IV skyrius. GRUPĖS

1. Grupės

1. 1 Šiame skyriuje nagrinėsime grupes,vieną iš labai svarbių algebrinių struktūrų, apibrėžiamų vienu aibės elementų vidiniu kompozicijos dėsniu, tenkinančiu tam tikras aksiomas.Tai paprasčiausias atvejis ta prasme, kad struktūra aibėje yra apibrėžiama vienu kompozicijos dėsniu.

Apibrėžimas. Aibė G joje apibrėžto kompozicijos dėsnio $*$ atžvilgiu yra vadinama grupe, jei

1. Kompozicijos dėsnis $*$ yra asociatyvus, t.y. bet kuriems g_1, g_2, $g_3 \in G$, teisinga lygybė

$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)).$$

Formaliai ši aksioma užrašoma taip:

$$\forall(g_1, g_2, g_3 \in G)((g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)).$$

2. Egzistuoja neutralus elementas $1 \in G$ kompozicijos dėsnio $*$ atžvilgiu, t.y. kiekvienam $g \in G$ teisinga lygybė

$$1 * g = g * 1 = g.$$

Elementas 1 yra vadinamas grupės vienetu ir,kaip žinome [?],yra vienintelis.

3. Kiekvienam elementui $g \in G$ egzistuoja simetrinis elementas g^{-1} kompozicijos dėsnio $*$ atžvilgiu:

$$g * g^{-1} = g^{-1} * g = 1.$$

Elementas g^{-1} yra vadinamas atvirkštiniu elementu elementui g ir,kaip žinome [ ], yra vienintelis.

1. 2. Apibrėžimas. Grupė $(G, *)$ yra vadinama komutatyviąja (arba Abelio) grupe, jei kompozicijos dėsnis $*$ yra komutatyvus.

Abelio grupės sudaro svarbią grupių klasę, bet grupės, vaidinančios ypatingą vaidmenį teorinėje fizikoje, fizikinės chemijos, kristalų bei kitose teorijose, jau nekalbant apie matematiką, beveik be išimčių yra nekomutatyvios. Todėl apsiriboti tik komutatyviosiomis grupėmis netikslinga.

Grupės apibrėžime 2-ąją ir 3-iąją aksiomas galima pakeisti silpnesnėmis.

1. 3. Antrasis grupės apibrėžimas. Aibė G joje apibrėžto jos elementų kompozicijos dėsnio $*$ atžvilgiu yra vadinama grupe, jei

1'. Kompozicijos dėsnis $*$ yra asociatyvus.

2'. Egzistuoja aibės G toks elementas e, kad kiekvienam $g \in G$

$$e * g = g$$

.
Šiuo atveju e yra vadinamas kairiuoju grupės vienetu.

3'. Kiekvienam aibės G elementui g egzistuoja aibės G toks elementas h, kad

$$h * g = e.$$

Šiuo atveju h yra vadinamas kairiuoju atvirkštiniu elementu elementui g.

1. 4. Įrodysime, kad šie grupės apibrėžimai yra ekvivalentūs. Visiškai akivaizdu, jei $(G, *)$ yra grupė pirmojo apibrėžimo prasme, tai $(G, *)$ yra grupė ir antrojo apibrėžimo prasme. Atvirkščiojo teiginio įrodymą sudaro keleto atskirų teiginių įrodymai.

1. Teiginys. Jei $(G, *)$ yra grupė antrojo apibrėžimo prasme, tai lygties $x * x = x$ sprendinys grupėje $(G, *)$ yra $x = e$.

Įrodymas. Jei grupės $(G, *)$ elementas x tenkina sąlygą $x * x = x$, tai šios lygybės abi puses iš kairės padauginę iš elementui x kairiojo atvirkštinio elemento y, gauname: $y * (x * x) = y * x$. Bet $y * (x * x) = (y * x) * x = e * x = x$, o $y * x = e$. Vadinasi, $x = e$. $\triangle$

2. Teiginys. Jei $(G, *)$ yra grupė antrojo apibrėžimo prasme, tai kiekvienam $g \in G$

1. $g * e = g$(kitaip tariant e yra grupės vienetas);
2. Jei h yra kairysis atvirkštinis elementas elementui g, tai h yra ir dešinysis atvirkštinis elementas elementui g.

Įrodymas. Pirmiausia įrodysime antrąją teiginio dalį. Jei h yra kairysis atvirkštinis elementas elementui g, tai galime parašyti lygybes:

$$g * h = g * e * h = g * (h * g) * h = (g * h) * (g * h),$$

t. y. elementas $g * h$ tenkina sąlygą: $(g * h) * (g * h) = g * h$. Remdamiesi 1-uoju teiginiu, gauname, kad $g * h = e$. Vadinasi, h yra tiek kairysis, tiek ir dešinysis atvirkštinis elementas elementui g.

Dabar įrodysime pirmąją teiginio dalį. Remdamiesi 2-ąją įrodyta teiginio dalimi, galime parašyti:

$$g * e = g * (h * g) = (g * h) * g = e * g = g,$$

t. y. $g * e = g$, čia h – atvirkštinis elementas elementui g. $\triangle$

1. 5. Dviejų grupės apibrėžimų ekvivalentumas. Taigi grupės $(G, *)$ antrojo apibrėžimo prasme kairysis vienetas e tenkina pirmojo grupės apibrėžimo 2-ąją aksiomą,

o elementui g kairysis atvirkštinis elementas h tenkina pirmojo grupės apibrėžimo 3-iąją aksiomą. Taigi abu grupės apibrėžimai yra ekvivalentūs.

Būtų galima pateikti ir trečiąjį grupės apibrėžimą, antrajame grupės apibrėžime žodį "kairysis" pakeičiant žodžiu "dešinysis" ir įrodyti visų apibrėžimų ekvivalentumą. Tai padaryti paliekame skaitytojui.

1. 6. Įrodysime paprastą faktą.

Teiginys. Tarkime, $(G, *)$ – grupė, $g, h \in G$. Tuomet $(g * h)^{-1} = h^{-1} * g^{-1}$.

Įrodymas. Elementas $(g * h)^{-1}$ yra atvirkštinis elementui $g * h$. Įsitikinsime, kad ir $h^{-1} * g^{-1}$ taip pat yra atvirkštinis elementas elementui $g * h$. Iš tikrųjų,

$$(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * 1 * g^{-1} = g * g^{-1} = 1.$$

Kadangi kiekvienam grupės elementui egzistuoja tik vienintelis atvirkštinis elementas, tai $(g * h)^{-1} = h^{-1} * g^{-1}$. $\triangle$

1. 7. Apibrėšime grupės elementų laipsnius sveikaisiais skaičiais. Tarkime, kad g yra grupės $(G, *)$ elementas. Sutarkime, kad $g^0 = 1, g^1 = g$. Elemento g $n-$ąjį laipsnį, $n > 0$, galima apibrėžti induktyviai: $g^n =: g * g^{n-1}$. Jei $n < 0$, tai elemento g $n-$ąjį laipsnį apibrėžiame taip: $g^n = (g^{-1})^{-n}$ (čia $-n > 0$).

Pratimai.

Įrodykite lygybes:
1. $g^m * g^n = g^{m+n}, m, n \in \mathbb{Z}$.
2. $(g^m)^n = g^{m \cdot n}, m, n \in \mathbb{Z}$.

Pastaba. Abelio grupės kompozicijos dėsnis dažniausiai yra žymimas + ir vadinamas grupės elementų sudėtimi, neutralus elementas – 0 ir vadinamas nuliumi, o elementui g simetrinis elementas yra žymimas $-g$ ir vadinamas priešingu elementų elementui g. Šie žymėjimai yra vadinami adiciniais, o ankstesni, kuriais iki šiol naudojomės, – multiplikaciniais. Perėjimas nuo multiplikacinių žymėjimų prie adicinių ir atvirkščiai – labai paprastas:

grupės elementas $x_1^{n_1} * x_2^{n_2} * \ldots * x_s^{n_s}$ multiplikaciniame žymėjime yra pakeičiamas grupės elementu $n_1 * x_1 + n_2 * x_2 + \ldots + n_s * x_s$ adiciniame žymėjime ir atvirkščiai, 1 – elementu 0 ir t. t.

1. 8. Apibrėžimas. Jei grupės $(G, *)$ aibė G yra baigtinė, tai grupė $(G, *)$ yra vadinama baigtine, o aibės G elementų skaičius $|G|$ yra vadinamas grupės $(G, *)$ eile. Jei grupės $(G, *)$ aibė G yra begalinė, tai grupė $(G, *)$ yra vadinama begaline.

Susitarimas. Dažniausiai paprastumo dėlei naudojant multiplikacinius žymėjimus tarp komponuojamųjų elementų nerašysime kompozicijo dėsnio ženklo.

Pavyzdžiai.

1. Akivaizdu, kad $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ – begalinės Abelio grupės.

2. Akivaizdu, kad $(\mathbb{Q}_+^*,\cdot),(\mathbb{R}_+^*,\cdot),(\mathbb{Q}^*,\cdot),(\mathbb{R}^*,\cdot)$ – begalinės Abelio grupės.

3. X – aibė, $P(X)$ – aibės X visų poaibių aibė. $(\mathbf{P}(X),\ominus)$ – Abelio grupė, nes
   1. $\ominus$ – simetrinė aibių atimtis yra asociatyvus kompozicijos dėsnis;
   2. $\emptyset$ – neutralus elementas simetrinės aibių atimties $\ominus$ atžvilgiu;
   3. Elementui $Y\in\mathbf{P}(X)$ (t. y. $Y\subset X$) simetrinis elementas yra Y (nes $Y\ominus Y=\emptyset$).

Jei X – baigtinė aibė ir $|X|=n$, tai grupės $\mathbf{P}(X)$ eilė lygi $|\mathbf{P}(X)|=2^n$.

4. **Simetrinė grupė.** Tarkime, kad X – netuščia aibė. $(AutX,\circ)$ – grupė, nes, kaip žinome:
   1. $\circ$ – asociatyvus kompozicijos dėsnis;
   2. $AutX\ni\mathrm{id}$ – neutralus elementas atvaizdžių kompozicijos $\circ$ atžvilgiu (priminsime, kad $\mathrm{id}(x)=x, x\in X$);
   3. $f\in AutX\Rightarrow f^{-1}\in AutX, f\circ f^{-1}=f^{-1}\circ f=\mathrm{id}$.

Jei X – begalinė aibė, tai ir grupė $(AutX,\circ)$ – begalinė. Jei $|X|=n$, tai šiuo atveju grupė $(AutX,\circ)$ yra žymima S_n (arba Σ_n) ir yra vadinama n-ojo laipsnio simetrine grupe.

n-ojo laipsnio simetrinės grupės S_n elementus galima nagrinėti kaip bijekcijas $f:\mathbb{N}_n\to\mathbb{N}_n$, čia $\mathbb{N}_n=\{1,2,\dots,n\}$. Pastebėsime, kad vietoje $\mathbb{N}_n$ galima imti bet kurią baigtinę aibę, turinčią n elementų. Dažnai bijekcija $f:X\to X$, kai X – baigtinė aibė, yra vadinama aibės X elementų keitiniu. Bijekciją $f:\mathbb{N}_n\to\mathbb{N}_n$ galima pavaizduoti lentele

$$\begin{pmatrix}1 & 2 & \dots & n\\ f(1) & f(2) & \dots & f(n)\end{pmatrix},$$

pirmoje eilutėje bet kuria tvarka surašius visus aibės $\mathbb{N}_n$ elementus (duotoje lentelėje aibės $\mathbb{N}_n$ elementai surašyti natūralia tvarka), o antroje eilutėje po kiekvienu pirmos eilutės elementu j parašius jo vaizdą $f(j)$. Kadangi f – bijekcija, tai $f(1),f(2),\dots,f(n)$, – visi tarpusavy skirtingi elementai. Dar kartą pabrėžiame, kad lentelės pirmoje eilutėje aibės $\mathbb{N}_n$ elementų tvarka nesvarbi, bet svarbu, kas parašyta po kiekvienu pirmos eilutės elementu! Pavyzdžiui, lentelės

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix},\begin{pmatrix}3 & 2 & 1\\ 1 & 3 & 2\end{pmatrix}$$

apibrėžia vieną ir tą patį atvaizdį $f:\mathbb{N}_3\to\mathbb{N}_3$. Tarp lentelių, vaizduojančių vieną ir tą patį atvaizdį, rašysime lygybės ženklą. Pavyzdžiui,

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}=\begin{pmatrix}3 & 2 & 1\\ 1 & 3 & 2\end{pmatrix},$$

bet

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\neq\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}.$$

Dabar nesunku suskaičiuoti, kiek elementų turi grupė S_n. Tuo tikslu reikia suskaičiuoti, kiek galima sudaryti lentelių

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

vaizduojančių visas skirtingas bijekcijas $f : \mathbb{N}_n \to \mathbb{N}_n$. Akivaizdu, kad po 1-ju galima parašyti bet kurį aibės $\mathbb{N}_n$ elementą, po 2-ju galima parašyti bet kurį vieną iš likusių $n-1$ aibės $\mathbb{N}_n$ elementų ir t. t.. Vadinasi, galima sudaryti iš viso $n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1 = n!$ skirtingų lentelių, t. y. $|S_n| = n!$.

Tarkime, kad

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}, g = \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix}$$

– bijekcijos.

Tuomet

$$f \circ g = f \circ \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ f(g(1)) & f(g(2)) & \dots & f(g(n)) \end{pmatrix},$$

nes kiekvienam j:

$$j \xrightarrow{g} g(j) \xrightarrow{f} f(g(j)).$$

Pastebėsime, kad

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Iš tikrųjų:

$$f \circ f^{-1} = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} \circ \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix} =$$

$$\begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = \mathrm{id}.$$

5. **Grupė** S_3.

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Pažymėkime

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Tuomet

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma^2 \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$\sigma^3 = \mathrm{id}, \tau^2 = \mathrm{id}$. Taigi $S_3 = \{\mathrm{id}, \sigma, \sigma^2, \tau, \sigma \circ \tau, \sigma^2 \circ \tau\}$, t. y. grupės S_3 elementai yra išreiškiami elementų σ ir τ sandaugomis. Elementus σ ir τ sieja lygybės

$$\sigma^3 = \tau^2 = \mathrm{id}, \ \ \tau \circ \sigma \circ \tau = \sigma^2.$$

Šių lygybių pakanka tam, kad galėtume atstatyti grupės S_3 elementų daugybos lentelę. Pavyzdžiui,

$$\tau \circ \sigma = \tau \circ \sigma \circ (\tau \circ \tau) = (\tau \circ \sigma \circ \tau) \circ \tau = \sigma^2 \circ \tau;$$

$$(\sigma \circ \tau) \circ (\sigma^2 \circ \tau) = \sigma \circ \tau \circ \sigma \circ \sigma \circ \tau = \sigma \circ \tau \circ \sigma \circ \tau \circ \tau \circ \sigma \circ \tau =$$

$$= \sigma \circ (\tau \circ \sigma \circ \tau) \circ (\tau \circ \sigma \circ \tau) = \sigma \circ \sigma^2 \circ \sigma^2 = \sigma^3 \circ \sigma^2 = \mathrm{id} \circ \sigma^2 = \sigma^2;$$

$$\tau \circ (\sigma^2 \circ \tau) = \tau \circ \sigma \circ \sigma \circ \tau = \tau \circ \sigma \circ \tau \circ \tau \circ \sigma \circ \tau = \sigma^2 \circ \sigma^2 = \sigma^3 \circ \sigma = \sigma$$

ir t. t..

Pastaba. Atvaizdžių kompozicijos dėsnis yra žymimas $\circ$. Šiuo ženklu žymėjome ir simetrinės grupės elementų kompoziciją, nes simetrinės grupės elementus interpretavome kaip bijekcijas. Bet vietoje žymens $\circ$ renkant formules kompiuteriu patogiau rašyti $*$. Todėl dažnai, nors kai kurių grupių elementus ir interpretuosime kaip atvaizdžius, tarp komponuojamų elementų vietoje žymens $\circ$ rašysime $*$.

6. **Diedro grupė** D_n (abstrakčiojo arba kombinatorinio taisyklingojo n-kampio simetrijų grupė).

Tarkime, kad aibė $\mathcal{F} = \{\{1,2\},\{2,3\},\dots\{n-1,n\},\{n,1\}\}$, t. y. sudaryta iš aibės $\mathbb{N}_n$ nurodytų poaibių. Porą $(\mathbb{N}_n, \mathcal{F})$ pavadinsime abstrakčiuoju taisyklinguoju n-kampiu. Bijekciją $f : \mathbb{N}_n \to \mathbb{N}_n$, tenkinančią sąlygą $X \in \mathcal{F} \iff f(X) \in \mathcal{F}$, pavadinsime abstrakčiojo taisyklingojo n-kampio $(\mathbb{N}_n, \mathcal{F})$ simetrija. Nesunku įsitikinti (o iš tikrųjų akivaizdu), kad abstrakčiojo taisyklingojo n-kampio $(\mathbb{N}_n, \mathcal{F})$ visos simetrijos atvaizdžių kompozicijos $*$ atžvilgiu sudaro grupę. Ši grupė yra vadinama diedro grupe. Sutarkime šią grupę žymėti D_n.

Norint apibrėžti $(\mathbb{N}_n, \mathcal{F})$ simetriją f, pakanka nurodyti, pavyzdžiui, aibės $\mathbb{N}_n$ elementų 1 ir 2 vaizdus: $f(1), f(2)$. Elemento 1 vaizdas gali būti bet kuris aibės $\mathbb{N}_n$ elementas i, o tuo tarpu 2 – tik toks j, kad $\{i,j\} \in \mathcal{F}$. Jei elementų 1 ir 2 vaizdai nurodyti, tai kitų aibės $\mathbb{N}_n$ elementų vaizdai vienareikšmiškai nurodomi (įrodykite).

Ypač lengvai yra aprašoma abstrakčiojo taisyklingojo n-kampio $(\mathbb{N}_n, \mathcal{F})$ simetrijų grupė, pavaizdavus $(\mathbb{N}_n, \mathcal{F})$ plokštumoje kaip geometrinį taisyklingąjį n-kampį (žr. pav.). Iš geometrinės prasmės nesunku suvokti, iš kokių atvaizdžių sudaryta grupė D_n. Ši grupė

turi n posūkių apie n-kampio simetrijos centrą O ir n atspindžių taisyklingojo n-kampio simetrijos ašių atžvlgiu. Pažymėję posūkį

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix},$$

kitus posūkius galime užrašyti σ laipsniais: $\sigma = \sigma^1, \sigma^2, \dots, \sigma^{n-1}, \sigma^n = \mathrm{id}$. Pažymėję atspindį

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix},$$

visus atspindžius galime užrašyti taip: $\tau, \sigma * \tau, \sigma^2 * \tau, \dots \sigma^{n-1} * \tau$. Iš geometrinės prasmės akivaizdu, kad $\tau * \sigma * \tau = \sigma^{-1} = \sigma^{n-1}$. Remdamiesi šia lygybe, galime užrašyti grupės D_n elementų daugybos lentelę:

$$\sigma^i * \sigma^j = \begin{cases} \sigma^{i+j}, & \text{jei } i+j < n, \\ \sigma^{i+j-n}, & \text{jei } i+j \geq n; \end{cases}$$

$$\sigma^i * (\sigma^j * \tau) = \begin{cases} \sigma^{i+j} * \tau, & \text{jei } i+j < n, \\ \sigma^{i+j-n} * \tau, & \text{jei } i+j \geq n; \end{cases}$$

$$(\sigma^i * \tau) * \sigma^j = \begin{cases} \sigma^{i-j} * \tau, & \text{jei } i-j \geq 0, \\ \sigma^{i-j+n} * \tau, & \text{jei } i-j < 0; \end{cases}$$

$$(\sigma^i * \tau) * (\sigma^j * \tau) = \begin{cases} \sigma^{i-j}, & \text{jei } i-j \geq 0, \\ \sigma^{i-j+n}, & \text{jei } i-j < 0. \end{cases}$$

Dabar glaustai galime apibrėžti diedro grupę:

$$D_n = \{\sigma^i * \tau^j |\ 0 \leq i < n, 0 \leq j \leq 1, \sigma^n = \tau^2 = \mathrm{id}, \tau * \sigma * \tau = \sigma^{-1} = \sigma^{\mathrm{n}-1}\},$$

t. y. grupė D_n turi $2n$ elementų, o šios grupės elementų daugybos lentelė yra apibrėžiama iš lygybių, siejančių elementus σ ir τ: $\sigma^n = \tau^2 = \mathrm{id}, \tau * \sigma * \tau = \sigma^{-1}$.

7. **Tetraedro simetrijų grupė.** Tetraedro simetrijų grupė turi 24 elementus ir šią simetrijų grupę galima sutapatinti su grupe $\mathbf{S_4}$ (įrodykite).

8. Panašiai galima nagrinėti ir kitų iškilųjų taisyklingųjų kūnų (kubo, oktaedro, dodekaedro, ikosaedro) simetrijų grupes. Pastebėsime, kad kai kurių iškilųjų taisyklingųjų kūnų simetrijų grupės sutampa, – tai kubo ir oktaedro, o taip pat ikosaedro ir dodekaedro. Kubas ir oktaedras, o taip pat ikosaedras ir dodekaedras yra vadinami dualiais kūnais. Pavyzdžiui, jei sujungsite atkarpomis kubo sienų centrus, tai gausite oktaedrą ,o jei sujungsite atkarpomis oktaedro sienų centrus, tai gausite kubą. Visiškai taip pat yra susieję ikosaedras ir dodekaedras. Norint aprašyti minėtų iškilųjų taisyklingųjų kūnų simetrijų grupes, pakanka, pavyzdžiui, aprašyti tik kubo ir dodekaedro simetrijų grupes.

1. 9. Taisyklingųjų kūnų simetrijų grupės.

Kubo simetrijų grupė. Dabar sužinosime, kiek yra kubo simetrijų. Pirmiausia suskaičiuokime, kiek yra posūkių, pervedančių kubą į save. Yra trys ašys, jungiančios kubo priešingų sienų centrus. Sukdami kubą apie kiekvieną iš jų, gauname po tris skirtingas simetrijas (tapatųjį atvaizdį id – neįskaičiuojame). Yra keturios ašys, jungiančios kubo priešingas viršūnes. Sukdami kubą apie kiekvieną iš jų, gauname po dvi skirtingas simetrijas. Yra šešios ašys, jungiančios kubo priešingų briaunų centrus. Sukdami kubą apie kiekvieną iš jų, gauname po vieną simetriją.

Taigi sukinėdami kubą iš viso gauname $3 \times 3 + 4 \times 2 + 6 \times 1 + 1 = 9 + 8 + 6 + 1 = 24$ (čia priskaičiuojame ir tapatųjį atvaizdį) simetrijas.

Paėmę vieną kubo veidrodinį atspindį kurios nors kubo simetrijos plokštumos atžvilgiu ir paėmę šio veidrodinio atspindžio kompoziciją su kiekviena kubo posūkio simetrija, gauname dar 24 kubo simetrijas. Taigi iš viso kubas turi 48 simetrijas.

Pratimas. Kubas turi keturias įstrižaines. Įrodykite, kad kubo posūkių grupės elementai perstatinėja kubo įstrižaines. Kadangi kubo posūkių yra 24, o keturių skirtingų elementų perstatinių – taip pat 24, tai kubo posūkių grupę galite sutapatinti su kubo keturių įstrižainių visų perstatinių grupe.

Dodekaedro simetrijų grupė. Įrodykite, kad, sukinėdami dodekaedrą apie jo centrą, gausite 60 dodekaedro simetrijų. Iš viso dodekaedras turi 120 simetrijų (įskaičiuojant ir dodekaedro veidrodinius atspindžius).

1. 10. Tiesės afiniųjų atvaizdžių grupė.

9. Apibrėžkime atvaizdį

$$T_{\alpha,a} : \mathbb{R} \to \mathbb{R},\ T_{\alpha,a}(x) = \alpha x + a,$$

čia $\alpha \in \mathbb{R}^*,\ a, x \in \mathbb{R}$.

Įsitikinsime, kad atvaizdžių $T_{\alpha,a}$ ir $T_{\beta,b}$ kompozicija yra atvaizdis $T_{\alpha\beta,a+\alpha b}$. Iš tikrųjų, kiekvienam $x \in \mathbb{R}$ galima parašyti lygybes:

$$(T_{\alpha,a} \circ T_{\beta,b})(x) = T_{\alpha,a}(T_{\beta,b}(x)) = T_{\alpha,a}(\beta x + b) =$$

$$= \alpha(\beta x + b) + a = (\alpha\beta)x + a + \alpha b = T_{\alpha\beta,a+\alpha b}(x).$$

Taigi atvaizdžių aibė $\mathcal{A}ff(\mathbb{R}) =: \{T_{\alpha,a} |\ \alpha \in \mathbb{R}^*, a \in \mathbb{R}\}$ yra stabili atvaizdžių kompozicijos $\circ$ atžvilgiu.

$\mathcal{A}ff(\mathbb{R})$ atvaizdžių kompozicijos $\circ$ atžvilgiu yra grupė. Iš tikrųjų, nes:

1. Atvaizdžių kopozicija $\circ$ yra asociatyvi;
2. $\mathrm{id} = \mathrm{T}_{1,0} \in \mathcal{A}\mathrm{ff}(\mathbb{R}), \mathrm{id}$ – neutralus elementas atvaizdžių kompozicijos $*$ atžvilgiu;

3. Atvaizdžiui $T_{\alpha,a}, \alpha \in \mathbb{R}_*, a \in \mathbb{R}$, atvirkštinis atvaizdis yra $T_{\alpha^{-1},-\alpha^{-1}a}$ (įsitikinkite).

Grupė $(\mathcal{A}ff(\mathbb{R}), \circ)$ nėra komutatyvi (įsitikinkite).

Atvaizdžiai $T_{\alpha,a}, \alpha \in \mathbb{R}^*, a \in \mathbb{R}$, yra vadinami realiosios tiesės $\mathbb{R}$ afiniosiomis transformacijomis, o grupė $(\mathcal{A}ff(\mathbb{R}), \circ)$ – realiosios tiesės $\mathbb{R}$ afiniųjų transformacijų grupe.

Realiosios tiesės $\mathbb{R}$ afiniosios transformacijos $T_{\alpha,a}, \alpha \in \mathbb{R}_*, a \in \mathbb{R}$, specialioms parametrų α ir a reikšmėms turi atskirus pavadinimus. Pavyzdžiui, transformacija $T_{-1,a}$, čia $a \in \mathbb{R}$, yra vadinama tiesės $\mathbb{R}$ veidrodiniu atspindžiu taško $\frac{a}{2}$ atžvilgiu. Transformacija $T_{\alpha,0},\ \alpha > 0$, yra vadinama homotetija centro 0 atžvilgiu, kurios koeficientas yra α ir t. t..

1. 11. Anksčiau nagrinėti grupių 4-9 pavyzdžiai yra bendros situacijos atskiras atvejis.

Tarkime, kad X – netuščia aibė, $\mathcal{F}$ – aibės X kai kurių poaibių aibė (t. y. $\mathcal{F} \subset P(X)$). Šiuo atveju sakysime, kad aibės X poaibių aibė $\mathcal{F}$ apibrėžia aibėje X struktūrą $\mathcal{F}$.Sutarkime aibę X su joje apibrėžta struktūra $\mathcal{F}$ žymėti $(X, \mathcal{F})$.

Apibrėžimas. Aibės X su joje apibrėžta struktūra $\mathcal{F}$ simetrija yra vadinama bijekcija $f : X \to X$, tenkinanti sąlygas:

$$\text{i) } Y \in \mathcal{F} \Rightarrow f(Y) \in \mathcal{F}, \quad \text{ii) } Y \in \mathcal{F} \Rightarrow f^{-1}(Y) \in \mathcal{F}.$$

Teiginys. Aibės X su joje apibrėžta struktūra $\mathcal{F}$ visos simetrijos atvaizdžių kompozicijos $*$ atžvilgiu sudaro grupę, kurią žymėsime $(\mathcal{A}ut(X, \mathcal{F}), *)$.

Įrodymas. Šį teiginį paliekame įrodyti skaitytojui.

Savaime suprantama, kad, bet kaip parinkę aibės X poaibių aibę $\mathcal{F}$, nieko įdomaus negausime. Žinomos svarbios aibėje X struktūros yra apibrėžiamos tokiomis aibės X poaibių aibėmis $\mathcal{F}$, kurios tenkina vienokias ar kitokias aksiomų sistemas. Dabar pailiustruosime pavyzdžiais kokrečias strukrūras aibėje X.

1. 12. Afinioji plokštuma.

Sutarkime aibės X elementus vadinti taškais, o aibės X poaibius, priklausančius $\mathcal{F}$, – tiesėmis. Tiesės $l, m \in \mathcal{F}$ (t. y. l, m yra aibės X poaibiai) yra vadinamos lygiagrečiomis ir žymima $l||m$, jei $l \cap m = \emptyset$ arba $l = m$.

Apibrėžimas. Aibės X poaibių aibė $\mathcal{F}$ apibrėžia aibėje X afiniosios plokštumos struktūrą, jei $\mathcal{F}$ tenkina aksiomų sistemą:

1. Kiekvienai aibės X skirtingų taškų porai A ir B egzistuoja vienintelė tiesė $l \in \mathcal{F}$ tokia, kad $\{A, B\} \subset l$ (t. y. $A, B \in l$);

2. Kiekvienai tiesei $l \in \mathcal{F}$ ir kiekvienam taškui $A \in X$ egzistuoja vienintelė tokia tiesė m, kad $A \in m$ ir $m||l$;

3. Egzistuoja trys taškai $A, B, C \in X$, kartu nepriklausantys nei vienai tiesei $l \in \mathcal{F}$.

Pora $(X, \mathcal{F})$ yra vadinama afiniąja plokštuma. Afiniosios plokštumos $(X, \mathcal{F})$ simetrijos yra vadinamos plokštumos X afiniosiomis transformacijomis.

