3. GRUPĖS IR POGRUPIAI

Gerai yra žinomos sveikųjų skaičių aibės $\mathbb{Z}$ sudėties ir sandaugos operacijos. Operacijos sąvoką apibendrinsime bet kuriai netuščiai aibei A.

4.1 apibrėžimas. *Bet kokia funkcija $f : A \times A \to A$ vadinama binariąja (algebrine) operacija aibėje A.*

Binariosios operacijos dažniausiai žymimos specialiais simboliais, pavyzdžiui, $*, \circ, \cdot$ arba $+$. Algebrines operacijas taip pat žymėsime šiais simboliais. Be to, simbolį $a \cdot b$ (dažniausiai žymimą ab be jokio žymens tarp a ir b) vadinsime elementų a ir b sandauga, o simbolį $a + b$ – elementų a ir b suma, nors kartais tai yra sąlyginiai pavadinimai.

4.2 apibrėžimas. *Algebrine struktūra vadinama aibė A, kurioje apibrėžtas baigtinis operacijų skaičius: $f_1, f_2, \ldots, f_n$.*

Norėdami algebrinėje struktūroje A išskirti kurią nors operaciją (operacijas), pavyzdžiui, f_1 $(f_1, f_2, \ldots, f_k)$, naudosime skliaustus $(A; f_1)$ $\big((A; f_1, f_2, \ldots, f_k)\big)$ ir sakysime, kad operacija f_1 (operacijos $f_1, f_2, \ldots, f_k$) aibėje A apibrėžia algebrinę struktūrą. Jei algebrinę struktūrą apibrėžia sumos (sandaugos) operacija, tai tokia struktūra vadinama adicine (multiplikacine) algebrine struktūra.

4.3 pavyzdžiai. 1. Aibių operacijos $\cup, \cap, -, \triangle$ apibrėžia algebrinę struktūrą aibės A poaibių aibėje 2^A : $\big(2^A; \cup, \cap, -, \triangle\big)$.

2. Binariosios operacijos $+, \cdot, +_5$ sveikųjų skaičių aibėje apibrėžia skirtingas algebrines struktūras $(\mathbb{Z}, +), (\mathbb{Z}, \cdot), (\mathbb{Z}, +_5)$.

Dabar apsistosime ties algebrinėmis struktūromis su viena binaria operacija. Nagrinėdami šias algebrines struktūras bendrai, binariąją operaciją jose žymėsime arba simboliu $*$, arba sandaugos simboliu $\cdot$. Abiem atvejais simbolių prasmė ta pati.

Binariosios operacijos, apibrėžtos baigtinėse aibėse, dažnai reiškiamos lentelėmis.

4.4 pavyzdys. Aibėje $\mathbb{Z}_6$ sudėties ir sandaugos operacijos reiškiamos lentelėmis:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Iš 4.1 apibrėžimo matome, kad algebrinė struktūra $(A, *)$ išsiskiria savybe:

$G1$ **(uždarumas operacijos atžvilgiu)**. Visiems $a, b \in A$, tai $a * b \in A$.

Algebrinė struktūra $(A, *)$ gali taip pat pasižymėti savybėmis:

$G2$ **(asociatyvumas)**. Visiems $a, b, c \in A$, teisinga lygybė $(a * b) * c = a * (b * c)$.

Algebrinė struktūra, išsiskirianti savybe $G2$, dažnai vadinama asociatyviąja algebrine struktūra.

$G3$ **(egzistuoja neutralusis elementas)**. Visiems $a \in A$ egzistuoja toks $e \in A$, kad $a * e = e * a = a$. Norėdami algebrinėje struktūroje A išskirti neutralųjį elementą e, žymėsime $(A, *, e)$. Adicinėje algebrinėje struktūroje neutralusis elementas vadinamas nuliu (žymuo 0), o multiplikacinėje – vienetu (žymuo 1).

4.5 teiginys. *Jeigu algebrinėje struktūroje $(A, *)$ egzistuoja neutralusis elementas e, tai jis yra vienintelis neutralusis elementas aibėje A.*

Įrodymas. Sakykime, dar vienas elementas e' tenkina $G3$: visiems $a \in A$, $a * e' = e' * a = a$. Tada

$$e' = e' * e = e * e' = e.$$

$\triangle$

$G4$ **(egzistuoja atvirkštinis elementas)**. Visiems $a \in A$ egzistuoja toks $b \in A$, kad $a * b = b * a = e$, kai e – neutralusis elementas iš $G3$. Elementas b vadinamas simetriniu, arba atvirkštiniu (vartosime šį terminą), elementui a ir dažniausiai žymimas $b = a^{-1}$.

