I SKYRIUS
GRUPIŲ TEORIJOS ELEMENTAI

1. Grupės, pogrupiai, normalieji dalikliai

1.1. Apibrėžimas. *Netuščia aibė G vadinama grupe, jei joje apibrėžta algebrinė operacija $\cdot$, kuri pasižymi savybėmis:*

1) *yra asociatyvi –*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G;$$

2) *aibei G priklauso vienetinis elementas e su savybe*

$$e \cdot a = a \cdot e = a \quad \forall a \in G;$$

3) *aibei G kartu su kiekvienu elementu a priklauso jam atvirkštinis elementas a^{-1}: $a \cdot a^{-1} = a^{-1} \cdot a = e$.*

1.2. Pavyzdžiai. 1) Natūraliųjų skaičių aibė N daugybos atžvilgiu grupės nesudaro, nes neišpildyta trečioji grupės apibrėžimo sąlyga. Praplėtę šią aibę iki teigiamų racionaliųjų skaičių aibės Q^+, gausime multiplikacinę grupę.

2) n-tojo laipsnio simetrinė grupė S_n – tai baigtinės aibės X, sudarytos iš n elementų, bijekcijų į save grupė atvaizdžių kompozicijos atžvilgiu.

3) 2-ojo laipsnio pilnoji tiesinė grupė $Gl(2, Q)$ virš racionaliųjų skaičių kūno Q:

$$Gl(2, Q) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; |A| \neq 0, \;\; a, b, c, d \in Q \right\}.$$

4) Pilnoji modulinė grupė Γ:

$$\Gamma = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \; |A| = 1, \;\; a, b, c, d \in Z \right\} \text{ – patikrinkite!}$$

1.3. Apibrėžimas. *Netuščias grupės G poaibis H vadinamas jos pogrupiu, kai:*

1) $h_1 \cdot h_2 \in H \quad \forall h_1, h_2 \in H$;

2) $h^{-1} \in H \quad \forall h \in H$.

Pastaba. *Šias dvi sąlygas galima pakeisti viena ekvivalenčia – $h_1 \cdot h_2^{-1} \in H$ $\forall h_1, h_2 \in H$.*

Kai H yra G pogrupis, žymėsime $H < G$.

Apibrėšime ekvivalentumo sąryšį grupėje G atžvilgiu pogrupio H. Sakysime, kad grupės G elementas a ekvivalentus b ir rašysime $a \sim b$, kai $a^{-1}b \in H$. Įrodysime, kad tai ekvivalentumo sąryšis grupėje G. Iš tikrųjų:

1) $a \sim a$, nes $a^{-1} \cdot a = e \in H$;

2) jei $a \sim b$, tai $a^{-1} \cdot b \in H$. $\Rightarrow (a^{-1} \cdot b)^{-1} = b^{-1} \cdot a \in H \Rightarrow b \sim a$;

3) jei $a \sim b$, $b \sim c$, tai $a^{-1} \cdot b$, $b^{-1} \cdot c \in H \Rightarrow (a^{-1} \cdot b) \cdot (b^{-1} \cdot c) = a^{-1} \cdot c \in H \Rightarrow a \sim c$. $\triangle$

Pažymėję klasę su atstovu a

$$\overline{a} = \{b \in G \mid b \sim a\},$$

suskaidome grupę ekvivalentumo klasių sąjunga –

$$G = \bigcup_{a \in G} \overline{a}.$$

Įrodysime, kad klasė $\overline{a}$ sutampa su aibe $aH = \{ah \mid h \in H\}$.

Tarkime, $b \in \overline{a}$. $\Rightarrow a \sim b \Rightarrow a^{-1} \cdot b \in H \Rightarrow \exists\, h \in H : a^{-1} \cdot b = h$. Padauginę šios lygybės abi puses iš kairės iš a, turime $b = ah$. $\Rightarrow b \in aH \Rightarrow \overline{a} \subset aH$.

Tarkime, $b \in aH$. $\Rightarrow \exists\, h \in H : b = ah$. Padauginę šios lygybės abi puses iš kairės iš a^{-1}, turime $a^{-1} \cdot b = h \in H$. $\Rightarrow a \sim b \Rightarrow b \in \overline{a} \Rightarrow aH \subset \overline{a}$.

Tokiu būdu, $\overline{a} = aH$. $\triangle$

Klasė aH yra vadinama grupės G *kairiuoju sluoksniu* pagal pogrupį H.

Panašiu būdu galima apibrėžti grupėje G dar vieną ekvivalentumo sąryšį – sakome, kad elementas a yra ekvivalentus b ir rašome, $a \sim b$, jei $a \cdot b^{-1} \in H$. Nesunku matyti, kad tai yra iš tikrųjų ekvivalentumo sąryšis ir klasė $\overline{a}$ sutampa su poaibiu Ha, kurį vadiname *dešiniuoju sluoksniu.* Tokiu būdu, grupė G gali būti išreikšta ir kairiųjų, ir dešiniųjų sluoksnių sąjunga:

$$G = \bigcup_{a \in G} aH = \bigcup_{b \in G} Hb.$$

Kairiųjų sluoksnių aibė $\{aH \mid a \in G\}$ nebūtinai turi sutapti su dešiniųjų sluoksnių aibe $\{Hb \mid b \in G\}$. Išskirsime tuos grupės G pogrupius H, kuriems šios aibės sutampa.

1.4. Apibrėžimas. *Sakome, kad grupės G pogrupis H yra normalusis daliklis ir žymime $H \triangleleft G$, kai grupės G pagal pogrupį H kairiųjų sluoksnių aibė sutampa su dešiniųjų sluoksnių aibe.*

1.5. Teorema (I normaliojo daliklio kriterijus). *Pogrupis H yra grupės G normalusis daliklis tada ir tik tada, kai $aH = Ha$ $\forall a \in G$.*

Įrodymas. Būtinumas. Tarkime, H yra normalusis daliklis ir aH – fiksuotas kairysis sluoksnis. Iš 1.4 apibrėžimo išplaukia, kad egzistuoja dešinysis sluoksnis Hb, lygus aH. Įrodysime, kad dešinieji sluoksniai Hb ir Ha sutampa. Tam pakanka parodyti, kad

$$Ha \cap Hb \neq \emptyset.$$

Iš tikrųjų, $a \in Ha$ ir $a \in aH = Hb$. Vadinasi, $a \in Ha \cap Hb$. Todėl $Ha = Hb = aH$. $\triangle$

Pakankamumas. Tarkime, $aH = Ha\ \forall a \in G$. Teiginio įrodymas išplaukia tiesiogiai iš aibių lygybės apibrėžimo. $\triangle$

1.6. Apibrėžimas. *Sakome, kad grupės G elementas a yra jungtinis tos grupės elementui b, kai egzistuoja $x \in G$ toks, kad $b = x \cdot a \cdot x^{-1}$.*

Įsitikinsime, kad sąryšis, siejantis grupės G jungtinius elementus, yra ekvivalentumo sąryšis toje grupėje:

1. $a \sim a$, nes $a = e \cdot a \cdot e^{-1}$.

2. Tarkime, $a \sim b$. $\Rightarrow \exists x \in G$: $b = x \cdot a \cdot x^{-1}$. Padauginę šios lygybės abi puses iš dešinės iš x, o iš kairės – iš x^{-1}, bei pasinaudoję lygybe $(x^{-1})^{-1} = x$, gauname $a = x^{-1} \cdot c \cdot (x^{-1})^{-1}$. Vadinasi, $b \sim a$.

3. Tarkime, $a \sim b$, $b \sim c$. $\Rightarrow \exists x, y \in G$: $b = x \cdot a \cdot x^{-1}$, $c = y \cdot b \cdot y^{-1}$. $\Rightarrow$ $c = y \cdot \left(x \cdot a \cdot x^{-1}\right) \cdot y^{-1} = y \cdot x \cdot a \cdot x^{-1} \cdot y^{-1} = (y \cdot x) \cdot a \cdot (y \cdot x)^{-1}$. $\Rightarrow a \sim c$. $\triangle$

Šis ekvivalentumo ryšys leidžia grupę G užrašyti jungtinių elementų klasių sąjunga –

$$G = \bigcup_{a \in G} \left\{xax^{-1} \mid x \in G\right\}.$$

Pritaikysime jungtinio elemento sąvoką kitoje normaliojo daliklio kriterijaus formuluotėje.

1.7. Teorema (II normaliojo daliklio kriterijus). *Pogrupis H yra grupės G normalusis daliklis tada ir tik tada, kai su kiekvienu to pogrupio elementu h jam priklauso ir visi jo jungtiniai elementai aha^{-1}, $a \in G$.*

Įrodymas. Būtinumas. Tarkime, H yra grupės G normalusis daliklis, a - fiksuotas grupės G elementas. Iš 1.5 teoremos išplaukia lygybė $aH = Ha$. Padauginę šios lygybės abi puses iš dešinės iš a^{-1}, gauname $aHa^{-1} = H$. Vadinasi, $aha^{-1} \in H\ \forall a \in G$. $\triangle$

Pakankamumas. Tarkime, $aha^{-1} \in H\ \forall a \in G,\ \forall h \in H$. $\Rightarrow ah \in Ha \Rightarrow aH \subset Ha$.

Iš kitos pusės, $a^{-1}h\left(a^{-1}\right)^{-1} = a^{-1}ha \in H$. $\Rightarrow ha \in aH \Rightarrow Ha \subset aH$.

Tokiu būdu, $aH = Ha\quad \forall a \in G$. Teiginio įrodymui pakanka pasinaudoti 1.5 teorema. $\triangle$

2. Faktorgrupė, grupių homomorfizmai

Tarkime, H yra grupės G normalusis daliklis, ir

$$G/_H = \{aH \mid a \in G\} -$$

grupės G kairiųjų sluoksnių aibė pagal pogrupį H. Šioje aibėje apibrėžiame algebrinę operaciją tokiu būdu:

$$aH \cdot bH = a \cdot bH.$$

Apibrėžiant algebrinę operaciją tarp klasių per jų atstovus, iškyla tos operacijos apibrėžimo korektiškumo klausimas – klasių operacijos rezultatas turi nepriklausyti nuo atstovų pasirinkimo. Įrodysime, kad ši operacija yra apibrėžta korektiškai.

Tarkime, $a'H = aH$ ir $b'H = bH$. Reikia įrodyti, kad $a' \cdot b'H = a \cdot bH$. Tam pakanka parodyti, kad šių sluoksnių sankirta yra netuščia aibė.

Turime $a \in aH \Rightarrow a \in a'H$, nes $a'H = aH$. $\Rightarrow \exists\, h_1 \in H : a = a' \cdot h_1$.

Analogiškai $\exists\, h_2 \in H$: $b = b' \cdot h_2$. $\Rightarrow a \cdot b = a'h_1 \cdot b' \cdot h_2$.

Kadangi $h_1 \cdot b' \in Hb'$ ir $Hb' = b'H$, $\exists\, h_3 \in H$: $h_1 \cdot b' = b' \cdot h_3$. Vadinasi, $a \cdot b = a'(h_1 \cdot b') \cdot h_2 = a' \cdot b' \cdot h_3 \cdot h_2 \in a' \cdot b'H$. Bet $a \cdot b \in a \cdot bH$. Vadinasi, $a \cdot bH \cap a' \cdot b'H \neq \emptyset$. $\Rightarrow a \cdot bH = a' \cdot b'H$. Todėl algebrinė operacija kairiųjų sluoksnių aibėje yra apibrėžta korektiškai. Šios operacijos atžvilgiu aibė $G/_H$ yra grupė. Iš tikrųjų:

1) operacija asociatyvi –

$$(aH \cdot bH) \cdot cH = a \cdot bH \cdot cH = a \cdot b \cdot cH = aH \cdot b \cdot cH = aH \cdot (bH \cdot cH);$$

2) egzistuoja vienetinis elementas $eH = H$ –

$$aH \cdot eH = a \cdot eH = aH \quad \forall aH \in G/_H;$$

3) su kiekvienu sluoksniu aH egzistuoja jam atvirkštinis sluoksnis $a^{-1}H$ –

$$a^{-1}H \cdot aH = a^{-1} \cdot aH = eH = H = a \cdot a^{-1}H = aH \cdot a^{-1}H.$$

2.1. Apibrėžimas. *Grupės G kairiųjų sluoksnių grupė $G/_H$ pagal normalųjį daliklį H yra vadinama grupės G faktorgrupe pagal normalųjį daliklį H.*

2.2. Apibrėžimas. *Grupės G homomorfizmu grupėje G' yra vadinamas toks atvaizdis $\varphi : G \to G'$, kai su kiekviena grupės G elementų pora a, b teisinga lygybė*

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

2.3. Pavyzdžiai. 1) Apibrėžiame atvaizdį $\varphi : G \to G$ lygybe $\varphi(g) = e \quad (\forall g \in G)$. φ – homomorfizmas, nes $\varphi(g \cdot h) = e = e \cdot e = \varphi(g) \cdot \varphi(h) \ (\forall g, h \in G)$.

2) Apibrėžiame realiųjų skaičių adicinės grupės R^+ atvaizdį multiplikacinėje grupėje $R^* = R \setminus \{0\}$ lygybe

$$\varphi(\alpha) = e^{\alpha} \quad (\forall \alpha \in R^+).$$

φ – homomorfizmas, nes

$$\varphi(\alpha + \beta) = e^{\alpha+\beta} = e^{\alpha} \cdot e^{\beta} = \varphi(\alpha) \cdot \varphi(\beta) \quad (\forall \alpha, \beta \in R^+).$$

3) Apibrėžiame pilnosios tiesinės grupės $Gl(2, Q)$ atvaizdį racionaliųjų skaičių multiplikacinėje grupėje $Q^* = Q \setminus \{0\}$ lygybe

$$\varphi(A) = |A| \quad \big(\forall A \in Gl(2, Q)\big).$$

φ – homomorfizmas, nes

$$\varphi(AB) = |AB| = |A||B| = \varphi(A)\,\varphi(B) \quad \big(\forall A, B \in Gl(2, Q)\big).$$

4) Fiksuojame grupės G elementą h ir apibrėžiame šios grupės atvaizdį φ_h joje pačioje lygybe

$$\varphi_h(g) = h \cdot g \cdot h^{-1} \quad (\forall g \in G).$$

φ_h – homomorfizmas, nes

$$\varphi_h(g_1 \cdot g_2) = h \cdot g_1 \cdot g_2 \cdot h^{-1} = h \cdot g_1 \cdot h^{-1} \cdot h \cdot g_2 \cdot h^{-1} = \varphi_h(g_1) \cdot \varphi_h(g_2) \quad (\forall g_1, g_2 \in G).$$

Įsitikinsime, kad atvaizdis φ_h yra bijekcija. Injekciją įrodome prieštaros būdu. Tarkime, $g_1 \neq g_2$, o jų vaizdai $\varphi_h(g_1)$ ir $\varphi_h(g_2)$ sutampa:

$$\begin{array}{ccc} \varphi_h(g_1) & = & \varphi_h(g_2) \\ \| & & \| \\ h \cdot g_1 \cdot h^{-1} & = & h \cdot g_2 \cdot h^{-1}. \end{array}$$

Padauginę abi pastarosios lygybės puses iš kairės iš h^{-1}, o iš dešinės – iš h, turėsime $g_1 = g_2$. O tai yra prieštara elementų g_1 ir g_2 pasirinkimui.