1. 13. Baigtinės afiniosios plokštumos pavyzdys.

Imkime $\mathbb{N}_4 = \{1, 2, 3, 4\}$,

$$\mathcal{F} = \big\{\{1,2\},\{2,3\},\{3,4\},\{1,4\}\{1,3\},\{2,4\}\big\}.$$

$(\mathbb{N}_4, \mathcal{F})$ – afinioji plokštuma, turinti 4 taškus ir 6 tieses. Afiniosios plokštumos $(\mathbb{N}_4, \mathcal{F})$ simetrijų grupė yra $\mathbf{S_4}$ (įrodykite).

Pratimai.

Tarkime, kad $(X, \mathcal{F})$, – baigtinė afinioji plokštuma, tiesė $l \in \mathcal{F}$ turi n taškų.

1. Įrodykite, kad bet kuri afiniosios plokštumos $(X, \mathcal{F})$ tiesė taip pat turi n taškų.

2. Įrodykite, kad kiekvienai afiniosios plokštumos $(X, \mathcal{F})$ tiesei $l \in \mathcal{F}$, lygiagrečių tiesių tiesei l yra taip pat n. Taigi $|X| = n^2$.

3. Įrodykite, kad afinioji plokštuma $(X, \mathcal{F})$ turi $n^2 + n$ tiesių (nurodymas: iš pradžių įrodykite, kad tiesių, turinčių bendrą tašką A, yra $n + 1$,o po to pasinaudokite 2-uoju pratimu).

1. 14. Projektyvinė plokštuma.

Aibės X elementus sutarkime vadinti taškais, o aibės X poaibius, priklausančius $\mathcal{F}$ – tiesėmis.

Apibrėžimas. Aibės X poaibių aibė $\mathcal{F}$) apibrėžia aibėje X projektyvinės plokštumos struktūrą, jei $\mathcal{F}$) tenkina aksiomų sistemą:

1. Kiekvienai aibės X skirtingai taškų porai A ir B egzistuoja tokia vienintelė tiesė $l \in \mathcal{F}$, kad $\{A, B\} \subset l$ (t. y. $A, B \in l$);

2. Bet kurios dvi tiesės $l, m \in \mathcal{F}$ turi bent vieną bendrą tašką;

3. Egzistuoja aibės X trys taškai A, B, C, kartu nepriklausantys nei vienai tiesei $l \in \mathcal{F}$;

4. Kiekviena tiesė $l \in \mathcal{F}$ turi bent tris taškus.

Pora $(X, \mathcal{F})$ yra vadinama projektyvine plokštuma. Projektyvinės plokštumos $(X, \mathcal{F})$ simetrijos yra vadinamos projektyvinėmis transformacijomis.

1. 15. Baigtinės projektyvinės plokštumos pavyzdys.

Imkime $\mathbb{N}_7 = \{1, 2, 3, 4, 5, 6, 7\}$,

$$\mathcal{F} = \big\{\{1,2,7\},\{2,3,6\},\{1,4,6\},\{3,4,7\},\{2,4,5\},\{1,3,5\},\{5,6,7\}\big\}.$$

Projektyvinė plokštuma $(\mathbb{N}_7, \mathcal{F})$ turi 7 taškus ir 7 tieses. Vėliau įrodysime, kad projektyvinės plokštumos $(\mathbb{N}_7, \mathcal{F})$ simetrijų grupė $(\mathcal{A}ut(\mathbb{N}_7, \mathcal{F}), \circ)$ turi 168 elementus.

Pratimai.

Tarkime, kad $(X, \mathcal{F})$ – baigtinė projektyvinė plokštuma, jos tiesė $l \in \mathcal{F}$ turi $n+1$ tašką.

1. Įrodykite, kad kiekviena projektyvinės plokštumos $(X, \mathcal{F})$ tiesė turi $n+1$ tašką (nurodymas: pirmiausia įrodykite, kad egzistuoja taškas A nepriklausantis tiesei l ir kuriai nors tiesei m, o po to nagrinėkite tiesių, kurioms priklauso taškas A ir kuris nors tiesės l taškas B, susikirtimą su tiese m).

2. Įrodykite, kad projektyvinės plokštumos $(X, \mathcal{F})$ tiesių, turinčių bendrą tašką A, yra $n+1$.

3. Įrodykite, kad projektyvinė plokštuma $(X, \mathcal{F})$ turi n^2+n+1 tašką ir tiek pat tiesių.

1. 16. Tarp afiniųjų ir projektyvinių plokštumų yra glaudus ryšys.

Pratimai.

1. Tarkime, kad $(X, \mathcal{F})$ – projektyvinė plokštuma, l – kuri nors šios plokštumos tiesė (t. y. $l \in \mathcal{F}$). Įrodykite, kad $(X \setminus l, \mathcal{F} \setminus \{l\})$ – afinioji plokštuma.

2. Tarkime, kad $(X, \mathcal{F})$ – afinioji plokštuma. Afiniosios plokštumos $(X, \mathcal{F})$ visas tarpusavyje lygiagrečias tieses pavadinkime lygiagrečių tiesių pluoštu. Kiekvieną afiniosios plokštumos $(X, \mathcal{F})$ tiesę l atitinka jai lygiagrečių tiesių pluoštas, kurį pavadinkime "idealiu" tašku ir žymėkime $[l]$. Pastebėsime, kad jei afiniosios plokštumos $(X, \mathcal{F})$ tiesės l ir m yra lygiagrečios, tai $[l] = [m]$. Aibę, gautą prie aibės X prijungus visus "idealius" taškus $[l]$, pažymėkime $\tilde{X}$. Aibės $\tilde{X}$ poaibį, sudarytą iš visų aibės $\tilde{X}$ "idealių" taškų pavadinkime "idealia" tiese (ji dažnai yra vadinama "begalo nutolusia" tiese) ir pažymėkime $\tilde{q}$. Prie kiekvienos afiniosios plokštumos $(X, \mathcal{F})$ tiesės l prijungę "idealų" tašką $[l]$,gauname "tiesę", kurią pažymėkime $\tilde{l}$. Apibrėžkime aibės X poaibių aibę $\tilde{\mathcal{F}}$, sudarytą iš visų tiesių l, t. y. iš visų afiniosios plokštumos $(X, \mathcal{F})$ tiesių l, papildytų "idealiais" taškais $[l]$,ir "idealiosios" tiesės $\tilde{q}$. Galite įsitikinti, kad$(\tilde{X}, \tilde{\mathcal{F}})$ – projektyvinė plokštuma.

1. 17. Afiniųjų ir projektyvinių plokštumų struktūras aibėje X apibrėžėme aibės X poaibių aibėmis $\mathcal{F}$, tenkinančiomis atitinkamas aksiomų sistemas. Panašiai galima apibrėžti orientuotus ir neorientuotus grafus, topologines, mačiąsias erdves ir kitus matematinius objektus. Bet į šią matematinių struktūrų apibrėžimų schemą nepatenka, pavyzdžiui, algebrinės strukrūros apibrėžimas. Todėl naudinga apibrėžti bendresnę struktūros aibėje sąvoką. Tai galima padaryti, pavyzdžiui, tariant, kad aibės $\mathcal{F}$ elementais gali būti aibių $X^n, P^k(X^n)$, čia $k, n \in \mathbb{N}$, kurie nors elementai ar poaibiai, tenkinantys vienokią ar kitokią aksiomų sistemą. Grupės $(X, *)$ struktūra šia prasme yra apibrėžiama aibe $\mathcal{F} = \{\Gamma_* |\ \Gamma_* \subset X \times X \times X\}$, čia Γ_* grupės X elementų kopozicijos dėsnio grafikas. Šia bendresne apibrėžiamų aibėse struktūrų prasme, tų struktūrų simetrijos apibrėžiamos panašiai kaip ir anksčiau.

2. Pogrupiai

2. 1. Apibrėžimas. Netuščias grupės $(G, *)$ poaibis H yra vadinamas grupės $(G, *)$ pogrupiu, jei

1. $g_1, g_2 \in H \Rightarrow g_1 * g_2 \in H$ (t. y. bet kurių dviejų poaibio H elementų sandauga priklauso H;

2. $g \in H \Rightarrow g^{-1} \in H$ (t. y. kiekvienam poaibio H elementui atvirkštinis elementas priklauso H.

Teiginys. Grupės $(G, *)$ pogrupis H yra grupė.

Įrodymas. Remdamiesi pogrupio apibrėžimo 1-ąja sąlyga, gauname, kad pogrupis H stabilus kompozicijos dėsnio $*$ atžvilgiu. Kadangi grupės $(G, *)$ elementų kompozicijos dėsnis $*$ yra asociatyvus, tai ir indukuotas kompozicijos dėsnis pogrupyje H yra asociatyvus. Įrodysime, kad grupės vienetas 1 priklauso H. Kadangi $H \neq \emptyset$, tai egzistuoja $g \in H$. Remdamiesi pogrupio apibrėžimo 2-ąja sąlyga, gauname: $g, g^{-1} \in H$. Remdamiesi 1-ąja pogrupio apibrėžimo sąlyga, gauname: $1 = g * g^{-1} \in H$. Remdamiesi pogrupio apibrėžimo 2-ąja sąlyga, matome, kad pogrupio H kiekvienam elementui atvirkštinis elementas priklauso H. $\triangle$

Jei H yra grupės $(G, *)$ pogrupis, tai sutarkime rašyti $(H, *) \subset (G, *)$ ar $(G, *) \supset (H, *)$. Paprastumo dėlei, kalbėdami apie grupę, nerašysime grupės elementų kopozicijos dėsnio ženklo.

2. 2. Antrasis pogrupio apibrėžimas. Netuščias grupės $(G, *)$ poaibis H yra vadinamas grupės $(G, *)$ pogrupiu, jei bet kuriems $g_1, g_2 \in H$, sandauga $g_1 * g_2^{-1} \in H$.

Pratimas. Įrodykite abiejų pogrupio apibrėžimai yra ekvivalentūs.

Pavyzdžiai.

1. Gupės $(\mathbb{Z}, +)$ poaibis $\mathbb{N}_n = \{1, 2, \ldots, n\}$ nėra pogrupis. Šiuo atveju netenkinama pogrupio apibrėžimo 1-oji sąlyga, nes, pavyzdžiui, $1, n \in \mathbb{N}_n$, bet $1+n \notin \mathbb{N}_n$. 2-oji pogrupio apibrėžimo sąlyga taip pat nėra tenkinama: $1 \in \mathbb{N}_n$, bet $-1 \notin \mathbb{N}_n$.

2. Grupės $(\mathbb{Z}, +)$ poaibis $\mathbb{N}$ nėra pogrupis, nes 1-oji pogrupio apibrėžimo sąlyga yra tenkinama, bet 2-oji – ne: $1 \in \mathbb{N}$, o $-1 \notin \mathbb{N}$.

3. Grupės $(\mathbb{Z}, +)$ poaibis $X = \{-2, -1, 0, 1, 2\}$ nėra pogrupis, nes, pavyzdžiui, $1, 2 \in X$, bet $1 + 2 = 3 \notin X$. 2-oji pogrupio apibrėžimo sąlyga yra tenkinama.

4. Grupės $(\mathbb{Q}, +)$ poaibis $\mathbb{Z}$ yra pogrupis.

5. Grupės $(\mathbb{Q}^*, \cdot)$ poaibis $\mathbb{Q}_+^*$ yra pogrupis.

6. Grupės $(\mathbb{Z}, +)$ poaibis $n\mathbb{Z}$, čia n – fiksuotas natūralus skaičius, yra pogrupis.

7. Poaibis $\{2^n | \ n \in \mathbb{Z}\}$ yra grupės $(\mathbb{Q}^*, *)$ pogrupis.

8. $(\mathbb{Q}^*, \cdot)$ yra grupė, $\mathbb{Q}^* \subset \mathbb{Q}$, bet grupė $(\mathbb{Q}^*, \cdot)$ nėra grupės $(\mathbb{Q}, +)$ pogrupis. $\mathbb{Q}^*$ – grupė daugybos atžvilgiu, tuo tarpu $\mathbb{Q}$ – grupė sudėties atžvilgiu.

9. $(\mathbb{Q}^*, \cdot)$ yra grupės $(\mathbb{R}^*, \cdot)$ pogrupis.

10. Tarkime, kad X – netuščia aibė, Y – aibės X poaibis. Tuomet $(P(Y), \ominus)$ yra grupės $(P(X), \ominus)$ pogrupis.

11. $(\mathbb{Z}[\frac{1}{m}], +)$ yra grupės $(\mathbb{Q}, +)$ pogrupis.

12. $\{T_{\alpha,0} |\ \alpha \in \mathbb{Q}^*\}$ yra grupės $\{T_{\alpha,a} |\ \alpha \in \mathbb{Q}^*, a \in \mathbb{Q}\}$ pogrupis (priminsime, kad $T_{\alpha,a} : \mathbb{Q} \to \mathbb{Q}\}, T_{\alpha,a} = \alpha x + a, x \in \mathbb{Q}$).

13. $\{T_{1,a} |\ a \in \mathbb{Q}\}$ yra grupės $\{T_{\alpha,a} |\ \alpha \in \mathbb{Q}^*, a \in \mathbb{Q}\}$ pogrupis.

14. $\{T_{\alpha,a} |\ \alpha \in \mathbb{Q}^*, a \in \mathbb{Q}\}$ yra grupės $\{T_{\alpha,a} |\ \alpha \in \mathbb{R}^*, a \in \mathbb{R}\} = \mathcal{A}ff(\mathbb{R})$ pogrupis.

15. Grupės

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

pogrupiai yra šie:

$$H_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\},\ H_2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\},$$

$$H_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\},\ H_4 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

ir dar du trivialūs pogrupiai: $\{\mathrm{id}\}$ ir S_3.

Pratimai.

1. Išrašykite grupės D_4 visus pogrupius.

2. Išrašykite grupės D_5 visus pogrupius.

3. Išrašykite grupės D_6 visus pogrupius.

4. Įrodykite: jei G grupės $(\mathbb{R}^*, \cdot)$ pogrupis, tai ir $\{T_{\alpha,a} |\ \alpha \in G, a \in \mathbb{R}\}$ yra grupės $\{T_{\alpha,a} |\ \alpha \in \mathbb{R}^*, a \in \mathbb{R}\} = \mathcal{A}ff(\mathbb{R})$ pogrupis.

5. Grupės $\mathcal{A}ff(\mathbb{R})$ pogrupis $\{T_{\alpha,a} |\ \alpha \in \{1, -1\}, a \in \mathbb{R}\}$ yra vadinamas atspindžių generuotu pogrupiu. Įrodykite: jei G yra grupės $(\mathbb{R}, +)$ pogrupis, tai ir

$$\{T_{\alpha,a} |\ \alpha \in \{1, -1\}, a \in G\}$$

yra grupės $\{T_{\alpha,a} |\ \alpha \in \{1, -1\}, a \in \mathbb{R}\}$ pogrupis.

2. 3. Teiginys. Jei H yra grupės $(G, *)$ pogrupis, o K – grupės H pogrupis, tai K yra grupės G pogrupis.

Įrodymas. Įrodymas akivaizdus.

Teiginys. Grupės $(G, *)$ pogrupių šeimos $\{H_\alpha\}_{\alpha\in I}$ sankirta $\bigcap\limits_{\alpha\in I} H_\alpha$ yra grupės $(G, *)$ pogrupis.

Įrodymas. Grupės vienetas $1 \in \bigcap\limits_{\alpha\in I} H_\alpha$, nes kievienam $\alpha \in I$, $1 \in H_\alpha$. Vadinasi, $\bigcap\limits_{\alpha\in I} H_\alpha \neq \emptyset$. Jei $g_1, g_2 \in \bigcap\limits_{\alpha\in I} H_\alpha$, tai ir $g_1 * g_2^{-1} \in \bigcap\limits_{\alpha\in I} H_\alpha$. Iš tikrųjų, jei $g_1, g_2 \in \bigcap\limits_{\alpha\in I} H_\alpha$, tai kiekienam $\alpha \in I$, $g_1, g_2 \in H_\alpha$. Kadangi $H_\alpha, \alpha \in I$ – pogrupiai, tai kiekvienam $\alpha \in I$, $g_1 * g_2^{-1} \in H_\alpha$. Vadinasi, $g_1 * g_2^{-1} \in \bigcap\limits_{\alpha\in I} H_\alpha$.

2. 4. Teiginys. Tarkime, kad X yra grupės $(G, *)$ poaibis. Egzistuoja grupės $(G, *)$ pogrupis H, tenkinantis sąlygas:

1. $X \subset H$;
2. Jei K grupės G pogrupis ir $X \subset K$, tai $H \subset K$.

Apibrėžimas. Pogrupis H yra vadinamas aibės X elementų (arba aibės X) generuotu pogrupiu ir yra žymimas $\langle X\rangle$. Aibės X elementai yra vadinami pogrupio H sudaromosiomis arba generuojančiaisiais elementais.

1. Pastaba. Grupės pogrupių aibė aibių įdėties $\subset$ atžvilgiu yra dalinai sutvarkyta aibė. Pogrupis H yra mažiausias šios tvarkos atžvilgiu tarp pogrupių, turinčių savyje poaibį X.

Teiginio įrodymas. Kadangi $X \subset G$, tai grupės $(G, *)$ pogrupių K, tenkinančių sąlygą $X \subset K$, aibė netuščia. Šių pogrupių sankirta $H =: \bigcap\limits_{X\subset K} K$ ir yra pogrupis, tenkinantis teiginyje išvardintas sąlygas. $\triangle$

2. Pastaba. Jei, pavyzdžiui, $X = \{x_1, x_2, \ldots, x_n\}$, tai vietoje $\langle\{x_1, x_2, \ldots, x_n\}\rangle$ rašysime $\langle x_1, x_2, \ldots, x_n\rangle$ arba $\langle X\rangle$.

Apibrėžimas. Jei grupė $(G, *) = \langle g_1, g_2, \ldots, g_n\rangle$, tai G yra vadinama baigtinai generuota grupe. Šiuo atveju kiekvienas grupės G elementas g yra užrašomas elementų g_1, g_2, …, g_n sveikųjų laipsnių sandauga:

$$g = g_{i_1}^{\alpha_1} g_{i_2}^{\alpha_2} \ldots g_{i_r}^{\alpha_r},$$

čia $\alpha_j \in \mathbb{Z}$, o g_{i_j}, $1 \leq j \leq r$, nebūtinai tarp savęs skirtingi. Be to elementas g nebūtinai vienareikšmiškai taip užrašomas.

3. Cikliniai pogrupiai

3. 1. Apibrėžimas. Grupės $(G, *)$ pogrupį $\langle g \rangle$, generuotą vieno elemento g vadinsime cikliniu. Jei $G = \langle g \rangle$, tai G yra vadinama cikline grupe.

Pastebėsime, kad grupės $(G, *)$ pogrupiui $\langle g \rangle$ priklauso visi elemento g sveikieji laipsniai.

Teiginys. Grupės $(G, *)$ bet kurio elemento g sveikųjų laipsnių aibė yra grupės G ciklinis pogrupis $\langle g \rangle$.

Įrodymas. Pastebėsime, kad elemento g sveikųjų laipsnių aibė netuščia. Jei imsime elemento g sveikuosius laipsnius g^r, g^s, tai $g^r * (g^s)^{-1} = g^{r-s}$ yra taip pat elemento g sveikasis laipsnis. $\triangle$

Apibrėžimas. Jei grupės $(G, *)$ ciklinis pogrupis $\langle g \rangle$ begalinis, tai g yra vadinamas begalinės eilės elementu. Jei $\langle g \rangle$ – baigtinis pogrupis, tai pogrupio eilė $|\langle g \rangle|$ yra vadinama elemento g eile.

3. 2. Teiginys. Jei grupės $(G, *)$ elemento g eilė yra lygi n, tai n yra toks mažiausias teigiamas sveikasis skaičius, kad $g^n = 1$. Be to, $\langle g \rangle = \{1, g, g^2, \ldots, g^{n-1}\}$.

Įrodymas. Kadangi pogrupis $\langle g \rangle$ yra baigtinis ($|\langle g \rangle| = n$), tai egzistuoja tokie $r, s \in \mathbb{N}, r < s$, kad $g^s = g^r$. Šios lygybės abi puses padauginę iš $(g^r)^{-1} = g^{-r}$, gauname: $g^{s-r} = 1, s - r \in \mathbb{N}$. Tarkime, m – toks mažiausias teigiamas sveikasis skaičius, kad $g^m = 1$. Poaibis $\{1, g, g^2, \ldots, g^{m-1}\}$ yra grupės G pogrupis. Iš tikrųjų:

$$g^i * g^j = \begin{cases} g^{i+j}, & \text{jei } i + j < m, \\ g^{i+j-m}, & \text{jei } i + j \geq m \end{cases},$$

čia $0 \leq i, j < m$. Elementui $g^i, 0 < i < m$, atvirkštinis yra g^{m-i}, čia, kaip matome, $0 < m - i < m$. Vadinasi, $\langle g \rangle = \{1, g, g^2, \ldots, g^{m-1}\}$. Kadangi $|\langle g \rangle| = n$, tai $m = n$. $\triangle$

Pavyzdžiai.

1. $(\mathbb{Z}, +)$ – begalinės eilės ciklinė grupė, 1 – šios grupės sudaromoji (-1 – taip pat šios grupės sudaromoji; kitų sudaromųjų ši grupė neturi).

2. $Z_n = (\{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, n - 1 + n\mathbb{Z}\}, +)$, čia n – fiksuotas natūralusis skaičius, yra n-tos eilės ciklinė grupė, $1 + n\mathbb{Z}$ –šios grupės sudaromoji.

Pastaba. Iš 1-o ir 2-om pavyzdžių matome, kad egzistuoja bet kurios eilės ciklinės grupės.

Pratimai.

1. Raskite grupės Z_5 visas sudaromąsias.

2. Raskite grupės Z_6 visas sudaromąsias.

3. Kiek sudaromųjų turi grupė Z_n?

4. Tarkime, kad grupės $(G,*)$ elemento g eilė yra lygi n. Įrodykite: jei kuriam nors $m \in \mathbb{Z}$, $g^m = 1$, tai $n \mid m$.

5. Tarkime, kad grupės $(G,*)$ elementų g_1 ir g_2 eilės yra lygios n_1 ir n_2 ir šie elementai yra perstatomi, t. y. $g_1 * g_2 = g_2 * g_1$ ir, be to, $\langle g_1\rangle \cap \langle g_2\rangle = \{1\}$. Įrodykite, kad elemento $g_1 * g_2$ eilė yra lygi skaičių n_1 ir n_2 mažiausiam bendrajam kartotiniui.

6. Imkime grupės $(\mathcal{A}ff(\mathbb{R}),\circ)$ elementus $T_{-1,2}$ ir $T_{-1,4}$ (priminsime, kad $T_{\alpha,a} : \mathbb{R} \to \mathbb{R}$, $T_{\alpha,a}(x) = \alpha x + a, x \in \mathbb{R}$). Kam yra lygios elementų $T_{-1,2}, T_{-1,4}$ ir $T_{-1,2} \circ T_{-1,4}$ eilės?

7. Imkime diedro grupės $D_n = \{\sigma^i * \tau^j |\ 0 \le i < n, 0 \le j \le 1, \sigma^m = \tau^2 = 1, \tau * \sigma * \tau = \sigma^{-1}\}$ elementus $\sigma * \tau$ ir $\sigma^2 * \tau$. Kam lygios elementų $\sigma * \tau, \sigma^2 * \tau$ ir $\sigma * \tau * \sigma^2 * \tau$ eilės?

4. Grupės skaidinys pogrupio gretutinėmis klasėmis

4. 1. Dabar nagrinėsime grupės $(G,*)$ išskaidymą į pogrupio H kairiąsias (dešiniąsias) gretutines klases.

Apibrėžimas. Tarkime, X, Y – grupės $(G,*)$ poaibiai. Tuomet $X * Y =: \{x * y |\ x \in X, y \in Y\}$. Jei, pavyzdžiui, $X = \{g\}$, tai vietoje $\{g\} * Y$ rašysime $g * Y$. Analogiškai, vietoje $X * \{g\}$ rašysime $X * g$.

Apibrėžimas. Grupės $(G,*)$ pogrupio H kairiąja (dešiniąja) gretutine klase yra vadinamas gupės $(G,*)$ poaibis $g * H$ (atitinkamai $H * g$), $g \in G$, o elementas g – šios klasės atstovu.

Teiginys. Tarkime, kad H yra grupės $(G,*)$ pogrupis. Tuomet $g_1 * H = g_2 * H$ tada ir tik tada, kai $g_1^{-1} * g_2 \in H$ (o $H * g_1 = H * g_2$ tada ir tik tada, kai $g_1 * g_2^{-1} \in H$).

Įrodymas. Jei $g_1 * H = g_2 * H$, tai $g_2 \in g_1 * H$. Vadinasi, egzistuoja toks $h \in H$, kad $g_2 = g_1 * h$. Šios lygybės abi puses iš kairės padauginę iš g_1^{-1}, gauname: $g_1^{-1} * g_2 = h \in H$, t. y. $g_1^{-1} * g_2 =\in H$. Pastebėsime: $g_1^{-1} * g_2 =\in H \iff g_2^{-1} * g_1 \in H$.

Jei $g_1^{-1} * g_2 = h \in H$, tai $g_2 = g_1 * h$. Tuomet kiekvienam $h' \in H$, $g_2 * h' = g_1 * h * h' \in g_1 * H$, t. y. $g_2 * H \subset g_1 * H$. Lygybę $g_2 = g_1 * h$ perrašę taip: $g_1 = g_2 * h^{-1}$, gauname, panašiai kaip ankščiau, $g_1 * H \subset g_2 * H$. Vadinasi, $g_1 * H = g_2 * H$.

Panašiai teiginys įrodomas ir pogrupio H dešiniosioms gretutinėms klasėms. $\triangle$

Išvada. Tarkime, kad H yra grupės $(G,*)$ pogrupis. Jei $g' \in g * H$, tai $g' * H = g * H$ (analogiškai: jei $g' \in H * g$, tai $H * g' = H * g$).

Įrodymas. Jei $g' \in g * H$, tai egzistuoja toks $h \in H$, kad $g' = g * h$. Tuomet $g^{-1} * g' = h \in H$ ir, remdamiesi ankščiau įrodytu teiginiu, gauname: $g' * H = g * H$ (analogiškai įrodoma lygybė $H * g' = H * g$). $\triangle$

Pastaba. Taigi grupės $(G,*)$ pogrupio H kairiosios (arba dešiniosios) gretutinės klasės $g * H$ (arba $H * g$) bet kuris elementas gali būti vadinamas šios klasės atstovu.

4. 2. Teiginys. Grupės $(G, *)$ pogrupio H kairiosios gretutinės klasės $g_1 * H$ ir $g_2 * H$ arba neturi bendrų elementų, arba sutampa (teiginio tvirtinimas teisingas ir pogrupio H dešiniosioms gretutinėms klasėms).

Įrodymas. Jei $g_1 * H \cap g_2 * H = \emptyset$, tai teiginys įrodytas. Tarkime, kad $g \in g_1 * H \cap g_2 * H$. Tuomet, remdamiesi išvada (žr.[4. 1.]), gauname $g_1 * H = g * H = g_2 * H$. $\triangle$

4. 3. Kaip matome, grupės $(G, *)$ pogrupio H kairiosios (dešiniosios) gretutinės klasės suskaido grupę G į netuščius, neturinčius bendrų elementų, poaibius. Kaip žinome [?], aibės skaidinys netuščiais, neturinčiais bendrų elementų, poaibiais yra gaunamas apibrėžus aibėje atitinkamą ekvivalentumo sąryšį ir atvirkščiai: apibrėžus aibės skaidinį netuščiais, neturinčiais bendrų elementų poaibiais, yra apibrėžiamas aibėje ekvivalentumo sąryšis. Tik pastebėsime, kad grupės skaidiniai pogrupio kairiosiomis ir dešiniosiomis gretutinėmis klasėmis bendruoju atveju yra skirtingi. Tai pailiustruosime paprasčiausiais pavyzdžiais.

Pavyzdys. Imkime $S_3 = D_3 = \{1, \sigma, \sigma^2, \tau, \sigma * \tau, \sigma^2 * \tau \mid \sigma^3 = \tau^2 = 1, \tau * \sigma * \tau = \sigma^2\}$. Imkime šios grupės pogrupį $H = \{1, \tau\}$. Tuomet $1 * H = \{1, \tau\}$, $\sigma * H = \{\sigma, \sigma * \tau\}$, $\sigma^2 * H = \{\sigma^2, \sigma^2 * \tau\}$, tuo tarpu $H * 1 = \{1, \tau\}$, $H * \sigma = \{\sigma, \tau * \sigma\} = \{\sigma, \sigma^2 * \tau\}$, $H * \sigma^2 = \{\sigma^2, \tau * \sigma^2\} = \{\sigma^2, \sigma * \tau\}$. Grupės $S_3 = D_3$ skaidinys pogrupio H kairiosiomis gretutinėmis klasėmis yra: $S_3 = D_3 = \{1, \tau\} \cup \{\sigma, \sigma * \tau\} \cup \{\sigma^2, \sigma^2 * \tau\}$, o šios grupės skaidinys pogrupio H dešiniosiomis gretutinėmis klasėmis yra: $S_3 = D_3 = \{1, \tau\} \cup \{\sigma, \sigma^2 * \tau\} \cup \{\sigma^2, \sigma * \tau\}$. Kaip matome, šie grupės $S_3 = D_3$ skaidiniai yra skirtingi.

Pastaba. Jei grupė $(G, *)$ yra komutatyvi, tai grupės G skaidiniai pogrupio H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis sutampa, nes šiuo atveju kiekvienam $g \in G$, $g * H = H * g$ (iš tikrųjų: $g * H = \{g * h \mid h \in H\} = \{h * g \mid h \in H\} = H * g$).