4.6 teiginys. *Jeigu asociatyvioje algebrinėje struktūroje $(A, *)$ elementui $a \in A$ egzistuoja atvirkštinis elementas a^{-1}, tai jis yra vienintelis toks elementas aibėje A.*

Įrodymas. Sakykime, dar vienas elementas $b_1 \in A$ tenkina $G4$: $a*b_1 = b_1 * a = e$. Tada

$$b_1 = b_1 * e = b_1 * \left(a * a^{-1}\right) = \left(b_1 * a\right) * a^{-1} = e * a^{-1} = a^{-1}.$$

$\triangle$

$G5$ **(komutatyvumas).** Visiems $a, b \in A$ $a * b = b * a$.

4.7 apibrėžimas. *Algebrinė struktūra $(A, *)$, tenkinanti:*
$G1$, $G2$, $G3$, $G4$, vadinama grupe;
$G1$, $G2$, $G3$, $G4$, $G5$, vadinama komutatyviąja arba Abelio[1]*, grupe.*

5.3 apibrėžimas. *Tegu $(A, *)$ yra grupė, o B - netuščias A poaibis. Jeigu $(B, *)$ – taip pat grupė, tai B yra vadinamas grupės A pogrupiu.*

Grupei yra būdingi šie teiginiai.

5.4 teiginys. *Grupės $(A, *)$ ir jos pogrupio $(B, *)$ neutralieji elementai sutampa.*

Įrodymas. Grupėje A galioja lygybės:

$$\begin{aligned} e_A * e_B &= e_B, \\ e_B * e_B &= e_B, \\ e_A * e_B &= e_B * e_B, \end{aligned}$$

todėl pagal prastinimo taisyklę grupėje A teisinga $e_A = e_B$.

$\triangle$

5.5 teiginys. *Jeigu grupės $(A, *)$ pogrupio $(B, *)$ elementas b yra elemento $a \in B$ atvirkštinis pogrupyje B, tai jis yra atvirkštinis ir pačioje grupėje A, t.y. $b = a^{-1}$.*

[1] N. H. Abel, 1802–1829, – norvegų matematikas.

Įrodymas. Jeigu $a \in B$, tai

$$a * b = e_B = e_A = a * a^{-1}$$

ir pagal prastinimo taisyklę grupėje A teisinga lygybė $b = a^{-1}$.

Paskutiniai teiginiai visiškai apibūdina grupės pogrupį. Tačiau dažniausiai naudojamasi tokia pogrupio charakterizacija.

5.7 teiginys. *$(B, *)$ yra grupės $(A, *)$ pogrupis tada ir tik tada, kai:*
1) B yra netuščias A poaibis;
2) visiems $a, b \in B$, $a * b^{-1} \in B$.

Įrodymas. Jei B yra grupės A pogrupis, tai pagal apibrėžimus sąlygos 1) ir 2) patenkintos. Kita vertus, jei aibei B sąlygos 1) ir 2) patenkintos, tai šioje aibėje teisingos ir grupės savybės.

a) Savybė $G2$ poaibiui B patenkinta, nes ji galioja grupei A.

b) Jeigu $a \in B$, tai pagal 2) $a * a^{-1} = e_A \in B$, ir, kai $a \in B$, tai

$$a * e_A = e_A * a = a \quad \text{ir} \quad e_A = e_B = e. \text{ Taigi } G3 \text{ patenkinta.}$$

c) Visiems $a \in B$ $e * a^{-1} = a^{-1} \in B$ ir

$$a * a^{-1} = a^{-1} * a = e, \text{todėl } G4 \text{ patenkinta.}$$

d) Visiems $a, b \in B$ turime $b^{-1} \in B$, $\left(b^{-1}\right)^{-1} \in B$, pagal 2)

$$a * \left(b^{-1}\right)^{-1} \in B, \text{ o } b^{-1} * \left(b^{-1}\right)^{-1} = e = \left(b^{-1}\right)^{-1} * b^{-1} = b * b^{-1}, \text{ todėl}$$

$$\left(b^{-1}\right)^{-1} = b \text{ ir } a * \left(b^{-1}\right)^{-1} = a * b \in B. \text{ Taigi } G1 \text{ patenkinta.}$$

$\triangle$

Baigtinių grupių pogrupiai apibūdinami kiek paprasčiau. Tam reikia šių apibrėžimų.