Atvaizdis φ_h – surjekcija, nes grupės G elemento g pirmvaizdžiu yra elementas $h^{-1} \cdot g \cdot h$:

$$\varphi_h\big(h^{-1} \cdot g \cdot h\big) = h \cdot h^{-1} \cdot g \cdot h \cdot h^{-1} = g.$$

2.4. Apibrėžimas. *Grupės G bijekcinis homomorfizmas toje pačioje grupėje yra vadinamas tos grupės automorfizmu.*

2.5. Apibrėžimas. *Automorfizmas* $\varphi_h : g \to h \cdot g \cdot h^{-1}$ *yra vadinamas grupės* G *vidiniu automorfizmu.*

2.6. Teiginys. *Grupės* G *vidinių automorfizmų aibė* $\mathrm{Int}\, G$ *sudaro grupę atvaizdžių kompozicijos atžvilgiu.*

Apibrėžiame algebrinę operaciją aibėje $\mathrm{Int}\, G$ *lygybe*

$$\varphi_h \circ \varphi_{h'} = \varphi_{h \cdot h'}.$$

1) *operacija asociatyvi* –

$$\big(\varphi_{h_1} \circ \varphi_{h_2}\big) \circ \varphi_{h_3} = \varphi_{h_1 \cdot h_2} \circ \varphi_{h_3} = \varphi_{h_1 \cdot h_2 \cdot h_3} = \varphi_{h_1} \circ \varphi_{h_2 \cdot h_3} = \varphi_{h_1} \circ \big(\varphi_{h_2} \circ \varphi_{h_3}\big);$$

2) *egzistuoja vienetinis elementas* φ_e –

$$\varphi_e \circ \varphi_h = \varphi_{e \cdot h} = \varphi_h = \varphi_{h \cdot e} = \varphi_h \circ \varphi_e \quad (\forall \varphi_h \in \mathrm{Int}\, G);$$

3) *kiekvienam aibės* $\mathrm{Int}\, G$ *elementui* φ_h *egzistuoja atvirkštinis elementas* $\big(\varphi_h\big)^{-1} = \varphi_{h^{-1}}$ –

$$\varphi_h \circ \varphi_{h^{-1}} = \varphi_{h \cdot h^{-1}} = \varphi_e = \varphi_{h^{-1} \cdot h} = \varphi_{h^{-1}} \circ \varphi_h. \ \triangle$$

3. Pagrindinė grupių homomorfizmų teorema

Tarkime, φ yra grupės G homomorfizmas grupėje G'. Pažymėkime šio homomorfizmo vaizdų aibę

$$\varphi(G) = \mathrm{Im}\, \varphi = \{\varphi(g) \mid g \in G\}.$$

Įrodysime, kad $\mathrm{Im}\, \varphi$ yra grupės G' pogrupis. Tarkime, $g_1', g_2' \in \mathrm{Im}\, \varphi$. $\Rightarrow \exists\, g_1, g_2 \in G$: $\varphi(g_1) = g_1'$, $\varphi(g_2) = g_2'$. $\Rightarrow g_1' \cdot {g_2'}^{-1} = \varphi(g_1) \cdot \big(\varphi(g_2)\big)^{-1} = \varphi(g_1) \cdot \varphi\big(g_2^{-1}\big) = \varphi\big(g_1 g_2^{-1}\big)$. $\Rightarrow$ $g_1' \cdot {g_2'}^{-1} \in \mathrm{Im}\, \varphi$. $\triangle$

Apibrėžiame homomorfizmo φ branduolį $\mathrm{Ker}\, \varphi$ –

$$\mathrm{Ker}\, \varphi = \{g \in G \mid \varphi(g) = e'\}.$$

Įrodysime, kad $\mathrm{Ker}\, \varphi$ yra grupės G normalusis daliklis. Tarkime, $g_1, g_2 \in \mathrm{Ker}\, \varphi$, $\Rightarrow$ $\varphi\big(g_1 \cdot g_2^{-1}\big) = \varphi(g_1) \cdot \varphi\big(g_2^{-1}\big) = \varphi(g_1)\big(\varphi(g_2)\big)^{-1} = e' \cdot e' = e' \Rightarrow g_1 \cdot g_2^{-1} \in \mathrm{Ker}\, \varphi$.

Taigi $\mathrm{Ker}\, \varphi$ – pogrupis. Tarkime, $h \in \mathrm{Ker}\, \varphi$, $g \in G \Rightarrow \varphi\big(g \cdot h \cdot g^{-1}\big) = \varphi(g) \cdot \varphi(h)\varphi(g^{-1}) = \varphi(g) \cdot e' \cdot \big(\varphi(g)\big)^{-1} = e' \Rightarrow g \cdot h \cdot g^{-1} \in \mathrm{Ker}\, \varphi \Rightarrow \mathrm{Ker}\, \varphi$ – normalusis daliklis. $\triangle$

3.1. Teorema (pagrindinė grupių homomorfizmų teorema). 1) *Tarkime, φ yra grupės G homomorfizmas grupėje G'. Tada faktorgrupė $G/_{\operatorname{Ker}\varphi}$ yra izomorfiška vaizdui* $\operatorname{Im}\varphi$:

$$G/_{\operatorname{Ker}\varphi} \cong \operatorname{Im}\varphi.$$

2) *Tarkime, H yra grupės G normalusis daliklis. Tada egzistuoja grupės G surjekcinis homomorfizmas φ faktorgrupėje $G/_H$ toks, kad šio homomorfizmo branduolys* $\operatorname{Ker}\varphi$ *sutampa su pogrupiu H.*

Įrodymas. 1) Tarkime,

$$\varphi : G \to G' -$$

homomorfizmas. Galime apibrėžti faktorgrupę $G/_{\operatorname{Ker}\varphi}$, nes, kaip buvo įrodyta, $\operatorname{Ker}\varphi$ yra normalusis daliklis. Apibrėžiame atvaizdį f: $G/_{\operatorname{Ker}\varphi} \to \operatorname{Im}\varphi$ lygybe

$$f(g\operatorname{Ker}\varphi) = \varphi(g).$$

Įsitikinsime, kad atvaizdis apibrėžtas korektiškai. Tarkime, $g'\operatorname{Ker}\varphi = g\operatorname{Ker}\varphi$ ir

$$f(g'\operatorname{Ker}\varphi) = \varphi(g').$$

Parodysime, kad $\varphi(g)$ sutampa su $\varphi(g')$. Iš tikrųjų, kadangi $g \in g\operatorname{Ker}\varphi \Rightarrow g \in g'\operatorname{Ker}\varphi$ $\Rightarrow \exists\, h \in \operatorname{Ker}\varphi$: $g = g' \cdot h \Rightarrow \varphi(g) = \varphi(g' \cdot h) = \varphi(g')\varphi(h) = \varphi(g') \cdot e' = \varphi(g')$.

Atvaizdis f – homomorfizmas:

$$\begin{aligned} &f(g_1\operatorname{Ker}\varphi \cdot g_2\operatorname{Ker}\varphi) = f(g_1 \cdot g_2\operatorname{Ker}\varphi) = \\ &= \varphi(g_1 \cdot g_2) = \varphi(g_1)\cdot\varphi(g_2) = f(g_1\operatorname{Ker}\varphi)\cdot f(g_2\operatorname{Ker}\varphi). \end{aligned}$$

Kad f – injekcija, įrodysime prieštaros būdu. Tarkime, $g_1\operatorname{Ker}\varphi \neq g_2\operatorname{Ker}\varphi$, o $f(g_1\operatorname{Ker}\varphi) = f(g_2\operatorname{Ker}\varphi)$. Vadinasi, $\varphi(g_1) = \varphi(g_2)$. Padauginkime abi šios lygybės puses iš dešinės iš $\varphi(g_2)^{-1}$. $\Rightarrow e' = \varphi(g_1)\cdot\varphi(g_2)^{-1} = \varphi(g_1)\cdot\varphi\big(g_2^{-1}\big) = \varphi\big(g_1 \cdot g_2^{-1}\big)$. $\Rightarrow$ $g_1g_2^{-1} \in \operatorname{Ker}\varphi \Rightarrow g_1 \in g_2\operatorname{Ker}\varphi$. Bet $g_1 \in g_1\operatorname{Ker}\varphi$. $\Rightarrow g_1 \in g_1\operatorname{Ker}\varphi \cap g_2\operatorname{Ker}\varphi$. $\Rightarrow$ $g_1\operatorname{Ker}\varphi \cap g_2\operatorname{Ker}\varphi \neq \emptyset \Rightarrow g_1\operatorname{Ker}\varphi = g_2\operatorname{Ker}\varphi$. Gavome prieštarą prielaidai.

Atvaizdis f – surjekcija. Iš tikrųjų, elementui $\varphi(g) \in \operatorname{Im}\varphi$ pirmvaizdžiu yra sluoksnis $g\operatorname{Ker}\varphi$, nes $f(g\operatorname{Ker}\varphi) = \varphi(g)$.

Tokiu būdu, f – izomorfizmas. $\triangle$

2) Tarkime, H yra grupės G normalusis daliklis. Sudarę faktorgrupę $G/_H$, apibrėžiame atvaizdį $\varphi : G \in G/_H$ lygybe

$$\varphi(g) = gH \quad (\forall g \in G).$$

Šia lygybe apibrėžtas atvaizdis yra homomorfizmas. Iš tikrųjų,

$$\varphi(g_1 \cdot g_2) = g_1 \cdot g_2H = g_1H \cdot g_2H = \varphi(g_1)\cdot\varphi(g_2).$$

Atvaizdis φ – surjekcija. Iš tikrųjų, sluoksniui gH pirmvaizdžiu yra elementas g – $\varphi(g) = gH$.

Liko įrodyti lygybę $\operatorname{Ker}\varphi = H$.

Tarkime, $g \in \operatorname{Ker}\varphi \Rightarrow \varphi(g) = H$. Iš kitos pusės, $\varphi(g) = gH$. $\Rightarrow gH = H \Rightarrow g \in H$ $\Rightarrow \operatorname{Ker}\varphi \subset H$.

Tarkime, $g \in H$. $\Rightarrow \varphi(g) = gH = H \Rightarrow g \in \operatorname{Ker}\varphi \Rightarrow H \subset \operatorname{Ker}\varphi$. $\Rightarrow H = \operatorname{Ker}\varphi$. $\triangle$

3.2. Teorema (injekcinio homomorfizmo kriterijus). *Homomorfizmas* $\varphi : G \to G'$ *yra injekcija tada ir tik tada, kai* $\operatorname{Ker}\varphi = \{e\}$.

Įrodymas. Būtinumas. Taikome prieštaros būdą. Tarkime, φ – injekcija, o $\operatorname{Ker}\varphi \neq \{e\}$. Vadinasi, $\exists\, h \in \operatorname{Ker}\varphi : h \neq e$. $\Rightarrow \varphi(h) = e'$. Bet ir $\varphi(e) = e'$. $\Rightarrow$ Gavome prieštarą injekcijos apibrėžimui. $\triangle$

Pakankamumas. Tarkime, $\operatorname{Ker}\varphi = \{e\}$, o φ nėra injekcija. Vadinasi, $\exists\, g \neq h$: $\varphi(g) = \varphi(h)$. Padauginę abi šios lygybės puses iš dešinės iš $\big(\varphi(h)\big)^{-1}$, turėsime $\varphi(g)\cdot\big(\varphi(h)\big)^{-1} = e'$. $\Rightarrow e' = \varphi(g)\cdot\varphi(h^{-1}) = \varphi(g \cdot h^{-1})$. $\Rightarrow g \cdot h^{-1} \in \operatorname{Ker}\varphi = \{e\} \Rightarrow g \cdot h^{-1} = e \Rightarrow g = h$. Vėl gavome prieštarą. $\triangle$

4. Grupių tiesioginė sandauga

Tarkime, A ir B yra grupės G pogrupiai. Pirmiausia išsiaiškinsime, ar pogrupių A ir B sankirta $A \cap B$, sąjunga $A \cup B$, sandauga $A \cdot B$ yra pogrupiai. Jei ne, kokių papildomų sąlygų reikia, kad galima būtų apibrėžti grupės struktūrą.

4.1. Teorema. *Grupės G pogrupių A ir B sankirta $A \cap B$ yra pogrupis.*

Įrodymas. Tarkime, $g, h \in A \cap B \Rightarrow g,\, h \in A$, $g, h \in B \Rightarrow g \cdot h^{-1} \in A$, $g \cdot h^{-1} \in B \Rightarrow$ $g \cdot h^{-1} \in A \cap B$. $\triangle$

4.2. Teorema. *Grupės G pogrupių A ir B sąjunga $A \cup B$ yra pogrupis tada ir tik tada, kai kuris nors pogrupis yra kito poaibis.*

Įrodymas. Būtinumas. Taikysime prieštaros būdą. Tarkime, $A \cup B < G$ ir $A \not\subset B$, $B \not\subset A$. $\Rightarrow \exists x \in A$, $x \notin B$ ir $\exists y \in B$, $y \notin A$. Bet $x, y \in A \cup B$. $\Rightarrow x \cdot y \in A \cup B$, nes $A \cup B$ pogrupis. $\Rightarrow$ Galimi du atvejai: 1. $x \cdot y \in A$. 2. $x \cdot y \in B$.

1. Tarkime, $x \cdot y \in A$. $x^{-1} \in A$, kadangi $A < G$. $\Rightarrow x^{-1} \cdot x \cdot y = y \in A$. Gavome prieštarą prielaidai.

2. Tarkime, $x \cdot y \in B$. $y^{-1} \in B$, nes $B < G$. $\Rightarrow x \cdot y \cdot y^{-1} = x \in B$. Vėl gavome prieštarą. $\triangle$

Pakankamumas. Akivaizdu, nes $A \cup B$ arba sutampa su A, arba sutampa su B.

4.3. Apibrėžimas. *Grupės G pogrupių A ir B sandauga $A \cdot B$ vadinama aibė*

$$A \cdot B = \{a \cdot b \mid a \in A, b \in B\}.$$

4.4. Teorema. *Grupės G pogrupių A ir B sandauga $A \cdot B$ yra pogrupis tada ir tik tada, kai $A \cdot B = B \cdot A$.*

Įrodymas. Būtinumas. Tarkime, $A \cdot B$ – pogrupis ir $g \in A \cdot B$. $\Rightarrow \exists\, a \in B, b \in B$: $g = a \cdot b$. Bet $g^{-1} \in A \cdot B \Rightarrow \exists a_1 \in A, b_1 \in B$: $g^{-1} = a_1 \cdot b_1$. $\Rightarrow \left(g^{-1}\right)^{-1} = g = (a_1 \cdot b_1)^{-1} = b_1^{-1} \cdot a_1^{-1} \in B \cdot A$, nes $b_1^{-1} \in B$, $a_1^{-1} \in A$. $\Rightarrow A \cdot B \subset B \cdot A$. Analogiškai įrodome, kad $B \cdot A \subset A \cdot B$. Todėl $A \cdot B = B \cdot A$. $\triangle$

Pakankamumas. Tarkime, $A \cdot B = B \cdot A$. Įrodysime, kad $A \cdot B$ yra grupės G pogrupis.