4. 4. Galime nurodyti ekvivalentumo sąryšius grupėje G, susiejusius su grupės G skaidiniais pogrupio H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis. Šie ekvivalentumo sąryšiai atrodo taip:

$$_H R = \{(g_1, g_2) \in G \times G \mid g_1^{-1} * g_2 \in H\}$$

ir

$$R_H = \{(g_1, g_2) \in G \times G \mid g_1 * g_2^{-1} \in H\}.$$

Teiginys. Faktoraibės $G/_H R$ ir G/R_H, apibrėžiamos grupės $(G, *)$ skaidiniais pogrupio H kairiosiomis ir dešiniosionis gretutinėmis klasėmis, kaip aibės yra ekvivalenčios.

Įrodymas. Tarkime, $G = \bigcup\limits_{\alpha \in I} g_\alpha * H$ – grupės G skaidinys pogrupio H skirtingomis kairiosiomis gretutinėmis klasėmis (t. y., $g_\alpha * H \cap g_\beta * H = \emptyset$, jei $\alpha \neq \beta, \alpha, \beta \in I$). Įrodysime, kad $\bigcup\limits_{\alpha \in I} H * g_\alpha^{-1}$ yra grupės G skaidinys pogrupio H skirtingomis dešiniosiomis gretutinėmis klasėmis. Tuo tikslu reikia įrodyti:

1. $G = \bigcup\limits_{\alpha \in I} H * g_\alpha^{-1}$;

2. Jei $H * g_\alpha^{-1} = H * g_\beta^{-1}$, tai $\alpha = \beta$.

Tarkime, $g \in G$. Tuomet $g^{-1} \in G = \bigcup\limits_{\alpha \in I} g_\alpha * H$. Vadinasi, egzistuoja toks $\alpha_0 \in I$, kad $g^{-1} \in g_{\alpha_0} * H$. Taigi $g^{-1} = g_{\alpha_0} * h$ su kuriuo nors $h \in H$. Pastarosios lygybės abi puses pakėlę -1 laipsniu, gauname: $g = h^{-1} * g_{\alpha_0}^{-1}$, čia $h^{-1} \in H$. Taigi $g \in H * g_{\alpha_0}^{-1} \subset \bigcup\limits_{\alpha \in I} H * g_\alpha^{-1}$, t. y. $G = \bigcup\limits_{\alpha \in I} H * g_\alpha^{-1}$.

Tarkime, kad $H * g_\alpha^{-1} = H * g_\beta^{-1}$. Tuomet egzistuoja toks $h \in H$, kad $g_\alpha^{-1} = h * g_\beta^{-1}$. Taigi $g_\alpha = g_\beta * h^{-1}$, čia $h^{-1} \in H$, t. y. $g_\alpha * H = g_\beta * H$. Ši lygybė galima tik tuo atveju, kai $\alpha = \beta$. $\triangle$

Apibrėžimas. Faktoraibes ${}_H G/R$ ir G/R_H žymėsime $H\backslash G$ ir G/H.

Apibrėžimas. Grupės $(G, *)$ pogrupio H skirtingų kairiųjų gretutinių klasių skaičius yra vadinamas pogrupio H indeksu grupėje G ir žymimas $[G : H]$. Šis skaičius taip pat yra lygus pogrupio H skirtingų dešiniųjų gretutinių klasių skaičiui.

4. 5. Teiginys. Grupės $(G, *)$ pogrupio H kieviena kairioji (taip pat ir dešinioji) gretutinė klasė $g * H$ $(H * g)$, $g \in G$, kaip aibė yra ekvivalenti aibei H.

Įrodymas. Įrodysime, kad $g * H$ ir H yra ekvivalenčios aibės. Štai bijekcija $f : H \to g * H, f(h) = g * h, h \in H$. Pirmiausia įsitikinsime, kad f – injekcija. Jei $f(h_1) = f(h_2)$, tai $g * h_1 = g * h_2$. Lygybės $g * h_1 = g * h_2$ abi puses padauginę iš kairės iš g^{-1}, gauname $h_1 = h_2$. Taigi f – injekcija.

Pagaliau įsitikinsime, kad f – siurjekcija. Jei $y \in g * H$, tai egzistuoja toks $h \in H$, kad $y = g * h$. Vadinasi, $f(h) = g * h = y$.

Panašiai įrodoma, kad atvaizdis $f : H \to H * g, f(h) = h * g, h \in H$, – bijekcija. $\triangle$

Išvada. Jei grupė $(G, *)$ baigtinė, tai grupės G pogrupio H kairiosios (o taip ir dešiniosios) gretutinės klasės turi vieną ir tą patį elementų skaičių, lygų pogrupio H elementų skaičiui.

4. 6. Lagranžo teorema. Baigtinės grupės $(G, *)$ pogrupio H eilė $|H|$ dalija grupės G eilę $|G|$.

Įrodymas. Grupės G pogrupio H skirtingos kairiosios gretutinės klasės apibrėžia grupės G skaidinį

$$G = H \cup g_2 * H \cup \ldots \cup g_r * H,$$

čia $1, g_2, \ldots, g_r$ tarp savęs neekvivalentūs ekvivalentumo klasių atstovai. Kadangi $|H| = |g_2 * H| = \ldots = |g_r * H|$, tai $|G| = r|H|$ (r – pogrupio H grupėje G indeksas). $\triangle$

1. Išvada. Baigtinės grupės $(G, *)$ elemento g eilė dalija grupės G eilę.

Įrodymas. Elemento g eilė yra lygi ciklinio pogrupio $[g]$ eilei, o pogrupio eilė dalija grupės eilę. $\triangle$

2. Išvada. Jei $(G, *)$ – baigtinė grupė, $g \in G$, tai $g^{|G|} = 1$.

Pastarąją išvadą baigtinėms Abelio grupėms galima įrodyti tiesiogiai.

4. 7. Teiginys. Tarkime, $(G, *)$ – baigtinė Abelio grupė. Tuomet $g^{|G|} = 1$, $g \in G$.

Įrodymas. Sakykime, $G = \{g_1, g_2, \ldots, g_n\}$. Imkime $g \in G$. Tuomet $G = \{g * g_1, g * g_2, \ldots, g * g_n\}$, nes atvaizdis $f : G \to G, f(g_j) = g * g_j, 1 \leq j \leq n$, – bijekcija. Vadinasi, $(g * g_1) * (g * g_2) * \ldots * (g * g_n) = g_1 * g_2 * \ldots * g_n$. Kairioji šios lygybės pusė yra lygi $g^n * g_1 * g_2 * \ldots * g_n$. Taigi $g^n * g_1 * g_2 * \ldots * g_n = g_1 * g_2 * \ldots * g_n$. Suprastinę šios lygybės abi puses iš $g_1 * g_2 * \ldots * g_n$, gauname: $g^{|G|} = 1$. $\triangle$

4. 8. Pastebėsime, kad bet kuriam baigtinės grupės $(G, *)$ eilės $|G|$ dalikliui d nebūtinai egzistuoja grupės G d eilės elementas. Pavyzdžiui, diedro grupės D_n, $n \geq 3$, eilė yra lygi $2n$, bet ši grupė neturi $2n$ eilės elemento. Jei toks elementas egzistuotų, tai grupė D_n būtų ciklinė ir tuo pačiu – komutatyvi. Bet grupė D_n nėra komutatyvi, kai $n \geq 3$. Kitus pavyzdžius rasite pratimuose.

Pratimai.

1. Diedro grupės D_{15} eilė yra lygi 30. Nors $6|30, 10|30$, bet ši grupė neturi nei 6-tos, nei 10-tos eilės elementų. Įsitikinkite, kad šioje grupėje yra 1 elementas 1-os eilės (tai grupės vienetas 1), 2 elementai 3-ios eilės, 4 elementai 5-tos eilės, 8 elementai 15-tos eilės ir 15 elementų 2-os eilės.

2. Kiek ir kokios eilės elementų yra grupėje D_{16}?

3. Kiek kokios eilės elementų yra grupėje D_{12}?

4. Kiek ir kokios eilės elementų yra grupėje S_4?

Atsakymai.

2. Grupėje D_{16} yra: 1 elementas 1-os eilės; 9 elementai 2-os eilės; 2 elementai 4-tos eilės ir 4 elementai 8-tos eilės.

3. Grupėje D_{12} yra: 1 elementas 1-os eilės; 13 elementų 2-os eilės; 2 elementai 3-ios eilės; 2 elementai 4-tos eilės; 2 elementai 6-tos eilės ir 4 elementai 12-tos eilės.

4. Grupėje S_4 yra: 1 elementas 1-os eilės; 9 elementai 2-os eilės; 8 elementai 3-ios eilės ir 6 elementai 4-tos eilės.

4. 9. Lagranžo teoremą įrodėme baigtinėms grupėms. Begalinių grupių atveju ši teorema praranda prasmę, bet ir šiuo atveju begalinės grupės pogrupio indeksas grupėje gali būti baigtinis. Pavyzdžiui, $(\mathbb{Z}, +)$ – begalinė grupė, $n\mathbb{Z}$ – grupės $(\mathbb{Z}, +)$ pogrupis. Grupės $(\mathbb{Z}, +)$ skaidinys pogrupio $n\mathbb{Z}$ kairiosiomis (ar dešiniosiomis) klasėmis atrodo taip:

$$\mathbb{Z} = n\mathbb{Z} \cup (1 + n\mathbb{Z}) \cup (2 + n\mathbb{Z}) \cup \ldots \cup (n - 1 + n\mathbb{Z}).$$

Kaip matome, pogrupio $n\mathbb{Z}$ skirtingų gretutinių klasių skaičius yra bagtinis ir lygus n. Taigi $[\mathbb{Z} : n\mathbb{Z}] = n$.

Pratimai.

1. Užrašykite grupės $S_3 = D_3 = \{\sigma^i * \tau^j |\ 0 \le i < 3, 0 \le j \le 1, \sigma^3 = \tau^2 = 1, \tau * \sigma * \tau = \sigma^{-1}\}$ skaidinį pogrupio H kairiosiomis gretutinėmis klasėmis, kai

$$\text{i)} H = \{1, \tau\};\ \text{ii)} H = \{1, \sigma * \tau\};\ \text{iii)} H = \{1, \sigma, \sigma^2\}.$$

2. Imkime grupę $G = (\{T_{\alpha,a} |\ \alpha \in \{1, -1\}, a \in \mathbb{Z}\}, \circ)$ ir jos pogrupį $H = \{T_{\alpha,a} |\ \alpha \in \{1, -1\}, a \in n\mathbb{Z}\}$ (priminsime, kad $T_{\alpha,a} : \mathbb{R} \to \mathbb{R}, T_{\alpha,a}(x) = \alpha x + a, x \in \mathbb{R}$). Raskite $[G : H]$.

3. Grupė G tokia pat , kaip ir 2-me pratime, o $H = \{T_{1,a} |\ a \in n\mathbb{Z}\}$. Raskite $[G : H]$.

4. Užrašykite grupės $(\mathbf{P}(\{1, 2, 3, 4\}), \ominus)$ skaidinį pogrupio $\mathbf{P}(\{1, 2\})$ kairiosiomis (ar dešiniosiomis) gretutinėmis klasėmis (čia $\mathbf{P}(X)$ – aibės X visų poaibių aibė, $\ominus$ – simetrinė aibių atimtis).

5. Tarkime, K – grupės H pogrupis, o H – grupės $(G, *)$ pogrupis, $[H : K] < \infty, [G : H] < \infty$. Įrodykite: $[G : K] = [G : H][H : K]$.

6. Tarkime, kad H ir K – grupės $(G, *)$ baigtinio indekso pogrupiai. Įrodykite, kad $H \cap K$ – grupės G baigtinio indekso pogrupis.

Nuoroda. Įrodykite: jei $k_1 * (H \cap K) \ne k_2 * (H \cap K)$, tai $k_1 * H \ne k_2 * H$, čia $k_1, k_2 \in K, H \cap K \subset K \subset G$. Dabar galima padaryti išvadą: $[K : H \cap K] \le [G : H]$ ir pasinaudoti 5-tuoju pratimu.

7. Jei $H_1, H_2, \ldots, H_s$ –grupės $(G, *)$ baigtinio indekso pogrupiai, tai ir $H_1 \cap H_2 \cap \ldots \cap H_s$ yra grupės G baigtinio indekso pogrupis.

4. 10. Dabar apibrėšime svarbius grupės pogrupius: grupės centrą ir grupės komutantą.

Apibrėžimas. Grupės $(G, *)$ poibis $Z(G) =: \{g \in G |\ (\forall x \in G)(g * x = x * g)\}$ yra vadinamas grupės G centru.

Teiginys. Grupės $(G, *)$ centras $Z(G)$ yra grupės G pogrupis.

Įrodymas. Pirmiausia pastebėsime, kad $Z(G) \ne \emptyset$, nes $1 \in Z(G)$. Dabar patikrinsime pogrupio apibrėžimo abi sąlygas.

1. Sakykime, $g_1, g_2 \in Z(G)$. Tuomet kiekvienam $x \in G$, $(g_1 * g_2) * x = g_1 * (g_2 * x) = g_1 * (x * g_2) = (g_1 * x) * g_2 = (x * g_1) * g_2 = x * (g_1 * g_2)$. Įrodėme: jei $g_1, g_2 \in Z(G)$, tai ir $g_1 * g_2 \in Z(G)$.

2. Lieka įrodyti: jei $g \in Z(G)$, tai ir $g^{-1} \in Z(G)$. Jei $g \in Z(G)$, tai kiekvienam $x \in G$, $g * x = x * g$. Pastaroji lygybė ekvivalenti lygybei: kiekvienam $x \in G$, $x * g^{-1} = g^{-1} * x$.

Apibrėžimas. Grupės $(G, *)$ elementų g ir h komutatoriumi yra vadinamas elementas $g * h * g^{-1} * h^{-1}$ ir žymimas $[g, h]$. Grupės G pogrupis, generuotas grupės G elementų komutatorių $[g, h]$, $g, h \in G$, yra vadinamas grupės G komutantu ir žymimas G'. Kitaip tariant: $G' = \big[\{[g, h] |\ g, h \in G\}\big]$.

Pastaba. Bendruoju atveju grupės dviejų komutatorių sandauga nėra šios grupės komutatorius. Pateikite pavyzdžių.

Pratimai.

1. Įrodykite, kad grupės S_4 centras $Z(S_4) = \{\mathrm{id}\}$.
2. Raskite grupių $\mathcal{A}ff(\mathbb{Q})$, $\mathcal{A}ff(\mathbb{R})$ centrus $Z(\mathcal{A}ff(\mathbb{Q}))$, $Z(\mathcal{A}ff(\mathbb{R}))$.
3. Raskite grupių $\mathcal{A}ff(\mathbb{Q})$, $\mathcal{A}ff(\mathbb{R})$ komutantus $\mathcal{A}ff(\mathbb{Q})'$, $\mathcal{A}ff(\mathbb{R})'$.
4. Raskite diedro grupių D_n, $n \geq 3$ centrus ir komutantus.

5. Normalieji pogrupiai

5. 1. Kaip matėme anksčiau, grupės $(G, *)$ skaidiniai pogrupio H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis bendru atveju yra skirtingi.Specialiu atveju, kai G – komutatyvi grupė, grupės G skaidiniai bet kurio pogrupio kairiosiomis ar dešiniosiomis gretutinėmis klasėmis sutampa. Bet ir nekomutatyviųjų grupių $(G, *)$ skaidiniai tam tikrų pogrupių H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis, kaip pamatysime, taipogi sutampa ir šiuo atveju galėsime apibrėžti naują grupę, – grupės G fatorgrupę G/H pagal pogrupį H.

Apibrėžimas. Grupės $(G, *)$ pogrupis H yra vadinamas normaliuoju (invariantiniu), jei kiekvienam $g \in G$, $g * H = H * g$.

1. Pastaba. Kadangi $g * H = H = H * g$, jei $g \in H$, tai normaliojo pogrupio H apibrėžime pakanka reikalauti, kad kiekvienam $g \in G \setminus H$ būtų $g * H = H * g$.

2. Pastaba. Normaliojo pogrupio apibrėžime kiekvienam $g \in G$ lygybės $g*H = H*g$ yra suprantamos kaip aibių lygybės. Remdamiesi lygybe $g * H = H * g$ negalime daryti išvados, kad bet kuriems $g \in Girh \in H$ teisinga lygybė $g * h = h * g$. Pavyzdžiui, imkime

$$G = S_3 = \{1, \sigma, \sigma^2, \tau, \sigma * \tau, \sigma^2 * \tau |\ \sigma^3 = \tau^2 = 1, \tau * \sigma * \tau = \sigma^2\},\ H = \{1, \sigma, \sigma^2\}.$$

Tuomet

$$\tau * H = \{\tau, \tau * \sigma, \tau * \sigma^2\} = \{\tau, \sigma^2 * \tau, \sigma * \tau\} = H * \tau,$$

bet $\tau * \sigma \neq \sigma * \tau$.

5. 2. Teiginys. Grupės $(G, *)$ pogrupis H yra normalusis, jei

$$g \in G, h \in H \Rightarrow g * h * g^{-1} \in H.$$

Įrodymas. Jei $g \in G, h \in H \Rightarrow g*h*g^{-1} \in H$, tai kiekvienam $g \in G$, $g*H*g^{-1} \subset H$. Bet jei kiekvienam $g \in G$, $g*H*g^{-1} \subset H$, tai ir $g^{-1}*H*g = g^{-1}*H*(g^{-1})^{-1} \subset H$, t. y. kiekvienam $g \in G$, $g^{-1}*H*g \subset H$. Bet, kiekvienam $g \in G$, $g*H*g-1 \subset H, g^{-1}*H*g \subset H$ $(g^{-1}*H*(g^{-1})^{-1} \subset H$ ekvivalentu $H \subset g*Hg^{-1})$, tai kiekvienam $g \in G$, $g*H*g^{-1} = H$. Pastorosios lygybės $g*H*g^{-1} = H$ ekvivalenčios lygybėms $g*H = H*g, g \in G$. $\triangle$

Pavyzdžiai.

1. Kiekvienas Abelio grupės $(G, *)$ pogrupis yra normalusis.

2. Diedro grupės $D_n = \{\sigma^i * \tau^j |\ 0 \leq i < n, 0 \leq j \leq 1, \sigma^n = \tau^2 = 1, \tau*\sigma*\tau = \sigma^{-1}\}, n \geq 3$, ciklinis pogrupis $[\sigma] = \{\sigma^j |\ 0 \leq j < n, \sigma^n = 1\}$ yra normalusis, o pogrupiai $H_j = \{1, \sigma^j * \tau\}$, čia $0 \leq j < n$, nėra normalieji. Pavyzdžiui, $\sigma * H_j * \sigma^{-1} = \{1, \sigma^{j+2} * \tau\} \neq H_j, 0 \leq j < n$ (priminsime: $\sigma^n = 1, n \geq 3$).

3. Afiniosios grupės $\mathcal{A}ff(\mathbb{R}) = (\{T_{\alpha,a} |\ \alpha \in \mathbb{R}^*, a \in \mathbb{R}\}, \circ)$ pogrupis $H = \{T_{1,a} |\ a \in \mathbb{R}\}$ yra normalusis. Iš tikrųjų: jei $T_{\alpha,a} \in \mathcal{A}ff(\mathbb{R}), T_{1,b} \in H$, tai

$$T_{\alpha,a} \circ T_{1,b} \circ T_{\alpha,a}^{-1} = T_{\alpha,a+\alpha b} \circ T_{\alpha^{-1},-\alpha^{-1}a} = T_{1,\alpha b} \in H$$

(priminsime: $T_{\alpha,a} \circ T_{\beta,b} = T_{\alpha\beta,a+\alpha b}, T_{\alpha,a}^{-1} = T_{\alpha^{-1},-\alpha^{-1}a}$).

Grupės $\mathcal{A}ff(\mathbb{R})$ pogrupis $K = \{T_{\alpha,0} |\ \alpha \in \mathbb{R}\}$ nėra normalusis, nes, pavyzdžiui, $T_{\alpha,0} \in K, \alpha \neq 0$, o $T_{1,a} \circ T_{\alpha,0} \circ T_{1,a}^{-1} = T_{\alpha,a} \circ T_{1,-a} = T_{\alpha,a-\alpha a} \not\subset K$, jei $a \neq 0, \alpha \neq 1$.

Pratimai.

1. Įrodykite, kad grupės $(G, *)$ indekso 2 pogrupis H grupėje G yra normalusis.

2. Įrodykite: jei H yra grupės $(G, *)$ normalusis pogrupis, K – grupės G pogrupis, tai $H * K = K * H$ yra grupės G pogrupis.

3. Įrodykite: jei H, K yra grupės $(G, *)$ normalieji pogrupiai, tai $H * K$ yra grupės G normalusis pogrupis.

4. Įrodykite: jei H yra grupės $(G, *)$ normalusis pogrupis, K – grupės G pogrupis, tai $H \cap K$ yra grupės K normalusis pogrupis.

5. Įrodykite: jei H yra grupės $(G, *)$ pogrupis, tai $\bigcap\limits_{g \in G} g * H * g^{-1}$ yra grupės G normalusis pogrupis.

6. Įrodykite: jei H yra grupės $(G, *)$ baigtinio indekso pogrupis, tai ir $\bigcap\limits_{g \in G} g*H*g^{-1} = \bigcap\limits_{i=1}^{r} g_i * H * g_i^{-1}$ yra grupės G baigtinio indekso normalusis pogrupis, čia $G = g_1 * H \cup g_2 * H \cup \ldots \cup g_r * H$ – grupės G skaidinys pogrupio H skirtingomis kairiosiomis gretutinėmis klasėmis.

7. Įrodykite, kad grupės $(G, *)$ centras $Z(G)$ yra grupės G normalusis pogrupis.

8. Įrodykite, kad grupės $(G, *)$ komutantas G' yra grupės G normalusis pogrupis.

6. Grupės faktorgrupė pagal normalųjį pogrupį

6. 1. Tarkime, kad H yra grupės $(G, *)$ normalusis pogrupis. Tuomet faktoraibės G/H ir $H\backslash G$ yra lygios. Faktoraibėje G/H apibrėšime jos elementų kompozicijos dėsnį (sandaugą) $*$ taip:

$$(g_1 * H) * (g_2 * H) =: g_1 * g_2 * H$$

Galite įsitikinti, kad taip apibrėžtas faktoraibės G/H elementų kompozicijos dėsnis nepriklauso nuo pogrupio H gretutinių klasių atstovų. Be to, pogrupio H gretutinių klasių $g_1 * H$ ir $g_2 * H$ sandaugą galime apibrėžti kaip grupės G poaibį, sudarytą iš poaibių $g_1 * H$ ir $g_2 * H$ elementų sandaugų $x * y, x \in g_1 * H, y \in g_2 * H$. Visais atvejais gauname vieną ir tą patį rezultatą. Galite įsitikinti, kad taip apibrėžę faktoraibės G/H elementų sandaugą, gauname grupę $(G/H, *)$

Apibrėžimas. Tarkime, kad H yra grupės $(G, *)$ normalusis pogrupis. Grupė $(G/H, *)$ yra vadinama grupės G faktorgrupe pagal normalalųjį pogrupį H.

6. 2. Teiginys. Grupės $(G, *)$ faktorgrupė $(G/G', *)$ pagal grupės G komutantą G' yra komutatyvi grupė.

Įrodymas. Tarkime, kad $x * G', y * G' \in G/G', x, y \in G$. Tuomet $(x * G') * (y * G') = x * y * G' = y * x * G' = (y * G') * (x * G')$, nes $(x * y) * (y * x)^{-1} = x * y * x^{-1} * y^{-1} = [x, y] \in G'$. $\triangle$

Teiginys. Jei grupės $(G, *)$ faktorgrupė $(G/H, *)$ pagal grupės G normalųjį pogrupį H yra komutatyvi grupė, tai $G' \subset H$, čia G' – grupės G komutantas.

Įrodymas. Kadangi bet kuriems $x, y \in G$, $(x * H) * (y * H) = (y * H) * (x * H)$, tai bet kuriems $x, y \in G$, $x * y * H = y * x * H$. Iš pastarosios lygybės gauname: bet kuriems $x, y \in G$, $(x * y) * (y * x)^{-1} = x * y * x^{-1} * y^{-1} = [x, y] \in H$. Kadangi bet kuriems $x, y \in G$, $[x, y] \in H$, tai $G' \subset H$. $\triangle$

Pratimai.

1. Raskite diedro grupių D_n, $n \geq 3$ faktorgrupes pagal jų centrus ir komutantus.

2. Raskite grupių $\mathcal{A}ff(\mathbb{Q})$ ir $\mathcal{A}ff(\mathbb{R})$ faktorgrupes pagal jų komutantus $\mathcal{A}ff(\mathbb{Q})'$ ir $\mathcal{A}ff(\mathbb{R})'$.

7. Homomorfizmai

7. 1. Nagrinėsime tokius atvaizdžius, vadinamus homomorfizmais, apibrėžtus vienoje grupėje ir įgyjančius reikšmes kitoje grupėje, kurie išsaugo grupės struktūrą. Izomorfizmas, – tai bijektyvus homomorfizmas. Jei tarp dviejų tiriamų objektų egzistuoja izomorfizmas,

tai tie objektai struktūriniu teorijos požiūriu identiški. Nagrinėjami izomorfiniai objektai gali būti labai skirtingai apibrėžiami. Todėl nepaprastai svarbu sugebėti atpažinti izomorfinius objektus ir skirti neizomorfinius. Idealiausias atvejis būtų visus tiriamus objektus suklasifikuoti, t. y. sudaryti visų tarp savęs neizomorfinių objektų sąrašą tokį, kad kiekvienas duotoje teorijoje tiriamas objektas būtų izomorfinis vienam ir tik vienam objektui iš pateikto sąrašo. Bet, deja, grupių klasifikacija, – neišsprendžiamas uždavinys. Neegzistuoja algoritmo atpažinti izomorfinėms grupėms. Šį nepaprastai gilų faktą griežtai įrodė P. Novikovas.

Daug yra pasiekta tiriant tik atskiras grupių klases.

Apibrėžimas. Tarkime, kad $(G, *), (H, \circ)$ – grupės. Atvaizdis $f : G \to H$ yra vadinamas homomorfizmu, jei bet kuriems $g_1, g_2 \in G$,

$$f(g_1 * g_2) = f(g_1) \circ f(g_2).$$

Homomorfizmas f yra vadinamas izomorfizmu, jei f – bijekcija. Grupės $(G, *)$ ir $(H, \circ)$ yra vadinamos izomorfinėmis ir rašoma $(G, *) \cong (H, \circ)$, jei egzistuoja bent vienas izomorfizmas $f : G \to H$. Izomorfizmas $f : G \to G$ yra vadinamas grupės $(G, *)$ automorfizmu.

Pavyzdžiai.

1. Grupės $(\mathbb{R}_+^*, *)$ ir $(\mathbb{R}, +)$ yra izomorfinės, $\ln : \mathbb{R}_+^* \to \mathbb{R}$ – izomorfizmas (įsitikinkite).

2. Grupės $(\mathbb{Z}, +)$ ir $(5\mathbb{Z}, +)$ – izomorfinės, $f : \mathbb{Z} \to 5\mathbb{Z}, f(n) = 5n, n \in \mathbb{Z}$, – izomorfizmas.

3. $(\mathbb{Z}, +), (\{1, -1\}, *)$ – grupės, atvaizdis $f : \mathbb{Z} \to \{1, -1\}, f(n) = (-1)^n, n \in \mathbb{Z}$ yra homomorfizmas.

4. $(\mathbb{Q}^*, *)$ – grupė, atvaizdis $f : \mathbb{Q}^* \to \mathbb{Q}^*, f(\alpha) = \alpha^3, \alpha \in \mathbb{Q}^*$, yra grupės $(\mathbb{Q}^*, *)$ automorfizmas.

5. $(\mathbb{Z}, +)$ – grupė, atvaizdis $f : \mathbb{Z} \to \mathbb{Z}, f(n) = 5n, n \in \mathbb{Z}$, yra homomorfizmas.

6. Atvaizdis $f : \mathbb{Q} \to \mathbb{Q}, f(\alpha) = 5\alpha, \alpha \in \mathbb{Q}$, yra grupės $(\mathbb{Q}, +)$ automorfizmas.

7. Atvaizdis $f : \mathbb{Q} \to \mathbb{Q}, f(\alpha) = a\alpha, \alpha, a \in \mathbb{Q}, a \neq 0$, yra grupės $(\mathbb{Q}, +)$ automorfizmas.

8. Atvaizdis $f : \mathbb{R} \to \mathbb{R}, f(\alpha) = a\alpha, \alpha, a \in \mathbb{R}, a \neq 0$, yra grupės $(\mathbb{R}, +)$ automorfizmas.

7. 2. Įrodysime keletą paprastų faktų apie homomorfizmus.

Teiginys. Jei $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – homomorfizmas, tai
1. $f(1_G) = 1_H$, čia 1_G – grupės G vienetas, 1_H – grupės H vienetas;
2. Kiekvienam $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Įrodymas. 1. $f(1_G) = f(1_G * 1_G) = f(1_G) \circ f(1_G)$. Lygybės $f(1_G) \circ f(1_G) = f(1_G)$ abi puses padauginę, pavyzdžiui, iš kairės iš elemento $f(1_G)^{-1}$, gauname:

$$f(1_G)^{-1} \circ ((1_G) \circ f(1_G)) = f(1_G)^{-1} \circ f(1_G) = 1_H.$$

Kairioji šios lygybės pusė, kaip nesunku matyti, yra $f(1_G)$. Taigi $f(1_G) = 1_H$.

