0 + \gamma_1\theta^{p^k} + \ldots + \gamma_{n-1}\left(\theta^{p^k}\right)^{n-1}:$$

Քանի որ $x^{p^k} - x$-ը բաժանվում է $f(x)$-ի վրա, ապա $f(x)$-ի արմատը նաև $x^{p^k} - x$-ի արմատն է, ուստի θ-ն բավարարում է $\theta^{p^k} = \theta$ հավասարմանը և

$$(\gamma_0 + \gamma_1\theta + \ldots + \gamma_{n-1}\theta^{n-1})^{p^k} = \gamma_0 + \gamma_1\theta + \ldots + \gamma_{n-1}\theta^{n-1}:$$

Սրեմն F_{p^n} դաշտի բոլոր տարրերը $x^{p^k} - x$ բազմանդամի արմատներն են, հետևաբար F_{p^n}-ը F_{p^k}-ի ենթադաշտն է և համաձայն Թեորեմ 37-ի k-ն պետք է բաժանվի առանց մնացորդի n-ի վրա:

Դիցուք այժմ k-ն բաժանվում է առանց մնացորդի n-ի վրա: Ունենք, որ $\theta^{p^n} = \theta$ և θ-ն $x^{p^n} - x$-ի արմատն է, հետևաբար, ինչպես արդեն պարզել ենք, $x^{p^n}-x$-ը բաժանվում է $f(x)$-ի վրա ($F_p[x]$-ի բոլոր բազմանդամները, որոնց համար θ-ն արմատ է, բաժանվում են $f(x)$-ի վրա)։ Համաձայն Պնդում 36-ի $x^{p^k}-x$-ը իր հերթին բաժանվում է $x^{p^n}-x$-ի վրա, ուստի $x^{p^k}-x$-ը բաժանվում է $f(x)$-ի վրա։

Թեորեմ 39.

Դիցուք F_{p^n} դաշտը կառուցված է n-րդ աստիճանի անվերածելի $f(x)$ բազմանդամի միջոցով, այսինքն F_{p^n} դաշտը ստացված է որպես $F_p[x]/(f(x))$ և θ-ն դա x բազմանդամի հարակից դասն է։ Այս դեպքում $f(x)$ բազմանդամի բոլոր արմատները պարզ են (դրանց պատիկությունը 1 է), դրանք բոլորը պատկանում են F_{p^n}-ին և դրանք հետևյալն են՝

$$\theta, \theta^p, \theta^{p^2}, \ldots, \theta^{p^{n-1}}$$

Ապացույց. Դիցուք $f(x)=\alpha_0+\alpha_1x+\ldots+\alpha_nx^n$։ Քանի որ θ-ն արմատ է, ապա $f(\theta)=\alpha_0+\alpha_1\theta+\ldots+\alpha_n\theta^n=0$։ $f(x)$-ի գործակիցները F_p դաշտից են, հետևաբար $\alpha_i^p=\alpha_i$, $i=0,1,\ldots,n$։

Հաշվենք՝

$$f(\theta^p)=\alpha_0+\alpha_1\theta^p+\alpha_2(\theta^p)^2+\ldots+\alpha_n(\theta^p)^n=$$

$$\alpha_0^p+\alpha_1^p(\theta)^p+\alpha_2^p(\theta^2)^p+\ldots+\alpha_n^p(\theta^n)^p\text{։}$$

Համաձայն (43)-ի ստանում ենք՝

$$f(\theta^p)=(\alpha_0+\alpha_1\theta+\alpha_2\theta^2+\ldots+\alpha_n\theta^n)^p=0$$

և θ^p-ն նույնպես արմատ է։ Նմանապես ապացուցվում է, որ արմատներ են նաև $\theta^{p^2},\ldots,\theta^{p^{n-1}}$ տարրերը։

Ցույց տանք այժմ, որ $\theta,\theta^p,\theta^{p^2},\ldots,\theta^{p^{n-1}}$ արմատները տարբեր են: Դիցուք $\theta^{p^k}=\theta^{p^m}$, որտեղ $0\le k<m\le n-1$: Հավասարության երկու կողմերը բարձրացնենք p^{n-m} աստիճան՝ $\left(\theta^{p^k}\right)^{p^{n-m}}=(\theta^{p^m})^{p^{n-m}}$: Ուստի, $\theta^{p^{n+k-m}}=\theta$ և θ-ն $x^{p^{n+k-m}}-x$ բազմանդամի արմատ է: Ինչպես գիտենք $F_p[x]$-ի յուրաքանչյուր բազմանդամ, որի համար θ-ն արմատ է, բաժանվում է առանց մնացորդի $f(x)$-ի վրա: Հետևաբար $x^{p^{n+k-m}}-x$ բազմանդամը բաժանվում է $f(x)$-ի վրա: Համաձայն Պնդում 38-ի $n+k-m$-ը բաժանվում է n-ի վրա: Սակայն $n+k-m<n$ և n-ը չի կարող լինել $n+k-m$-ի բաժանարար: Ուստի բոլոր $\theta,\theta^p,\theta^{p^2},\ldots,\theta^{p^{n-1}}$ արմատները տարբեր են: Քանի որ այս արմատների քանակը հավասար է $f(x)$-ի աստիճանին, ապա բոլոր արմատների պատիկությունը 1 է: Թեորեմն ապացուցված է:

Թեորեմ 40.