1) Tarkime, $g, h \in A \cdot B \Rightarrow \exists a_1 \in A, b_1 \in B$: $g = a_1 \cdot b_1$ ir $\exists a_2 \in A, b_2 \in B$: $h = a_2 \cdot b_2$ $\Rightarrow g \cdot h = a_1 \cdot b_1 \cdot a_2 \cdot b_2$. Bet $b_1 \cdot a_2 \in B \cdot A = A \cdot B$. Vadinasi, $\exists a_3 \in A, b_3 \in B$: $b_1 \cdot a_2 = a_3 \cdot b_3$. $\Rightarrow g \cdot h = a_1 \cdot b_1 \cdot a_2 \cdot b_2 = a_1 \cdot a_3 \cdot b_3 \cdot b_2 = (a_1 \cdot a_3) \cdot (b_3 \cdot b_2) \in A \cdot B$.

2) Tarkime, $g \in A \cdot B \Rightarrow \exists\, a \in A, b \in B$: $g = a \cdot b \Rightarrow g^{-1} = (a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \in B \cdot A = A \cdot B \Rightarrow A \cdot B < G$. $\triangle$

4.5. Apibrėžimas. *Grupė G yra vadinama savo pogrupių A ir B tiesiogine sandauga ir žymima $G = A \otimes B$, kai:*

1) $G = A \cdot B$;

2) $A \lhd G$, $B \lhd G$;

3) $A \cap B = \{e\}$.

Tiesioginės sandaugos reikšmė ir privalumai išplaukia iš tiesioginės sandaugos kriterijaus.

4.6. Teorema (tiesioginės sandaugos kriterijus). *Grupė G yra savo pogrupių A ir B tiesioginė sandauga tada ir tik tada, kai kiekvieną tos grupės elementą g galima vienareikšmiškai užrašyti tų pogrupių elementų sandauga $g = a \cdot b$ ir $x \cdot y = y \cdot x$ $\forall x \in A$, $\forall y \in B$.*

Įrodymas. Būtinumas. Tarkime, $G = A \otimes B$ ir $g \in G$. Iš tiesioginės sandaugos apibrėžimo išplaukia, kad $\exists\, a \in A, b \in B$: $g = a \cdot b$. Įrodysime šio skaidinio vienareikšmiškumą. Taikysime prieštaros būdą. Tarkime, elementą g galima išskaidyti ir kitu būdu: $g = a_1 \cdot b_1$, $a_1 \in A$, $b_1 \in B$. Turime lygybę $a \cdot b = a_1 \cdot b_1$. Padauginę abi šios lygybės puses iš kairės iš a_1^{-1}, o iš dešinės – iš b^{-1}, gauname $a_1^{-1} \cdot a = b_1 \cdot b^{-1}$. Bet $a_1^{-1} \cdot a \in A$, $b_1 \cdot b^{-1} \in B$. Vadinasi, $a_1^{-1} \cdot a$, $b_1 \cdot b^{-1} \in A \cap B = \{e\}$. Todėl $a_1^{-1} \cdot a = e$, $b_1 \cdot b^{-1} = e$. Iš čia $a = a_1$, $b = b_1$. Gavome prieštarą prielaidai. Vadinasi, elementas g išskaidomas elementų iš A ir B sandauga vienareikšmiškai.

Įrodysime, kad $x \cdot y = y \cdot x \quad \forall x \in A, \ \forall y \in B$. Sudarykime sandaugą $x \cdot y \cdot x^{-1} \cdot y^{-1}$. Kadangi $B \lhd G$, iš II-ojo normaliojo daliklio kriterijaus išplaukia, kad $x \cdot y \cdot x^{-1} \in B$. Vadinasi, ir $x \cdot y \cdot x^{-1} \cdot y^{-1} \in B$. Analogiškai $y \cdot x^{-1} \cdot y^{-1} \in A$ ir $x \cdot y \cdot x^{-1} \cdot y^{-1} \in A$. Todėl $x \cdot y \cdot x^{-1} \cdot y^{-1} \in A \cap B = \{e\}$. Gauname lygybę $x \cdot y \cdot x^{-1} \cdot y^{-1} = e$. Padauginę abi šios lygybės puses pirma iš y, po to – iš x, gauname $x \cdot y = y \cdot x$. $\triangle$

Pakankamumas. Tarkime, $\forall g \in G$ yra vienareikšmiškai užrašomas elementų iš A ir B sandauga $g = a \cdot b$, ir $x \cdot y = y \cdot x \quad \forall x \in A, \ \forall y \in B$.

1) Lygybė $G = A \cdot B$ akivaizdi.

2) Įrodysime, kad A yra grupės G normalusis daliklis. Tarkime, $a \in A$, $g \in G$. Turime parodyti, kad $g \cdot a \cdot g^{-1} \in A$. Išskaidome elementą g elementų iš A ir B sandauga – $g = a_1 \cdot b_1$. Todėl $g \cdot a \cdot g^{-1} = a_1 \cdot b_1 \cdot a \cdot (a_1 \cdot b_1)^{-1} = a_1 \cdot b_1 \cdot a \cdot b_1^{-1} \cdot a_1^{-1}$. Bet $b_1 \cdot a = a \cdot b_1$. Vadinasi, $g \cdot a \cdot g^{-1} = a_1 \cdot a \cdot b_1 \cdot b_1^{-1} \cdot a_1^{-1} = a_1 \cdot a \cdot a_1^{-1} \in A$.

Analogiškai įrodome, kad $B \lhd G$.

3) Tarkime, $g \in A \cap B$. Galimi du elemento g skaidiniai elementų iš A ir B sandauga:

$$g = g \cdot e \quad (g \in A, \ e \in B),$$
$$g = e \cdot g \quad (e \in A, \ g \in B).$$

Iš skaidinio vienareikšmiškumo išplaukia lygybė $g = e$. Todėl $A \cap B = \{e\}$. $\triangle$

Pastaba. *Kai G -adicinė grupė, jos skaidinį pogrupiais A ir B vadiname tiesiogine suma ir žymime $G = A \oplus B$.*

Nesunku ir tiesioginės sandaugos apibrėžimą, ir jos kriterijų apibendrinti baigtiniam pogrupių skaičiui.

4.7. Apibrėžimas. *Sakoma, kad grupė G yra savo pogrupių $H_1, H_2, \dots, H_m$ tiesioginė sandauga ir rašoma $G = H_1 \otimes H_2 \otimes \dots \otimes H_m$, kai:*

1) $G = H_1 \cdot H_2 \cdot \ldots \cdot H_m$;

2) $H_i \lhd G, \ i = \overline{1, m}$;

3) $H_i \cap H_i' = \{e\}, \ i = \overline{1, m}$; *čia* $H_i' = H_1 \cdot H_2 \cdot \ldots \cdot H_{i-1} \cdot H_{i+1} \cdot \ldots \cdot H_m$.

4.8. Teorema (tiesioginės sandaugos kriterijus). *Grupė G yra savo pogrupių $H_1, H_2, \dots, H_m$ tiesioginė sandauga tada ir tik tada, kai $\forall g \in G$ vienareikšmiškai užrašomas sandauga $g = h_1 \cdot h_2 \cdot \ldots \cdot h_m$ ($h_i \in H_i$, $i = \overline{1, m}$) ir $h_i \cdot h_j = h_j \cdot h_i \ (i \neq j)$.*

Teorema įrodoma analogiškai 4.6 teoremai.

Apibendrinsime tiesioginės sandaugos sąvoką. Tarkime, A ir B – dvi grupės. Pažymėkime $A \times B$ tų grupių Dekarto sandaugą:

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

Šioje aibėje apibrėžiame algebrinę operaciją:

$$(a,b)\cdot(c,d)=(a\cdot c,b\cdot d)\quad\big((a,b),(c,d)\in A\times B\big).$$

Įrodysime, kad šios operacijos atžvilgiu aibė $A\times B$ sudaro grupę. Iš tikrųjų:

1) operacija asociatyvi –

$$\big(\big((a_1,b_1)\cdot(a_2,b_2)\big)\cdot(a_3,b_3)=(a_1\cdot a_2,b_1\cdot b_2)\cdot(a_3,b_3)=$$
$$(a_1\cdot a_2\cdot a_3,b_1\cdot b_2\cdot b_3)=(a_1,b_1)(a_2\cdot a_3,b_2\cdot b_3)=(a_1,b_1)\big((a_2,b_2)\cdot(a_3,b_3)\big);$$

2) egzistuoja vienetinis elementas (e_1,e_2) (čia e_1 yra grupės A vienetinis elementas, e_2 – grupės B vienetinis elementas) –

$$(a,b)\cdot(e_1,e_2)=(a\cdot e_1,b\cdot e_2)=(a,b)\quad\big(\forall(a,b)\in A\times B\big);$$

3) $\forall(a,b)\in A\times B$ egzistuoja atvirkštinis elementas $(a,b)^{-1}=(a^{-1},b^{-1})$ –

$$(a,b)\cdot(a^{-1},b^{-1})=(a\cdot a^{-1},b\cdot b^{-1})=(e_1,e_2).\ \triangle$$

Įrodysime, kad Dekarto sandaugą $A\times B$ galima išreikšti jos pogrupių $A\times\{e_2\}$ ir $\{e_1\}\times B$ tiesiogine sandauga:

1) Tarkime, $(a\cdot b)\in A\times B$. Tada

$$(a,b)=(a,e_2)\cdot(e_1,b)\in\big(A\times\{e_2\}\big)\cdot\big(\{e_1\}\times B\big).$$

2) Įrodysime, kad $A\times\{e_2\}$ yra grupės $A\times B$ normalusis daliklis. Tarkime, $(a,e_2)\in A\times\{e_2\}$, $(a_1,b_1)\in A\times B$. $\Rightarrow$ $(a_1,b_1)(a,e_2)(a_1,b_1)^{-1}=(a_1,b_1)(a,e_2)(a_1^{-1},b_1^{-1})=$ $=(a_1aa_1^{-1},\,b_1e_2b_1^{-1})=(a_1aa_1^{-1},e_2)\in A\times\{e_2\}$. $\triangle$

Analogiškai įrodoma, kad $\{e_1\}\times B$ yra taip pat grupės $A\times B$ normalusis daliklis.

3) Beliko parodyti, kad pogrupių $A\times\{e_2\}$ ir $\{e_1\}\times B$ sankirta yra vienetinė. Tarkime, $(a,b)\in\big(A\times\{e_2\}\big)\cap\big(\{e_1\}\times B\big)$. Kadangi $(a,b)\in A\times\{e_2\}$, tai $b=e_2$. Taip pat iš elemento (a,b) priklausomumo pogrupiui $\{e_1\}\times B$ išplaukia $a=e_1$. $\Rightarrow$

$$\big(A\times\{e_2\}\big)\cap\big(\{e_1\}\times B\big)=\big\{(e_1,e_2)\big\}.\ \triangle$$

4.9. Apibrėžimas. *Grupių A ir B Dekarto sandauga $A\times B$ yra vadinama jų tiesiogine išorine sandauga.*

Pastaba. *Grupės $A\times B$ pogrupius $A\times\{e_2\}$ ir $\{e_1\}\times B$ izomorfizmo tikslumu galima sutapatinti atitinkamai su grupėmis A ir B.* Iš tikrųjų, parodysime, kad grupė $A\times\{e_2\}$ izomorfiška A. Tuo tikslu apibrėžiame atvaizdį $\varphi: A\times\{e_2\}\to A$ lygybe

$$\varphi\big((a,e_2)\big)=a.$$

Šis atvaizdis – homomorfizmas:

$$\begin{aligned}&\varphi\big((a_1, e_2)(a_2, e_2)\big) = \varphi\big((a_1 a_2, e_2)\big) = a_1 a_2 = \\ &= \varphi\big((a_1, e_2)\big)\, \varphi\big((a_2, e_2)\big) \quad \forall (a_1, e_2), (a_2, e_2) \in A \times \{e_2\}.\end{aligned}$$

Šio homomorfizmo branduolys – vienetinis: jei $(a, e_2) \in \operatorname{Ker} \varphi \Rightarrow$

$$\varphi\big((a, e_2)\big) = a = e_1. \quad \Rightarrow \operatorname{Ker} \varphi = \big\{(e_1, e_2)\big\}.$$

Homomorfizmas – surjektyvus: $\forall a \in A \;\; \exists\, (a, e_2) \in A \times \{e_2\} : \varphi\big((a, e_2)\big) = a. \quad \triangle$

Analogiškai įrodoma, kad $\{e_1\} \times B \cong B$.

5. Baigtinių Abelio grupių struktūra

Ieškosime baigtinių Abelio grupių išraiškos jų pogrupių tiesioginėmis sandaugomis.

5.1. Abelio grupių lema. *Tarkime, Abelio grupės G elemento g eilė $|g|$ yra tarpusavyje pirminių skaičių m ir n sandauga. Tada elementą g galima vienareikšmiškai užrašyti m-tos eilės elemento a ir n-tos eilės elemento b sandauga – $g = ab$.*

Įrodymas. Kadangi m ir n yra tarpusavyje pirminiai skaičiai, egzistuoja sveikųjų skaičių u ir v pora tokia, kad

$$mu + nv = 1.$$

Šios išraiškos dėka elementą g galima užrašyti tokiu būdu:

$$g = g^1 = g^{mu+nv} = g^{nv} \cdot g^{mu}.$$

Pažymėkime $a = g^{nv}$ ir $b = g^{mu}$, ir įsitikinkime, kad elemento a eilė lygi m, o b – n.

Tarkime, $|a| = s$, $|b| = t$. Pakėlę elementą g laipsniu st, gauname:

$$g^{st} = (ab)^{st} = a^{st} \cdot b^{st} = (a^s)^t \cdot (b^t)^s = e.$$

Iš elemento eilės savybių išplaukia, kad $mn \mid st$. Iš lygybių

$$\begin{aligned}a^m &= (g^{nv})^m = g^{mnv} = (g^{mn})^v = e \text{ ir} \\ b^n &= (g^{mu})^n = g^{mnu} = (g^{mn})^u = e\end{aligned}$$

gauname, kad $s \mid m$ ir $t \mid n$. Todėl $st \mid mn$ ir pagaliau $st = mn$. Iš šios lygybės, kadangi $(t, m) = 1$ išplaukia, kad $m \mid s$. Todėl $m = s$ ir $n = t$. Taigi, $|a| = m$ ir $|b| = n$.