2. Kadangi $f(1_G) = 1_H$, tai $f(g * g^{-1}) = f(g) \circ f(g^{-1}) = 1_H$. Panašiai galima gauti lygybę: $f(g^{-1}) \circ f(g) = 1_H$. Vadinasi, kiekviemam $g \in G$, $f(g^{-1}) = f(g)^{-1}$ (remiantis elementui atvirkštinio elemento apibrėžimu). $\triangle$

7. 3. Apibrėžimas. Tarkime, $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – homomorfizmas. Grupės G poaibis

$$\text{Ker } f =: \{g \in G |\ f(g) = 1_H\}$$

yra vadinamas homomorfizmo f branduoliu.

Teiginys. Tarkime, $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – homomorfizmas. Homomorfizmo f branduolys Ker f yra grupės G normalusis pogrupis.

Įrodymas. $1_G \in \text{Ker } f$, nes $f(1_G) = 1_H$. Vadinasi, Ker $f \neq \emptyset$. Pirmiausia įrodysime, kad Ker f yra grupės G pogrupis.

1. Sakykime, $g_1, g_2 \in \text{Ker } f$, t. y. $f(g_1) = 1_H, f(1_H) = 1_H$. Tuomet $f(g_1 * g_2) = f(g_1) \circ f(g_2) = 1_H \circ 1_H = 1_H$, t. y. $g_1 * g_2 \in \text{Ker } f$.

2. Sakykime, $g \in \text{Ker } f$, t. y. $f(g) = 1_H$. Tuomet $f(g^{-1}) = f(g)^{-1} = 1_H^{-1} = 1_H$, t. y. $g^{-1} \in \text{Ker } f$.

Taigi Ker f – grupės G pogrupis. Dabar įsitikinsime, kad Ker f yra grupės G normalusis pogrupis. Tuo tikslu įrodysime: jei $g \in G, g' \in \text{Ker } f$, tai $g * g' * g^{-1} \in \text{Ker } f$. Tikriname: $f(g * g' * g^{-1}) = f(g) \circ f(g') \circ f(g^{-1}) = f(g) \circ 1_H \circ f(g^{-1}) = f(g) \circ f(g^{-1}) = 1_H$ (nes $f(g^{-1}) = f(g)^{-1}$). $\triangle$

Teiginys. Tarkime, $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – homomorfizmas. Jei Ker $f = \{1_G\}$, tai f – injektyvus homomorfizmas.

Įrodymas. Jei $f(g_1) = f(g_2)$, tai $f(g_1) \circ f(g_2)^{-1} = 1_H$. Bet $f(g_1) \circ f(g_2)^{-1} = f(g_1) \circ f(g_2^{-1}) = f(g_1 * g_2^{-1}) = 1_H$. Vadinasi, $g_1 * g_2^{-1} \in \text{Ker } f = \{1_G\}$, t. y. $g_1 * g_2^{-1} = 1_G$ arba $g_1 = g_2$. $\triangle$

Išvada. Baigtinės izomorfinės grupės $(G, *), (H, \circ)$ vienos ir tos pačios eilės elementų turi vieną ir tą patį skaičių.

Įrodymas. Tarkime, kad $f : G \to H$ – izomorfizmas, $g \in G$, – n-tos eilės elementas (t. y. $g^n = 1_G$, bet $g^j \neq 1_G$, jei $0 < j < n$). Tuomet $f(g^n) = f(g)^n = 1_H$, bet $f(g^j) = f(g)^j \neq 1_H$, kai $0 < j < n$, nes $g^j \neq 1_G$ ir f – bijekcija. $\triangle$

7. 4. Pavyzdžiui, remdamiesi pastarąja išvada, įsitikinsime, kad diedro grupė D_{12} nėra izomorfinė grupei S_4 (kieviena iš šių grupių turi po 24 elementus). Iš tikrųjų: grupė D_{12} 2-os eilės elementų turi 13, o grupė S_4 2-os eilės elementų turi tik 9. Grupės $D_{2^{n-1}}$ ir $(\mathbf{P}(\mathbb{N}_n), \ominus)$, čia $n > 2$, taip pat nėra izomorfinės, nors $|D_{2^{n-1}}| = |(\mathbf{P}(\mathbb{N}_n)| = 2^n$. Grupė $(\mathbf{P}(\mathbb{N}_n), \ominus)$ – komutatyvi, o grupė $D_{2^{n-1}}$ nėra komutatyvi.

Pratimai.

1. Įrodykite, kad grupės $(G, *)$ automorfizmų aibė $\mathcal{A}ut(G, *)$ atvaizdžių kompozicijos $\circ$ atžvilgiu sudaro grupę $(\mathcal{A}ut(G, *), \circ)$.

Pastaba. Priminsime, kad anksčiau pakankamai bendru atveju apibrėžėme aibės X su struktūta $\mathcal{F}$ (algebrine ar kitokia) simetrijų grupę $(\mathcal{A}ut(X, \mathcal{F}), \circ)$ [?]. Aibės X atveju $\mathcal{A}ut(X)$ žymėjome visų bijekcijų $f : X \to X$ aibę. Ir šiuo atveju $(\mathcal{A}ut(X), \circ)$ galime interpretuoti kaip aibės X simetrijų grupę ir šis žymėjimas yra suderintas su ankstesniu žymėjimu $(\mathcal{A}ut(X, \mathcal{F}), \circ)$, kai $\mathcal{F} = \emptyset$. Jei aibėje G yra apibrėžta grupės struktūra, tai $\mathcal{A}ut(G, *)$ žymime visų bijekcijų $f : G \to G$, išsaugančių grupės G struktūrą, aibę. Ir šiuo atveju grupę $(\mathcal{A}ut(G, *), \circ)$ galime interpretuoti kaip grupės G simetrijų grupę. Kaip matome, visi žymėjimai yra suderinti ir jokių dviprasmybių negali iškilti. Sutarsime grupės G automorfizmų grupės $(\mathcal{A}ut(G, *), \circ)$ žymėjimą sutrumpinti ir vietoje $(\mathcal{A}ut(G, *), \circ)$ rašyti $\mathcal{A}ut(G)$.

2. Kiekvienam grupės $(G, *)$ elementui g galime priskirti izomorfizmą $f_g : G \to G, f_g(x) = g * x * g^{-1}, x \in G$, vadinamą grupės G vidiniu automorfizmu. Įsitikinkite, kad f_g iš tikrųjų yra grupės G automorfizmas. Visų grupės G vidinių automorfizmų aibė $\mathcal{I}nt(G)$ atvaizdžių kompozicijos $\circ$ atžvilgiu sudaro grupę $(\mathcal{I}nt(G), \circ)$ – vadinamą grupės G vidinių automorfizmų grupe. Šią grupę sutarkime žymėti $\mathcal{I}nt(G)$. Grupė $\mathcal{I}nt(G)$ yra izomorfinė grupei $G/Z(G)$.

3. Įrodykite, kad atvaizdis $F : G \to \mathcal{I}nt(G), F(g) = f_g, g \in G$, čia $f_g : G \to G, f_g(x) = g * x * g^{-1}, x \in G$, – grupės G vidinis automorfizmas, yra homomorfizmas. Įrodykite, kad šio homomorfizmo branduolys Ker F yra grupės G centras $Z(G)$ (priminsime: $Z(G) =: \{g \in G |\ g * x = x * g, x \in G\}$). Galima apibrėžti grupės G išorinių automorfizmų grupę kaip $\mathcal{A}ut(G)/\mathcal{I}nt(G)$.

4. Įrodykite, kad grupės $(G, *)$ vidinių automorfizmų grupė $\mathcal{I}nt(G)$ yra grupės G visų automorfizmų grupės $\mathcal{A}ut(G)$ normalusis pogrupis.

5. Raskite diedro grupių D_6, D_7, D_8 vidinių automorfizmų grupes (raskite šių grupių centrus, o po to faktogrupes $D_6/Z(D_6)$, $D_7/Z(D_7)$, $D_8/Z(D_8)$.

6. Raskite grupių $\mathcal{A}ff(\mathbb{Q}), \mathcal{A}ff(\mathbb{R})$ vidinių automorfizmų grupes.

7. Raskite grupės S_4 vidinių automorfizmų grupę.

8. Įrodykite, kad Abelio grupės G vidinių automorfizmų grupė $\mathcal{I}nt(G) = \{\mathrm{id}\}$.

9. Tarkime, kad $f : X \to X$ – bijekcija. Ar aibės X bijekcija f generuoja grupės $(\mathbf{P}(X), \ominus)$ automorfizmą?

7. 5. Teiginys. Tarkime, $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – homomorfizmas. Tuomet

1. Jei K – grupės G pogrupis, tai $f(K)$ yra grupės H pogrupis.

2. Jei N – grupės H pogrupis, tai $f^{-1}(N)$ yra grupės G – pogrupis ir Ker $f \subset f^{-1}(N)$.

3. Jei N – grupės H normalusis pogrupis, tai $f^{-1}(N)$ yra grupės G normalusis pogrupis.

4. Jei f – siurjektyvus homomorfizmas (t. y. f(G)=H), K – grupės G normalusis pogrupis, tai ir $f(K)$ yra grupės H normalusis pogrupis.

Įrodymas. 1. Sakykime, $y_1, y_2 \in f(K)$. Tuomet egzistuoja tokie $k_1, k_2 \in K$, kad $f(k_1) = y_1, f(k_2) = y_2$. Vadinasi, $y_1 * y_2^{-1} = f(k_1) \circ f(k_2)^{-1} = f(k_1) \circ f(k_2^{-1}) = f(k_1 * k_2^{-1}) \in f(K)$, nes $k_1 * k_2^{-1} \in K$.

2. Sakykime, $x_1, x_2 \in f^{-1}(N)$, t. y. $f(x_1), f(x_2) \in N$. Tuomet $x_1 * x_2^{-1} \in f^{-1}(N)$, nes $f(x_1 * x_2^{-1}) = f(x_1) \circ f(x_2)^{-1} \in N$ (priminsime: N yra pogrupis ir jei $f(x_1), f(x_2) \in N$, tai $f(x_1) \circ f(x_2)^{-1} \in N$). Kadangi $1_H \in N$, tai $f^{-1}(1_H) =$ Ker $f \subset f^{-1}(N)$.

3. Sakykime, $g \in G, x \in f^{-1}(N)$. Tuomet $g * x * g^{-1} \in f^{-1}(N)$, nes $f(g * x * g^{-1}) = f(g) \circ f(x) \circ f(g)^{-1} \in N$ (N –normalusis pogrupis, $f(x) \in N$).

4. Sakykime, $h \in H, y \in f(K)$. Vadinasi, egzistuoja toks $g \in G$, kad $f(g) = h$ ir egzistuoja toks $k \in K$, kad $f(k) = y$. Tuomet $h \circ y \circ h^{-1} = f(g) \circ f(k) \circ f(g)^{-1} = f(g * k * g^{-1}) \in f(K)$, nes $g * k * g^{-1} \in K$ (priminsime, kad K – normalusis pogrupis, $k \in K$). $\triangle$

Teorema. Jei H, K yra grupės $(G, *)$ pogrupiai, H – normalusis pogrupis, tai $H*K = K * H$ yra grupės G pogrupis.

Įrodymas. Priminsime, kad $H*K = \{h*k|\ h \in H, k \in K$. Sakykime, $h_1*k_1, h_2*k_2 \in H*K$. Tuomet $h_1*k_1(h_2*k_2)^{-1} = h_1*k_1*k_2*h_2 = h_1*(k_1*k_2^{-1})*h_2^{-1}*(k_1*k_2^{-1})^{-1}*k_1*k_2^{-1} \in H*K$, nes $h_1 \in H, (k_1 * k_2^{-1}) * h_2^{-1} * (k_1 * k_2^{-1})^{-1} \in H$ (todėl, kad H normalusis pogrupis, $h_2^{-1} \in H, k_1 * k_2^{-1} \in G$), o $k_1 * k_2^{-1} \in K$ (K – pogrupis, vadinasi, jei $k_1, k_2 \in K$, tai ir $k_1 * k_2^{-1} \in K$). Taigi įrodėme, kad $H * K$ yra grupės G pogrupis. Jei $k * h \in K * H$, tai $(k * h * k^{-1}) * k \in H * K$, t. y. $K * H \subset H * K$. Panašiai įrodoma, kad $H * K \subset K * H$. Taigi $H * K = K * H$. $\triangle$

7. 6. Teiginys. Tarkime, $(G, *), (H, \circ)$ – grupės, N – grupės G pogrupis, $f : G \to H$ – homomorfizmas. Tuomet

$$f^{-1}(f(N)) = N * \text{Ker } f = \text{Ker } f * N$$

Įrodymas. Akivaizdu, kad $N \subset f^{-1}(f(N))$ ir Ker $f \subset f^{-1}(f(N))$ (kadangi $1_H \in f(N)$, o Ker $f = f^{-1}(1_H)$). Vadinasi, $N *$ Ker $f \subset f^{-1}(f(N))$, nes $f^{-1}(f(N))$ – grupės G pogrupis (žr.[?]). Tarkime, kad $x \in f^{-1}(f(N))$. Tuomet $f(x) \in f(N)$. Vadinasi, egzistuoja toks $k \in N$, kad $f(k) = f(x)$. Lygybę $f(k) = f(x)$, čia $k \in N, x \in f^{-1}(f(N))$, perrašome taip: $1_H = f(k)^{-1} \circ f(x) = f(k^{-1} * x)$. Matome, kad $k^{-1} * x \in$ Ker f, čia $k \in N, x \in f^{-1}(f(N))$. Vadinasi, $x \in k *$ Ker $f \subset N *$ Ker f. Įrodėme: $f^{-1}(f(N)) = N *$ Ker $f =$ Ker $f * N$. $\triangle$

Išvada. Jei $(G,*),(H,\circ)$ – grupės, $f: G \to H$ – siurjektyvus homomorfizmas, tai atvaizdis F, apibrėžtas grupės H visų pogrupių aibėje

$$H \supset K \overset{F}{\Rightarrow} f^{-1}(K) \subset G,$$

čia K – grupės H pogrupis, yra bijekcija tarp grupės H visų pogrupių ir grupės G visų tokių pogrupių N, kad $\operatorname{Ker} f \subset N$. Be to, $f^{-1}(K)$ – grupės G normalusis pogrupis tada ir tik tada, kai K yra grupės H normalusis pogrupis.

Įrodymas. Sakykime, K, K_1, K_2 –grupės H pogrupiai. Akivaizdu, kad jei $K_1 \neq K_2$, tai $F(K_1) = f^{-1}(K_1) \neq f^{-1}(K_2) = F(K_2), \operatorname{Ker} f \subset f^{-1}(K) = F(K)$. Jei N grupės G toks pogrupis, kad $\operatorname{Ker} f \subset N$, tai $f(N)$ yra grupės H pogrupis ir $F(f(N)) = f^{-1}(f(N)) = N * \operatorname{Ker} f = N$. Remiantis teiginiu (žr.[?]) paskutinis išvados teiginys akivaizdus. $\triangle$

7. 7. Pirmoji teorema apie izomorfizmą. Tarkime, kad $(G,*),(H,\circ)$ – grupės, $f: G \to H$ – homomorfizmas. Tuomet grupės G faktorgrupė $G/\operatorname{Ker} f$ pagal homomorfizmo f branduolį $\operatorname{Ker} f$ yra izomorfinė grupei $f(G) \subset H$.

Įrodymas. Kadangi homomorfizmo f branduolys $\operatorname{Ker} f$ yra grupės G normalusis pogrupis, tai galima nagrinėti grupės G faktorgrupę $G/\operatorname{Ker} f$ pagal $\operatorname{Ker} f$. Apibrėžkime atvaizdį $\bar{f}: G/\operatorname{Ker} f \to H, \bar{f}(g * \operatorname{Ker} f) =: f(g), g \in G$. Įsitikinsime, kad atvaizdis $\bar{f}$ korektiškai apibrėžtas, t. y. nepriklauso nuo normaliojo pogrupio $\operatorname{Ker} f$ kairiosios gretutinės klasės $g * \operatorname{Ker} f$ atstovo parinkimo. Jei $g_1 * \operatorname{Ker} f = g_2 * \operatorname{Ker} f$, $g_1^{-1} * g_2 \in \operatorname{Ker} f$. Vadinasi, $f(g_1^{-1} * g_2) = 1_H$ arba $f(g_1) = f(g_2)$. Iš pastoriosios lygybės gauname: jei $g_1 * \operatorname{Ker} f = g_2 * \operatorname{Ker} f$, tai $\bar{f}(g_1 * \operatorname{Ker} f) = \bar{f}(g_2 * \operatorname{Ker} f)$.

Atvaizdis $\bar{f}: G/\operatorname{Ker} f \to H$ yra homomorfizmas. Iš tikrųjų: bet kuriems $g_1, g_2 \in G$,

$$\bar{f}((g_1 * \operatorname{Ker} f) * (g_2 * \operatorname{Ker} f)) = \bar{f}(g_1 * g_2 * \operatorname{Ker} f) =$$
$$= f(g_1 * g_2) = f(g_1) \circ f(g_2) = f(g_1 * \operatorname{Ker} f) \circ f(g_2 * \operatorname{Ker} f).$$

Dabar įsitikinsime, kad $\bar{f}$ – injektyvus homomorfizmas. Sakykime, $\bar{f}(g_1 * \operatorname{Ker} f) = \bar{f}(g_2 * \operatorname{Ker} f)$, t. y. $f(g_1) = f(g_2)$. Lygybę $f(g_1) = f(g_2)$ perrašykime taip: $1_H = f(g)^{-1} \circ f(g_2) = f(g_1^{-1} * g_2)$. Vadinasi, $g_1^{-1} * g_2 \in \operatorname{Ker} f$, t. y. $g_1 * \operatorname{Ker} f = g_2 * \operatorname{Ker} f$.

Grupės $G/\operatorname{Ker} f$ vaizdas yra $\bar{f}(G/\operatorname{Ker} f) = f(G)$. Taigi $\bar{f}: G/\operatorname{Ker} f \to f(G)$ – bijektyvus homomorfizmas, t. y. izomorfizmas. $\triangle$

Išvada. Jei $(G,*),(H,\circ)$ – grupės, $f: G \to H$ – siurjektyvus homomorfizmas, tai grupė $G/\operatorname{Ker} f$ yra izomorfinė grupei H.

7. 8. Antroji teorema apie izomorfizmą. Jei H, K yra grupės $(G,*)$ pogrupiai, H – normalusis pogrupis, tai $H \cap K$ yra grupės K normalusis pogrupis ir grupė $K/K \cap H$ yra izomorfinė grupei $H * K/H$.

Įrodymas. Atvaizdis $j: G \to G/H, j(g) = g * H, g \in G$, yra grupių homomorfizmas. Iš tikrųjų: $j(g_1 * g_2) = g_1 * g_2 * H = (g_1 * H) * (g_2 * H) = j(g_1) * j(g_2), g_1, g_2 \in G$. Akivaizdu,

kad Ker $j = H$. Rasime pogrupio K vaizdą $j(K)$: $j(K) = \{k * H |\ k \in K\}$ yra sudarytas iš pogrupio H kairiųjų (tas pats, kas ir iš dešiniųjų) gretutinių klasių $k * H, k \in K$. Taigi $j(K) = K * H/H$. Homomorfizmo $j\big|_K : K \to G/H$ branduolys Ker $j\big|_K = K \cap H$. Remdamiesi 1-ąja teorema apie izomorfizmą, gauname: grupė $K/K \cap H$ yra izomorfinė grupei $K * H/H$. $\triangle$

Išvada. Jei K, H – baigtinės grupės $(G, *)$ pogrupiai, H – normalusis pogrupis, tai $|K * H||K \cap H| = |H||K|$.

Įrodymas. Kadangi grupės $K/K \cap H$ ir $K * H/H$ yra izomorfinės, tai $\left|K/K \cap H\right| = \left|K * H/H\right|$. Iš šios lygybės gauname: $|K|/|K \cap H| = |K * H|/|H|$ arba $|K * H||K \cap H| = |K||H|$. $\triangle$

7. 9. Trečioji teorema apie izomorfizmą. Jei K, H – grupės $(G, *)$ normalieji pogrupiai ir $K \subset H$, tai H/K yra grupės G/K normalusis pogrupis ir grupė $G/K\big/H/K$ yra izomorfinė grupei G/H.

Įrodymas. Šią teoremą įrodyti paliekame skaitytojui.

8. Grupių tiesioginės sandaugos

8. 1. Jei grupė $(G, *)$ turi normalųjį pogrupį H, pagal kurį grupės G faktorgrupė G/H yra izomorfinė grupei K, tai grupė G yra vadinama grupės H plėtiniu grupe K. Bendruoju atveju aprašyti grupės H plėtinius grupe K, – gana sudėtingas uždavinys. Šio bendrojo uždavinio paprastesni variantai, – tai grupių H ir K pusiautiesioginės ir tiesioginė sandaugos. Dabar aptarsime grupių tiesioginę sandaugą.

Tarkime, $(H, *), (K, \circ)$ – grupės. Apibrėžkime aibių H ir K Dekarto sandaugos $H \times K$ elementų daugybą $\bullet$:

$$(h_1, k_1) \bullet (h_2, k_2) =: (h_1 * h_2, k_1 \circ k_2), (h_1, k_1), (h_2, k_2) \in H \times K.$$

Akivaizdu, kad aibės ($H \times K$ elementų daugyba $\bullet$ yra asociatyvi, $(1_H, 1_K)$ – šios daugybos atžvilgiu vienetas, elementui (h, k) atvirkštinis elementas yra (h^{-1}, k^{-1}). Kaip matome, aibė $H \times K$ jos elementų daugybos $\bullet$ atžvilgiu yra grupė.

Apibrėžimas. Grupė $(H \times K, \bullet)$ yra vadinama grupių $(H, *), (K, \circ)$ išorine tiesiogine sandauga, o grupės $(H, *), (K, \circ)$ – tiesioginės sandaugos komponentėmis.

Pastabos.

1. Tikriausiai pastebėjote, kad grupių tiesioginės sandaugos apibrėžime skirtingoms grupėms naudojome skirtingus grupių elementų daugybos ženklus. Tai darėme norėdami pabrėžti, kad gali būti imamos bet kokios grupės, o šias grupes tiesiogiai sudauginę, gauname visiškai naują grupę. Grupių $(H, *), (K, \circ)$ tisioginės sandaugos elementų daugybos ženklą būtų logiška žymėti $* \times \circ$. Bet tai per daug gremėzdiška. Sutarkime nuo šiol

grupių elementų daugybos ženklus vėl žymėti žvaigždute, tašku ar kokiu nors kitokiu simboliu arba visiškai praleisti. Tarp tiesioginės sandaugos komponenčių elementų dažniausiai kompozicijos ženklų nerašysime. Grupių H ir K išorinę tiesioginę sandaugą dažniausiai žymėsime $H \times K$.

2. Grupės $H \times K$ ir $K \times H$ yra izomorfinės: atvaizdis $f : H \times K \to K \times H$, $f((h,k)) = (k,h)$, $h \in H, k \in K$ yra izomorfizmas.

8. 2. Jei $(H \times K, *)$ yra grupių H ir K išorinė tiesioginė sandauga, tai grupės $H \times K$ pogrupiai $\tilde{H} =: \{(h, 1_K) |\ h \in H\}$ ir $\tilde{K} =: \{(1_H, k) |\ k \in K\}$ yra izomorfiniai grupėms H ir K. Grupės $H \times K$ pogrupiai $\tilde{H}$ ir $\tilde{K}$ tenkina sąlygas:

1. Kiekvienas grupės $H \times K$ elementas (h,k) yra išreiškiamas pogrupių $\tilde{H}$ ir $\tilde{K}$ elementų $(h, 1_K)$ ir $(1_H, k)$ sandauga: $(h,k) = (h, 1_K) * (1_H, k)$;
2. $\tilde{H}$ ir $\tilde{K}$ yra normalieji pogrupiai;
3. $\tilde{H} \cap \tilde{K} = \{(1_H, 1_K)\}$.

Įrodysime 2-ąją iš šių savybių.

Jei $(h', k') \in H \times K, (h, 1_K) \in \tilde{H}$, tai $(h', k') * (h, 1_K) * (h', k')^{-1} = (h'hh'^{-1}, 1_K) \in \tilde{H}$. Panašiai įrodoma, kad $\tilde{K}$ taip pat yra grupės $H \times K$ normalusis pogrupis.

Grupės $H \times K$ pogrupių $\tilde{H}$ ir $\tilde{K}$ 1-ąją, 2-ąją ir 3-iąją savybes galima pakeisti ekvivalenčiomis savybėmis:

1'. Kiekvienas grupės $H \times K$ elementas (h,k) yra vienareikšmiškai išreiškiamas pogrupių $\tilde{H}$ ir $\tilde{K}$ elementų $(h, 1_K)$ ir $(1_H, k)$ sandauga: $(h,k) = (h, 1_K) * (1_H, k)$.

2'. Kievienas pogrupio $\tilde{H}$ elementas yra perstatomas su kiekvienu pogrupio $\tilde{K}$ elementu.

Apibrėžimas. Grupė $(G, *)$ yra vadinama pogrupių H ir K (vidine) tiesiogine sandauga ir yra žymima $G = H \times K$, jei:

1. $G = H * K$;
2. H, K – grupės G yra normalieji pogrupiai;
3. $H \cap K = \{1\}$.

8. 3. Teiginys. Jei grupė $(G, *)$ yra pogrupių H ir K tiesioginė sandauga, tai kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga ir, be to, kiekvienas pogrupio H elementas yra perstatomas su kiekvienu pogrupio K elementu.

Įrodymas. Kadangi grupė G yra pogrupių tiesioginė sandauga, tai pogrupiai H, K yra normalieji, jų sankirta sudaryta iš grupės vieneto ir kievienas grupės G elementas yra išreiškiamas pogrupių H ir K elementų sandauga.

Jei $h \in H, k \in K$, tai elementų h, k komutatorius $[h,k] = h * k * h^{-1} * k^{-1} \in H \cap K$. Iš tikrųjų, kadangi H normalusis pogrupis ir $h \in H$, tai gauname, kad $h^{-1} \in H$, $k * h^{-1} * k^{-1} \in H$, vadinasi, ir $h * k * h^{-1} * k^{-1} \in H$. Kadangi K yra normalusis pogrupis ir $k \in K$, tai

panašiai kaip ir anksčiau, gauname, kad $h*k*h^{-1}*k^{-1} \in K$. Įrodėme, kad $[h,k] \in H \cap K$. Remdamiesi 3-ąja pogrupių H, K savybe, gauname $[h,k] = 1$, t. y. $h*k = k*h$. Dabar įrodysime, kad kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga. Jei $g = h*k = h'*k'$, tai $h'^{-1}*h = k'*k^{-1} \in H \cap K$, nes kairiojoje lygybės pusėje esantis elementas priklauso pogrupiui H, o dešiniojoje – pogrupiui K. Vadinasi, $h'^{-1}*h = k'*k^{-1} = 1$, t. y. $h = h', k = k'$. $\triangle$

Pastaba. Jei grupė $(G,*)$ yra pogrupių H ir K tiesioginė sandauga, tai kiekvienam grupės G elementui g egzistuoja tokie vieninteliai $h \in H$ ir $k \in K$, kad $g = h*k = k*h$. Ir šiuo atveju rašysime $G = H \times K = K \times H$.

8. 4. Teiginys. Jei kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga ir, be to, kiekvienas pogrupio H elementas yra perstatomas su kiekvienu pogrupio K elementu, tai grupė G yra pogrupių H ir K tiesioginė sandauga.

Įrodymas. Kadangi kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga, tai $G = H*K$. Iš sąlygos, kad kiekvienas pogrupio H elementas yra perstatomas su kiekvienu pogrupio K elementu, gauname: kiekvienam $k \in K$, $k*H = \{k*h|\ h \in H\} = \{h*k|\ h \in H\} = H*k$. Panašiai, kiekvienam $h \in H$ teisinga lygybė: $h*K = K*h$. Kadangi kiekvienam $h \in H$, $h*H = H = H*h$ ir kiekvienam $k \in K$, $k*K = K = K*k$, tai kiekvienam grupės G elementui g, $g*H = h*k*H = h*H*k = H*h*k = H*g$ (čia elementas g yra išreikštas pogrupių H, K elementų sandauga: $g = h*k$). Panašiai įrodoma lygybė $g*K = K*g, g \in G$. Kaip matome, pogrupiai H, K yra grupės G normalieji pogrupiai.

Įrodysime, kad pogrupių H ir K sankirta $H \cap K = \{1\}$. Jei būtų $q \in H \cap K$, $q \neq 1$, tai grupės G elemento g išraišką pogrupių H, K elementų h ir k sandauga $g = h*k$ galėtume užrašyti taip: $g = h*k = h*(q*q^{-1}*k) = (h*q)*(q^{-1}*k)$. Taigi matome, kad $h, h*q \in H$,$h \neq h*q$, $k, q^{-1}*k \in K$, t. y. grupės G elementas g yra išreiškiamas pogrupių H ir K elementų sandauga bent dviem skirtingais būdais. Tai prieštarauja teiginio sąlygai, kad kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga. $\triangle$

Pastabos.

1. Tai, kad grupė yra pogrupių tiesioginė sandauga, galima apibrėžti dviem skirtingais ekvivalenčiais būdais. Pirmasis grupės tiesioginės sandaugos apibrėžimas nusakomas šiomis sąlygomis:

(i) grupės kiekvienas elementas yra išreiškiamas pogrupių elementų sandauga;

(ii) šie pogrupiaiyra grupės normalieji pogrupiai;

(iii) šių pogrupių sankirta yra sudaryta tik iš grupės vieneto.

Antrasis, ekvivalentus pirmajam, – nusakomas taip:

(i) grupės kiekvienas elementas vienareikšmiškai yra išskaidomas į pogrupių elementų sandaugą;

(ii) šių pogrupių elementai tarpusavyje yra perstatomi.