***Դիցուք** $P_d(x)$-ը $F_p[x]$-ում բոլոր d աստիճանի անվերածելի նորմավորված (x փոփոխականի ամենամեծ աստիճանի գործակիցը հավասար է 1-ի) բազմանդամների արտադրյալն է: Ստույգ է հետևյալ բանաձևը՝*

$$x^{p^n}-x=\prod_{d\,|\,n}P_d(x)$$

Ապացույց. Համաձայն Թեորեմ 25-ի հետևանքի $F_p[x]$-ը ֆակտորիալ օղակ է և $x^{p^n}-x$ բազմանդամը միարժեքորեն ներկայացվում է անվերածելի բազմանդամների արտադրյալով: Այդ ներկայացման մեջ յուրաքանչյուր անվերածելի արտադրիչ կփոխարինենք նրան ասոցիացված նորմավորված բազմանդամով փակագծերից դուրս հանելով x-ի ամենամեծ աստիճանի գործակիցը: Քանի որ $x^{p^n}-x$ բազմանդամը նորմավորված է, ապա այդ գործակիցների արտադրյալը կլինի հավասար 1-ի:

Համաձայն Պնդում 38-ի, $f(x)$ անվերածելի բազմանդամը $x^{p^n}-x$ բազմանդամի բաժանարար է միայն և միայն այն դեպքում, երբ $\deg f(x)$-ը n-ի բաժանարարն է: Ուրեմն $x^{p^n}-x$-ը բոլոր այն անվերածելի նորմավորված բազմանդամների արտադրյալն է, որոնց աստիճանը n-ի բաժանարարն է: Թեորեմն ապացուցված է:

Նշանակենք N_d-ով $F_p[x]$-ում բոլոր d աստիճանի անվերածելի նորմավորված բազմանդամների քանակը:

Թեորեմ 40-ի բանաձևի աջ և ձախ մասերի աստիճաններն իրար հավասարեցնելով ստանում ենք՝

$$p^n = \sum_{d|n} dN_d \qquad (45)$$

Թեորեմ 41.

Յուրաքանչյուր $n \geq 1$ համար $F_p[x]$-ում գոյություն ունի n-րդ աստիճանի անվերածելի բազմանդամ:

Ապացույց. $n = 1$ դեպքում կամայական գծային բազմանդամ անվերածելի է, այդ պատճառով համարենք, որ $n \geq 2$: (45)-ից հետևում է, որ $p^n \geq nN_n$ բոլոր $n \geq 1$ համար: Նշանակենք $\lfloor m \rfloor$-ով m

թվի ամբողջ մասը: Քանի որ n-ի ամենամեծ բաժանարարը կամ $\frac{n}{2}$ է (զույգ n-ի դեպքում), կամ էլ չի գերազանցում $\lfloor \frac{n}{2} \rfloor$-ը, ապա

$$p^n = nN_n + \sum_{\substack{d \mid n \\ d \neq n}} dN_d \leq nN_n + \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} dN_d \leq$$

$$nN_n + \sum_{d=1}^{\lfloor \frac{n}{2} \rfloor} p^d \leq nN_n + \frac{n}{2} p^{\frac{n}{2}}$$

և

$$nN_n \geq p^n - \frac{n}{2} p^{\frac{n}{2}} \tag{46}$$

Մյուս կողմից, քանի որ $n \geq 2$, ապա

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \geq 1 + n + \frac{n(n-1)}{2} =$$

$$\frac{n^2 + n + 2}{2} > \frac{n^2}{4},$$

ուստի $2^{\frac{n}{2}} > \frac{n}{2}$: Հետևաբար, $p^{\frac{n}{2}} \geq 2^{\frac{n}{2}} > \frac{n}{2}$ և $p^n > \frac{n}{2} p^{\frac{n}{2}}$: Վերջապես, (46)-ից ստանում ենք, որ $nN_n > 0$ և $N_n > 0$: Թեորեմն ապացուցված է:

Հետևանք

Յուրաքանչյուր p պարզ թվի և $n \geq 1$ բնական թվի համար գոյություն ունի F_{p^n} վերջավոր դաշտը:

ԳՐԱԿԱՆՈՒԹՅՈՒՆ

1. С.Ленг. **Алгебра**, “Мир”, Москва 1968
2. Б.Л. ван дер Варден. **Алгебра**, “Наука”, Москва 1979
3. А.И.Кострикин. **Введение в алгебру**, “Наука”, Москва 1977
4. М.И.Каргаполов, Ю.И.Мерзляков. **Основы теории групп**, “Наука”, Москва 1972
5. М.Холл. **Теория групп**, ИЛ.,Москва 1962
6. Р.Лидл, Г.Нидеррайтер. **Конечные поля**, Том. 1, “Мир”, Москва 1988