Įrodysime tokio skaidinio vienetinumą. Taikysime prieštaros būdą. Tarkime,

$$g = ab = a_1 b_1 \quad \text{ir} \quad |a| = |a_1| = m, \;\; |b| = |b_1| = n.$$

Abi lygybės $ab = a_1b_1$ puses padauginę iš kairės iš a_1^{-1}, ir iš dešinės – iš b^{-1}, turime

$$a_1^{-1}a = b_1b^{-1}.$$

Pažymėję $a_1^{-1}a = c$, paskaičiuojame to elemento eilę. Tarkime $|c| = k$. Iš lygybių

$$c^n = (b_1b^{-1})^n = b_1^n \cdot (b^{-1})^n = b_1^n \cdot (b^n)^{-1} = e \text{ ir}$$
$$c^m = (a_1^{-1}a)^m = (a_1^{-1})^m \cdot a^m = (a_1^m)^{-1} \cdot a^m = e$$

gauname: $k \mid n$ ir $k \mid m$. Vadinasi, $k \mid (m, n)$. Bet $(m, n) = 1$, todėl $k = 1$. Taigi

$$a_1^{-1}a = b_1b^{-1} = e.$$

Iš čia išplaukia lygybės $a = a_1$ ir $b = b_1$. $\triangle$

5.2. Apibendrinta Abelio grupių lema. *Tarkime, Abelio grupės G elemento g eilė $|g|$ yra poromis tarpusavyje pirminių skaičių r_i sandauga – $|g| = r_1r_2 \ldots r_s$ $\big((r_i, r_j) = 1, i \neq j\big)$. Tada elementą g galima vienareikšmiškai užrašyti elementų $g_1, g_2, \ldots, g_s$ sandauga, kur $|g_i| = r_i$, $i = \overline{1, s}$.*

Įrodymas – 5.1 lemos įrodymo apibendrinimas. $\triangle$

5.3. Apibrėžimas. *Tarkime, p – fiksuotas pirminis skaičius. Abelio grupė G vadinama p-primariąja grupe, kai kiekvieno jos elemento eilė yra pirminio skaičiaus p laipsnis.*

5.4. I-oji struktūrinė teorema. *Kiekvieną baigtinę Abelio grupę G galima išskaidyti jos p-primariųjų pogrupių tiesiogine sandauga. Skaidinys užrašomas vienareikšmiškai dauginamųjų tvarkos tikslumu.*

Įrodymas. Tarkime, grupės G eilė $|G| = n$ ir skaičiaus n kanoninis skaidinys pirminių skaičių sandauga yra $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s}$. Parodysime, kad šią grupę galima išskaidyti jos p_i-primariųjų pogrupių tiesiogine sandauga ($i = \overline{1, s}$).

Pažymėkime

$$P_i = \big\{g \in G \mid |g| = p_i^{t_i},\ 0 \leq t_i \leq k_i\big\} \quad (i = \overline{1, s}).$$

Įrodysime, kad P_i yra grupės G pogrupis. Tarkime, $g, h \in P_i$ ir $|g| = p_i^{t_i}$, $|h| = p_i^{u_i}$. Pažymėkime $v_i = \max\{u_i, t_i\}$. Aišku, kad

$g^{p_i^{v_i}} = h^{p_i^{v_i}} = e. \Rightarrow (g \cdot h)^{p_i^{v_i}} = g^{p_i^{v_i}} \cdot h^{p_i^{v_i}} = e. \Rightarrow |gh| \mid p_i^{v_i} \Rightarrow |gh| = p_i^{m_i},\ 0 \leq m_i \leq v_i$ $\Rightarrow gh \in P_i$.

Tarkime, $g \in P_i$ ir $|g| = p_i^{t_i}$. $\Rightarrow |g^{-1}| = p_i^{t_i} \Rightarrow g^{-1} \in P_i$. Taigi P_i – grupės G p_i-primarusis pogrupis. Beliko įrodyti, kad grupė G yra pogrupių P_i tiesioginė sandauga. Tarkime, $g \in G$. Kadangi $|g| \mid |G|$, tai elemento g eilę galima užrašyti tokiu būdu –

$$|g| = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_s^{l_s} \quad (0 \leq l_i \leq k_i,\ i = \overline{1, s}).$$

Pažymėkime $p_i^{l_i} = r_i$. Skaičiai r_i yra poromis tarpusavyje pirminiai, todėl elementui g galima pritaikyti apibendrintąją Abelio lemą: jį galima vienareikšmiškai išreikšti elementų $g_i \in P_i$ sandauga ($|g_i| = p_i^{l_i}$). Teiginio įrodymui tereikia panaudoti apibendrintąjį tiesioginės sandaugos kriterijų. $\triangle$

5.5. II-oji struktūrinė teorema. *p-primariąją Abelio grupę P galima išskaidyti jos ciklinių pogrupių tiesiogine sandauga.*

Įrodymas. Taikysime indukciją grupės P eilės atžvilgiu. Tarkime, grupės P eilė yra n.

1. Kai $n = 1$, teiginys trivialus.

2. Tarkime, teiginys teisingas visoms p-primariosioms grupėms, kurių eilė mažesnė už n. Įrodysime, kad indukcinė prielaida yra teisinga p-primariajai n-tosios eilės grupei P. Pasirinkime grupėje maksimalios eilės elementą a. Tarkime, $|a| = p^k$. Galime laikyti, kad $k \geq 1$, nes kitu atveju grupė P būtų vienetinė. Pažymėkime H ciklinį pogrupį, generuotą elemento a: $H = \langle a \rangle$. Aišku, kad $|H| = |a| = p^k$. Iš Lagranžo teoremos turime

$$|\, P/_H \,| = \frac{|P|}{|H|} = np^{-k}.$$

Taigi faktorgrupės $P/_H$ eilė yra mažesnė už n. Kad šiai grupei galėtumėme taikyti indukcinę prielaidą, įrodysime, jog ji yra p-primarioji grupė. Tarkime $bH \in P/_H$. Kadangi $b \in P$, jo eilė yra pirminio skaičiaus p laipsnis: $|b| = p^m$. Iš lygybės

$$(bH)^{p^m} = b^{p^m} \cdot H = eH = H$$

turime, kad $|bH|$ yra skaičiaus p^m daliklis. Tokiu būdu, $|bH| = p^l$, $l \leq m$. Vadinasi, $P/_H$ yra p-primarioji grupė. Pritaikę šiai grupei indukcinę prielaidą, išskaidome ją ciklinių pogrupių tiesiogine sandauga –

$$P/_H = \langle a_1 H \rangle \otimes \langle a_2 H \rangle \otimes \ldots \otimes \langle a_s H \rangle.$$

Pažymėkime $|a_i H| = |\langle a_i H \rangle| = p^{n_i}$, $i = \overline{1, s}$. Elemento a_i eilė nebūtinai turi būti lygi p^{n_i}. Kiekviename sluoksnyje $a_i H$ surasime atstovą b_i, kurio eilė yra p^{n_i}. Iš lygybės

$$(a_i H)^{p^{n_i}} = H = a_i^{p^{n_i}} H$$

turime, kad elementas $a_i^{p^{n_i}}$ priklauso pogrupiui H. Vadinasi, egzistuoja neneigiamas sveikas skaičius t_i toks, kad $a_i^{p^{n_i}} = a^{t_i}$. Abi šios lygybės puses pakėlę laipsniu p^{k-n_i} gausime lygybę

$$\left(a_i^{p^{n_i}}\right)^{p^{k-n_i}} = \left(a^{t_i}\right)^{p^{k-n_i}} = a_i^{p^k} = a^{t_i \cdot p^{k-n_i}} = e,$$

nes grupėje P maksimalios eilės elementas yra p^k-osios eilės. Vadinasi, $p^k \mid t_i p^{k-n_i}$ ir todėl $p^{n_i} \mid t_i$. Pažymėkime $t_i = p^{n_i} \cdot q_i$, kur q_i – neneigiamas sveikasis skaičius, ir pasirinkime sluoksnyje a_iH atstovą $b_i = a_i \cdot a^{-q_i}$. Parodysime, kad $|b_i| = p^{n_i}$. Iš tikrųjų,

$$b_i^{p^{n_i}} = a_i^{p^{n_i}} \cdot a^{p^{n_i} \cdot (-q_i)} = a^{t_i} \cdot a^{-t_i} = e.$$

Vadinasi, $|b_i| \mid p^{n_i}$. Pažymėkime $|b_i| = p^{m_i}$ ir pakelkime sluoksnį b_iH laipsniu p^{m_i}:

$$(b_iH)^{p^{m_i}} = b_i^{p^{m_i}} \cdot H = H = (a_iH)^{p^{m_i}} = a_i^{p^{m_i}} \cdot H.$$

Vadinasi, $p^{n_i} \mid p^{m_i}$. Iš čia $|b_i| = p^{n_i}$.

Pakeitę faktorgrupės $P/_H$ skaidinyje atstovus a_i sluoksniuose a_iH atstovais b_i, turėsime lygybę

$$P/_H = \langle b_iH \rangle \otimes \langle b_2H \rangle \otimes \ldots \otimes \langle b_sH \rangle.$$

Įsitikinsime, kad grupę P galima išskaidyti taip:

$$P = \langle b_1 \rangle \otimes \langle b_2 \rangle \otimes \ldots \otimes \langle b_s \rangle \otimes \langle a \rangle.$$

Tarkime, $g \in P$. Paėmę sluoksnį gH, išskaidome jį:

$$gH = \big(b_1H\big)^{r_1} \cdot \big(b_2H\big)^{r_2} \cdot \ldots \cdot \big(b_sH\big)^{r_s} = b_1^{r_1}H \cdot b_2^{r_2}H \cdot \ldots \cdot b_s^{r_s}H = b_1^{r_1} \cdot b_2^{r_2} \cdot \ldots \cdot b_s^{r_s} \cdot H.$$

Vadinasi, $g \in b_1^{r_1} \cdot b_2^{r_2} \cdot \ldots \cdot b_s^{r_s} \cdot H$. Todėl g galima užrašyti taip: $g = b_1^{r_1} \cdot b_2^{r_2} \cdot \ldots \cdot b_s^{r_s} \cdot a^l$. Liko įrodyti, kad skaidinys užrašomas vienareikšmiškai. Taikome prieštaros būdą. Tarkime,

$$g = b_1^{r_1} \cdot b_2^{r_2} \cdot \ldots \cdot b_s^{r_s} \cdot a^l = b_1^{r_1'} \cdot b_2^{r_2'} \cdot \ldots \cdot b_s^{r_s'} \cdot a^{l'}. \quad \Rightarrow$$

$$\begin{aligned} gH &= b_1^{r_1} \cdot b_2^{r_2} \cdot \ldots \cdot b_s^{r_s} \cdot a^lH = \\ &= b_1^{r_1}H \cdot b_2^{r_2}H \cdot \ldots \cdot b_s^{r_s} \cdot H = b_1^{r_1'} \cdot b_2^{r_2'} \cdot \ldots \cdot b_s^{r_s'} \cdot a^{l'}H = b_1^{r_1'}H \cdot b_2^{r_2'}H \cdot \ldots \cdot b_s^{r_s'}H. \quad \Rightarrow \end{aligned}$$

$$r_i = r_i', \quad i = \overline{1,s} \text{ (iš sluoksnio } gH \text{ vienareikšmio skaidinio)}$$

$$\Rightarrow \quad g = b_1^{r_1} \cdot b_2^{r_2} \ldots b_s^{r_s} \cdot a^l = b_1^{r_1} \cdot b_2^{r_2} \ldots b_s^{r_s} \cdot a^{l'}. \quad \Rightarrow \ a^l = a^{l'} \ \Rightarrow \ l = l'. \ \triangle$$

5.6. Išvada. *p-primariosios grupės eilė yra pirminio skaičiaus p laipsnis.*

Įrodymas. Iš 5.5 teoremos turime

$$P = \langle b_1 \rangle \otimes \langle b_2 \rangle \otimes \ldots \otimes \langle b_s \rangle \otimes \langle a \rangle,$$

kur $|b_i| = p^{n_i}$, $i = \overline{1,s}$, $|a| = p^k$. Todėl

$$\begin{aligned} |P| &= |\langle b_1 \rangle| \cdot |\langle b_2 \rangle| \cdot |\langle b_s \rangle| \cdot |\langle a \rangle| = \\ &= p^{n_1} \cdot p^{n_2} \cdot \ldots \cdot p^{n_s} \cdot p^k = p^{n_1+n_2+\ldots+n_s+k}. \ \triangle \end{aligned}$$

5.7. Apibrėžimas. *Grupė P vadinama neskaidžia, jei jos negalima užrašyti tikrinių pogrupių tiesiogine sandauga.*

5.8. Lema. *Tarkime, primariosios ciklinės grupės $P = \langle a \rangle$ eilė yra p^k, $k \geq 1$. Tada kiekvienam šios grupės tikriniam pogrupiui priklauso elementas $b = a^{p^{k-1}}$.*

Įrodymas. Tarkime, H – tikrinis grupės P pogrupis. Tada $H = \langle a^s \rangle$, nes ciklinės grupės kiekvienas pogrupis yra ciklinis. Be to, $0 < s < p^k$. Užrašome skaičių s pavidalu $s = p^l \cdot q$, kur $l \geq 0$, $(q, p) = 1$. Kadangi skaičiai p ir q yra tarpusavyje pirminiai, egzistuoja sveikieji skaičiai u ir v tokie, kad $qu + pv = 1$. Pasinaudoję šia išraiška, elementą b galime užrašyti taip:

$$b = b^1 = b^{qu+pv} = \left(a^{p^{k-1}}\right)^{qu+pv} = a^{p^{k-1} \cdot qu} \cdot a^{p^{k-1} \cdot pv} =$$
$$= a^{p^{k-1} \cdot qu} \cdot \left(a^{p^k}\right)^v = a^{p^{k-1} \cdot qu}.$$

Kadangi $s < p^k$, galioja nelygybė $l < k$. Todėl $l \leq k - 1$, arba $k - 1 - l \geq 0$. Remdamiesi šia nelygybe, toliau pertvarkome elemento b išraišką:

$$b = a^{p^{k-1} \cdot qu} = a^{p^{k-1-l+l} \cdot qu} = a^{p^{k-1-l} \cdot p^l \cdot qu} =$$
$$= a^{p^{k-1-l} \cdot su} = \left(a^s\right)^{p^{k-1-l} \cdot u} \in H. \quad \triangle$$

5.9. Teorema. *Primarioji ciklinė grupė yra neskaidi.*

Įrodymas. Taikysime prieštaros būdą. Tarkime, $|P| = p^k$, $P = \langle a \rangle$ ir grupę P galima išskaidyti jos tikrinių pogrupių A ir B tiesiogine sandauga: $P = A \otimes B$. Tuomet iš 5.8 lemos išplaukia, kad elementas $b = a^{p^{k-1}}$ priklauso ir pogrupiui A, ir pogrupiui B. Skiriame du atvejus.

1. $k = 1$. Tuomet $|P| = p$. Bet pirminės eilės grupė neturi iš viso tikrinių pogrupių. Gauname prieštarą.