2. Grupių išorinės tiesioginės sandaugos ir tiesioginės sandaugos sąvokos yra ekvivalenčios. Jei grupė $(H \times K, *)$ yra grupių H ir K išorinė tiesioginė sandauga, tai ji yra anksčiau apibrėžtų pogrupių $\tilde{H}$ ir $\tilde{K}$, izomorfinių atitinkamai grupėms H, K, tiesioginė sandauga. Teisingas ir toks teiginys: jei grupė $(G, *)$ yra pogrupių H ir K tiesioginė sandauga, tai ji yra izomorfinė grupių H ir K išorinei tiesioginei sandaugai $H \times K$. Pastarąjį teiginį įrodysime.

Įrodymas. Kiekvienam grupės G elementui g egzistuoja tokia vienintelė sutvarkyta pora (h_g, k_g), $h_g \in H$, $k_g \in K$, kad $g = h_g * k_g$. Kiekvienam elementui $g \in G$ priskyrę porą $(h_g, k_g) \in H \times K$, gauname bijekciją $f : G \to H \times K$ (čia $G \to H \times K$ suprantame kaip išorinę grupių G ir H tiesioginę sandaugą). Jei $g_1 = h_{g_1} * k_{g_1}$, $g_2 = h_{g_2} * k_{g_2}$, tai

$$f(g_1 * g_2) = f((h_{g_1} * k_{g_1}) * (h_{g_2} * k_{g_2})) = f((h_{g_1} * h_{g_2}) * (k_{g_1} * k_{g_2})) =$$

$$(h_{g_1} * h_{g_2}, k_{g_1} * k_{g_2}) = (h_{g_1}, k_{g_1}) * (h_{g_2}, k_{g_2}) = f(g_1) * f(g_2).$$

Kaip matome, bijekcija $f : G \to H \times K$ yra homomorfizmas. $\triangle$

8. 5. Dabar galime apibrėžti baigtinio grupių skaičiaus tiesioginę sandaugą.

Sakykime, $(H_1, *_1), (H_2, *_2), \ldots, (H_n, *_n)$ yra grupės. Apibrėžkime aibių H_1, H_2, ..., H_n Dekarto sandaugos

$$H_1 \times H_2 \times \ldots \times H_n$$

elementų daugybą $*$:

$$(h_1, h_2, \ldots, h_n) * (h'_1, h'_2, \ldots, h'_n) = (h_1 *_1 h'_1, h_2 *_2 h'_2, \ldots, h_n *_n h'_n),$$

$$(h_1, h_2, \ldots, h_n), \;\; (h_1, h_2, \ldots, h_n) \in H_1 \times H_2 \times \ldots \times H_n.$$

Panašiai, kaip ir dviejų grupių atveju, įrodoma, kad $H_1 \times H_2 \times \ldots \times H_n$ jos elementų apibrėžtos daugybos $*$ atžvilgiu yra grupė.

Apibrėžimas. Grupė $(H_1 \times H_2 \times \ldots \times H_n, *)$ yra vadinama grupių $(H_1, *_1)$, $(H_2, *_2)$, ..., $(H_n, *_n)$ išorine tiesiogine sandauga.

Apibrėžimas. Grupė $(G, *)$ yra vadinama pogrupių $H_1, H_2, \ldots, H_n$, tiesiogine sandauga, jei:

1. $G = H_1 * H_2 * \ldots * H_n$;
2. Grupės pogrupiai $H_1, H_2, \ldots, H_n$ yra normalieji;
3. Kiekvienam j, $1 \leq j \leq n$,

$$(H_1 * H_2 * \ldots * \hat{H}_j * \ldots * H_n) \cap H_j = \{1\}$$

čia stogelis virš pogrupio reiškia, kad to pogrupio pogrupių sandaugoje nėra.

8. 6. Panašiai, kaip ir dviejų pogrupių atveju, tai, kad grupė yra pogrupių tiesioginė sandauga, galima apibrėžti ir kitaip.

Apibrėžimas. Grupė $(G, *)$ yra vadinama pogrupių H_1, H_2, ..., H_n, tiesiogine sandauga, jei:

1. Kiekvienas grupės G elementas vienareikšmiškai yra išskaidomas pogrupių H_1, H_2, ..., H_n elementų sandauga:

$$(\forall g \in G)(\exists! h_1 \in H_1, h_2 \in H_2, \ldots, h_n \in H_n)(g = h_1 * h_2 * \ldots * h_n);$$

2. Bet kurių dviejų skirtingų pogrupių H_i ir H_j, $1 \leq i, j \leq n, i \neq j$, elementai tarpusavyje yra perstatomi:

$$h_i \in H_i, h_j \in H_j \Rightarrow h_i * h_j = h_j * h_i,\ 1 \leq i, j \leq n, i \neq j.$$

Kaip ir dviejų grupių atveju, grupių išorinės tiesioginės sandaugos ir tiesioginės sandaugos sąvokos yra ekvivalenčios.

Pratimai.

1. Įrodykite, kad abu grupių tiesioginės sandaugos apibrėžimai yra ekvivalentūs.

2. Įrodykite, jei grupės $(H_1, *_1), (H_2, *_2), \ldots, (H_n, *_n)$ yra komutatyvios, tai šių grupių išorinė tiesioginė sandauga – taip pat komutatyvi.

3. Įrodykite, kad dviejų baigtinių ciklinių grupių, kurių eilės yra tarpusavyje pirminės, tiesioginė sandauga yra ciklinė grupė.

4. Apibendrinkite 3-iąjį pratimą baigtinio skaičiaus baigtinių ciklinių grupių atvejui.

8. 7. Grupių tiesioginę sandaugą galima apibrėžti ir begalinio grupių skaičiaus atveju.

Sakykime, $\{(G_\alpha, *)\}_{\alpha \in I}$ yra grupių šeima. Aibių šeimos $\{G_\alpha\}_{\alpha \in I}$ tiesioginės sandaugos $\prod\limits_{\alpha \in I} G_\alpha$ elementų daugybą $*$ apibrėžkime taip: jei $\{g_\alpha\}_{\alpha \in I}, \{h_\alpha\}_{\alpha \in I} \in \prod\limits_{\alpha \in I} G_\alpha$, tai

$$\{g_\alpha\}_{\alpha \in I} * \{h_\alpha\}_{\alpha \in I} =: \{g_\alpha * h_\alpha\}_{\alpha \in I}$$

Akivaizdu, kad aibė $\prod\limits_{\alpha \in I} G_\alpha$ apibrėžtos jos elementų daugybos $*$ atžvilgiu sudaro grupę, kurią žymėsime $(\prod\limits_{\alpha \in I} G_\alpha, *)$.

Apibrėžimas. Grupę $(\prod\limits_{\alpha \in I} G_\alpha, *)$ vadinsime grupių šeimos $\{(G_\alpha, *)\}_{\alpha \in I}$ tiesiogine sandauga.

Ši grupių tiesioginė sandauga yra vadinama išorine. Galima apibrėžti ir grupių vidinę tiesioginę sandaugą. Bet tuo atveju, kai duota grupių šeima yra begalinė, grupių išorinės ir vidinės tiesioginių sandaugų apibrėžimai nėra ekvivalentūs.

Teiginys. Tarkime, kad $\{G_\alpha\}_{\alpha\in I}$ yra grupės $(G,*)$ normaliųjų pogrupių šeima, generuojanti grupę G ir kiekvienam $\alpha_0 \in I$,

$$G_{\alpha_0} \cap \prod_{\alpha\in I\setminus\alpha_0} G_\alpha = \{1\}.$$

Tuomet kiekvienas grupės $(G,*)$ elementas vienareikšmiškai yra išreiškiamas normaliųjų pogrupių šeimos $\{G_\alpha\}_{\alpha\in I}$ elementų baigtine sandauga.

Įrodymas. Pirmiausia įrodysime, kad šeimos $\{G_\alpha\}_{\alpha\in I}$ bet kurių dviejų skirtingų pogrupių G_α, G_β elementai $g_\alpha \in G_\alpha, g_\beta \in G_\beta$ yra perstatomi, t.y., bet kuriems $g_\alpha \in G_\alpha, g_\beta \in G_\beta, \alpha \neq \beta$,

$$g_\alpha * g_\beta = g_\beta * g_\alpha$$

Imkime elementų $g_\alpha \in G_\alpha, g_\beta \in G_\beta$ komutatorių $[g_\alpha, g_\beta] = g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1}$. Kadangi G_α ir G_β yra normalieji pogrupiai, tai $g_\beta * g_\alpha^{-1} * g_\beta^{-1} \in G_\alpha$, vadinasi, ir $g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1} \in G_\alpha$. Panašiai gauname, kad $g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1} \in G_\beta$. Vadinasi, elementas $[g_\alpha, g_\beta] \in G_\alpha \cap G_\beta, \alpha \neq \beta$. Bet remdamiesi sąlyga: kiekvienam $\alpha_0 \in I$,

$$G_{\alpha_0} \cap \prod_{\alpha\in I\setminus\alpha_0} G_\alpha = \{1\},$$

gauname, kad $G_\alpha \cap G_\beta = \{1\}$, jei tik $\alpha \neq \beta$. Taigi $[g_\alpha, g_\beta] = g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1} = 1$ arba $g_\alpha * g_\beta = g_\beta * g_\alpha$.

Remdamiesi teoremos sąlyga, gauname, kad grupės $(G,*)$ kiekvienas elementas yra išreiškiamas pogrupių šeimos $\{G_\alpha\}_{\alpha\in I}$ elementų baigtine sandauga. Daugiklių tvarka nesvarbi, nes įrodėme, kad skirtingų šeimos pogrupių elementai yra perstatomi. Lieka įrodyti, kad kiekvienas grupės G elementas yra vienareikšmiškai išreiškiamas pogrupių šeimos $\{G_\alpha\}_{\alpha\in I}$ elementų sandauga. Tarkime, kad

$$g = \prod_{\alpha\in I} g_\alpha = \prod_{\alpha\in I} h_\alpha,$$

čia beveik visiems $\alpha \in I$, $g_\alpha = 1$. Reikia įrodyti, kad kiekvienam $\alpha \in I$, $g_\alpha = h_\alpha$. Nagrinėkime elementą

$$(\prod_{\alpha\in I} g_\alpha) * (\prod_{\alpha\in I} h_\alpha)^{-1} = \prod_{\alpha\in I} (g_\alpha * h_\alpha^{-1}) = 1.$$

Jei kuriam nors $\alpha_0 \in I$ būtų $g_{\alpha_0} * h_{\alpha_0}^{-1} \neq 1$,tai, remdamiesi lygybe

$$\prod_{\alpha\in I} (g_\alpha * h_\alpha^{-1}) = 1$$

gautume:

$$1 \neq g_{\alpha_0}^{-1} * h_{\alpha_0} \in G_{\alpha_0} \cap \prod_{\alpha \in I \setminus \alpha_0} G_\alpha = \{1\},$$

kas prieštarautų teoremos sąlygai. $\triangle$

9. Grupės ir aibės elementų išorinis kompozicijos dėsnis

9. 1. Tegu G – grupė, X – aibė. Nagrinėkime grupės G, kaip operatorių aibės, ir aibės X elementų išorinį kompozicijos dėsnį $F : G \times X \to X$, tenkinantį sąlygas:

1. Kiekvienam $x \in X$, $F(1, x) = x$, čia 1 – grupės G vienetas;
2. Bet kuriems $g_1, g_2 \in G$, $x \in X$, $F(g_1 g_2, x) = F(g_1, F(g_2, x))$.

Jei išorinį kompozicijos dėsnį F pažymėtume $*$ ir rašytume tarp komponuojamųjų elementų, tai anksčiau užrašytos sąlygos atrodytų taip:

1. Kiekvienam $x \in X$, $1 * x = x$, čia 1 – grupės G vienetas;
2. Bet kuriems $g_1, g_2 \in G$, $x \in X$, $(g_1 g_2) * x = g_1 * (g_2 * x)$.

Pastaba. Tegu apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis su reikšmėmis aibėje X. Tuomet patogus išsireiškimas: "aibės X elementą x, paveikę grupės G elementu g, gauname $g * x$".

9. 2. Grupės G, kaip operatorių aibės, ir aibės X elementų išorinis kompozicijos dėsnis $*$ apibrėžia aibėje X ekvivalentumo sąryšį: aibės X elementas x_2 yra vadinamas ekvivalenčiu elementui x_1, jei egzistuoja toks grupės G elementas g, kad $x_2 = g * x_1$. Įsitikinsime, kad tai iš tikrųjų ekvivalentumo sąryšis.

Pirma, kiekvienam aibės X elementui x, x yra ekvivalentus x, nes, remiantis pirmąja išorinio kompozicijos dėsnio $*$ savybe, $x = 1 * x$.

Antra, tegu x_2 yra ekvivalentus x_1, t. y. egzistuoja toks grupės G elementas g, kad $x_2 = g * x_1$. Tuomet šios lygybės abi puses paveikę grupės G elementu g^{-1}, gauname: $g^{-1} * x_2 = g^{-1} * (g * x_1) = (g^{-1} g) * x_1 = 1 * x_1 = x_1$, t. y. x_1 yra ekvivalentus x_2.

Trečia, tarkime, x_3 yra ekvivalentus x_2, o x_2 yra ekvivalentus x_1, t. y. egzistuoja tokie $g, h \in G$, kad $x_3 = g * x_2$, $x_2 = h * x_1$. Tuomet, remdamiesi antrąja išorinio kompozicijos dėsnio $*$ savybe, gauname: $x_3 = g * x_2 = g * (h * x_1) = (gh) * x_1$, t. y. x_3 yra ekvivalentus x_1.

Apibrėžimas. Kiekvienam aibės X elementui x apibrėžkime aibės X poaibį $G * x =: \{g * x \mid g \in G\}$. Aibės X poaibis $G * x$ yra vadinamas elemento x orbita. Elemento x orbita $G * x$ yra elemento x ekvivalentumo klasė, ekvivalentumo sąryšio, apibrėžto išorinio kompozicijos dėsnio $*$, atžvilgiu.

Pastaba. Tegu apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis su reikšmėmis aibėje X. Tuomet galime užrašyti lygybę:

$$X = \bigcup_{\alpha \in I} G * x_\alpha,$$

čia x_alpha, $\alpha \in I$, – skirtingų ekvivalentumo klasių atstovai. Kaip žinome, $G*x_\alpha \neq G*x_\beta$, jei $\alpha \neq \beta$, $\alpha \in I$.

9.3. Tarkime, kad apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis su reikšmėmis aibėje X.

Apibrėžimas. Tegu $x \in X$. Grupės G poaibis $\{g \in G \mid g * x = x\}$ yra vadinamas elemento x stabilizatoriumi ir yra žymimas $\mathrm{St}_G(x)$

Teiginys. Aibės X elemento x stabilizatorius $\mathrm{St}_G(x)$ yra grupės G pogrupis.

Šio teiginio įrodymas akivaizdus.

Teiginys. Jei aibės X elementas y priklauso elemento x orbitai $G*x$, tai elemento y stabilizatorius $\mathrm{St}_G(y)$ yra sujungtinis grupės G pogrupis pogrupiui $\mathrm{St}_G(x)$.

Įrodymas. Priminsime, kad grupės G pogrupis H yra vadinamas sujungtiniu pogrupiu pogrupiui N, jei egzistuoja toks grupės G elementas g, kad $H = gNg^{-1}$.

Kadangi elementas $y \in G*x$, tai egzistuoja toks grupės G elementas g, kad $y = g*x$. Tuomet kiekvienam pogrupio $\mathrm{St}_G(x)$ elementui h elementas ghg^{-1} priklauso elemento y stabilizatoriui $\mathrm{St}_G(y)$, nes

$$(ghg^{-1}) * y = (gh) * (g^{-1} * y) = (gh) * x = g * (h * x) = g * x = y.$$

Vadinasi, $g\mathrm{St}_G(x)g^{-1} \subset \mathrm{St}_G(y)$. Panašiai galite įsitikinti, kad $g\mathrm{St}_G(x)g^{-1} \supset \mathrm{St}_G(y)$. $\triangle$

9. 4. Teiginys. Aibės X elemento x orbitos $G*x$ elementų skaičius yra lygus elemento x stabilizatoriaus $\mathrm{St}_G(x)$ indeksui $[G : \mathrm{St}_G(x)]$ grupėje G.

Įrodymas. Nagrinėkime grupės G skaidinį pogrupio $\mathrm{St}_G(x)$ kairiosiomis gretutinėmis klasėmis:

$$G = \mathrm{St}_G(x) \cup g_2\mathrm{St}_G(x) \cup \ldots \cup g_r\mathrm{St}_G(x).$$

Įrodysime, kad elemento x orbitą $G*x$ sudaro aibės X elementai x, g_2*x, …, g_r*x.

Pirmiausia pastebėsime, kad $h_1*x = h_2*x$ tada ir tik tada, kai grupės G elementai h_1 ir h_2 priklauso vienai ir tai pačiai pogrupio $\mathrm{St}_G(x)$ kairiajai gretutinei klasei. Iš tikrųjų, lygybės $h_1*x = h_2*x$ abi puses, paveikę grupės elementu h_2^{-1}, gauname

$$h_2^{-1} * (h_1 * x) = h_2^{-1} * (h_2 * x) = (h_2^{-1}h_2) * x = x,$$

t. y. $(h_2^{-1}h_1) * x = x$. Vadinasi, jei $h_1*x = h_2*x$, tai $h_2^{-1}h_1 \in \mathrm{St}_G(x)$, t. y. h_1 ir h_2 priklauso vienai ir tai pačiai pogrupio $\mathrm{St}_G(x)$ kairiajai gretutinei klasei. Kadangi grupės G elementai 1, g_2, …, g_r yra skirtingų pogrupio $\mathrm{St}_G(x)$ kairiųjų gretutinių klasių atstovai, tai aibės X elementai x, g_1*x, …, g_r*x yra tarpusavy skirtingi. Lieka įrodyti, kad kiekvienas orbitos $G*x$ elementas sutampa su kuriuo nors aibės $\{x,\ g_1*x,\ \ldots,\ g_r*x\}$ elementu.

Tarkime, $y \in G * x$. Tuomet egzistuoja toks grupės G elementas g, kad $y = g * x$. Jei grupės G elementas g priklauso pogrupio $\mathrm{St}_G(x)$ kairiajai gretutinei klasei $g_j\mathrm{St}_G(x)$, tai $y = g * x = g_j * x$. $\triangle$

9. 5. Pavyzdžiai.

1. Tarkime, G – baigtinė grupė. Apibrėžkime atvaizdį

$$* : G \times G \to G,\ (g,\ h) \mapsto g * h = ghg^{-1},\ g, h \in G.$$

Apibrėžimas. Elemento $h \in G$ ekvivalentumo klasė $\{ghg^{-1} \mid g \in G\}$ yra vadinama elementui h sujungtinių elementų klase ir yra žymima $C_G(h)$.

Elemento $h \in G$ stabilizatorius $\mathrm{St}_G(h)$ yra sudarytas iš visų tokių grupės G elementų g, kurių kiekvienas yra perstatomas su elementu h. Grupių teorijoje elemento h stabilizatorius $\mathrm{St}_G(h)$ yra vadinamas elemento h centralizatoriumi ir yra žymimas $Z_G(h)$. Grupės G elementui h sujungtinių elementų skaičius yra lygus elemento h centralizatoriaus $Z_G(h)$ indeksui $[G : Z_G(h)]$ grupėje G. Taigi kiekvienam elementui $h \in G$ sujungtinių elementų skaičius $|C_G(h)|$ dalija grupės G eilę $|G|$. Galime parašyti:

$$G = C_G(h_1) \cup C_G(h_2) \cup \ldots \cup C_G(h_s),$$

čia h_1, h_2, …, h_s – sujungtinių elementų skirtingų klasių atstovai.

2. Tarkime, G – grupė, $X = \mathbf{P}_0(G)$ – grupės G visų pogrupių aibė. Apibrėžkime grupės G ir aibės X elementų išorinį kompozicijos dėsnį taip:

$$* : G \times X \to X,\ (g, H) \mapsto g * H =: gHg^{-1},\ g \in G,\ G \supset H -\ \text{pogrupis}.$$

Aibės X elemento H ekvivalentumo klasė yra sudaryta iš vieno elemento H tada ir tik tada, kai H yra grupės G normalusis pogrupis. Aibės X elementai H ir N yra ekvivalentūs tada ir tik tada, kai grupės G pogrupiai H ir N yra sujungtiniai. Kitaip tariant, aibės X elementai H ir N yra ekvivalentūs tada ir tik tada, jei egzistuoja toks grupės G elementas g, kad $H = gNg^{-1}$.

Aibės X elemento H stabilizatorius $\mathrm{St}_G(H)$ grupių teorijoje yra vadinamas grupės G pogrupio H normalizatoriumi ir yra žymimas $N_G(H)$. Kaip ir pirmojo pavyzdžio atveju, grupės G pogrupiui H sujungtinių pogrupių skaičius dalija grupės G eilę $|G|$.

3. Remdamiesi grupės G ir aibės X elementų išorinio kompozicijos dėsnio sąvoka, įrodysime svarbų faktą apie p-grupes.

Apibrėžimas. Grupė G yra vadinama p-grupe, jei šios grupės kiekvieno elemento eilė yra lygi pirminio skaičiaus p laipsniui.

Pastaba. Jei p-grupė G yra baigtinė, tai remdamiesi Koši teorema (kurią įrodysime vėliau): jei baigtinės grupės eilė dalijasi iš pirminio skaičiaus p, tai grupė turi p eilės

elementą, gauname, kad grupės G eilė $|G|$ yra lygi pirminio skaičiaus p laipsniui p^n. Taigi baigtinės grupės atveju, p-grupę galima apibrėžti, kaip grupę G, kurios eilė $|G|$ yra lygi pirminio skaičiaus laipsniui p^n.

9. 6. Teorema. Kiekviena baigtinė p-grupė G turi netrivialų centrą $Z(G)$.

Įrodymas. Apibrėžkime p-grupės G, kaip operatorių aibės, ir aibės $X = G$ išorinį kompozicijos dėsnį:

$$* : G \times G \to G,\ g * h = ghg^{-1},\ g, h \in G.$$

Šiuo atveju aibės G elemento h orbita $G * h = \{ghg^{-1} \mid g \in G\}$ yra grupės G elementui h sujungtinių elementų klasė. Sakykime, $G * h_1$, $G * h_2$, ..., $G * h_s$ – visos skirtingos G elementų orbitos, t. y.,

$$G = G * h_1 \cup G * h_2 \cup \ldots \cup G * h_s.$$

Remdamiesi šia lygybe, galime užrašyti

$$|G| = |G * h_1| + |G * h_2| + \ldots + |G * h_s|. \tag{1}$$

Kadangi kiekvienos orbitos elementų skaičius yra lygus šios orbitos bet kurio elemento stabilizatoriaus indeksui, tai kiekvienos orbitos elementų skaičius yra pirminio skaičiaus p laipsnis (p-grupės tiek kiekvieno pogrupio eilė, tiek ir pogrupio indeksas yra pirminio skaičiaus p laipsnis). Vadinasi, jei kurio nors p-grupės G elemento h orbita $G * h$ sudaryta daugiau nei iš vieno elemento, tai $p \mid |G * h|$. Grupės G vieneto 1 orbita yra $\{1\}$. Kadangi $p \mid |G|$ ir tai pirminis skaičius p dalija ir dešiniąją (1) lygybės pusę. Kadangi (1) lygybės dešinėje pusėje yra vienas dėmuo lygus 1, tai dešinėje pusėje turi būti dar bent vienas dėnuo lygus $1 = p^0$. Tarkime, $|G * h_j| = 1$, čia h_j nėra grupės G vienetas. $|G * h_j| = 1$ tada ir tik tada, kai $G * h_j = \{h_j\}$, t. y., kai kiekvienam $g \in G$, $gh_jg^{-1} = h_j$. O tai ir reiškia, kad $h_j \in Z(G)$. $\triangle$

9. 7. Sakykime, apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis $*$. Galima užrašyti aibės X elementų skirtingų orbitų skaičiaus formulę. Pažymėkime $N(g)$ aibės X elementų, tenkinančių sąlygą $g * x = x$, skaičių. Nagrinėkime sumą $\sum\limits_{g \in G} N(g)$. Imkime $x \in X$. Elementas x į užrašytą sumą yra įskaičiuojamas $|\mathrm{St}_G(x)|$ kartų, nes kiekvienam $g \in \mathrm{St}_G(x)$, $g * x = x$. Į anksčiau užrašytą sumą $|\mathrm{St}_G(x)|$ kartų yra įskaičiuojamas ir kiekvienas elemento x orbitos $G * x$ elementas. Taigi elemento x orbitos $G * x$ elementų indėlis į nagrinėjamą sumą yra lygus

$$|G * x||\mathrm{St}_G(x)| = [G : \mathrm{St}_G(x)]|\mathrm{St}_G(x)| = |G|.$$

Vadinasi,

$$\text{aibės } X \text{ elementų skirtingų orbitų skaičius} = \frac{1}{|G|} \sum_{g \in G} N(g).$$

10. Baigtinių Abelio grupių struktūra

10. 1. Nagrinėsime baigtines Abelio grupes.

Apibrėžimas. Grupė G, kurios kiekvieno elemento eilė yra lygi pirminio skaičiaus p laipsniui, yra vadinama p-grupe. Abelio p-grupė dažnai yra vadinama primariąja p-grupe.

Koši teorema. Jei Abelio grupės G eilė n dalijasi iš pirminio skaičiaus p, tai grupė G turi p eilės elementą.

Įrodymas. Teoremą įrodysime matematinės indukcijos metodu. Jei $n = 1$, tai teoremos teiginys teisingas, nes 1 nesidalija iš jokio pirminio skaičiaus. Tarkime, kad teoremos teiginys teisingas kiekvienai Abelio grupei, kurios eilė $m < n$. Imkime grupės G elementą $g \neq 1$ ir nagrinėkime ciklinę grupę $[g]$. Jei $[g] = G$, tai elemento $g^{\frac{n}{p}}$ eilė yra p. Jei $[g] \subset G$, $[g] \neq G$, tai galimi du atvejai: (i) $p \big| |[g]|$ ir (ii) $p \not| |[g]|$. Pirmuoju atveju pogrupio $[g]$ eilė $|[g]| < n$ ir dalijasi iš skaičiaus p. Vadinasi, remdamiesi indukcine prielaida, gauname, kad šiuo atveju teorema įrodyta. Antruoju atveju grupės G faktorgrupės $G/[g]$ pagal pogrupį $[g]$ eilė $|G/[g]| = \frac{|G|}{|[g]|} < n$ ir dalijasi iš skaičiaus p. Remdamiesi indukcine prielaida, gauname, kad grupė $G/[g]$ turi p eilės elementą $h * [g]$, t. y. $(h * [g])^p = [g]$, $(h * [g])^j \neq [g]$, kai $0 < j < p$. Lygybė $(h * [g])^p = [g]$ ekvivalenti sąlygai $h^p \in [g]$, t. y. egzistuoja toks $s \in \mathbb{N}$, kad $h^p = g^s$. Elemento h eilė yra lygi pt, čia t – toks mažiausias teigiamas skaičius, kad $(g^s)^t = 1$. Vadinasi, elemento h^t eilė yra lygi p.

Išvada. Baigtinės Abelio p-grupės G eilė yra lygi pirminio skaičiaus p laipsniui. Iš tikrųjų, jei Abelio p-grupės G eilė $|G|$ dalytųsi iš pirminio skaičiaus $q \neq p$, tai, remiantis įrodyta teorema, grupė Gturėtų q eilės elementą. O tai prieštarautų sąlygai, kad G yra p-grupė. $\triangle$

10. 2. Dabar įrodysime Koši teoremą bendruoju atveju.

Koši teorema. Jei baigtinės grupės G eilė dalijasi iš pirminio skaičiaus p, tai grupė G turi p eilės elementą.

Įrodymas. Šią teoremą įrodysime taip pat matematinės indukcijos metodu. Jei grupės G eilė lygi 1, tai teoremos teiginys teisingas. Tarkime, kad teoremos teiginys teisingas kiekvienai grupei, kurios eilė $m < n$. Jei egzistuoja grupės G pogrupis H, $H \neq G$, kurio eilė dalijasi iš piminio skaičiaus p, tai, remdamiesi indukcine prielaida, gauname, kad teoremos teiginys teisingas. Nagrinėkime atvejį, kai nei vieno grupės G pogrupio eilė nesidalija iš skaičiaus p. Sudarykime grupės G skaidinį sujungtinių elementų klasėmis

$$G = \bigcup_{j=1}^{r} C(g_j) \cup \bigcup_{z \in Z(G)} \{z\},$$

čia g_j sujungtinių elementų skirtingų klasių atstovai, nepriklausantys grupės G centrui, $Z(G)$ – grupės G centras. Taigi galime užrašyti lygybę: $|G| = |Z(G)| + \sum_{j=1}^{r} |C(g_j)|$.

Grupės G elementui g sujungtinių elementų skaičius $|C(g)|$ yra lygus elemento g centralizatoriaus $Z_G(g)$ indeksui $[G : Z_G(g)]$ grupėje G. Grupės G elemento z, priklausančio grupės G centrui, sujungtinių elementų klasė sudaryta tik iš vieno elemento $\{z\}$, nes kiekvieno grupės centro elemento centralizatorius sutampa su grupe G. Elemento g, nepriklausančio centrui, centralizatorius $Z_G(g)$ yra grupės G pogrupis, nesutampantis su grupe G. Kadangi pogrupio $Z_G(g)$ eilė pagal padarytą prielaidą nesidalija iš pirminio skaičiaus p, o grupės G eilė dalijasi iš p, tai ir pogrupio $Z_G(g)$ indeksas $[G : Z_G(g)]$ grupėje G dalijasi iš p. Vadinasi, kiekvienas sumos $\sum_{j=1}^{r} |C(g_j)|$ dėmuo $|C(g_j)|$, $1 \leq j \leq r$, dalijasi iš p. Gauname, kad iš skaičiaus p dalijasi ir grupės G centro $Z(G)$ eilė. Tai įmanoma, remiantis padaryta prielaida, kad grupės G kiekvieno netrivialaus pogrupio eilė nesidalija iš pirminio skaičiaus p, tik tuo atveju, jei $Z(G) = G$. O Abelio grupėms šią teoremą įrodėme. $\triangle$

Išvada. Jei G yra baigtinė p-grupė, tai grupės G eilė $|G|$ yra pirminio skaičiaus p laipsnis.