5.8 apibrėžimai. *1. Grupėse, panašiai kaip ir monoiduose, apibrėžiamas grupės elemento laipsnis:*

multiplikatyvioji operacija	*adityvioji operacija*
$a^n = aa \cdots a$ *(n dauginamųjų)*	$n \cdot a = a + a + \ldots + a$ *(n dėmenų)*
$a^{-n} = \left(a^{-1}\right)^n$	$(-n)a = n(-a)$
$a^m a^n = a^{m+n}$	$ma + na = (m+n)a$

$(a^m)^n = a^{mn}$ $\qquad$ $m(na) = (mn)a, \quad n, m \in \mathbb{N}$

$a^0 = 1$ $\qquad$ $0 \cdot a = 0$

2. Jeigu egzistuoja toks natūralusis skaičius $n \geqslant 1$, kad $a^n = 1$, tai mažiausias toks skaičius n_0, kad $a^{n_0} = 1$, vadinamas *elemento* $a \in A$ *eile ir žymimas* $n_0 = \mathrm{ord}_A a$. Jeigu toks natūralusis skaičius neegzistuoja, tai sakoma, kad elemento eilė yra begalinė, ir žymima $\mathrm{ord}_A a = \infty$.

5.9 teiginys. *$(B, \cdot)$ yra baigtinės grupės $(A, \cdot)$ pogrupis tada ir tik tada, kai:*

1) B – netuščias A poaibis;

2) $(B, *)$ visiems $a, b \in B$ $a \cdot b \in B$.

Įrodymas. Grupės A pogrupiui B galioja 5.7 teiginio 1) ir 2) sąlygos. Todėl mums užtenka parodyti, kad su visais $a, b \in B$ teisinga $a \cdot b^{-1} \in B$.

a) Remiantis 2) visi sekos $b = b^1, b^2, \ldots$ nariai priklauso B.

b) Kadangi B – baigtinė aibė, tai egzistuoja tokie natūralieji skaičiai m ir n, $0 < m < n$, kad $b^m = b^n$. Pasinaudoję prastinimo taisykle grupėje, gausime

$$1 \cdot b^m = b^{n-m} \cdot b^m$$

$$1 = b^{n-m}, \text{ t.y.}$$

$$1 \in B \quad \text{ir} \quad \mathrm{ord}_A b < \infty.$$

c) Remiantis atvirkštinio elemento vienatinumu grupėje, iš lygybių

$$b^{\mathrm{ord}_A b - 1} \cdot b = b \cdot b^{\mathrm{ord}_A b - 1} = b^{\mathrm{ord}_A b} = e$$

gauname $b^{-1} = b^{\mathrm{ord}_A b - 1} \in B$.

d) Jeigu $a, b \in B$, tai $b^{-1} \in B$ ir pagal 2) $a \cdot b^{-1} \in B$.

$\triangle$

Norint rasti grupės elemento eilę, reikia mokėti pakankamai efektyviai skaičiuoti grupės $(A, \cdot)$ elemento a laipsnį a^n (ypač, kai n didelis). Paprasčiausias būdas tai padaryti – atlikti $n - 1$ grupės veiksmą. Greitesnis kelias – tai algoritmas, grindžiamas tuo, kad skaičius n reiškiamas dvejetainėje sistemoje suma $n = \sum_i \alpha_i 2^i$; čia α_i arba 0, arba 1, o

$$a^n = \prod_{\alpha_i = 1} a^{2^i}.$$

5.11 algoritmas. *Žinoma: grupės $(A, \cdot)$ elementas a, $n \in \mathbb{Z}$, 1 – neutralusis A elementas.*

Rezultatas: algoritmas skaičiuoja $x = a^n$.

1. $x := 1$.

Jeigu $n = 0$, tai x išvedamas; skaičiavimų pabaiga.

Jeigu $n < 0$, tai $N := -n$, $y := a^{-1}$.

Jeigu $n > 0$, tai $N := n$, $y := a$.

2. Jeigu N nelyginis, tai $x := x \cdot y$.

3. $N := [N/2]$. Jeigu $N = 0$, tai x išvedamas; skaičiavimų pabaiga.

Priešingu atveju $y := y \cdot y$ ir vykdoma 2.

$\triangle$