2. $k \geq 2$. Tuomet $|b| > 1$, $b \in A \cap B = \{e\}$. Prieštara. $\triangle$

5.10. III-oji struktūrinė teorema. *Jeigu p-primariąją grupę galima užrašyti jos ciklinių pogrupių tiesiogine sandauga dviem būdais, tai šių skaidinių dauginamųjų skaičius yra vienodas ir, atitinkamai sutvarkius ciklinių pogrupių eiles, šie pogrupiai poromis bus izomorfiški.*

Įrodymas. Tarkime, grupę P galima išskaidyti jos ciklinių pogrupių tiesiogine sandauga dvejopai–

$$P = \langle a_1 \rangle \otimes \langle a_2 \rangle \otimes \ldots \otimes \langle a_s \rangle \quad \text{ir}$$
$$P = \langle b_1 \rangle \otimes \langle b_2 \rangle \otimes \ldots \otimes \langle b_t \rangle.$$

Pažymėkime $|a_i| = p^{k_i}$, $i = \overline{1, s}$ ir $|b_j| = p^{l_j}$, $j = \overline{1, t}$ ir laikykime, kad $p^{k_1} \geq p^{k_2} \geq \ldots \geq p^{k_s}$, ir $p^{l_1} \geq p^{l_2} \geq \ldots \geq p^{l_t}$.

1. Įrodysime, kad $s = t$. Pažymėkime

$$P^* = \{g \in P \mid g^p = e\}.$$

Įrodysime, kad P^* yra grupės P pogrupis. Tarkime, $g, h \in P^* \Rightarrow g^p = h^p = e \Rightarrow (gh)^p = g^p \cdot h^p = e \cdot e = e \Rightarrow gh \in P^*$. Tarkime, $g \in P^* \Rightarrow g^p = e \Rightarrow (g^{-1})^p = (g^p)^{-1} = e^{-1} = e \Rightarrow g^{-1} \in P^*$. Taigi, P^* yra grupės P pogrupis. Surasime šio pogrupio išraišką jo ciklinių pogrupių tiesiogine sandauga. Pažymėkime

$$H = \langle a_1^{p^{k_1-1}} \rangle \otimes \langle a_2^{p^{k_2-1}} \rangle \otimes \ldots \otimes \langle a_s^{p^{k_s-1}} \rangle.$$

Kadangi elemento a_i $(i = \overline{1,s})$ eilė yra p^{k_i}, tai elemento $a_i^{p^{k_i-1}}$ eilė yra p. Todėl $|H| = p^s$. Parodysime, kad pogrupis P^* sutampa su H. Tarkime, $g \in P^*$. Tada $g^p = e$. Elementą g galima užrašyti elementų a_i laipsnių sandauga: $g = a_1^{r_1} \cdot a_2^{r_2} \cdot \ldots \cdot a_s^{r_s}$. Pakėlę abi šios lygybės puses p-tuoju laipsniu, gauname lygybę

$$g^p = e = a_1^{pr_1} \cdot a_2^{pr_2} \cdot \ldots \cdot a_s^{pr_s} = \underbrace{e \cdot e \cdot \ldots \cdot e}_{s\,\text{kartų}}.$$

Iš elemento e skaidinio vienareikšmiškumo gauname lygybę $a_i^{pr_i} = e$ $(i = \overline{1,s})$. Iš čia $p^{k_i} \,|\, pr_i$ arba $p^{k_i-1} \,|\, r_i$. Vadinasi, egzistuoja natūralusis skaičius q_i toks, kad $r_i = p^{k_i-1} \cdot q_i$. Pertvarkome elemento g išraišką:

$$\begin{aligned} g &= a_1^{r_1} \cdot a_2^{r_2} \cdot \ldots \cdot a_s^{r_s} = a_1^{p^{k_1-1} \cdot q_1} \cdot a_2^{p^{k_2-1} \cdot q_2} \cdot \ldots \cdot a_s^{p^{k_s-1} \cdot q_s} = \\ &= \left(a_1^{p^{k_1-1}}\right)^{q_1} \cdot \left(a_2^{p^{k_2-1}}\right)^{q_2} \cdot \ldots \cdot \left(a_s^{p^{k_s-1}}\right)^{q_s} \in H. \end{aligned}$$

Vadinasi, $P^* \subset H$. Tarkime, $g \in H$:

$$g = \left(a_1^{p^{k_1-1}}\right)^{v_1} \cdot \left(a_2^{p^{k_2-1}}\right)^{v_2} \cdot \ldots \cdot \left(a_s^{p^{k_s-1}}\right)^{v_s}.$$

Pakeliame abi šios lygybės puses p-tuoju laipsniu:

$$\begin{aligned} g^p &= \left(a_1^{p^{k_1-1}}\right)^{pv_1} \cdot \left(a_2^{p^{k_2-1}}\right)^{pv_2} \cdot \ldots \cdot \left(a_s^{p^{k_s-1}}\right)^{pv_s} = \\ &\left(a_1^{p^{k_1}}\right)^{v_1} \cdot \left(a_2^{p^{k_2}}\right)^{v_2} \cdot \ldots \cdot \left(a_s^{p^{k_s}}\right)^{v_s} = e. \end{aligned}$$

Tokiu būdu, $g \in P^*$. Vadinasi, $H \subset P^*$ ir $P^* = H$. Analogiškai įrodome, kad pogrupis P^* sutampa su pogrupiu

$$H' = \langle b_1^{p^{l_1-1}} \rangle \otimes \langle b_2^{p^{l_2-1}} \rangle \otimes \ldots \otimes \langle b_t^{p^{l_t-1}} \rangle.$$

Bet $|H'| = p^t$. Todėl $p^s = p^t$ ir $s = t$. $\triangle$

2. Įrodysime, kad $k_i = l_i$ $(i = \overline{1,s})$. Iš čia išplauks antrasis teoremos teiginys, nes vienodų eilių ciklinės grupės yra izomorfiškos. Taikysime indukciją grupės P eilės atžvilgiu.

1) Tarkime, $|P| = p$. Tuomet teiginys trivialus, nes grupė P tikrinių pogrupių neturi.

2) Tarkime, teiginys yra teisingas kiekvienam grupės P tikriniam pogrupiui. Išskirsime tikrinį pogrupį, kad galėtumėme jam pritaikyti indukcinę prielaidą. Pažymėkime $P_* = \{g^p \mid g \in P\}$. Parodysime, kad P_* yra grupės P tikrinis pogrupis.

Tarkime, $g, h \in P_*$. Vadinasi, egzistuoja $g_1, h_1 \in P$: $g = g_1^p$, $h = h_1^p$. Todėl $g \cdot h = g_1^p \cdot h_1^p = (g_1 h_1)^p$. Taigi, $gh \in P_*$.

Tarkime, $g \in P_*$. Egzistuoja $g_1 \in P$: $g = g_1^p$. Tuomet $g^{-1} = \left(g_1^p\right)^{-1} = \left(g_1^{-1}\right)^p$. Vadinasi, $g^{-1} \in P_*$ ir P_* yra grupės P pogrupis.

Įrodysime, kad P^* nesutampa su P. Pasirinkę grupėje P maksimalios eilės elementą a $(|a| = p^k,\ k \geq 1)$, parodysime, kad $a \notin P_*$. Tarkime priešingai, $a \in P_*$. Tuomet egzistuoja $g \in P$: $a = g^p$. Tokiu atveju elemento g eilė $|g| > p^k$, o tai yra prieštara elemento a pasirinkimui. Tam, kad galėtumėme pogrupiui P_* pritaikyti indukcinę prielaidą, išskaidysime šį pogrupį ciklinių pogrupių tiesiogine sandauga dviem būdais. Pažymėkime $F = \langle a_1^p \rangle \otimes \langle a_2^p \rangle \otimes \ldots \otimes \langle a_i^p \rangle$, kur skaičius i parenkamas iš sąlygų $k_1 \geq k_2 \geq \ldots \geq k_i > k_{i+1} = \ldots = k_s = 1$. Įsitikinsime, kad pogrupis F sutampa su P_*.

Tarkime, $g \in F$. Vadinasi,

$$\begin{aligned} g &= \left(a_1^p\right)^{r_1} \cdot \left(a_2^p\right)^{r_2} \cdot \ldots \cdot \left(a_i^p\right)^{r_i} = \\ &= \left(a_1^{r_1}\right)^p \cdot \left(a_2^{r_2}\right)^p \cdot \ldots \cdot \left(a_i^{r_i}\right)^p = \left(a_1^{r_1} \cdot a_2^{r_2} \cdot \ldots \cdot a_i^{r_i}\right)^p = h^p, \end{aligned}$$

kur $h = a_1^{r_1} \cdot a_2^{r_2} \cdot \ldots \cdot a_i^{r_i}$. Vadinasi, $g \in P_*$ ir $F \subset P_*$.

Tarkime, $g \in P_*$. Egzistuoja $h \in P$: $g = h^p$. Elementą h užrašome elementų a_i $(i = \overline{1,s})$ laipsnių sandauga: $h = a_1^{r_1} \cdot a_2^{r_2} \cdot \ldots \cdot a_i^{r_i} \cdot a_{i+1}^{r_{i+1}} \cdot \ldots \cdot a_s^{r_s}$. Iš indekso i pasirinkimo išplaukia lygybės $a_{i+1}^p = a_{i+2}^p = \ldots = a_s^p = e$. Todėl

$$\begin{aligned} g &= h^p = a^{r_1 p} \cdot a^{r_2 p} \cdot \ldots \cdot a_i^{r_i p} \cdot a_{i+1}^{r_{i+1} p} \cdot \ldots \cdot a_s^{r_s p} = \\ &= a^{r_1 p} \cdot a^{r_2 p} \cdot \ldots \cdot a_i^{r_i p} = \left(a_1^p\right)^{r_1} \cdot \left(a_2^p\right)^{r_2} \cdot \ldots \cdot \left(a_i^p\right)^{r_i} \in F. \end{aligned}$$

Vadinasi, $P^* \subset F$ ir P^* sutampa su F.

Pažymėję $F' = \langle b_1^p \rangle \otimes \langle b_2^p \rangle \otimes \ldots \otimes \langle b_j^p \rangle$, kur j skaičius yra parenkamas iš sąlygų $l_1 \geq l_2 \geq \ldots \geq l_j > l_{j+1} = \ldots = l_s = 1$, analogiškai gauname kitą pogrupio P_* išraišką:

$$P_* = \langle b_1^p \rangle \otimes \langle b_2^p \rangle \otimes \ldots \otimes \langle b_j^p \rangle.$$

Taikydami pogrupiui P_* indukcinę prielaidą, gauname lygybes $i = j$ ir

$$\begin{aligned} k_1 - 1 &= l_1 - 1, \\ k_2 - 1 &= l_2 - 1, \\ &\ldots\ldots\ldots\ldots \\ k_i - 1 &= l_i - 1. \end{aligned}$$

Todėl $k_t = l_t$, kai $t = \overline{1, i}$ ir $k_t = l_t = 1$, kai $t = \overline{i + 1, s}$. $\triangle$

Tarkime, P yra p-primarioji p^n-osios eilės Abelio grupė. Atsakysime į klausimą, keliais būdais šią grupę galima išskaidyti ciklinių pogrupių tiesiogine sandauga taip, kad skaidiniai nebūtų izomorfiški. Tarkime, $P = \langle a_1 \rangle \otimes \langle a_2 \rangle \otimes \ldots \otimes \langle a_s \rangle$ yra vienas iš galimų skaidinių. Pažymėkime $|a_i| = |\langle a_i \rangle| = p^{n_i}$ $(i = \overline{1, s})$. Rodikliai n_i turi tenkinti sąlygas

$$n_1 + n_2 + \ldots + n_s = n, \tag{1}$$

$$n_1 \geq n_2 \geq \ldots \geq n_s > 0. \tag{2}$$

Kiek bus (1) lygties sprendinių su natūraliosiomis komponentėmis, tenkinančių (2) sąlygas, tiek bus p^n-osios eilės neizomorfiškų p-primariųjų grupių. Tai išplaukia iš III-iosios struktūrinės teoremos.

Ciklinių pogrupių $\langle a_1 \rangle, \langle a_2 \rangle, \ldots, \langle a_s \rangle$ eilės $p^{n_1}, p^{n_2}, \ldots, p^{n_s}$ yra vadinamos p-primariosios Abelio grupės invariantais.

5.11. Pavyzdys. Užrašysime visas neizomorfiškas 16-osios eilės Abelio grupes. Ieškome lygties

$$n_1 + n_2 + \ldots + n_s = 4$$

sprendinių su natūraliosiomis komponentėmis, tenkinančių sąlygas

$$n_1 \geq n_2 \geq \ldots \geq n_s.$$

Galimi atvejai:

1) kai $s = 1$, tai $n_1 = 4$;

2) kai $s = 2$, tai arba $n_1 = 3$, $n_2 = 1$, arba $n_1 = n_2 = 2$;

3) kai $s = 3$, tai $n_1 = 2$, $n_2 = n_3 = 1$;

4) kai $s = 4$, tai $n_1 = n_2 = n_3 = n_4 = 1$;

5) kai $s \geq 5$, lygtis sprendinių neturi.

Šias penkias rodiklių sistemas atitiks penki skirtingi skaidiniai:

1) $P = Z_{16}$;

2) $P = Z_8 \otimes Z_2$;

3) $P = Z_4 \otimes Z_4$;

4) $P = Z_4 \otimes Z_2 \otimes Z_2$;

5) $P = Z_2 \otimes Z_2 \otimes Z_2 \otimes Z_2$.

Iš III-iosios struktūrinės teoremos išplaukia, kad bet kuri 16-osios eilės Abelio grupė yra izomorfiška vienam iš šių penkių skaidinių.

6. Dvi izomorfizmo teoremos

6.1. I-oji izomorfizmo teorema. *Tarkime, H yra grupės G normalusis daliklis, T – pogrupis. Tada TH yra grupės G pogrupis, $H \cap T$ – pogrupio T normalusis daliklis, ir faktorgrupės $TH/_H$ bei $T/_{T \cap H}$ yra izomorfiškos.*

Įrodymas. Kadangi H yra grupės G normalusis daliklis, lygybė $HT = TH$ išplaukia iš II-ojo normaliojo daliklio kriterijaus. Parodysime, kad $H \cap T \triangleleft T$. Tarkime, $h_t \in H \cap T$, $t \in T$. Tuomet:

1) $th_tt^{-1} \in T$, nes $t \in T$, $h_t \in T$;

2) $th_tt^{-1} \in H$, nes $h_t \in H$ ir $H \triangleleft G$.

Todėl $hh_tt^{-1} \in H \cap T$ ir teiginio įrodymui pakanka pasinaudoti II-uoju normaliojo daliklio kriterijumi.