10. 3. Teorema. Sakykime, kad baigtinės Abelio grupės G eilė yra n,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

– skaičiaus n kanoninis skaidinys pirminiais skaičiais. Tuomet grupė G yra vienareikšmiškai išskaidoma į p_j-pogrupių G_j, $1 \leq j \leq r$, tiesioginę sandaugą $G = \prod_{j=1}^{r} G_j$ (t. y. vienareikšmiškai yra nusakomi pogrupiai G_j, $1 \leq j \leq r$). Pogrupio G_j eilė yra lygi $p_j^{\alpha_j}$, $1 \leq j \leq r$.

Įrodymas. Sudarykime skaičius $n_j = n/p_j^{\alpha_j}$, $1 \leq j \leq r$. Šių skaičių didžiausias bendrasis daliklis yra lygus 1 (akivaizdu: $p_i \mid n_j$, $i \neq j$, bet $p_i \not| n_i$, $1 \leq i, j \leq r$). Vadinasi, egzistuoja tokie sveikieji skaičiai q_j, $1 \leq j \leq r$, kad $\sum_{j=1}^{r} n_j q_j = 1$. Kadangi G yra Abelio grupė, tai grupės G elementų g, pakeltų n_j laipsniais, aibė $G_j = \{g^{n_j} \mid g \in G\}$, $1 \leq j \leq r$ yra grupės G pogrupis. Iš tikrųjų, jei $g_1^{n_j}, g_2^{n_j} \in G_j$, tai $g_1^{n_j}(g_2^{n_j})^{-1} = (g_1 g_2^{-1})^{n_j} \in G_j$, $1 \leq j \leq r$. Kiekvienam j, $1 \leq j \leq r$, G_j yra grupės G p_j – pogrupis, nes pogrupio G_j kiekvienas elementas, pakeltas $p_j^{\alpha_j}$ laipsniu, yra grupės G vienetas 1. Iš tikrųjų, jei $g^{n_j} \in G_j$, tai $(g^{n_j})^{p_j^{\alpha_j}} = g^n = 1$ (priminsime, kad grupės elemento eilė dalija grupės eilę). Dabar įrodysime, kad kiekvienas grupės G elementas g yra vienareikšmiškai išreiškiamas pogrupių G_j, $1 \leq j \leq r$, elementų sandauga. Imkime $g \in G$. Tuomet

$$g^1 = g^{\sum_{j=1}^{r} n_j q_j} = \prod_{j=1}^{r} (g^{n_j})^{q_j}.$$

Kiekvienam j, $1 \leq j \leq r$, elementas g^{n_j} priklauso pogrupiui G_j, vadinasi, ir $(g^{n_j})^{q_j} \in G_j$. Pažymėję $g_j =: (g^{n_j})^{q_j}$, gauname: $g = \prod_{j=1}^{r} g_j$. Lieka įrodyti šios sandaugos vienatį.

Tarkime, kad

$$g = \prod_{j=1}^{r} g_j = \prod_{j=1}^{r} g'_j.$$

Lygybę

$$\prod_{j=1}^{r} g_j = \prod_{j=1}^{r} g'_j$$

galime perrašyti taip: kiekvienam s, $1 \leq s \leq r$,

$$g_s {g'}_s^{-1} = \prod_{\substack{j=1 \\ j \neq s}}^{r} g_j {g'}_j^{-1}.$$

Gavome, kad kiekvienam s, $1 \leq s \leq r$, elementas $g_s {g'}_s^{-1}$ priklauso ir pogrupiui G_s ir pogrupiui $\prod\limits_{\substack{j=1 \\ j \neq s}}^{r} G_j$. Vadinasi, $(g_s {g'}_s^{-1})^{p_s} = 1$ ir $(g_s {g'}_s^{-1})^{n_s} = 1$, nes

$$(\prod_{\substack{j=1 \\ j \neq s}}^{r} g_j {g'}_j^{-1})^{n_s} = \prod_{\substack{j=1 \\ j \neq s}}^{r} (g_j {g'}_j^{-1})^{n_s} = \prod_{\substack{j=1 \\ j \neq s}}^{r} g_j^{n_s} ({g'}_j^{-1})^{n_s} = 1$$

(kiekvienam j, $1 \leq j \leq r$, $j \neq s$, $p_j^{\alpha_j} \mid n_s$, o $h_j^{p_j^{\alpha_j}} = 1$, jei $h_j \in G_j$). Kadangi kiekvienam s, $1 \leq s \leq r$, skaičiai p_s ir n_s yra tarpusavyje pirminiai, tai egzistuoja tokie sveikieji skaičiai a_s ir b_s, kad $p_s a_s + n_s b_s = 1$. Taigi kiekvienam s, $1 \leq s \leq r$, $g_s {g'}_s^{-1} = (g_s {g'}_s^{-1})^{p_s a_s + n_s b_s} = 1$, t. y. gavome, kad $g_s = g'_s$. Įrodėme, kad grupė G yra pogrupių G_j, $1 \leq j \leq r$, tiesioginė sandauga. Remdamiesi lygybe $|G| = n = \prod\limits_{j=1}^{r} p_j^{\alpha_j} = \prod\limits_{j=1}^{r} |G_j|$ gauname,kad kiekvienam j, $1 \leq j \leq r$, $|G_j| = p_j^{\alpha_j}$, nes pogrupio G_j eilė yra lygi pirminio skaičiaus p_j, $1 \leq j \leq r$, laipsniui.

Visiškai akivaizdu, kad pogrupiai G_j, $1 \leq j \leq r$ yra vienareikšmiškai apibrėžiami: kiekvienam j, $1 \leq j \leq r$, pogrupis G_j yra sudarytas iš grupės G elementų, kurių eilė yra pirminio skaičiaus p_j laipsnis. $\triangle$

10. 4. Ką tik įrodyta teorema dažnai yra formuluojama ir įrodoma adiciniais žymėjimais. Mes tai pat pateiksime šios teoremos formuluotę adicinėje terminalogijoje. Štai perėjimo nuo multiplikacinių žymėjimų ir terminų prie adicinių žymėjimų ir terminų žodynėlis:

Sandaugos ženklą $\prod$ atitinka sumos ženklas $\sum$;
Elemento laipsnį g^n atitinka skaičiaus n ir elemento g sandauga ng;
Elementų sandaugą $g_1^{n_1} g_2^{n_2} \dots g_s^{n_s}$ atitinka elementų suma $n_1 g_1 + n_2 g_2 + \dots + n_s g_s$;
Elementą 1 atitinka elementas 0;

Daugybos ženklą $*$ (ar $\cdot$) atitinka sudėties ženklas $+$;
Terminą "tiesioginė sandauga" atitinka terminas "tiesioginė suma";
Ženklą $\oplus$ naudosime tiesioginei sumai žymėti.

10. 5. Dabar suformuluosime anksčiau įrodytą teoremą adiciniais žymėjimais.

Teorema. Sakykime, kad baigtinės Abelio grupės G eilė yra n, $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ – skaičiaus n kanoninis skaidinys pirminiais skaičiais. Tuomet grupė G yra vienareikšmiškai išskaidoma į p_j-pogrupių G_j, $1 \le j \le r$, tiesioginę sumą $G = \bigoplus_{j=1}^{r} G_j$ (t. y. pogrupiai G_j, $1 \le j \le r$ yra vienareikšmiškai apibrėžiami). Pogrupio G_j eilė yra lygi $p_j^{\alpha_j}$, $1 \le j \le r$.

10. 6. Dabar įrodysime, kad kiekvieną baigtinę Abelio p-grupę G galima išskaidyti į ciklinių pogrupių tiesioginę sandaugą.

Teorema. Kiekviena baigtinė Abelio p-grupė G yra išskaidoma į ciklinių p-pogrupių tiesioginę sandaugą $\prod_{j=1}^{r} G_j$.

Įrodymas. Sakykime, kad g_1 yra grupės G didžiausios eilės p^{n_1} elementas. Jei ciklinis pogrupis $[g_1] = G$, tai teoremos įrodymas baigtas. Jei $[g_1] \neq G$, tai išrinkime grupės G tokį elementą g_2', kad elementas $g_2'[g_1]$ faktorgrupėje $G/[g_1]$ turėtų didžiausią eilę p^{n_2}. Tuomet ${g'_2}^{p^{n_2}} \in [g_1]$, t. y. kuriam nors j, $0 \le j < p^{n_1}$, ${g'_2}^{p^{n_2}} = g_1^j$. Kadangi elementas g_1 grupėje G yra didžiausios eilės, tai $(g_1^j)^{p^{n_1-n_2}} = g_1^{jp^{n_1-n_2}} = {g'_2}^{p^{n_1}} = 1$. Vadinasi, $p^{n_1} \mid jp^{n_1-n_2}$, t. y. $p^{n_2} \mid j$. Galime parašyti $j = p^{n_2} j'$. Įrašę šią j išraišką į lygybę ${g'_2}^{p^{n_2}} = g_1^j$, gauname: ${g'_2}^{p^{n_2}} = g_1^{p^{n_2} j'}$ arba ${g'_2}^{p^{n_2}} g_1^{-p^{n_2} j'} = ({g'}_2 g_1^{-j'})^{p^{n_2}} = 1$. Pažymėkime elementą ${g'}_2 g_1^{-j'}$ ženklu g_2. Tuomet gauname: $g_2^{p^{n_2}} = 1$. Įrodysime, kad elemento g_2 eilė yra lygi p^{n_2} (vadinasi, šiuo atveju teisinga nelygybė $n_2 \le n_1$) ir $[g_1] \cap [g_2] = 1$. Jei būtų $g_2^{p^m} = 1$ ir $0 < m < n_2$, tai gautume

$$g_2^{p^m} = ({g'}_2 g_1^{-j'})^{p^m} = 1 \quad \text{arba} \quad {g'_2}^{p^m} = g_1^{j' p^m},$$

t. y. $(g_2'[g_1])^{p^m} = [g_1]$, kas prieštarautų tam, kad elemento $g_2'[g_1]$ eilė yra p^{n_2}. Jei būtų $[g_1] \cap [g_2] \neq 1$, tai kuriam nors m, $0 < m < n_2$, gautume $g_2^{p^m} \in [g_1]$. Vėl gautume prieštarą tam, kad elemento $g_2'[g_1]$ eilė yra p^{n_2}.

Jei $[g_1] \times [g_2] \neq G$, tai galime išrinkti grupės G tokį elementą g_3', kad faktorgrupės $G/([g_1] \times [g_2])$ elemento $g_3'[g_1][g_2]$ eilė p^{n_3} būtų didžiausia. Vėl galime parašyti ${g'_3}^{p^{n_3}} \in [g_1] \times [g_2]$, t. y. egzistuoja tokie i, j, $0 < i < p^{n_1}$, $0 < j < p^{n_2}$, kad ${g'_3}^{p^{n_3}} = g_1^i g_2^j$. Panašiai kaip ir anksčiau,

$$g_1^{ip^{n_1-n_3}} g_2^{jp^{n_1-n_3}} = (g_1^i g_2^j)^{p^{n_1-n_3}} = {g'_3}^{p^{n_1}} = 1,$$

t. y. $g_1^{ip^{n_1-n_3}} = 1$, $g_2^{jp^{n_1-n_3}} = 1$. Taigi $p^{n_1} \mid ip^{n_1-n_3}$ ir $p^{n_2} \mid jp^{n_1-n_3}$ arba $p^{n_3} \mid i$, $p^{n_3} \mid j$. Sakykime, $i = p^{n_3} i'$, $j = p^{n_3} j'$. Tuomet lygybę ${g'_3}^{p^{n_3}} = g_1^i g_2^j$ galime perrašyti taip:

$${g'_3}^{p^{n_3}} g_1^{-p^{n_3} i'} g_2^{-p^{n_3} j'} = ({g'}_3 g_1^{-i'} g_2^{-j'})^{p^{n_3}} = 1.$$

Pažymėkime $g_3 = g'_3 g_1^{-i'} g_2^{-j'}$. Panašiai kaip ir anksčiau, galima įrodyti, kad elemento g_3 eilė yra lygi p^{n_3} ir

$$[g_1] \times [g_2] \cap [g_3] = 1.$$

Elementų $g_1, g_2, \ldots, g_r$, tenkinančių sąlygą: elemento

$$g_j[g_1] \times [g_2] \times \ldots \times [g_{j-1}]$$

faktorgrupėje

$$G/([g_1] \times [g_2] \times \ldots \times [g_{j-1}]$$

eilė p^{n_j} yra didžiausia ir

$$([g_1] \times [g_2] \times \ldots \times [g_{j-1}] \cap [g_j] = 1,\ 1 \leq j \leq r,$$

išrinkimą galime tęsti iki gausime

$$G = [g_1] \times [g_2] \times \ldots \times [g_r].\ \triangle$$

Antras teoremos įrodymas. Sakykime, $g_1 \in G$ – didžiausios eilės elementas, jo eilė yra lygi p^{n_1}. Jei $[g_1] = G$, tai teoremos įrodymas baigtas. Jei $[g_1] \neq G$, tai išrinkime didžiausios eilės grupės G pogrupį H, tenkinantį sąlygą: $[g_1] \cap H = \{1\}$. Įrodysime, kad $G = [g_1] \times H$. Įrodę šią lygybę, teoremos įrodymą galėsime užbaigti matematinės indukcijos metodu, tarę, kad teoremos teiginys teisingas kiekvienai baigtinei Abelio p – grupei, kurios eilė yra mažesnė nei grupės G.

Sakykime, kad $[g_1] \times H \neq G$. Imkime mažiausios eilės elementą $a \in G$, nepriklausantį pogrupiui $[g_1] \times H \neq G$. Sakykime, kad elemento a eilė yra lygi p^m. Jei būtų $m = 1$, tai, remdamiesi sąlyga $a \notin [g_1] \times H$, gautume: kiekvienam j, $0 < j < p$, $a^j \notin [g_1] \times H$. Tuomet grupės G pogrupis $H' =: H \times [a]$ tenkintų sąlygą $[g_1] \cap H' = \{1\}$ ir jo eilė būtų $|H'| = |H|p$, kas prieštarautų pogrupio H parinkimui. Taigi būtinai $m > 1$. Elemento $a^p \neq 1$ eilė yra mažesnė už elemento a eilę. Vadinasi, $a^p \in [g_1] \times H$, t. y. egzistuoja tokie j, $1 \leq j < p^{n_1}$ ir $h \in H$, kad $a^p = g_1^j h$. Šios lygybės abi puses pakėlę p^{m-1} laipsniu, gauname:

$$(g_1^j h)^{p^{m-1}} = g_1^{jp^{m-1}} h^{p^{m-1}} = a^{p^m} = 1,$$

t. y. $g_1^{jp^{m-1}} = 1$ ir $h^{p^{m-1}} = 1$. Remdamiesi lygybe $g_1^{jp^{m-1}} = 1$, darome išvadą, kad $p^{n_1} \mid jp^{m-1}$, t. y. $p^{n_1-m+1} \mid j$. Kadangi $n_1 - m + 1 > 0$, tai $p \mid j$. Sakykime, kad $j = pj'$. Tuomet lygybę $a^p = g_1^j h$ galime perrašyti taip:

$$a^p g_1^{-j} = a^p (g_1^{-j'})^p = (a g_1^{-j'})^p = h.$$

Pažymėję elementą $a g_1^{-j'}$ raide h', gauname: $h' \notin [g_1] \times H$, $h'^p \in H$. Nagrinėkime grupės G pogrupį $[h', H]$. Šio pogrupio eilė yra didesnė už pogrupio H eilę. Vadinasi,

$[h', H] \cap [g_1] \neq \{1\}$, t. y. egzistuoja tokie i, j, $0 < i < p$, $0 < j < p^{n_1}$, $h \in H$, kad $h'^i h = g_1^j$. Remdamiesi šia lygybe, darome išvadą, kad $h'^i \in [g_1] \times H$. Bet $h'^p \in H \subset [g_1] \times H$. Kadangi skaičiai i ir p tarpusavyje pirminiai, tai egzistuoja tokie $u, v \in \mathbb{Z}$, kad $1 = iu + pv$. Vadinasi,

$$h' = h'^{iu+pv} = (h'^i)^u (h'^p)^v \in [g_1] \times H.$$

Gavome prieštarą prielaidai, kad $[g_1] \times H \neq G$. Vadinasi, $G = [g_1] \times H$. Kaip anksčiau minėjome, teoremos įrodymą galima užbaigti matematinės indukcijos metodu. Jei $H = [g_2] \times \ldots \times [g_r]$, tai $G = [g_1] \times [g_2] \times \ldots \times [g_r]$. $\triangle$

10. 7. Pastaba. Grupės G skaidinio $G = [g_1] \times [g_2] \times \ldots \times [g_r]$ ciklinių pogrupių tiesiogine sandauga cikliniai pogrupiai $[g_j]$, $1 \leq j \leq r$, nėra vienareikšmiškai apibrėžiami. Du grupės G skaidiniai ciklinių pogrupių tiesiogine sandauga gali neturėti nei vieno to paties ciklinio pogrupio. Išnagrinėkime keletą pavyzdžių.

Pavyzdžiai.

1. Grupė $G = \{1, a, b, ab |\ a^2 = b^2 = 1, ab = ba\}$ yra išskaidoma į pogrupių tiesioginę sandaugą taip:
   1. $G = \{1, a |\ a^2 = 1\} \times \{1, b |\ b^2 = 1\}$;
   2. $G = \{1, a |\ a^2 = 1\} \times \{1, ab |\ (ab)^2 = 1\}$;
   3. $G = \{1, b |\ b^2 = 1\} \times \{1, ab |\ (ab)^2 = 1\}$.

Kaip matome, grupės G skaidiniai ciklinių pogrupių tiesiogine sandauga skiriasi, bet visuose skaidiniuose tų pogrupių eilės yra lygios skaičiams 2, 2.

2. Imkime grupės $G = \{a^i b^j |\ 0 \leq i, j < 3, a^3 = b^3 = 1, ab = ba\}$ ciklinių pogrupių tiesiogine sandauga tokius skaidinius:
   1. $G = \{1, a, a^2\} \times \{1, b, b^2\} = [a] \times [b]$;
   2. $G = \{1, ab, a^2b^2\} \times \{1, ab^2, a^2b\} = [ab] \times [a^2b]$

Kaip matome, šie grupės G skaidiniai ciklinių pogrupių tiesiogine sandauga neturi bendrų ciklinių pogrupių. Bet ir šį kartą kiekviename grupės G skaidinyje yra po du ciklinius pogrupius, kurių eilės tiek viename, tiek kitame skaidinyje yra lygios 3 ir 3.

Kaip matome iš pavyzdžių, baigtinės Abelio p – grupės bet kurie du skaidiniai ciklinių pogrupių tiesiogine sandauga ciklinių pogrupių turi vieną ir tą patį skaičių ir, be to, ciklinių pogrupių vienos ir tos pačios eilės taip pat turi vieną ir tą patį skaičių. Kitaip tariant, baigtinės Abelio p – grupės skaidinio ciklinių pogrupių tiesiogine sandauga vienareikšmiškai yra apibrėžiamas ciklinių pogrupių skaičius tame skaidinyje, o šie cikliniai pogrupiai vienareikšmiškai nusakomi tik izomorfizmo tikslumu. Grupių teorijos požiūriu to pakanka, kad galėtume suklasifikuoti baigtines Abelio grupes.

10. 8. Abelio p-grupės skaidinio ciklinių pogrupių tiesiogine sandauga vienareikšmiškumas. Įrodėme, kad grupę G galima išskaidyti į ciklinių pogrupių $[g_j]$, $1 \leq j \leq r$, tiesioginę sandaugą $G = [g_1][g_2] \ldots [g_r]$. Lieka įrodyti, kad grupės G kiekviename

skaidinyje ciklinių pogrupių tiesiogine sandauga vienos ir tos pačios eilės ciklinių pogrupių yra vienas ir tas pats skaičius.

Įrodymas. Tarkime, kad G – Abelio grupė, kurios eilė yra lygi p^n. Nagrinėkime atvaizdį

$$f_p : G \to G,\ f_p(g) = g^p,\ \ g \in G.$$

Šis atvaizdis yra homomorfizmas. Iš tikrųjų, bet kuriems $g_1, g_2 \in G$, $f_p(g_1g_2) = (g_1g_2)^p = g_1^p g_2^p = f_p(g_1)f_p(g_2)$. Kadangi G yra p-grupė, tai, remdamiesi Koši teorema, gauname, kad Ker $f_p \neq \{1\}$, t. y. $|\text{Ker } f_p| = p^r$, $r \geq 1$. Jei $|G| = p^n$, tai kiekvienam $g \in G$, $f_p^n(g) = g^{p^n} = 1$, t. y. Ker $f_p^n = G$. Sakykime, kad n_1 – toks mažiausias teigiamas sveikasis skaičius, kad Ker $f_p^{n_1} = G$. Sudarykime grupės G pogrupių seką:

$$G = \text{Ker } f_p^{n_1} \supset \text{Ker } f_p^{n_1-1} \supset \ldots \supset \text{Ker } f_p \supset \text{Ker } f_p^0 = \{1\}.$$

Įdėtys Ker $f_p^{j-1} \subset$ Ker f_p^j, $1 \leq j \leq n_1$, yra akivaizdžios. Įrodysime, kad Ker $f_p^{j-1} \neq$ Ker f_p^j, $1 \leq j \leq n_1$. Jei kuriam nors j_0, $1 \leq j_0 \leq n_1$, būtų Ker $f_p^{j_0-1} =$ Ker $f_p^{j_0}$, tai gautume prieštaravimą skaičiaus n_1 parinkimui. Tai įrodysime.

Akivaizdu, kad $G =$ Ker $f_p^{n_1} \neq$ Ker $f_p^{n_1-1}$, nes priešingu atveju vietoje n_1 imtume $n_1 - 1$. Sakykime, kad $g \in G$, bet $g \notin$ Ker $f_p^{n_1-1}$, t. y. $g^{p^{n_1}} = 1$, bet $g^{p^{n_1-1}} \neq 1$. Lygybę $g^{p^{n_1}} = 1$ perrašykime taip: $(g^{p^{n_1-j_0}})^{p_0^j} = 1$. Remdamiesi šia lygybe, matome, kad $g^{p^{n_1-j_0}} \in$ Ker $f_p^{j_0}$. Jei būtų Ker $f_p^{j_0-1} =$ Ker $f_p^{j_0}$, tai gautume $(g^{p^{n_1-j_0}})^{p^{j_0-1}} = g^{p^{n_1-1}} = 1$, t. y. gautume prieštarą sąlygai: elementas $g^{p^{n_1-1}} \neq 1$. Taigi kiekvienam j, $1 \leq j \leq n_1$, Ker $f_p^{j-1} \subset$ Ker f_p^j, bet Ker $f_p^{j-1} \neq$ Ker f_p^j.

Galime nagrinėti faktorgrupes Ker f_p^j/Ker f_p^{j-1}. Pažymėkime $|\text{Ker } f_p^j/\text{Ker } f_p^{j-1}| = p^{\alpha_{n_1-j+1}}$, $1 \leq j \leq n_1$. Dabr įrodysime, kad $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_{n_1}$. Tuo tikslu pastebėsime, kad $f_p(\text{Ker } f_p^{j+1}) \subset$ Ker f_p^j kiekvienam j, $1 \leq j \leq n_1$. Vadinasi, atvaizdis f_p generuoja atvaizdį

$$(\overline{f}_p)_{j+1} : \text{Ker } f_p^{j+1}/\text{Ker } f_p^j \to \text{Ker } f_p^j/\text{Ker } f_p^{j-1},$$

$1 \leq j \leq n_1 - 1$. Įsitikinsime, kad atvaizdžiai $(\overline{f}_p)_{j+1}$, $1 \leq j \leq n_1 - 1$, yra injektyvūs. Iš tikrųjų, jei

$$(\overline{f}_p)_{j+1}(g\text{Ker } f_p^j) = \text{Ker } f_p^{j-1},$$

tai $g^p \in$ Ker f_p^{j-1}, t. y. $(g^p)^{p^{j-1}} = g^{p^j} = 1$. Vadinasi, $g \in$ Ker f_p^j ir gKer $f_p^j =$ Ker f_p^j. Taigi $\alpha_{n_1-j} \leq \alpha_{n_1-j+1}$, kiekvienam j, $1 \leq j \leq n_1 - 1$, arba $\alpha_1 \leq \alpha_2 \leq \ldots \leq \alpha_{n_1}$.

Dabar nagrinėkime atvejį, kai grupė G yra ciklinių pogrupių $[g_j]$, $1 \leq j \leq r$, tiesioginė sandauga:

$$G = [g_1] \times [g_2] \times \ldots \times [g_r].$$

Sakykime, kad ciklinio pogrupio $[g_j]$ eilė yra lygi p^{n_j}, $1 \leq j \leq r$, o cikliniai pogrupiai tiesioginėje sandaugoje išdėstyti tokia tvarka, kad $n_1 \geq n_2 \geq \ldots \geq n_r$. Tuomet toks mažiausias teigiamas sveikasis skaičius m, kad Ker $f_p^m = G$, yra lygus skaičiui n_1. Iš

tikrųjų. Kadangi grupė G yra ciklinių pogrupių $[g_j]$, $1 \le j \le r$, tiesioginė sandauga, tai kiekvienas grupės G elementas g vienareikšmiškai yra užrašomas $g = g_1^{a_1} g_2^{a_2} \dots g_r^{a_r}$, $0 \le a_j < p^{n_j}$, $1 \le j \le r$. Remdamiesi šia lygybe, matome, kad $g^{n_1} = 1$. Gauname, kad $m \le n_1$. Jei $m < n_1$, tai $g_1^m \ne 1$. Vadinasi, $m = n_1$.

Sakykime, kad

$$\begin{aligned} n_1 = \dots = n_{j_1} > n_{j_1+1} = \dots = n_{j_2} > \dots > n_{j_{s-1}+1} \\ = \dots = n_{j_s} > n_{j_s+1} = \dots = n_{j_{s+1}} > \dots > n_{j_t+1} = \dots = n_r, \end{aligned}$$

o $n_{t+1} = r$. Jei $n_{j_s} \ge m > n_{j_s+1}$, tai

$$|\text{Ker } f_p^m / \text{Ker } f_p^{m-1}| = p^{j_s},$$

o

$$|\text{Ker } f_p^{n_{j_s+1}} / \text{Ker } f_p^{n_{j_s+1}-1}| = p^{j_{s+1}},$$

$1 \le s \le t$. Tai įrodysime. Visų pirmiausia, teigiame, kad

$$\text{Ker } f_p^m = [g_1^{p^{n_{j_1}-m}}] \times \dots \times [g_{j_1}^{p^{n_{j_1}-m}}] \times \dots \times [g_{j_{s-1}+1}^{p^{n_{j_s}-m}}] \times \dots \times [g_{j_s}^{p^{n_{j_s}-m}}],$$

o

$$\text{Ker } f_p^{m-1} = [g_1^{p^{n_{j_1}-m+1}}] \times \dots \times [g_{j_1}^{p^{n_{j_1}-m+1}}] \times \dots \times [g_{j_{s-1}+1}^{p^{n_{j_s}-m+1}}] \times \dots \times [g_{j_s}^{p^{n_{j_s}-m+1}}],$$

$1 \le s \le t$. Įrodysime pirmąją iš šių lygybių. Akivaizdu, kad

$$[g_1^{p^{n_{j_1}-m}}] \times \dots \times [g_{j_1}^{p^{n_{j_1}-m}}] \times \dots \times [g_{j_{s-1}+1}^{p^{n_{j_s}-m}}] \times \dots \times [g_{j_s}^{p^{n_{j_s}-m}}] \subset \text{Ker } f_p^m,$$

$1 \le s \le t$. Sakykime,

$$g = g_1^{a_1} g_2^{a_2} \dots g_{j_1}^{a_{j_1}} \dots g_{j_s}^{a_{j_s}} g_{j_s+1}^{a_{j_s+1}} \dots g_r^{a_r}$$

ir $g \in \text{Ker } f_p^m$. Tuomet

$$g^{p^m} = g_1^{a_1 p^m} g_2^{a_2 p^m} \dots g_{j_1}^{a_{j_1} p^m} \dots g_{j_s}^{a_{j_s} p^m} = 1,$$

t. y. $g_1^{a_1 p^m} = 1$, $g_2^{a_2 p^m} = 1$, …, $g_{j_1}^{a_{j_1} p^m} = 1$, $\dots g_{j_s}^{a_{j_s} p^m} = 1$. Remdamiesi šiomis kygybėmis, matome, kad $p^{n_1} \mid a_1 p^m$, $p^{n_2} \mid a_2 p^m$, …, $p^{n_{j_1}} \mid a_{j_1} p^m$, $\dots p^{n_{j_s}} \mid a_{j_s p^m}$, t. y. $p^{n_1-m} \mid a_1$, $p^{n_2-m} \mid a_2$, …, $p^{n_{j_1}-m} \mid a_{j_1}$, $\dots p^{n_{j_s}-m} \mid a_{j_s}$. Prisiminę, kad

$$\begin{aligned} n_1 = \dots = n_{j_1} > n_{j_1+1} = \dots = n_{j_2} > \dots > n_{j_{s-1}+1} \\ = \dots = n_{j_s} > n_{j_s+1} = \dots = n_{j_{s+1}} > \dots > n_{j_t+1} = \dots = n_r, \end{aligned}$$

o $n_{t+1} = r$, gauname, kad $g \in \text{Ker } f_p^m$.