Kadangi $H \triangleleft TH$ ir $T \cap H \triangleleft H$, galime apibrėžti faktorgrupes $TH/_H$ ir $T/_{T \cap H}$. Apibrėžkime atvaizdį

$$\varphi : TH/_H \to T/_{T \cap H}$$

lygybe

$$\varphi(thH) = tT \cap H \quad (\forall t \in T, \ \forall h \in H).$$

Pirmiausia įrodysime, kad atvaizdis yra apibrėžtas korektiškai, t. y. apibrėžimas nepriklauso nuo atstovų pasirinkimo. Tarkime, $t'h'$ yra kitas sluoksnio thH atstovas, t. y. $t'h'H = thH$. Tuomet $\varphi(t'h'H) = t'T \cap H$. Atvaizdis bus apibrėžtas korektiškai, jei įrodysime, kad $\varphi(thH) = \varphi(t'h'H)$, t. y. $tT \cap H = t'T \cap H$. Kadangi $h, h' \in H$, iš lygybės $thH = t'h'H$ turime $tH = t'H$. Elementas t priklauso sluoksniui tH, vadinasi, ir $t'H$. Todėl egzistuoja $h_1 \in H$: $t = t'h_1$. Padauginę abi šios lygybės puses iš kairės iš ${t'}^{-1}$, turime $h_1 = {t'}^{-1} \cdot t \in T$. Vadinasi, $h_1 \in T \cap H$. Todėl $t \in t'T \cap H$ ir $\big(tT \cap H\big) \cap \big(t'T \cap H\big) \neq \emptyset$. Kadangi sluoksniai $tT \cap H$ ir $t'T \cap H$ kertasi netuščiai, tai jie sutampa.

Parodysime, kad atvaizdis φ yra grupių izomorfizmas.

1) φ – homomorfizmas. Iš tikrųjų,

$$\begin{aligned}
&\varphi\big(t_1h_1H \cdot t_2h_2H\big) = \varphi\big(t_1H \cdot t_2H\big) = \\
&= \varphi\big(t_1t_2H\big) = t_1t_2T \cap H = t_1T \cap Ht_2T \cap H = \\
&= \varphi\big(t_1h_1H\big)\,\varphi\big(t_2h_2H\big) \quad \big(\forall t_1h_1H, \, t_2h_2H \in TH/_H\big). \quad \triangle
\end{aligned}$$

2) φ – injekcija. Tarkime $thH \in \operatorname{Ker}\varphi$:

$$\begin{array}{ccc}
\varphi(thH) & = & T \cap H \\
\| & & // \\
tT \cap H. & &
\end{array}$$

Vadinasi, $t \in T \cap H$. Todėl $t \in H$ ir $thH = tH = H$. Taigi $\operatorname{Ker} \varphi = \{H\}$. $\triangle$

3) φ – surjekcija. Iš tikrųjų, sluoksnio $tT \cap H$ pirmvaizdžiu yra sluoksnis teH: iš atvaizdžio φ apibrėžimo išplaukia lygybė $\varphi(teH) = tT \cap H$. $\triangle$

6.2. II-oji izomorfizmo teorema. *Tarkime, H yra grupės G normalusis daliklis, T – faktorgrupės G/H normalusis daliklis, φ – grupės G kanoninis homomorfizmas grupėje G/H. Tada pogrupio T pirmvaizdis $\varphi^{-1}(T)$ yra grupės G normalusis daliklis ir faktorgrupės $G/\varphi^{-1}(T)$ bei $\varphi(G)/T$ izomorfiškos.*

Įrodymas. Pirmiausia įrodysime, kad pirmvaizdis $\varphi^{-1}(T)$ yra grupės G normalusis daliklis.

Tarkime, $g_1, g_2 \in \varphi^{-1}(T)$. Tuomet $\varphi(g_1), \varphi(g_2) \in T$. Kadangi $T < G$, tai $\varphi(g_1) \cdot \varphi(g_2) \in T$. Bet $\varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2)$. Vadinasi, $\varphi(g_1 g_2) \in T$. Iš čia $g_1 g_2 \in \varphi^{-1}(T)$.

Tarkime, $g \in \varphi^{-1}(T)$. Tada $\varphi(g) \in T$ ir $\big(\varphi(g)\big)^{-1} = \varphi(g^{-1}) \in T$. Todėl $g^{-1} \in \varphi^{-1}(T)$. Vadinasi, $\varphi^{-1}(T)$ yra grupės G pogrupis.

Tarkime, $g \in \varphi^{-1}(T)$, $a \in G$. Tada $\varphi(aga^{-1}) = \varphi(a)\varphi(g)\varphi(a)^{-1} \in T$, nes $\varphi(g) \in T$ ir $T \lhd G/H$. Todėl $aga^{-1} \in \varphi^{-1}(T)$ ir iš II-ojo normaliojo daliklio kriterijaus išplaukia, kad $\varphi^{-1}(T)$ yra grupės G normalusis daliklis. Vadinasi, grupę G šiuo normaliuoju dalikliu galime faktorizuoti. Apibrėžkime atvaizdį

$$f : G/\varphi^{-1}(T) \to \varphi(G)/T$$

lygybe

$$f\big(g\varphi^{-1}(T)\big) = \varphi(g)T.$$

Parodysime, kad šis atvaizdis yra apibrėžtas korektiškai. Tarkime, sluoksniai $g'\varphi^{-1}(T)$ ir $g\varphi^{-1}(T)$ yra lygūs. Parodysime, kad ir jų vaizdai $f\big(g'\varphi^{-1}(T)$ ir $f\big(g\varphi^{-1}(T)\big)$ sutampa. Tam pakanka įrodyti, kad sluoksniai $\varphi(g)T$ ir $\varphi(g')T$ kertasi netuščiai. Iš lygybės $g'\varphi^{-1}(T) = g\varphi^{-1}(T)$ gauname, kad $g = g' \cdot g_1$, kur $g_1 \in \varphi^{-1}(T)$. Pažymėkime $\varphi(g_1) = t \in T$. Turime $\varphi(g) = \varphi(g' \cdot g_1) = \varphi(g') \cdot t \in \varphi(g')T$. Bet $\varphi(g) \in \varphi(g)T$. Vadinasi, sluoksniai $\varphi(g')T$ ir $\varphi(g)T$ kertasi netuščiai ir todėl sutampa.

Įrodysime, kad atvaizdis f yra izomorfizmas.

1) f – homomorfizmas. Iš tikrųjų,

$$\begin{aligned} &f\big(g_1\varphi^{-1}(T)g_2\varphi^{-1}(T)\big) = f\big(g_1 g_2\varphi^{-1}(T)\big) = \\ &= \varphi(g_1g_2)T = \varphi(g_1)\varphi(g_2)T = \varphi(g_1)T\,\varphi(g_2)T = \\ &= f\big(g_1\varphi^{-1}(T)\big)f\big(g_2\varphi^{-1}(T)\big) \quad \big(\forall g_1\varphi^{-1}(T),\ g_2\varphi^{-1}(T) \in G/\varphi^{-1}(T)\big). \quad \triangle \end{aligned}$$

2) f – injekcija. Tarkime, $g\varphi^{-1}(T) \in \operatorname{Ker} f$. Todėl

$$\begin{array}{ccc} f\big(g\varphi^{-1}(T)\big) & = & T \\ \backslash\backslash & & // \\ & \varphi(g)T & \end{array}$$

Vadinasi, $\varphi(g) \in T$ ir $g \in \varphi^{-1}(T)$. Taigi $g\varphi^{-1}(T) = \varphi^{-1}(T)$ ir $\operatorname{Ker} f = \{\varphi^{-1}(T)\}$. $\triangle$

3) f – surjekcija. Iš tikrųjų, sluoksnio $\varphi(g)T$ pirmvaizdžiu iš atvaizdžio f apibrėžimo yra sluoksnis $g\varphi^{-1}(T)$:

$$f\big(g\varphi^{-1}(T)\big) = \varphi(g)T. \quad \triangle$$

7. Grupės sudaromosios

7.1. Apibrėžimas. *Tarkime, S yra grupės G poaibis. Sakome, kad aibė S generuoja pogrupį $\langle S\rangle$, jei jis yra minimalus pogrupis, kuriam priklauso ta aibė, t. y., jei S yra pogrupio T poaibis, tai $\langle S\rangle \subset T$.*

Aibė S yra vadinama pogrupio $\langle S\rangle$ *sudaromųjų aibe.*

7.2. Teorema. *Kiekvienam grupės G poaibiui S egzistuoja minimalusis pogrupis $\langle S\rangle$.*

Įrodymas. Pažymėkime visų grupės G pogrupių H, kuriems priklauso aibė S, sankirtą

$$\langle S\rangle = \bigcap_{S\subset H} H.$$

Kadangi pogrupių sankirta yra pogrupis, teoremos įrodymui pakanka patikrinti $\langle S\rangle$ minimalumo sąlygą. Tarkime, T yra pogrupis, kuriam priklauso aibė S. Tada T įeina į sankirtą

$$\bigcap_{S\subset H} H = \langle S\rangle.$$

Iš aibių sankirtos savybės išplaukia, kad $\langle S\rangle \subset T$. $\triangle$

7.3. Teorema. *Minimalusis pogrupis $\langle S\rangle$ sutampa su aibe T, kurią sudaro vienetinis elementas e ir visos galimos sandaugos $t_1t_2\dots t_n$, $n \in N$, kur arba $t_i \in S$, arba $t_i^{-1} \in S$, $i = \overline{1,n}$.*

Įrodymas. Iš aibės T apibrėžimo išplaukia, kad $S \subset T$. Įrodysime pirmiausia, kad T yra pogrupis.

Tarkime, $g, h \in T$. Vadinasi, $g = t_1t_2\dots t_k$, $h = t_{k+1}t_{k+2}\dots t_l$, kur arba $t_i \in S$, arba $t_i^{-1} \in S$. Tuomet $g \cdot h = t_1t_2\dots t_kt_{k+1}\dots t_l \in T$.

Tarkime, $g \in T$. Vadinasi, $g = t_1t_2\dots t_k$ ir arba $t_i \in S$, arba $t_i^{-1} \in S$. Tuomet $g^{-1} = t_k^{-1}t_{k-1}^{-1}\dots t_2^{-1}t_1^{-1}$ ir arba $t_i^{-1} \in S$, arba $\big(t_i^{-1}\big)^{-1} = t_i \in S$. Vadinasi, T yra grupės G pogrupis. Parodysime, kad T sutampa su minimaliuoju pogrupiu $\langle S\rangle$. Kadangi $S \subset T$, tai pogrupis T įeina į pogrupio $\langle S\rangle$, kaip pogrupių sankirtą. Taigi $\langle S\rangle \subset T$. Įrodysime, kad pogrupis T priklauso kiekvienam tos sankirtos nariui, o tuo pačiu ir visai sankirtai. Iš čia išplauks ir teoremos įrodymas. Tarkime, H yra bet kuris pogrupis, kuriam priklauso aibė

S. Imkime $t \in T$. Tuomet $t = t_1 t_2 \dots t_n$, kur arba $t_i \in S$, arba $t_i^{-1} \in S$. Bet kuriuo atveju $t_i \in H$. Iš tikrųjų, jei $t_i \in S$, tai trivialu. Tarkime, $t_i \notin S$. Vadinasi, $t_i^{-1} \in S$. Tuo būdu $t_i^{-1} \in H$. Bet H – pogrupis, todėl $\left(t_i^{-1}\right)^{-1} = t_i \in H$. Taigi $t \in H$ ir tuo pačiu $T \subset \langle S \rangle$. $\triangle$

7.4. Pavyzdžiai. 1. Parodysime, kad simetrinė grupė S_n yra generuojama transpozicijų $(12), (13), \dots, (1n)$:

$$S_n = \langle \{(12), (13), \dots, (1n)\} \rangle.$$

Kadangi transpozicija (ij) sutampa su savo atvirkštine transpozicija, pakanka įrodyti, kad bet kokį ciklą $(a_1 a_2 \dots a_k)$ galima užrašyti transpozicijų $(12), (13), \dots, (1n)$ sandauga. Įrodymas išplaukia iš lygybių

$$(a_1 a_2 \dots a_k) = (a_1 a_2)(a_1 a_3) \dots (a_1 a_k) \quad \text{ir}$$

$$(ij) = (1i)(1j)(1i). \quad \triangle$$

2. Parodysime, jog ženklo keitimo pogrupis A_n yra generuojamas ciklų $(123), (124), \dots, (12n)$:

$$A_n = \langle \{(123), (124), \dots, (12n)\} \rangle.$$

Tarkime, σ – lyginis keitinys. Kadangi transpozicija yra nelyginis keitinys, tai σ-os skaidinyje transpozicijomis jų turi būti lyginis skaičius. Kiekvieną tokią transpozicijų porą $(1i)(1j)$ galima užrašyti trijų skaičių ciklu $(1ij)$.

Išskaidysime ciklą $(1ij)$ ciklų pavidalo $(12k)$ sandauga. Jei $i = 2$, nėra ko skaidyti. Jei $i \neq 2$, $j = 2$, tai $(1i2) = (12i)(12i)$. Jei $i, j \neq 2$, tai $(1ij) = (12j)(12i)(12j)(12j)$. $\triangle$

7.5. Apibrėžimai. 1. *Dviejų grupės G elementų g ir h komutatoriumi vadiname elementą $[g, h] = ghg^{-1}h^{-1}$.*

2. *Grupės G komutantu arba 1-ąja išvestine vadiname pogrupį, generuotą visų tos grupės komutatorių ir žymime $[G, G]$ arba $G^{(1)}$:*

$$[G, G] = G^{(1)} = \langle \{[g, h] \mid g, h \in G\} \rangle.$$

3. *Grupės G k-osios eilės išvestine vadiname $(k-1)$-osios išvestinės komutantą ir žymime*

$$G^{(k)} = \left[G^{(k-1)}, G^{(k-1)}\right].$$

8. Normaliosios ir kompozicinės eilutės

8.1. Apibrėžimas. 1. *Grupės G normaliąja eilute vadinama eilutė*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_m = \{e\},$$

kur G_{i+1} yra pogrupio G_i normalusis daliklis ($i = \overline{0, m-1}$).

2. *Normaliosios eilutės faktoriumi yra vadinama faktorgrupė G_i/G_{i+1} ($i = \overline{0, m-1}$).*

3. *Normaliosios eilutės eile vadinamas jos faktorių skaičius.*

8.2. Pavyzdžiai. 1. Kiekviena grupė turi bent vieną normaliąją eilutę, pvz.,

$$G \supset \{e\}.$$

2. Simetrinės grupės S_3 normalioji eilutė:

$$S_3 \supset A_3 \supset \{(1)\}$$

(A_3 – lyginių keitinių pogrupis).

3. Simetrinės grupės S_4 normaliosios eilutės:

$$S_4 \supset H_1 \supset H_3 \supset \{(1)\},$$
$$S_4 \supset A_4 \supset H_1 \supset H_2 \supset \{(1)\}.$$

Čia A_4 – lyginių keitinių pogrupis,

$$H_1 = \big\{(1), (12)(34), (13)(24), (14)(23)\big\},$$
$$H_2 = \big\{(1), (12)\big\},$$
$$H_3 = \big\{(1), (13)\big\}.$$

4. Tarkime, $G = \langle a \rangle$ – begalinė ciklinė grupė. Viena galimų normaliųjų eilučių –

$$G \supset \langle a^2 \rangle \supset \langle a^4 \rangle \supset \ldots \langle a^{2^m} \rangle \supset \ldots \supset \{e\}.$$

8.3. Apibrėžimas. 1. *Normalioji eilutė*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_m = \{e\},$$

kurioje $G_{i+1} \subsetneq G_i$ ($i = \overline{0, m-1}$), vadinama eilute be pasikartojimų.

2. *Grupės G normalioji eilutė*

$$G = G_0 \supset \ldots \supset G_1 \supset \ldots G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset G_r = \{e\} \tag{1}$$

yra vadinama normaliosios eilutės

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_m = \{e\} \qquad (2)$$

papildymu, jei kiekvienas (2)-osios eilutės narys G_i įeina į (1)-ąją eilutę. Žymėsime (2) $\uparrow$ (1).

8.4. Pavyzdys. Eilutė

$$S_4 \supset A_4 \supset H_1 \supset H_2 \supset \{(1)\}$$

yra eilutės

$$S_4 \supset H_1 \supset \{(1)\}$$

papildymas.

8.5. Apibrėžimas. *Grupės G kompozicine eilute yra vadinama jos normalioji eilutė, kurios negalima papildyti be pasikartojimų.*

Grupė gali ir neturėti kompozicinės eilutės, pavyzdžiui, begalinė ciklinė grupė.

8.6. Apibrėžimas. *Grupė, neturinti tikrinių normaliųjų daliklių, yra vadinama pirmine.*

8.7. Kompozicinės eilutės kriterijus. *Normalioji eilutė yra kompozicinė tada ir tik tada, kai kiekvienas jos faktorius yra pirminis.*

Įrodymas. Būtinumas. Taikysime prieštaros būdą. Tarkime, eilutė

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_i \supset G_{i+1} \ldots \supset G_r = \{e\} \qquad (1)$$

yra kompozicinė, o kuris nors faktorius, pavyzdžiui, G_i/G_{i+1}, nėra pirminis. Vadinasi, egzistuoja šio faktoriaus tikrinis normalusis daliklis H. Tarkime, $\varphi : G_i \to G_i/G_{i+1}$ yra kanoninis homomorfizmas. Kadangi H yra grupės G_i/G_{i+1} normalusis daliklis, iš II-osios izomorfizmo teoremos išplaukia, kad šio pogrupio pirmvaizdis $\varphi^{-1}(H)$ yra grupės G_i normalusis daliklis. Parodysime, kad $\varphi^{-1}(H)$ yra tikrinis grupės G_i pogrupis. Iš tikrųjų, jeigu $\varphi^{-1}(H) = G_i$, tai $H = \varphi(G_i) = G_i/G_{i+1}$, bet iš H pasirinkimo turime, kad jis nesutampa su G_i/G_{i+1}. Jeigu $\varphi^{-1}(H) = \{e\}$, tai $H = G_{i+1}$. Tokiu būdu H būtų vienetinis grupės G_i/G_{i+1} elementas, kas vėlgi prieštarauja H pasirinkimui. Vadinasi, $\{e\} \subsetneq \varphi^{-1}(H) \subsetneq G_i$. Tokiu būdu, $\varphi^{-1}(H) \triangleleft G_i$. O tai reiškia, kad (1)-ąją eilutę galima papildyti be pasikartojimų:

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_i \supsetneq \varphi^{-1}(H) \supsetneq G_{i+1} \supset \ldots \supset G_r = \{e\}, \qquad (2)$$

kas prieštarauja sąlygai, kad (1)-oji eilutė yra kompozicinė. $\triangle$

Pakankamumas. Tarkime, visi eilutės

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_r = \{e\} \tag{3}$$

faktoriai yra pirminiai, o ši eilutė nėra kompozicinė. Vadinasi, ją galima papildyti be pasikartojimų. Tarkime, papildome (3)-iąją eilutę nariu H:

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_i \supsetneq H \supsetneq G_{i+1} \supset \ldots \supset G_r = \{e\}. \tag{4}$$

Pažymėkime φ grupės G_i kanoninį homomorfizmą faktorgrupėje G_i/G_{i+1}. Tada pogrupio H vaizdas $\varphi(H)$ yra šios faktorgrupės normalusis daliklis. Kadangi faktorgrupė G_i/G_{i+1} tikrinių normaliųjų daliklių neturi, galimi du atvejai:

1) $\varphi(H) = G_i/G_{i+1}$. Tada $H = \varphi^{-1}\big(G_i/G_{i+1}\big) = G_i$, o tai yra prieštara H pasirinkimui;

2) $\varphi(H) = G_{i+1}$. Tada $H \subset \operatorname{Ker}\varphi = G_{i+1}$, ir $H = G_{i+1}$ – prieštara.

Iš abiem atvejais gautos prieštaros išplaukia, kad (4)-oji eilutė yra kompozicinė. $\triangle$.

8.8. Apibrėžimas. *Dvi vienos grupės normaliosios eilutės vadinamos izomorfiškomis, kai kiekvienas vienos eilutės faktorius yra izomorfiškas tam tikram kitos eilutės faktoriui, ir atvirkščiai.*

8.9. Pavyzdys. Tarkime $G = \langle a \rangle$ yra šeštosios eilės ciklinė grupė. Nesunku įsitikinti, kad eilutės

$$G \supset \langle a^2 \rangle \supset \{e\} \quad \text{ir}$$
$$G \supset \langle a^3 \rangle \supset \{e\}$$

yra izomorfiškos. Iš tikrųjų,

$$G/\langle a^2 \rangle \cong \langle a^3 \rangle \quad \text{ir}$$
$$G/\langle a^3 \rangle \cong \langle a^2 \rangle.$$

8.10. Lema. *Jei dvi vienos grupės normaliosios eilutės yra izomorfiškos, tai kiekvienam vienos eilutės papildymui galima rasti izomorfišką kitos eilutės papildymą.*

Įrodymas. Tarkime,

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{1}$$

$$G = H_0 \supset H_1 \supset \ldots \supset H_j \supset H_{j+1} \supset \ldots \supset H_r = \{e\}, \tag{2}$$

yra dvi izomorfiškos normaliosios eilutės: (1) $\cong$ (2). Be to, tarkime, eilutė

$$G = G_0 \supset \ldots \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset G_r = \{e\} \tag{3}$$

yra (1)-osios papildymas: (1) $\uparrow$ (3). Įrodysime, kad egzistuoja (2)-osios eilutės papildymas, izomorfiškas (3)-iajai eilutei. Tam pakanka rasti kiekvienam (1)-osios eilutės papildomajam nariui iš (3)-iosios eilutės papildomąjį (2)-osios eilutės narį tokį, kad atitinkami faktoriai būtų izomorfiški.

Konkrečiai, tarkime faktoriai G_i/G_{i+1} ir H_j/H_{j+1} yra izomorfiški ir pogrupis T yra papildomasis narys tarp G_i ir G_{i+1}: $G_i \supsetneq T \supsetneq G_{i+1}$. Rasime papildomąjį narį V tarp pogrupių H_j ir H_{j+1} tokį, kad faktoriai G_i/T ir T/G_{i+1} būtų atitinkamai izomorfiški faktoriams H_j/V ir V/H_{j+1}. Pažymėkime φ grupės G_i kanoninį homomorfizmą grupėje G_i/G_{i+1}, ψ – grupės H_j kanoninį homomorfizmą grupėje H_j/H_{j+1}, f – grupės G_i/G_{i+1} izomorfizmą grupėje H_j/H_{j+1}. Turime atvaizdžių seką

$$\begin{array}{ccccc} G_i & \xrightarrow{\varphi} & G_i/G_{i+1} & \xrightarrow{f} & H_j/H_{j+1} \\ & & & & \uparrow \psi \\ & & & & H_j \end{array}$$

Pogrupis $\psi^{-1}\Big(f\big(\varphi(T)\big)\Big) = V$ yra pogrupio H_j normalusis daliklis. Tai ir yra ieškomasis papildomasis (2)-osios eilutės narys. Iš tikrųjų,

$$H_j/V = H_j\Big/\psi^{-1}\Big(f\big(\varphi(T)\big)\Big) \overset{\text{(II-oji izomorfizmo teorema)}}{\cong} \psi^{-1}(H_j)\Big/f\big(\varphi(T)\big) =$$

$$= H_j/H_{j+1}\Big/f\big(\varphi(T)\big) \cong f^{-1}\Big(H_j/H_{j+1}\Big)\Big/f^{-1}\Big(f\big(\varphi(T)\big)\Big) =$$

$$= G_i/G_{i+1}\Big/\varphi(T) = \varphi(G_i)\Big/\varphi(T) \overset{\text{(II-oji izomorfizmo teorema)}}{\cong} G_i\Big/T.$$

Susiejame ir kitus du faktorius izomorfizmų seka:

$$V/H_{j+1} = \psi(V) = f\big(\varphi(T)\big) \cong f^{-1}\big(f\big(\varphi(T)\big) =$$
$$= \varphi(T) = T/G_{i+1}. \qquad \triangle$$

8.11. Šrajerio teorema. *Bet kurioms dviem vienos eilutės normaliosioms eilutėms galima rasti izomorfiškus papildymus.*

Įrodymas. Tarkime,

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \qquad (1)$$

$$G = H_0 \supset H_1 \supset \ldots \supset H_j \supset H_{j+1} \supset \ldots \supset H_s = \{e\} \qquad (2)$$

yra dvi grupės G normaliosios eilutės. Įrodymą išskaidysime į kelis atvejus.

1. Tarkime $s = 1$. Tada galima laikyti, kad (1)-oji eilutė yra (2)-osios papildymas. Be to, (1)-oji eilutė yra ir jos pačios papildymas, taigi radome abiejų eilučių izomorfiškus papildymus, nes eilutė yra pati sau izomorfiška. $\triangle$

2. Tarkime, $s = 2$. Taikysime indukciją pagal (2)-osios eilutės ilgį r.

1) Jei $r = 1$, pasinaudojame pirmąja įrodymo dalimi.

2) Tarkime, teiginys yra teisingas visoms normaliųjų eilučių poroms, kurių viena yra 2-osios eilės, o kitos eilė mažesnė už r. Įrodysime teiginį eilučių porai, kurių viena yra 2-osios eilės, o kita – r-tosios eilės.

Pažymėkime $H_1G_1 = T$, $H_1 \cap G_1 = V$. Nesunku įsitikinti, kad $T \triangleleft G$, $V \triangleleft H_1$,$V \triangleleft G_1$. Todėl galime sudaryti dvi grupės T normaliąsias eilutes:

$$T \supset G_1 \supset V \supset \{e\}, \tag{3'}$$

$$T \supset H_1 \supset V \supset \{e\}. \tag{4'}$$

Įrodysime, kad šios dvi eilutės yra izomorfiškos. Pasinaudoję I-ąja izomorfizmo teorema, gauname

$$T/_{G_1} = H_1G_1/_{G_1} \cong H_1/_{H_1 \cap G_1} = H_1/_V,$$
$$T/_{H_1} = G_1H_1/_{H_1} \cong G_1/_{H_1 \cap G_1} = G_1/_V.$$

Vadinasi, (3′) ir (4′) eilutės yra izomorfiškos.

Grupės G_1 normaliosioms eilutėms, gautoms iš (1)-osios ir (3′)-iosios eilučių, nubraukus po narį iš kairės –

$$G_1 \supset G_2 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{1''}$$
$$G_1 \supset V \supset \{e\}, \tag{3''}$$

taikome indukcinę prielaidą. Egzistuoja šių eilučių izomorfiški papildymai

$$G_1 \supset G_2 \supset \ldots \supset G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{5''}$$
$$G_1 \supset \ldots \supset V \supset \ldots \supset \{e\}. \tag{6''}$$

Prijungę iš kairės prie šių eilučių po narį T, gausime šios grupės dvi normaliąsias izomorfiškas eilutes

$$T \supset G_1 \supset G_2 \supset \ldots \supset G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{5'}$$
$$T \supset G_1 \supset \ldots \supset V \supset \ldots \supset \{e\}. \tag{6'}$$

Pastaroji eilutė yra (3′) eilutės papildymas. Bet (3′) eilutė yra izomorfiška (4′). Pritaikę šiai porai lemą apie izomorfiškus papildymus, turime, kad egzistuoja (4′) eilutės papildymas

$$T \supset \ldots \supset H_1 \supset \ldots \supset V \supset \ldots \supset \{e\}, \tag{7'}$$

izomorfiškas (6′) eilutei.

Prijunkime prie ($5'$), ($6'$), ($7'$) eilučių kairiųjų pusių po narį G:

$$G \supset T \supset G_1 \supset G_2 \supset \ldots \supset G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{5}$$
$$G \supset T \supset G_1 \supset \ldots \supset V \supset \ldots \supset \{e\}, \tag{6}$$
$$G \supset T \supset \ldots \supset H_1 \supset \ldots \supset V \supset \ldots \supset \{e\}. \tag{7}$$

Turime (5) $\cong$ (6) ir (6) $\cong$ (7). Iš tranzityvumo gauname (5) $\cong$ (7). Bet (5)-oji eilutė yra (1)-osios papildymas, o (7)-oji – (2)-osios. $\triangle$

3. Nagrinėjame bendrąjį atvejį:

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{1}$$
$$G = H_0 \supset H_1 \supset \ldots \supset H_j \supset H_{j+1} \supset \ldots \supset H_s = \{e\}. \tag{2}$$

Taikysime indukciją pagal s.

1) Kai $s = 1$, įrodyta pirmoje dalyje.

2) Tarkime, kad teiginys yra teisingas visoms normaliųjų eilučių poroms, kurių vienos eilė mažesnė už s.