Akivaizdu, kad $|\text{Ker } f_p| = p^r$.

Kaip matome, skaičius n_1 vienareikšmiškai yra apibrėžiamas sąlyga: n_1 – toks mažiausias teigiamas sveikasis skaičius, kad Ker $f_p^{n_1} = G$. Po to vienareikšmiškai yra apibrėžiami skaičiai n_{j_s+1}, $1 \leq s \leq t$: tik kai $m = n_{j_s+1}$, $1 \leq s \leq t$, faktorgrupių Ker f_p^m/Ker f_p^{m-1}, $1 \leq m \leq n_1$, eilė padidėja. Taip pat vienareikšmiškai yra apibrėžiami skaičiai j_1, j_2,..., j_t ir r: kaip matėme

$$|\text{Ker } f_p^m/\text{Ker } f_p^{m-1}| = p^{j_s},$$

kai $n_{j_s+1} < m \leq n_{j_s}$ ir

$$|\text{Ker } f_p^{n_{j_s+1}}/\text{Ker } f_p^{n_{j_s+1}-1}| = p^{j_{s+1}},$$

$|\text{Ker } f_p| = p^r$, $1 \leq s \leq t$.

Taigi, jei grupė G yra ciklinių pogrupių tiesioginė sandauga

$$G = [g_1] \times [g_2] \times \ldots \times [g_r],$$

$|[g_i]| = p^{n_i}$, $1 \leq i \leq r$, ir

$$\begin{aligned} n_1 = \ldots = n_{j_1} > n_{j_1+1} = \ldots = n_{j_2} > \ldots > n_{j_{s-1}+1} \\ = \ldots = n_{j_s} > n_{j_s+1} = \ldots = n_{j_{s+1}} > \ldots > n_{j_t+1} = \ldots = n_r, \end{aligned}$$

$n_{t+1} = r$, tai grupės G terminais vienareikšmiškai yra apibrėžiamas ciklimnių pogrupių skaičius r ir vienareikšmiškai yra apibrėžiamos šių ciklinių pogrupių eilės n_i, $1 \leq i \leq r$. $\triangle$

10. 9. Apibrėžimas. Jei baigtinė Abelio p-grupė G yra ciklinių pogrupių $[g_j]$, $1 \leq j \leq r$, kurių eilės atitinkamai yra lygios p^{n_j}, $1 \leq j \leq r$, tiesioginė sandauga

$$G = [g_1] \times [g_2] \times \ldots \times [g_r],$$

tai skaičiai n_1, n_2, ..., n_r yra vadinami grupės G invariantais. Ciklinius pogrupius tiesioginėje sandaugoje galima surašyti tokia tvarka, kad grupės G invariantai tenkintų sąlygą: $n_1 \geq n_2 \geq \ldots \geq n_r$.

10. 10. Teorema Baigtinės Abelio p-grupės G ir H yra izomorfinės tada ir tik tada, kai jų invariantai yra lygūs.

Akivaizdu, jei baigtinės Abelio p-grupės G ir H yra izomorfinės, tai jų invariantai yra lygūs.

Sakykime, baigtinių Abelio p-grupių G ir H invariantai yra $n_1 \geq n_2 \geq \ldots \geq n_r$. Tuomet grupės G ir H yra išskaidomos ciklinių pogrupių tiesiogine sandauga:

$$G = [g_1] \times [g_2] \times \ldots \times [g_r]$$

ir

$$H = [h_1] \times [h_2] \times \ldots \times [h_r].$$

Ciklinių pogrupių $[g_1]$ ir $[h_1]$, $[g_2]$ ir $[h_2]$, ..., $[g_r]$ ir $[h_r]$ eilės yra lygios p^{n_1}, p^{n_2}, ..., p^{n_r}. Apibrėžkime atvaizdį

$$f : G \to H, \;\; f(g_1^{a_1} g_2^{a_2} \dots g_r^{a_r}) = h_1^{a_1} h_2^{a_2} \dots h_r^{a_r}, \; 0 \le a_j < p^{n_j}, \; 1 \le j \le r.$$

Akivaizdu, kad f yra izomorfizmas. $\triangle$

11. Simetrinė grupė

11. 1. Sakykime, $\mathbb{N}_n =: \{1, 2, \dots, n\}$. Nagrinėkime visų bijekcijų $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ aibę S_n. Bijekcija $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ dažnai yra vadinama aibės $\mathbb{N}_n$ elementų keitiniu arba perstatiniu. Kadangi dviejų bijekcijų $\sigma, \tau \in S_n$ kompozicija $\tau \circ \sigma$ yra bijekcija, tai galima apibrėžti aibės S_n elementų kompozicijos dėsnį $\circ$:

$$\circ : S_n \times S_n \to S_n, \; (\sigma, \tau) \mapsto \tau \circ \sigma, \; \sigma, \tau \in S_n.$$

Priminsime, kad dviejų atvaizdžių $\sigma, \tau \in S_n$ kompozicija $\tau \circ \sigma$ apibrėžiama taip:

$$(\tau \circ \sigma)(j) =: \tau(\sigma(j)), \; j \in \mathbb{N}_n.$$

Aibė S_n kompozicijos dėsnio $\circ$ atžvilgiu yra grupė, nes

1. Kompozicijos dėsnis $\circ$ yra asociatuvus;
2. $S_n \ni \mathrm{id}$ – neutralus elementas $\circ$ atžvilgiu (grupės vienetas);
3. Kiekvienam $\sigma \in S_n$ egzistuoja $\sigma^{-1} \in S_n$ ir $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}$ (σ^{-1} – atvirkštinis elementas elementui σ).

Apibrėžimas. Grupė $(S_n, \circ)$ yra vadinama n-ojo laipsnio simetrine grupe. Jos eilė yra lygi $n!$.

11. 2. Bijekciją $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ galima pavaizduoti lentele

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix};$$

pirmoje lentelės eilutėje bet kuria tvarka surašant visus aibės $\mathbb{N}_n$ elementus (duotoje lentelėje aibės $\mathbb{N}_n$ elementai surašyti natūralia tvarka), o antroje lentelės eilutėje po kiekvienu pirmos eilutės elementu j parašant jo vaizdą $\sigma(j)$. Kadangi σ – bijekcija, tai $\sigma(1)$, $\sigma(2)$, ..., $\sigma(n)$, – visi tarpusavy skirtingi elementai. Pabrėžiame, kad lentelės pirmoje eilutėje aibės $\mathbb{N}_n$ elementų tvarka nesvarbi, bet svarbu, kas parašyta po kiekvienu pirmos eilutės elementu! Jei bijekcijos $\sigma, \tau \in S_n$ pavaizduojamos lentelėmis

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}, \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix},$$

tai bijekcija $\tau \circ \sigma$ pavaizduojama lentele

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \dots & \tau(\sigma(n)) \end{pmatrix}.$$

11. 3. Sakykime, σ yra grupės S_n elementas. Grupės S_n elementą $\underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{m}$ žymėsime σ^m. σ^m – tai grupės S_n elemento σ m-asis laipsnis. Kadangi grupė S_n baigtinė, tai kiekvieno grupės S_n elemento eilė yra baigtinė, t. y., jei $\sigma \in S_n$, tai egzistuoja toks mažiausias teigiamas sveikasis skaičius r, kad $\sigma^r = \mathrm{id}$, $\sigma^j \neq \mathrm{id}$, jei $0 < j < r$. Elemento $\sigma \in S_n$, kurio eilė yra lygi r, laipsniai $\{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{r-1}\}$ sudaro grupės S_n ciklinį pogrupį $[\sigma]$.

Apibrėžimas. Elementas $\sigma \in S_n$ yra vadinamas ciklu ir žymimas $(j_1\ j_2\ \ldots\ j_r)$, jei j_1, j_2, …, j_r – tarpusavy skirtingi aibės $\mathbb{N}_n$ elementai, $\sigma(j_1) = j_2$, …, $\sigma(j_{r-1}) = j_r$, $\sigma(j_r) = j_1$, o kiekvienam aibės $\mathbb{N}_n$ elementui $j \notin \{j_1, j_2, \ldots, j_r\}$, $\sigma(j) = j$. Skaičius r yra vadinamas ciklo $(j_1\ j_2\ \ldots\ j_r)$ ilgiu. Dažnai ilgio r ciklas yra vadinamas r-ciklu. Ciklai $(i; j)$ (jų ilgis lygus 2) yra vadinami transpozicijomis.

Pastabos.

1. Bet kuriems tarpusavy skirtingiems skaičiams j_1, j_2, …, j_r, priklausantiems aibei $\mathbb{N}_n$, apibrėžkime atvaizdį $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ tokį, kad $\sigma(j_1) = j_2$, $\sigma(j_2) = j_3$, …, $\sigma(j_{r-1}) = j_r$, $\sigma(j_r) = j_1$, o kiekvienam elementui $j \in \mathbb{N}_n \setminus \{j_1, j_2, \ldots, j_r\}$, $\sigma(j) = j$. Akivaizdu, kad šis atvaizdis yra ilgio r ciklas $(j_1\ j_2\ \ldots\ j_r)$.

2. Remiantis ciklo apibrėžimu, akivaizdu, kad $(j_1\ j_2\ \ldots\ j_r) = (j_r\ j_1\ \ldots\ j_{r-1}) = \ldots = (j_2\ j_3\ \ldots\ j_1)$. r ilgio ciklo $(j_1\ j_2\ \ldots\ j_r)$ eilė yra lygi r.

Apibrėžimas. Ciklai $(i_1\ i_2\ \ldots\ i_s)$ ir $(j_1\ j_2\ \ldots\ j_r)$ yra vadinami nepriklausomais, jei

$$\{i_1,\ _2,\ \ldots,\ i_s\} \cap \{j_1,\ j_2,\ \ldots,\ j_r\} = \emptyset.$$

Teiginys. Grupės S_n nepriklausomi ciklai yra perstatomi.

Įrodymas. Įrodymas akivaizdus.

11. 4. Kiekvienam grupės S_n elementui σ apibrėžkime aibėje $\mathbb{N}_n$ ekvivalentumo sąryšį $\underset{\sigma}{\sim}$: $i \underset{\sigma}{\sim} j$, jei egzistuoja toks elemento σ sveikasis laipsnis σ^m, kad $\sigma^m(i) = j$.

Apibrėžimas. Aibės $\mathbb{N}_n$ elementų ekvivalentumo klasės pagal ekvivalentumo sąryšį $\underset{\sigma}{\sim}$ yra vadinamos elemento σ orbitomis.

Elemento $\sigma \in S_n$ orbita, kuriai priklauso aibės $\mathbb{N}_n$ elementas j, sudaryta iš elementų j, $\sigma(j)$, $\sigma^2(j)$, …, $\sigma^{p-1}(j)$, čia p – toks mažiausias teigiamas sveikasis skaičius, kad $\sigma^p(j) = j$.

Apibrėžimas. Jei elemento $\sigma \in S_n$ orbita sudaryta iš vieno aibės $\mathbb{N}_n$ elemento j (t. y. $\sigma(j) = j$), tai j yra vadinamas σ-nejudamu elementu.

Dabar ciklą galime apibūdinti ir kitaip. Grupės S_n elementas σ yra ciklas, jei elemento σ visos orbitos, išskyrus vieną, sudarytos iš aibės $\mathbb{N}_n$ σ-nejudamų elementų.

Teiginys. Jei neatsižvelgtume į dauginamųjų tvarką, tai kiekvienas grupės S_n elementas vienareikšmiškai užrašomas nepriklausomų ciklų sandauga.

Įrodymas. Sakykime, $\sigma \in S_n$, o $X_1, X_2, \ldots, X_t$ – elemento σ orbitos. Taigi $X_i \cap X_j = \emptyset$, jei $i \neq j$, $1 \leq i, j \leq t$, $X_1 \cup X_2 \cup \ldots \cup X_t = \mathbb{N}_n$. Apibrėžkime atvaizdžius $\sigma_i : \mathbb{N}_n \to \mathbb{N}_n$, $1 \leq i \leq t$:

$$\sigma_i(j) = \begin{cases} \sigma(j), & \text{jei } j \in X_i \\ j, & \text{jei } j \in \mathbb{N}_n \setminus X_i \end{cases}.$$

Remdamiesi atvaizdžių σ_i, $1 \leq i \leq t$, apibrėžimu, matome, kad kiekvienam i, $1 \leq i \leq t$, σ_i – ciklai. Įrodysime, kad $\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_t$. Tuo tikslu įsikinsime, kad kiekvienam $j \in \mathbb{N}_n$, $\sigma(j) = (\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_t)(j)$. Kadangi $j \in \mathbb{N}_n = X_1 \cup X_2 \cup \ldots \cup X_t$ ir bet kurios skirtingos elemento σ orbitos neturi bendrų elementų, tai egzistuoja toks vienintelis indeksas i, $1 \leq i \leq t$, kad $j \in X_i$. Tuomet

$$(\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_t)(j) = \sigma_i(j) = \sigma(j). \triangle$$

Pastabos.

1. Grupės S_n vienetas id nepriklausomų ciklų sandauga yra užrašomas taip: id $= (1)(2)\ldots(n)$. Grupės S_n elementų išraiškose ciklais ilgio 1 ciklus sutarkime praleisti, o vietoje id sutarkime rašyti (1).

2. Sutarkime tarp ciklų nerašyti grupės S_n elementų kompozicijos dėsnio ženklo $\circ$.

11.5. Kiekvienas ciklas $(j_1\ j_2\ \ldots\ j_r)$ gali būti užrašomas transpozicijų sadauga:

$$(j_1\ j_2\ \ldots\ j_r) = (j_1\ j_r)(j_1\ j_{r-1})\ldots(j_1\ j_2).$$

Ciklai transpozicijų sandauga užrašomi nevienareikšmiškai. Pavyzdžiui, grupės S_n, $n \geq 3$, ciklą (1 2 3) galime išskaidyti transpozicijų sandauga taip: (1 2 3) = (1 3)(1 2) = (1 2)(2 3) = (2 3)(1 3) = (2 3)(1 2)(1 3)(2 3). Be to, kaip matome, ciklo skirtinguose skaidiniuose transpozicijomis gali būti skirtingi [?] dauginamųjų skaičiai.

Išvada. Kiekvienas grupės S_n elementas yra išskaidomas transpozicijų sandauga. Grupės S_n transpozicijos yra šios grupės sudaromosios.

11. 6. Nors grupės S_n elemento skirtinguose skaidiniuose transpozicijomis dauginamųjų skaičiai gali būti ir skirtingi, bet dauginamųjų skaičiaus lyginumas grupės S_n elemento kiekviename skaidinyje transpozicijomis yra vienas ir tas pats.

Apibrėžkime skaičių $A = \prod_{1\le i<j\le n}(j-i)$. Bet kuriam $\sigma \in S_n$ apibrėžkime $\sigma(A) =: \prod_{1\le i<j\le n}(\sigma(j)-\sigma(i))$. Skaičiai A ir $\sigma(A)$ skiriasi daugikliu ± 1. Apibrėžkime atvaizdį $\operatorname{sgn} : S_n \to \{1,-1\}$ taip: $\sigma(A) = \operatorname{sgn}(\sigma)A$, $\sigma \in S_n$. Atvaizdis sgn yra homomorfizmas. Iš tikrųjų: jei $\sigma, \tau \in S_n$, tai

$$\operatorname{sgn}(\sigma\circ\tau)A = (\sigma\circ\tau)(A) = \sigma(\tau(A)) = \operatorname{sgn}(\tau)\sigma(A) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)A,$$

t. y. $\operatorname{sgn}(\sigma\circ\tau) = \operatorname{sgn}(\tau)\operatorname{sgn}(\sigma)$.

Teiginys. Kiekvienai transpozicijai $(i\ j) \in S_n$ $\operatorname{sgn}((i\ j)) = -1$.

Įrodymas. Nesunku matyti, kad $\operatorname{sgn}((1\ 2)) = -1$. Iš tikrųjų, skaičius $(1\ 2)(A)$ yra gaunamas pakeičiant skaičiaus A tik šiuos daugiklius $2-1$, $3-1$, …, $n-1$, $3-2$, $4-2$, …, $n-2$ daugikliais $1-2$, $3-2$, …, $n-2$, $3-1$, $4-1$, …, $n-1$. Taigi homomorfizmas $\operatorname{sgn} : S_n \to \{1,-1\}$ yra siurjektyvus. Vadinasi, šio homomorfizmo branduolys $\operatorname{Ker}\operatorname{sgn}$, žymimas A_n, yra grupės S_n indekso 2 pogrupis. Kaip žinome, grupės indekso 2 pogrupis yra normalusis pogrupis. Įrodysime, kad nei viena transpozicija nepriklauso pogrupiui A_n. Jei transpozicija $(i\ j) \in S_n$ priklausytų normaliajam pogrupiui A_n, tai ir transpozicija $(1\ 2)$ priklausytų pogrupiui A_n. Iš tikrųjų, tai gautume remdamiesi lygybe $(1\ 2) = \underbrace{(2\ j)(1\ i)}(i\ j)\underbrace{(1\ i)(2\ j)}$, nes elementai, pažymėtieji riestiniais skliaustais, yra vienas kitam atvirkštiniai. Bet, kaip matėme, transpozicija $(1\ 2)$ nepriklauso normaliajam pogrpiui A_n, vadinasi, grupės S_n normaliajam pogrupiui A_n nepriklauso nei viena transpozicija $(i;j) \in S_n$. $\triangle$

Išvada. Jei grupės S_n elementas σ yra užrašomas transpozicijų sandaugomis $\sigma = (i_1\ j_1)(i_2\ j_2)\dots(i_r\ j_r) = (l_1\ m_1)(l_2\ m_2)\dots(l_s\ m_s)$, tai $r \equiv s(\mathrm{mod}2)$.

Įrodymas. $\operatorname{sgn}(\sigma) = (-1)^r = (-1)^s$. Taigi gauname $r \equiv s(\mathrm{mod}2)$. $\triangle$

Apibrėžimas. Grupės S_n elementas σ yra vadinamas lyginiu (nelyginiu), jei $\operatorname{sgn}(\sigma) = 1$ ($\operatorname{sgn}(\sigma) = -1$).

11. 7. Grupėje S_n yra $n!/2$ lyginių ir tiek pat nelyginių elementų. Lyginio elemento bet kuriame skaidinyje transpozicijomis yra lyginis dauginamųjų skaičius, o nelyginio elemento bet kuriame skaidinyje transpozicijomis – nelyginis dauginamųjų skaičius. Nelyginio ilgio ciklas yra lyginis elementas, o lyginio ilgio ciklas yra nelyginis elementas. Tai gauname remdamiesi šia lygybe:

$$(j_1\ j_2\ \dots\ j_r) = (j_1\ j_r)(j_1\ j_{r-1})\dots(j_1\ j_2).$$

Teiginys. Grupę S_n generuoja transpozicijos $(1\ 2)$, $(1\ 3)$, …, $(1\ n)$, o grupės S_n normalųjį pogrupį A_n generuoja 3-ciklai $(1\ i\ j)$, $1 \le i < j \le n$.

Įrodymas. Grupę S_n generuoja transpozicijos $(i\ j)$, $1 \le i < j \le n$. Kadangi bet kuriems i, j, $1 \le i < j \le n$, $(i\ j) = (1\ i)(1\ j)(1\ i)$, tai, kaip matome, grupę S_n generuoja transpozicijos (1 2), (1 3), ..., (1 n).

Grupės S_n normalųjį pogrupį $A_n = \mathrm{Ker}\ \mathrm{sgn}$ generuoja transpozicijų sandaugos $(i\ j)(l\ m)$, $1 \le i < j \le n$, $1 \le l < m \le n$. Pastebėję, kad $(1\ i)(1\ j) = (1\ j\ i)$, $1 \le i, j \le n$, galime parašyti:

$$(i\ j)(l\ m) = (1\ i)(1\ j)(1\ i)(1\ l)(1\ m)(1\ l) = (1\ j\ i)(1\ l\ i)(1\ l\ m).$$

Kaip matome, grupės S_n normalųjį pogrupį A_n generuoja 3-ciklai $(1\ i\ j)$, $1 \le i < j \le n$. $\triangle$

12. Simetrinės grupės sujungtinių elementų klasės

12. 1. Apibrėžimas. Grupės S_n elementai x ir y yra vadinami sujungtiniais, jei egzistuoja toks grupės S_n elementas σ, kad $y = \sigma x \sigma^{-1}$. Tarp grupės S_n sujungtinių elementų x ir y sutarkime rašyti ženklą $\sim$: $x \sim y$.

Teiginys. Sąryšis $\sim$ yra ekvivalentumo sąryšis grupėje S_n.

Įrodymas. Įsitikinsime, kad sąryšis $\sim$ tenkina ekvivalentumo sąryšio apibrėžimo tris sąlygas.

1. Kiekvienam $x \in S_n$, $x \sim x$, nes $x = (1)x(1)$ ((1) – grupės S_n vienetas);

2. Jei $x \sim y$, t. y. egzistuoja toks $\sigma \in S_n$, kad $y = \sigma x \sigma^{-1}$, tai ir $y \sim x$, nes $x = \sigma^{-1} y \sigma = \sigma^{-1} y (\sigma{-}1)^{-1}$;

3. Jei $x \sim y$, $y \sim z$, tai ir $x \sim z$. Iš tikrųjų, kadangi egzistuoja tokie $\sigma, \tau \in S_n$, kad $z = \tau y \tau{-}1$, $y = \sigma x \sigma^{-1}$, tai $z = \tau\sigma x \sigma^{-1} \tau{-}1 = \tau\sigma x (\tau\sigma)^{-1}$.

Apibrėžimas. Elemento $x \in S_n$ ekvivalentumo klasė pagal ekvivalentumo sąryšį $\sim$ yra vadinama elementui x sujungtinių elementų klase.

12. 2. Apibrėžkime grupės S_n poaibį K_x, sudarytą iš visų tokių elementų σ, kurie yra perstatomi su elementu $x \in S_n$: $K_x =: \{\sigma \in S_n |\ \sigma x = x\sigma\}$.

Teiginys. Kiekvienam grupės S_n elementui x grupės S_n poaibis K_x yra grupės S_n pogrupis.

Įrodymas. Visų pirma pastebėsime, jei τ yra perstatomas su x, tai ir τ^{-1} yra perstatomas su x. Iš tikrųjų, lygybė $\tau x = x\tau$ yra ekvivalenti lygybei $x\tau^{-1} = \tau^{-1}x$.

Sakykime, $\sigma, \tau \in K_x$. Tuomet

$$(\sigma\tau^{-1})x = \sigma x \tau^{-1} = x(\sigma\tau^{-1}).$$

Vadinasi, jei $\sigma, \tau \in K_x$, tai $\sigma\tau^{-1} \in K_x$. Taigi K_x yra grupės S_n pogrupis. $\triangle$

Apibrėžimas. K_x yra vadinamas grupės S_n elemento stacionariuoju pogrupiu.

Teiginys. Grupės S_n elementui x sujungtinių elementų klasės elementų skaičius yra lygus elemento x stacionariojo pogrupio K_x indeksui grupėje S_n.

Įrodymas. Sakykime, $\{x_1, x_2, \ldots, x_r\}$ – elementui $x = x_1$ sujungtinių elementų klasė, $g_1 = (1)$, g_2, …, g_r – grupės S_n tokie elementai, kad $x_1 = g_1 x_1 g_1^{-1}$, $x_2 = g_2 x_1 g_2^{-1}$, …, $x_r = g_r x_1 g_r^{-1}$.

Kiekvienam $h \in S_n$ egzistuoja vienintelis toks j, $1 \le j \le r$, kad $h x_1 h^{-1} = x_j$. Taigi $h x_1 h^{-1} = g_j x_1 g_j^{-1}$. Šią lygybę iš kairės padauginę iš g_j^{-1}, o iš dešinės – iš g_j, gauname: $g_j^{-1} h x_1 h^{-1} g_j = x_1$ arba $g_j^{-1} h x_1 (g_j^{-1} h)^{-1} = x_1$. Vadinasi, $g_j^{-1} h \in K_x$ arba $h \in g_j K_x$. Ir atvirkščiai, jei $h \in g_j K_x$, tai $g_j^{-1} h \in K_x$. Tuomet $g_j^{-1} h x_1 (g_j^{-1} h)^{-1} = x_1$ arba $h x_1 h^{-1} = g_j x_1 g_j^{-1} = x_j$.

Kaip matome, kiekvieną kairiąją pogrupio K_x gretutinę klasę $g_j K_x$, $1 \le j \le r$, atitinka elementui $x = x_1$ sujungtinis elementas $x_j = h x_1 h^{-1}$, $h \in g_j K_x$, $1 \le j \le r$. Kadangi $S_n = \bigcup_{j=1}^{r} g_j K_x$, tai teoremos įrodymas baigtas. $\triangle$

12. 3. Apibrėžimas. Nedidėjanti sveikųjų skaičių seka $\lambda_1 \ge \lambda_2 \ge \lambda_3 \ge \ldots \ge \lambda_s \ge 0$ yra vadinama skaičiaus $n \in \mathbb{N}$ skaidiniu, jei $\sum_{j \ge 1} \lambda_j = n$. Skaičiaus n visų skaidinių skaičius yra žymimas $p(n)$.

Pavyzdžiui, skaičiaus 7 skaidiniai yra šie:

7				;		3	2	2					;
6	1			;		3	2	1	1				;
5	2			;		3	1	1	1	1			;
5	1	1		;		2	2	2	1				;
4	3			;		2	2	1	1	1			;
4	2	1		;		2	1	1	1	1	1		;
4	1	1	1	;		1	1	1	1	1	1	1	.
3	3	1		;									

Taigi $p(7) = 15$.

Skaičiaus $n \in \mathbb{N}$ skaidinį $\lambda_1 \ge \lambda_2 \ge \lambda_3 \ge \ldots \ge \lambda_m \ge 0$ yra susitarta užrašyti trumpiau. Sakykime,

$$\lambda_1 = \lambda_2 = \ldots = \lambda_{s_1} > \lambda_{s_1+1} = \ldots = \lambda_{s_1+s_2} > \ldots$$

$$> \lambda_{s_1+s_2+\ldots+s_{r-1}+1} = \ldots = \lambda_{s_1+s_2+\ldots+s_{r-1}+s_r}.$$

Pažymėję $\lambda_1 = \mu_1$, $\lambda_{s_1+1} = \mu_2$, …, $\lambda_{s_1+s_2+\ldots+s_{r-1}+1} = \mu_r$, anksčiau nurodytą skaičiaus n skaidinį galime užrašyti taip:

$$(\mu_1^{(s_1)}, \mu_2^{(s_2)}, \ldots, \mu_r^{(s_r)}),\ \mu_1 > \mu_2 > \ldots > \mu_r,\ \sum_{j=1}^{r} s_j \mu_j = n.$$

Skaičiaus n skaidinį $(\mu_1^{(s_1)}, \mu_2^{(s_2)}, \ldots, \mu_r^{(s_r)})$, čia $\mu_1 > \mu_2 > \ldots > \mu_r$, $\sum\limits_{j=1}^{r} s_j\mu_j = n$, trumpumo dėlei pažymėkime $\widehat{\mu}$.

12. 4. Kiekvienas grupės S_n elementas σ yra išskaidomas į nepriklausomų ciklų sandaugą $\sigma = \sigma_1\sigma_2 \ldots \sigma_m$. Į grupės S_n elemento sandaugą nepriklausomais ciklais, kaip susitarta, neįrašomi ciklai, kurių ilgis lygus 1. Kadangi nepriklausomi ciklai yra perstatomi, tai sakykime, kad σ_1, σ_2, …, σ_m šiame skaidinyje yra išdėstyti jų ilgių nedidėjimo tvarka. Surašę šių ciklų ilgius ir pirašę tiek vienetų, kiek elemento σ skaidinyje praleista ilgio 1 ciklų, gauname skaičiaus n skaidinį:

$$(\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \ldots, \lambda_r^{(s_r)});$$

čia $\lambda_1 > \lambda_2 > \ldots > \lambda_r \geq 1$.

Taigi kiekvieną grupės S_n elementą σ atitinka skaičiaus n skaidinys

$$\widehat{\lambda} = (\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \ldots, \lambda_r^{(s_r)}), ; \lambda_1 > \lambda_2 > \ldots > \lambda_r;$$

čia s_1 – ilgio λ_1 ciklų, s_2 – ilgio λ_2 ciklų ir t. t. skaičiai elemento σ skaidinyje nepriklausomais ciklais, įskaitant ir praleistų ilgio 1 ciklų ilgius.

Apibrėžimas. Jei grupės S_n elementą σ atitinka skaičiaus n skaidinys $\widehat{\lambda}$, tai σ yra vadinamas ciklinio tipo $\widehat{\lambda}$ elementas.

Pratimas. Sakykime,

$$\widehat{\lambda} = (\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \ldots, \lambda_r^{(s_r)}),$$

čia $\lambda_1 > \lambda_2 > \ldots > \lambda_r \geq 1$, skaičiaus n skaidinys (t. y. $\sum\limits_{j=1}^{r} s_j\lambda_j = n$). Įrodykite, kad grupėje S_n yra

$$\frac{n!}{\lambda_1^{s_1}\lambda_2^{s_2}\ldots\lambda_r^{s_r}s_1!s_2!\ldots s_r!}$$

elementų ciklinio tipo $\widehat{\lambda}$.

12. 5. Teiginys. Grupės S_n ciklui $(j_1\ j_2\ \ldots\ j_r)$ sujungtinis elementas

$$\pi(j_1\ j_2\ \ldots\ j_r)\pi^{-1},\ \ \pi \in S_n,$$

yra ciklas $(\pi(j_1)\ \pi(j_2)\ \ldots\ \pi(j_r))$ (čia $\pi(j)$ – bijekcijos $\pi : \mathbb{N}_n \to \mathbb{N}_n$ reikšmė taške $j \in \mathbb{N}_n$).

Įrodymas. Bijekcija $\alpha = \pi(j_1\ j_2\ \ldots\ j_r)\pi^{-1}$ aibės $\mathbb{N}_n$ elementą $\pi(j_i)$ perveda į $\pi(j_{i+1})$, $1 \leq i \leq r-1$, elementą $\pi(j_r)$ – į $\pi(j_1)$, o elementai

$$\pi(l) \in \mathbb{N}_n \setminus \{\pi(j_1), \pi(j_2), \ldots, \pi(j_r)\}$$

yra α-nejudami. $\triangle$

Teiginys. Grupės S_n elementai σ ir τ yra sujungtiniai tada ir tik tada, kai jų cikliniai tipai sutampa.

Įrodymas. Jei elementai σ ir τ yra sujungtiniai, tai egzistuoja toks $\pi \in S_n$, kad $\sigma = \pi\tau\pi^{-1}$. Sakykime, $\tau = \tau_1\tau_2 \dots \tau_m$, čia nepriklausomi ciklai surašyti jų ilgių nedidėjimo tvarka. Tuomet

$$\sigma = \pi\tau\pi^{-1} = (\pi\tau_1\pi^{-1})(\pi\tau_2\pi^{-1}) \dots (\pi\tau_m\pi^{-1}).$$

Lieka pastebėti, kad ciklui τ_j sujungtinis elementas $\pi\tau_j\pi^{-1}$ yra ciklas tokio pat ilgio kaip ir ciklas τ_j, $1 \le j \le m$. Vadinasi, grupės S_n sujungtiniai elementai yra to paties ciklinio tipo.

Sakykime, grupės S_n elementai σ ir τ yra to paties ciklinio tipo

$$\widehat{\lambda} = (\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \dots, \lambda_r^{(s_r)}),$$

čia $\lambda_1 > \lambda_2 > \ldots > \lambda_r \ge 1$, $\sum\limits_{j=1}^{r} s_j\lambda_j = n$. Užrašykime elementus σ ir τ nepriklausomų ciklų sandaugomis, įskaitant ir ilgio 1 ciklus, surašydami ciklus jų ilgių nedidėjimo tvarka. Tuomet parašę elementą σ po elementu τ taip, kad atitinkamo ilgio ciklai būtų vienas po kitu ir praleidę ciklų skliaustelius, gauname bijekciją $\pi : \mathbb{N}_n \to \mathbb{N}_n$. Akivaizdu, kad $\sigma = \pi\tau\pi^{-1}$. $\triangle$

Pavyzdys.

1. Imkime grupės S_8 elementus $\sigma = (1\ 3\ 7)(2\ 8\ 5\ 4)$ ir $\tau = (2\ 6\ 5)(4\ 1\ 7\ 8)$. Šių elementų cikliniai tipai sutampa. Vadinasi, šie elementai yra sujungtiniai, t. y. egzistuoja toks elementas π, kad $\sigma = \pi\tau\pi^{-1}$. Remdamiesi teoremos įrodymu, gauname:

$$\pi = \begin{pmatrix} 4 & 1 & 7 & 8 & 2 & 6 & 5 & 3 \\ 2 & 8 & 5 & 4 & 1 & 3 & 7 & 6 \end{pmatrix} = (1\ 8\ 4\ 2)(3\ 6)(5\ 7).$$

Iš tikrųjų,

$$\pi\tau\pi^{-1} = (1\ 8\ 4\ 2)(3\ 6)(5\ 7)(2\ 6\ 5)(4\ 1\ 7\ 8)(1\ 2\ 4\ 8)(3\ 6)(5\ 7) = (1\ 3\ 7)(2\ 8\ 5\ 4).$$

Pastebėsime, kad egzistuoja ne vienas toks elementas π, kad $\sigma = \pi\tau\pi^{-1}$. Pavyzdžiui, jei imtume

$$\pi_2 = \begin{pmatrix} 4 & 1 & 7 & 8 & 2 & 6 & 5 & 3 \\ 8 & 5 & 4 & 2 & 1 & 3 & 7 & 6 \end{pmatrix} = (1\ 5\ 7\ 4\ 8\ 2)(3\ 6),$$

tai $\sigma = \pi_2\tau\pi_2^{-1}$. Iš tikrųjų,

$$(1\ 5\ 7\ 4\ 8\ 2)(3\ 6)(2\ 6\ 5)(4\ 1\ 7\ 8)(1\ 2\ 8\ 4\ 7\ 5)(3\ 6) = (1\ 3\ 7)(2\ 8\ 5\ 4).$$

Įrodykite, kad egzistuoja 12 tokių elementų $\pi \in S_8$, kad $\sigma = \pi\tau\pi^{-1}$ ir nurodykite juos.

Pratimai.

1. Kokia grupės S_7 elemento (1 2)(3 4 5) eilė? Kokia elemento (1 2 3)(4 5 6 7) eilė?

2. Sakykime, σ_1, σ_2, ..., σ_m yra nepriklausomi grupės S_n ciklai, kurių ilgiai yra lygūs λ_1, λ_2, ..., λ_m. Įrodykite, kad elemento $\sigma_1\sigma_2 \dots \sigma_m$ eilė yra lygi skaičių λ_1, λ_2, ..., λ_m mažiausiam bendrajam kartotiniui.

3. Raskite grupėje S_7 didžiausios eilės elementą. Kiek grupėje S_7 yra didžiausios eilės elementų? Kokia šių elementų eilė?

4. Raskite grupėje S_8 didžiausios eilės elementą. Kiek grupėje S_8 yra didžiausios eilės elementų? Kokia šių elementų eilė?

5. Raskite grupės S_7 elemento (1 2)(3 4 5) stacionarųjį pogrupį. Kokia šio pogrupio eilė? Kiek elementų turi elementui (1 2)(3 4 5) sujungtinių elementų klasė.

6. Įrodykite, kad grupėje S_n yra $\frac{n!}{l(n-l)!}$ ilgio l ($l \leq n$) ciklų.

13. Sylovo teoremos

13. 1. Nagrinėkime grupę G, kurios eilė yra lygi n. Sakykime, skaičiaus n kanoninis skaidinys pirminiais skaičiais yra $n = \prod_{j=1}^{s} p_j^{a_j}$. Ką galime pasakyti apie grupės G pogrupius, žinodami grupės eilės kanoninį skaidinį pirminiais skaičiais? Anksčiau įrodėme (Koši teorema), jei grupės G eilę n dalija pirminis skaičius p, tai egzistuoja grupės G elementas, kurio eilė yra lygi p. Kiekvienas grupės G p eilės elementas g generuoja grupės G p eilės ciklinį pogrupį $[g]$. Anksčiau, nagrinėdami pavyzdžius, įsitikinome, kad ne kiekvienam grupės eilės n dalikliui d egzistuoja grupės d eilės elementas. Bendruoju atveju į šį klausimą atsako trys Sylovo teoremos, kurias šiame skyrelyje suformuluosime ir įrodysime.

Pirmoji Sylovo teorema. Jei pirminio skaičiaus p laipsnis p^r dalija grupės G eilę n, tai egzistuoja grupės G p^r eilės pogrupis.

Apibrėžimas. Sakykime, grupės G eilė yra lygi n, p – pirminis skaičius. Jei $p^a \mid n$, $p^{a+1} \not| n$, tai grupės G p^a eilės pogrupis yra vadinamas grupės G Sylovo p-pogrupiu.

Išvada. Jei pirminis skaičius p dalija grupės G eilę n, tai egzistuoja bent vienas grupės G Sylovo p-pogrupis.

Antroji Sylovo teorema. Bet kurie baigtinės grupės G Sylovo p-pogrupiai yra sujungtiniai.

Trečioji Sylovo teorema. Sakykime, grupės G eilė yra lygi n, p – pirminis skaičius dalija skaičių n. Grupės G Sylovo p-pogrupių skaičius l tenkina sąlygas:

i)$l \equiv 1(\mathrm{mod} p)$;

ii)$l|n$.

13. 2. Pirmosios Sylovo teoremos įrodymo planas štai toks. Pirmiausia įrodysime pirmąją Sylovo teoremą atskiru atveju, pirminiam skaičiui p ir simetrinei grupei S_{p^n}. Po to įrodysime, kad kiekviena baigtinė grupė G yra izomorfinė simetrinės grupės S_{p^n} pogrupiui, kai $n \in \mathbb{N}$ yra pakankamai didelis. Pagaliau įrodysime, jei grupė G yra grupės H pogrupis ir grupėje H egzistuoja Sylovo p-pogrupis, tai ir grupėje G egzistuoja Sylovo p-pogrupis.

13. 3. Dabar nagrinėsime p^n-ojo laipsnio simetrinę grupę S_{p^n}, čia p – pirminis skaičius. Įrodysime, kad šioje grupėje egzistuoja Sylovo p-pogrupis. Išsiaiškinkime, kokia grupės S_{p^n} Sylovo p-pogrupio eilė. Tuo tikslu išsiaiškinkime, koks didžiausias pirminio skaičiaus p laipsnis dalija grupės S_{p^n} eilę $p^n!$.

Kadangi skaičius $p^n!$ yra visų skaičių j, $1 \le j \le p^n$, sandauga, tai daugikliai, kurie dalijasi iš pirminio skaičiaus p, yra šie: pj, $1 \le j \le p^{n-1}$. Šių daugiklių sandauga yra lygi $p^{p^{n-1}} p^{n-1}!$. Tarę, kad didžiausias pirminio skaičiaus p laipsnis, kuris dalija $p^n!$, $n \ge 1$, yra $p^{t(n)}$, galime parašyti lygybę: $p^{t(n)} = p^{p^{n-1}+t(n-1)}$, $n \ge 1$. Vadinasi, $t(n) = p^{n-1} + t(n-1) = \ldots = p^{n-1} + p^{n-2} + \ldots + p + t(1)$. Kadangi skaičių $p!$ dalija tik p^1, tai $t(n) = 1 + p + \ldots + p^{n-1} = \frac{p^n-1}{p-1}$.

13. 4. Matematinės indukcijos metodu pagal skaičių n įrodysime, kad simetrinėje grupėje S_{p^n} egzistuoja Sylovo p-pogrupis, t. y. pogrupis, kurio eilė yra lygi $p^{t(n)} = p^{p^{n-1}+p^{n-2}+\ldots+1}$.

Teorema. Simetrinėje grupėje S_{p^n} egzistuoja Sylovo p-pogrupis.

Įrodymas. Pirmasis žingsnis. Atvejis, kai $n = 1$ akivaizdus. Grupėje S_p elementas $(1\ 2\ \ldots\ p)$ generuoja p eilės pogrupį.

Antrasis žingsnis. Sakykime, kad simetrinėje grupėje $S_{p^{n-1}}$ egzistuoja Sylovo p-pogrupis. Šio pogrupio eilė yra lygi $p^{t(n-1)} = p^{p^{n-2}+p^{n-3}+\ldots+1}$.

Trečiasis žingsnis. Įrodysime, kad ir simetrinėje grupėje S_{p^n} egzistuoja Sylovo p-pogrupis, t. y. pogrupis, kurio eilė yra lygi $p^{t(n)} = p^{p^{n-1}+p^{n-2}+\ldots+1}$.

Suskirstikime aibės $\mathbb{N}_{p^n}$ elementus į p poaibių: $A_0 = \{1, 2, \ldots, p^{n-1}\}$, $A_1 = \{p^{n-1} + 1,\ p^{n-1} + 2, \ldots, 2p^{n-1}\}$, …, $A_j = \{jp^{n-1} + 1,\ jp^{n-1} + 2, \ldots, (j+1)p^{n-1}\}$, … , $A_{p-1} = \{(p-1)p^{n-1} + 1,\ (p-1)p^{n-1} + 2, \ldots, p^n\}$. Nagrinėkime simetrinės grupės S_{p^n} tokius elementus $f : \mathbb{N}_{p^n} \to \mathbb{N}_{p^n}$, kad $f(j) = j$, kai $p^{n-1} < j \le p^n$. Šie elementai sudaro grupės S_{p^n} pogrupį H_0, izomorfinį grupei $S_{p^{n-1}}$. Kitaip tariant, H_0 sudaro tik tie aibės $\mathbb{N}_n$ elementų keitiniai, kurie perstatinėja tik poaibio A_0 elementus, tuo tarpu kitų poaibių A_j, $1 \le j \le p-1$, elementus palieka nejudamus. Pagal indukcinę prielaidą grupėje H_0 egzistuoja Sylovo p-pogrupis P_0, kurio eilė yra lygi $p^{t(n-1)}$. Imkime simetrinės grupės S_{p^n} elementą

$$\pi = (1\ p^{n-1}+1\ 2p^{n-1}+1\ \ldots\ (p-1)p^{n-1}+1)\ldots$$

$$\ldots(j\ p^{n-1}+j\ 2p^{n-1}+j\ \ldots\ (p-1)p^{n-1}+j)\ldots$$

$$\dots (p^{n-1}\ 2p^{n-1}\ 3p^{n-1}\ \dots\ p^n).$$

Šis keitinys poaibio A_0 elementus perveda į poaibio A_1 elementus, poaibio A_1 elementus – į poaibio A_2 elementus ir t. t. ir pagaliau poaibio A_{p-1} elementus – į poaibio A_0 elementus. Kitaip tariant, aibės $\mathbb{N}_n$ elementų keitinys π perstato cikliškai poaibius A_j, $0 \le j \le p-1$. Elemento eilė yra lygi p. Pastebėsime, kad kiekvienam $f \in H_0$, $\pi^j f \pi^{-j}$, $0 \le j \le p-1$, tik aibės A_j elementus perstatinėja, o aibės $\mathbb{N}_{p^n}$ elementus, nepriklausančius poaibiui A_j, palieka nejudamus. Vadinasi, grupės S_{p^n} pogrupiai $H_j =: \pi^j H_0 \pi^{-j}$, $0 \le j \le p-1$ yra izomorfiniai grupei $S_{p^{n-1}}$ ir kiekviename pogrupyje H_j egzistuoja Sylovo p-pogrupis $P_j = \pi^j P_0 \pi^{-j}$, $0 \le j \le p-1$. Grupės S_{p^n} pogrupių H_i ir H_j elementai, kai $i \ne j$, yra perstatomi, nes šių pogrupių elementai perstatinėja nesikertančių aibių A_i ir A_j elementus. Vadinasi, grupės S_{p^n} pogrupis $P' = P_0 P_1 \dots P_{p-1}$, generuotas pogrupių $P_j \subset H_j$, $0 \le j \le p-1$, yra izomorfinis tiesioginei sandaugai $P_0 \times P_1 \times \dots \times P_{p-1}$. Taigi pogrupio P' eilė yra lygi $p^{t(n-1)p} = p^{t(n)-1}$. Kadangi $P_j = \pi^j P_0 \pi^{-j}$, $0 \le j \le p-1$, tai $\pi P' = P' \pi$. Vadinasi, grupės S_{p^n} pogrupio P, generuoto ciklinio pogrupio $[\pi]$ ir P', kiekvienas elementas gali būti vienareikšmiškai užrašomas taip: $\pi^j \sigma_0 \sigma_1 \dots \sigma_{p-1}$, čia $\sigma_i \in P_i$, $0 \le i, j \le p-1$. Simetrinės grupės S_{p^n} pogrupio P eilė yra lygi $p^{t(n)}$. P ir yra simetrinės grupės S_{p^n} ieškomas Sylovo p-pogrupis. $\triangle$

13. 5. Keili teorema. Grupė, kurios eilė yra lygi n, yra izomorfinė simetrinės grupės S_n pogrupiui.

Įrodymas. Sakykime, grupės G eilė yra lygi n, $\{g_1, g_2, \dots, g_n\}$ – grupės G elementai. Grupės G elementui x priskirkime atvaizdį $f_x : G \to G$, $f_x(g_j) = xg_j$, $1 \le j \le n$. Atvaizdis $f_x : G \to G$ yra injektyvus. Iš tikrųjų, jei $f_x(g_i) = f_x(g_j)$, $1 \le i, j \le n$, tai $xg_i = xg_j$ arba $g_i = g_j$ (priminsime, kad grupėje galima prastinti tiek iš kairės, tiek iš dešinės). Vadinasi, atvaizdis $f_x : G \to G$ yra aibės G elementų keitinys, t. y. $f_x \in S_n$. Taigi apibrėžtas atvaizdis $f : G \to S_n$, $x \mapsto f_x$, $x \in G$. Įsitikinsime, kad f yra homomorfizmas.

Imkime grupės G elementus x, y. Tuomet kiekvienam $g_j \in G$, $f_{xy}(g_j) = xyg_j = f_x(yg_j) = f_x(f_y(g_j)) = (f_x \circ f_y)(g_j)$, t. y. $f_{xy} = f_x \circ f_y$. Be to, homomorfizmas $f : G \to S_n$ yra injektyvus. Iš tikrųjų, jei $f_x = f_y$, $x, y \in G$, tai kiekvienam $z \in G$, $f_x(z) = f_y(z)$, t. y. $xz = yz$ arba $x = y$ (grupėje G lygybę $xz = yz$ suprastinome iš dešinės iš elemento z). Vadinasi, grupės G vaizdas $f(G)$, izomorfinis grupei G, yra simetrinės grupės S_n pogrupis. $\triangle$

13. 6. Teorema. Sakykime, grupė G yra grupės H pogrupis ir grupėje H egzistuoja Sylovo p-pogrupis P. Tuomet ir grupėje G egzistuoja Sylovo p-pogrupis.

Įrodymas. Sakykime, $|G| = p^s a$, $p \not| a$, $|H| = p^m b$, $p \not| b$, P – grupės H Sylovo p-pogrupis, t. y. toks pogrupis, kurio eilė yra lygi p^m. Įrodysime, kad egzistuoja bent vienas toks grupės H elementas x, kad $G \cap xPx^{-1}$ yra grupės G Sylovo p-pogrupis, t. y. toks pogrupis, kurio eilė yra lygi p^s.

Nagrinėkime grupėje H dvigubas gretutines klases GxP, $x \in H$. Įrodysime, kad dvi tokios klasės arba sutampa arba neturi bendrų elementų. Sakykime, kad $z \in GxP \cap GyP$.

Tuomet elementą z galime užrašyti taip: $z = g_1xh_1 = g_2yh_2$, $g_1, g_2 \in G$, $h_1, h_2 \in P$. Remdamiesi lygybe $g_1xh_1 = g_2yh_2$, gauname $x = g_1^{-1}g_2yh_2h_1^{-1} \in GyP$, t. y. $GxP \subset GyP$. Panašiai gauname, kad $y = g_2^{-1}g_1xh_1h_2^{-1} \in GxP$, t. y. $GyP \subset GxP$.

Taigi įrodėme, jei grupės H dvigubos gretutinės klasės GxP ir GyP turi bendrą elementą, tai jos ir sutampa. Vadinasi, grupės H dvigubos gretutinės klasės GxP, $x \in H$ suskaido grupę H į netuščius, neturinčių bendrų elementų, poaibius. Tuomet galime užrašyti $H = \bigcup_{j=1}^{r} Gx_jP$, čia x_j, $1 \le j \le r$, skirtingų dvigubų gretutinių klasių atstovai. Dviguboje gretutinėje klasėje Gx_jP elementų skaičius yra lygus

$$|Gx_jP| = |Gx_jPx_j^{-1}| = \frac{|G||x_jPx_j^{-1}|}{|G \cap x_jPx_j^{-1}|} = \frac{|G||P|}{|G \cap x_jPx_j^{-1}|},\ 1 \le j \le r.$$

Sakykime, $|G \cap x_jPx_j^{-1}| = p^{t_j}$, $0 \le t_j < s$, $1 \le j \le r$. Tuomet dviguboje gretutinėje klasėje Gx_jP elementų skaičius yra lygus

$$|Gx_jP| = \frac{|G||P|}{|G \cap x_jPx_j^{-1}|} = \frac{p^sp^mab}{p^{t_j}} = p^{s-t_j+m}ab, 1 \le j \le r.$$

Dabar įsitikinsime, kad bent vienam j, $1 \le j \le r$, $|G \cap x_jPx_j^{-1}| = p^s$. Jei kiekvienam j, $1 \le j \le r$, būtų $|G \cap x_jPx_j^{-1}| = p^{t_j}$ ir $0 \le t_j < s$, tai kiekvienos dvigubos gretutinės klasės Gx_jP, $1 \le j \le r$, elementų skaičius $p^{s-t_j+m}ab$ dalytųsi iš p^{m+1}. Vadinasi, iš p^{m+1} dalytųsi ir grupės H eilė $|H|$. Taip negali būti, nes $|H| = p^mb$, $p \not| b$. Taigi egzistuoja bent vienas toks j_0, $1 \le j_0 \le r$, kad $|G \cap x_{j_0}Px_{j_0}^{-1}| = p^s$, t. y. $G \cap x_{j_0}Px_{j_0}^{-1}$ yra grupės G Sylovo p-pogrupis. $\triangle$

13. 7. Sakykime, G – grupė, $|G| = p^sa = n$, $p \not| a$. Teigiame, kad grupėje G egzistuoja Sylovo p-pogrupis. Pirmiausia pastebėsime, kad grupė G yra izomorfinė simetrinės grupės S_n pogrupiui G'. Parinkime tokį m, kad būtų teisinga nelygybė $n < p^m$. Simetrinę grupę S_n galime nagrinėti kaip simetrinės grupės S_{p^m} pogrupį. Taigi $G' \subset S_n \subset S_{p^m}$. Kadangi grupėje S_{p^m} egzistuoja Sylovo p-pogrupis, tai ir grupės S_{p^m} pogrupyje G' taip pat egzistuoja Sylovo p-pogrupis P'. Jei $f : G' \to G$ – izomorfizmas, tai $f(P') = P$ yra grupės G Sylovo p-pogrupis.

13. 8. Antrosios Sylovo teoremos įrodymas. Sakykime, G – grupė, P ir P' – grupės G Sylovo p-pogrupiai. Įrodysime, kad pogrupiai P ir P' yra sujungtiniai, t. y. egzistuoja grupės G toks elementas g, kad $P' = gPg^{-1}$.

Sakykime, $|G| = p^sa = n$, $p \not| a$, $|P| = |P'| = p^s$. Nagrinėkime grupės G dvigubas gretutines klases $P'xP$, $x \in G$. Užrašykime grupės skaidinį dvigubomis gretutinėmis klasėmis:

$$G = \bigcup_{j=1}^{r} P'x_jP,$$

čia x_j, $1 \le j \le r$, skirtingų dvigubų gretutinių klasių atstovai. Dvigubos gretutinės klasės $P'x_jP$ elementų skaičius yra lygus

$$|P'x_jP| = \frac{|P'||P|}{|P' \cap x_jPx_j^{-1}|},\ 1 \le j \le r.$$

Sakykime, $|P' \cap x_jPx_j^{-1}| = p^{t_j}$, $0 \le t_j \le s$, $1 \le j \le r$. Tuomet $|P'x_jP| = p^{2s-t_j}$, $1 \le j \le r$. Jei kiekvienam j, $1 \le j \le r$, būtų $0 \le t_j < s$, tai skaičius p^{2s-t_j} dalytųsi iš p^{s+1}, vadinasi, iš p^{s+1} dalytųsi ir grupės G eilė $|G|$. Taip negali būti, nes $|G| = p^sa$, $p \not| a$. Taigi egzistuoja toks j_0, $1 \le j_0 \le r$, kad $|P' \cap x_{j_0}Px_{j_0}^{-1}| = p^s$, t. y. $P' = x_{j_0}Px_{j_0}^{-1}$. $\triangle$

13. 9. Trečiosios Sylovo teoremos įrodymas. Sakykime, G – grupė, $n = |G| = p^sa$, $p \not| a$, P – grupės G Sylovo p-pogrupis, t. y. P – grupės G pogrypis, kurio eilė yra lygi $|P| = p^s$. Nagrinėkime pogrupio P normalizatorių $N_G(P)$ grupėje G. Pagal apibrėžimą

$$N_G(P) = \{x \in G |\ xPx^{-1} = P\}.$$

Sakykime, $G = \bigcup_{j=1}^{l} x_jN_G(P)$ – grupės G skaidinys kairiosiomis gretutinėmis klasėmis pagal pogrupį $N_G(P)$, x_j, $1 \le j \le l$, skirtingų kairiųjų gretutinių klasių atstovai. Teigiame, kad grupės G visi skirtingi Sylovo p-pogrupiai yra šie: $x_jPx_j^{-1}$, $1 \le j \le l$.

Jei $x \in x_jN_G(P)$, tai $x = x_jg$, $g \in N_G(P)$. Tuomet $xPx^{-1} = x_jgP(x_jg)^{-1} = x_jgPg^{-1}x_j^{-1} = x_jPx_j^{-1}$.

Jei $xPx^{-1} = x_jPx_j^{-1}$, tai $x_j^{-1}xPx^{-1}x_j = P$, t. y. $x_j^{-1}x \in N_G(P)$ arba $x \in x_jN_G(P)$.

Kaip matome, yra abipus vienareikšmė atitinkamybė tarp grupės G Sylovo p-pogrupių ir grupės G kairiųjų gretutinių klasių pagal Sylovo p-pogrupio P normalizatorių $N_G(P)$ grupėje G. Vadinasi, gupės G Sylovo p-pogrupių yra l. Kadangi pogrupio indeksas dalija grupės G eilę, tai $l \mid n$. Lieka įrodyti, kad $l \equiv 1(\mathrm{mod} p)$.

Užrašykime grupės G skaidinį dvigubomis gretutinėmis klasėmis PxP, $x \in G$:

$$G = \bigcup_{j=1}^{r} Px_jP,$$

čia x_j, $1 \le j \le r$, – skirtingų dvigubų gretutinių klasių atstovai. Jei $x_j \in N_G(P)$, tai $Px_jP = PPx_j = Px_j$. Jei $x_j \notin N_G(P)$, tai $P \cap x_jPx_j^{-1} \subset P$, $P \cap x_jPx_j^{-1} \ne P$. Vadinasi, jei $x_j \notin N_G(P)$, tai dvigubos gretutinės klasės Px_jP elementų skaičius yra lygus

$$|Px_jP| = \frac{|P||x_jPx_j^{-1}|}{|P \cap x_jPx_j^{-1}|} = p^{2s-t_j},$$

čia $|P \cap x_jPx_j^{-1}| = p^{t_j}$, $t_j < s$, ir, kaip matome, dalijasi iš p^{s+1}. Grupės G skaidinį dvigubomis gretutinėmis klasėmis suskirstykime į dvi sumas: į vieną surinkime dvigubas

gretutines klases, kurių atstovai priklauso Sylovo p-pogrupio normalizatoriui $N_G(P)$, o į kitą – dvigubas gretutines klases, kurių atstovai nepriklauso Sylovo p-pogrupio normalizatoriui $N_G(P)$:

$$G = \bigcup_{x_j \in N_G(P)} Px_jP \cup \bigcup_{x_j \notin N_G(P)} Px_jP.$$

Kadangi $P \subset N_G(P)$, tai pirmoji suma $\bigcup_{x_j \in N_G(P)} Px_jP$ yra $N_G(P)$ skaidinys pogrupio P dešiniosiomis gretutinėmis klasėmis (grupėje $N_G(P)$ kairiosios ir dešiniosios pogrupio P klasės sutampa, nes P yra normalusis pogrupis grupėje $N_G(P)$). Vadinasi, galime parašyti lygybę:

$$|G| = |N_G(P)| + \sum_{\substack{j \\ x_j \notin N_G(P)}} p^{2s-t_j} = |N_G(P)| + p^{s+1}q.$$

Kadangi $p^s = |P| \| |N_G(P)|$, $|N_G(P)| \| |G| = p^s a$, $p \not| a$, tai skaičius $|N_G(P)|$ dalijasi tik iš p^s ir nesidalija iš pirminio skaičiaus p didesnio laipsnio. Lygybę $|G| = |N_G(P)| + p^{s+1}q$ padaliję iš $|N_G(P)|$, gauname $l = 1 + \frac{p^{s+1}q}{|N_G(P)|}$. Akivaizdu, kad sveikasis skaičius $\frac{p^{s+1}q}{|N_G(P)|}$ dalijasi iš p, t. y. $l \equiv 1 (\mathrm{mod} p)$. $\triangle$

Pavyzdžiai.

1. Įrodysime, kad grupė G, kurios eilė lygi 15, yra ciklinė.

Kadangi $15 = 3 \cdot 5$, tai egzistuoja grupės G Sylovo 3-pogrupis H_1 ir 5-pogrupis H_2. Sylovo 3-pogrupių yra $1 + 3m$ ir, be to, $1 + 3m \mid 15$. Tai galima tik tuo atveju, kai $m = 0$. Kitaip tariant, egzistuoja tik vienas Sylovo 3-pogrupis H_1. Kadangi kiekvienam $x \in G$, xH_1x^{-1} yra 3-pogrupis, tai kiekvienam $x \in G$, $xH_1x^{-1} = H_1$. Taigi H_1 yra grupės G normalusis pogrupis. Panašiai įrodoma, kad H_2 yra taip pat grupės G normalusis pogrupis. Bet kuriems $h_1 \in H_1$, $h_2 \in H_2$, elementas $h_1h_2h_1^{-1}h_2^{-1} \in H_1 \cap H_2 = \{1\}$, t. y. bet kuriems $h_1 \in H_1$, $h_2 \in H_2$, gauname $h_1h_2 = h_2h_1$. Taigi grupė G yra ciklinių pogrupių H_1 ir H_2 tiesioginė sandauga. Kadangi ciklinių pogrupių H_1 ir H_2 eilės yra 3 ir 5, t. y. tarpusavyje pirminiai skaičiai, tai G yra taip pat ciklinė grupė.