Nagrinėkime eilutę
$$G = H_0 \supset H_1 \supset \{e\}. \tag{3}$$

Pritaikome šiai ir (1) eilutei antrąją įrodymo dalį: egzistuoja (1) eilutės papildymas

$$G = G_0 \supset \ldots \supset G_1 \supset \ldots \supset G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{4}$$

izomorfiškas (3) eilutės papildymui

$$G = H_0 \supset \ldots \supset H_1 \supset \ldots \supset \{e\}. \tag{5}$$

Pažymėkime ($5'$) pastarosios eilutės dalį, kuri prasideda nariu H_1:

$$H_1 \supset \ldots \supset \{e\}, \tag{$5'$}$$

o ($2'$) – (2) eilutės dalį, kuri prasideda tuo pačiu nariu H_1:

$$H_1 \supset H_2 \supset \ldots \supset H_j \supset H_{j+1} \supset \ldots \supset H_s = \{e\}. \tag{$2'$}$$

Šiai eilučių porai tinka indukcinė prielaida. Vadinasi, egzistuoja ($2'$) ir ($5'$) eilučių izomorfiški papildymai ($6'$) ir ($7'$):

$$H_1 \supset \ldots \supset H_2 \supset \ldots \supset H_j \supset \ldots \supset H_{j+1} \supset \ldots \supset H_s = \{e\}, \tag{$6'$}$$
$$H_1 \supset \ldots \supset \ldots \supset \{e\}. \tag{$7'$}$$

Prijungę prie šių eilučių kairiųjų pusių po (5) eilutės dalį, esančią tarp G ir H_1, gausime taip pat izomorfiškas eilutes

$$G \supset \ldots \supset H_1 \supset \ldots \supset H_2 \supset \ldots \supset H_j \supset \ldots \supset H_{j+1} \supset \ldots \supset H_s = \{e\}, \tag{6}$$

$$G \supset \ldots \supset H_1 \supset \ldots \supset \ldots \supset \{e\}. \tag{7}$$

Kadangi (5) $\uparrow$ (7) ir (5) $\cong$ (4), iš lemos apie izomorfiškus papildymus išplaukia, kad egzistuoja (4) eilutės papildymas

$$G = G_0 \supset \ldots \supset \ldots \supset G_1 \supset \ldots \supset \ldots \supset G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{8}$$

izomorfiškas (7) eilutei. Bet (6) $\cong$ (7), vadinasi iš tranzityvumo išplaukia, kad (6) $\cong$ (8). Bet (6) eilutė yra (1) eilutės papildymas, o (8) – (2) eilutės papildymas. $\triangle$

1 išvada (Žordano–Hiolderio teorema). *Bet kurios dvi grupės kompozicinės eilutės yra izomorfiškos.*

Įrodymas. Pritaikę Šrajerio teoremą šioms eilutėms, turime, kad joms egzistuoja izomorfiški papildymai. Bet kompozicinės eilutės papildymas be pasikartojimų sutampa su pačia eilute, vadinasi duotosios kompozicinės eilutės yra izomorfiškos. $\triangle$

2 išvada. *Jei grupė turi kompozicinę eilutę, tai kiekvieną normaliąją tos grupės eilutę galima papildyti iki kompozicinės.*

Įrodymas. Tarkime,

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_r = \{e\}, \tag{1}$$

yra kompozicinė eilutė, o

$$G = H_0 \supset H_1 \supset \ldots \supset H_j \supset H_{j+1} \supset \ldots \supset H_s = \{e\} \quad - \tag{2}$$

normalioji eilutė.

Iš Šrajerio teoremos išplaukia, kad egzistuoja šių eilučių izomorfiški papildymai

$$G = G_0 \supset \ldots \supset G_1 \supset \ldots \supset \ldots \supset G_i \supset \ldots \supset G_{i+1} \supset \ldots \supset \ldots \supset G_r = \{e\} \tag{3}$$

ir

$$G = H_0 \supset \ldots \supset H_1 \supset \ldots \supset \ldots \supset H_j \supset \ldots \supset H_{j+1} \supset \ldots \supset \ldots \supset H_s = \{e\}. \tag{4}$$

Kadangi (1) eilutė yra kompozicinė, ji sutampa su savo papildymu (3). Vadinasi (4) eilutė, kuri yra (2) eilutės papildymas, yra kompozicinė. $\triangle$

9. Išsprendžiamos grupės

Pirmiausia suformuluosime ir įrodysime dažnai taikomą komutanto teoremą:

9.1. Teorema. 1. *Jei grupės G komutantas $[G, G]$ yra pogrupio H poaibis, tai pogrupis H yra grupės G normalusis daliklis.*

2. *Faktorgrupė $G/[G, G]$ yra Abelio grupė.*

3. *Jei T yra grupės G normalusis daliklis ir faktorgrupė G/T – Abelio grupė, tai komutantas $[G, G]$ yra pogrupio T poaibis.*

Įrodymas. 1. Tarkime, H yra grupės G pogrupis ir $[G, G] \subset H$. Fiksuokime elementus $g \in G$ ir $h \in H$. Įrodysime, kad $ghg^{-1} \in H$. Iš tikrųjų,

$$ghg^{-1} = ghg^{-1}h^{-1}h = [g, h]h \in H.$$

Vadinasi, pagal II-ąjį normaliojo daliklio kriterijų H yra grupės G normalusis daliklis. $\triangle$

2. Tarkime, $g_1[G, G]$ ir $g_2[G, G]$ yra fiksuoti faktorgrupės $G/[G, G]$ elementai. Įrodysime, jog jie yra perstatomi. Iš tikrųjų,

$$\begin{aligned} g_1[G, G] \cdot g_2[G, G] &= g_1g_2[G, G] = g_2g_1g_2^{-1}g_2^{-1}g_1g_2[G, G] = \\ &= g_2g_1[g_1^{-1}, g_2^{-1}][G, G] = g_2g_1[G, G] = g_2[G, G] \cdot g_1[G, G]. \end{aligned}$$

Tokiu būdu, faktorgrupė $G/[G, G]$ – Abelio grupė. $\triangle$

3. Pakanka įrodyti, kad kiekviena komutanto sudaromoji $[g_1, g_2]$ priklauso pogrupiui T (kai $g_1, g_2 \in G$). Iš teoremos sąlygos turime

$$g_1^{-1}Tg_2^{-1}T = g_2^{-1}Tg_1^{-1}T.$$

Vadinasi,

$$g_1^{-1}g_2^{-1}T = g_2^{-1}g_1^{-1}T.$$

Padauginę šios lygybės abi puses iš kairės pirma iš g_2, o po to iš g_1, gauname lygybę

$$g_1g_2g_1^{-1}g_2^{-1}T = T.$$

Bet $g_1g_2g_1^{-1}g_2^{-1} = [g_1, g_2]$. Vadinasi, $[g_1, g_2] \in T$. $\triangle$

9.2. Apibrėžimas. *Grupė G yra vadinama išsprendžiama grupe, kai išpildyta viena iš šių ekvivalenčių sąlygų:*

1) *egzistuoja grupės G normalioji eilutė su Abelio faktoriais;*

2) *grupės G komutantų eilutė nutrūksta baigtiniame žingsnyje, t. y. egzistuoja natūralusis skaičius m toks, kad $G^{(m)} = \{e\}$.*

Įrodysime šių sąlygų ekvivalentumą.

„$\Longrightarrow$“ Tarkime, egzistuoja grupės G normalioji eilutė su Abelio faktoriais –

$$G = G_0 \supset G_1 \supset \ldots \supset G_i \supset G_{i+1} \supset \ldots \supset G_r = \{e\}.$$

Kadangi faktorgrupė G/G_1 yra Abelio grupė, iš komutanto teoremos išplaukia, kad $G^{(1)} = [G, G] \subset G_1$. Be to, $G^{(2)} = [G^{(1)}, G^{(1)}] \subset [G_1, G_1]$. Kadangi faktorgrupė G_1/G_2 yra Abelio grupė, iš komutanto teoremos taip pat gauname, kad $[G_1, G_1] \subset G_2$. Vadinasi, $G^{(2)} \subset G_2$. Analogiškai įrodome, kad $G^{(3)} \subset G_3, G^{(4)} \subset G_4, \ldots, G^{(r)} \subset G_r = \{e\}$. Taigi $G^{(r)} = \{e\}$, t. y. komutantų eilutė nutrūksta baigtiniame žingsnyje. $\triangle$

„$\Longleftarrow$“ Tarkime, grupės G komutantų eilutė nutrūksta baigtiniame žingsnyje:

$$G \supset G^{(1)} \supset G^{(2)} \supset \ldots \supset G^{(m)} = \{e\}.$$

Iš komutanto teoremos išplaukia, kad $G^{(i+1)}$ yra pogrupio $G^{(i)}$ normalusis daliklis ir faktorius $G^{(i)}/G^{(i+1)}$ yra Abelio grupė. Vadinasi, komutantų eilutė yra grupės G normalioji eilutė su Abelio faktoriais. $\triangle$

Ištirsime simetrinės grupės S_n išsprendžiamumą.

9.3. Teorema. *Grupės S_2, S_3, S_4 yra išsprendžiamos.*

1. Grupė S_2 yra Abelio grupė, todėl ji yra išsprendžiama. $\triangle$
2. Sudarome grupės S_3 normaliąją eilutę

$$S_3 \supset A_3 \supset (1)$$

(čia A_3 – alternuojančioji grupė). Faktoriaus S_3/A_3 eilė yra 2, o faktoriaus eilė $A_3/(1)$ – 3. Pirminės eilės grupės yra Abelio grupės, todėl normalioji eilutė yra su Abelio faktoriais. Vadinasi, S_3 – išsprendžiama grupė. $\triangle$

3. Sudarome grupės S_4 normaliąją eilutę

$$S_4 \supset A_4 \supset H_1 \supset H_2 \supset (1)$$

(čia A_4 – alternuojančioji grupė, $H_1 = \{(1), (12)(34), (13)(24), (14)(23)\}$ – alternuojančiosios grupės A_4 normalusis daliklis, $H_2 = \{(1), (12)(34)\}$ – grupės H_1 normalusis daliklis).

Faktoriaus S_4/A_4 eilė yra 2, faktoriaus A_4/H_1 eilė – 3, faktoriaus H_1/H_2 eilė 2, faktoriaus $H_2/(1)$ eilė – 2. Vadinasi, kaip ir antroje įrodymo dalyje, visi faktoriai yra pirminės eilės, todėl yra Abelio, ir grupė S_4 – išsprendžiama.

9.4. Lema. *Jei ciklas iš trijų elementų (ijk) priklauso alternuojančios grupės A_n $(n > 4)$ normaliajam dalikliui H, tai pogrupis H sutampa su A_n.*

Įrodymas. Žinoma, kad alternuojančią grupę A_n generuoja ciklai $(12l)$, $l = \overline{3,n}$, todėl pakanka įrodyti, kad $(12l) \in H$.

Nagrinėkime atvejį, kai nė vienas iš skaičių i, j, k nesutampa nei su 1, nei su 2.

Kadangi H yra normalusis grupės A_n daliklis, tai

$$(1ij)(1jk)(1ji) = (1ik) \in H.$$

Todėl ir $(1ik)^2 = (1ki) \in H$. Analogiškai

$$(2ik)(1ki)(2ki) = (1i2) \in H$$

ir $(1i2)^2 = (12i) \in H$.

Kai $l \neq i$, turime

$$(12)(il)(1i2)(12)(il) = (12l) \in H. \quad \triangle$$

9.5. Teorema. *Simetrinė grupė S_n, kai $n > 4$, yra neišsprendžiama.*

Įrodymas. Įrodymui pakanka sudaryti grupės S_n kompozicinę eilutę, kurios nors vienas faktorius nebūtų Abelio grupe.

Sudarę normaliąją eilutę

$$S_n \supset A_n \supset (1),$$

įrodysime, kad ji yra kompozicinė, t. y. jos negalima papildyti be pasikartojimų.

Įrodysime prieštaros būdu. Skiriame du atvejus.

1. Tarkime, duotą eilutę galima papildyti be pasikartojimų nariu tarp S_n ir A_n:

$$S_n \supsetneq H \supsetneq A_n \supset (1).$$

Kadangi H yra tikrinis S_n pogrupis, tai faktorgrupė H/A_n nesutampa su faktorgrupe S_n/A_n, kurios eilė yra 2. Vadinasi, H/A_n yra vienetinė grupė ir todėl H turi sutapti su A_n. Gavome prieštarą prielaidai. $\triangle$

2. Tarkime, normaliąją eilutę galime papildyti nariu be pasikartojimų tarp A_n ir (1):

$$S_n \supset A_n \supsetneq H \supsetneq (1).$$

Įrodysime, kad alternuojančios grupės A_n normaliajam dalikliui H priklauso ciklas iš trijų elementų.

Pasirinkime pogrupio H keitinį, perstatantį mažiausią elementų skaičių. Šis skaičius negali būti lygus dviem – tuo atveju keitinys būtų nelyginis ir negalėtų priklausyti H, kuris sudarytas tik iš lyginių keitinių. Jei šis keitinys perstatinėtų lygiai tris elementus, tai ir būtų reikalingas ciklas. Tarkime, keitinys perstato lygiai keturis elementus. Tada jis būtų arba ciklu iš keturių elementų $(ijkl)$, arba dviejų transpozicijų (ij) ir (kl) sandauga $(ij)(kl)$. Pirmuoju atveju šis keitinys būtų nelyginis ir negalėtų priklausyti H. Tarkime, keitinys $\tau = (i_1i_2)(i_3i_4) \in H$.

Pažymėję $\sigma = (i_3i_4i_5) \in A_n$, turime

$$\tau_1 = \sigma\tau\sigma^{-1} = (i_3i_4i_5)(i_1i_2)(i_3i_4)(i_3i_4i_5) = (i_1i_2)(i_3i_5) \in H,$$

nes H yra grupės A_n normalusis daliklis. Kadangi $\tau, \tau_1 \in H$, tai ir

$$\tau \cdot \tau_1 = (i_1i_2)(i_3i_4)(i_1i_2)(i_3i_5) = (i_3i_4i_5) \in H.$$

Tarkime, keitinys perstato ne mažiau kaip penkis elementus. Tada jis gali būti pavidalo

$$\tau = (i_1i_2i_3i_4i_5\ldots)\ldots,$$
$$\tau = (i_1i_2i_3)(i_4i_5\ldots)\ldots,$$
$$\tau = (i_1i_2)(i_3i_4)(i_5i_6)\ldots.$$

Įrodysime, kad bet kuriuo atveju perstatomų elementų skaičių bent vienetu galima sumažinti.

Pažymėkime $\sigma = (i_2i_3i_4) \in A_n$ ir visais trim atvejais sudarykim keitiniui τ jungtinį keitinį $\tau_1 = \sigma\tau\sigma^{-1}$, priklausantį pogrupiui H:

$$\tau_1 = (i_2i_3i_4)(i_1i_2i_3i_4i_5\ldots)\ldots(i_2i_4i_3) = (i_1i_4i_2i_3i_5\ldots)\ldots.$$

$$\tau_1 = (i_2i_3i_4)(i_1i_2i_3)(i_4i_5\ldots)\ldots(i_2i_4i_3) = (i_1i_4i_2)(i_3i_5\ldots)\ldots.$$

$$\tau_1 = (i_2i_3i_4)(i_1i_2)(i_3i_4)(i_5i_6)\ldots(i_2i_4i_3) = (i_1i_4)(i_2i_3)(i_5i_6)\ldots.$$

Visais atvejais gauname, kad $\tau \neq \tau_1$, t. y. $\tau_1^{-1}\tau \neq (1)$. Be to, jei $k \neq i_1, i_2, i_3, i_4$, matome, kad

$$\tau_1(k) = \tau(k),$$

t. y. keitinys $\tau_1^{-1}\tau$ perstato daugiausia keturis elementus. Vadinasi, visada galima surasti pogrupyje H ciklą iš trijų elementų. Iš 9.4 lemos išplaukia, kad pogrupis H turi sutapti su A_n, o tai yra prieštara pogrupio H pasirinkimui. $\triangle$

Tokiu būdu normalioji eilutė

$$S_n \supset A_n \supset (1)$$

yra kompozicinė. Bet alternuojančioji grupė A_n yra nekomutatyvi, vadinasi faktorius $A_n/(1) = A_n$ nėra Abelio. Taigi negalime sudaryti grupės S_n normaliosios eilutės su Abelio faktoriais, todėl grupė S_n $(n > 4)$ neišsprendžiama. $\triangle$