Paskaita 7

Abelio grupė. Pogrupiai. Ciklinės grupės. ~~Dekompozicija~~

Primename, kad jei $G = (A, \circ)$ yra grupė ir $\forall a, b \in A$ $\boxed{a \circ b = b \circ a}$ tai tokia grupė vadinama <u>Abelio</u>.

Def. Jeigu $A_1 \subset A$ ir struktūra $G_1 = (A_1, \circ)$ yra grupė, tai G_1 yra vadinama grupės G pogrupiu.

Reikia tikrinti ar teisingos grupių sąlygos

1. $\forall a, b \in A_1 \Rightarrow a \circ b \in A_1$ (uždara operacijos atžvilgiu)
2. $e \in A_1$; $\forall a \in A_1 \Rightarrow a' \in A_1$

Šios sąlygos yra būtinos. Jos yra ir pakankamos.

$\overset{\text{def}}{=} 2\mathbb{Z}$

1. $G_1 = (\mathbb{Z}_2, +)$ yra grupės

$G = (\mathbb{Z}, +)$ pogrupis.

$\mathbb{Z}_2 = \{2k \mid k \in \mathbb{Z}\}$.

1) $e = 0 \in \mathbb{Z}_2$
2) $2k + 2\ell = 2(k+\ell) \in \mathbb{Z}_2$
3) $-2k = (2k)' \in \mathbb{Z}_2$
   $2(-k)$

Pav. 2 (pratybos)

$G_1 = \{A, \cdot\}$ $A = \{2^m, \ m \in \mathbb{Z}\}$

yra $G = \{\mathbb{R}_+, \cdot\}$ pogrupis.

Def. Grupė $G = (A, \circ)$, kurios bazinė aibė A yra baigtinė, vadinama baigtine grupe, o jos elementų skaičius

$E(A) = |A|$ vadinamas grupės eile.

galinės grupės pogrupis gali būti
galinis arba baigtinis.

Pav. $G_1 = (\mathbb{Z}_2, +)$ yra begalinės
grupės $G = (\mathbb{Z}, +)$ pogrupis.

$G_2 = (\{1, -1\}, \cdot)$ yra baigtinės
(2-os eilės) grupės $(\mathbb{R}, \cdot)$ pogrupis.

(įrodyti, kad G_2 yra pogrupis!)

$G = (A, \circ)$ - grupė.

Def. $a \in A$, $a^m = \underbrace{a \circ a \circ \dots \circ a}_{m\text{-kartų}}$

$m \in \mathbb{N}$

$a^m = a \circ a^{m-1}$ rekursinė apibrėžtis

$a^1 = a$

Def $a^0 = e$ (def.) (Tai suderinta $a^1 = a \circ a^0$)

Def $a^{-m} = (a')^m$ (def) a' - simetrinis elementas

⊗ T. $a^m a^n = a^{m+n}$, $m, n \in \mathbb{Z}$.

---

1) $m, n > 0$, 2) $m > 0$, $n < 0$ 3) $m < 0$, $n < 0$

nlidime pvz. $m=-k$, $n>0$, $k>n$.

$$a^m \circ a^n = \underbrace{a' \circ a \circ \dots a'}_{k} \overbrace{\circ a \circ a \dots \circ a}^{e} \underbrace{}_{n} \quad (a' \circ a)$$

$$= \underbrace{a' \circ \dots a'}_{k-n} = a'^{-(k-n)} = a^{n-k} = a^{n+m}$$

Kitu atvejai yra nagrinėjami panašiai.

Def $G=(A,\circ)$ - grupė. Imkime $a \in A$.

$G_1 = (\{a^m \mid m \in \mathbb{Z}\}, \circ)$ yra G pogrupis (įrodykite!)

1) uždarumas $a^m \circ a^n = a^{m+n}$ 2) $e = a^0 \in G_1$ 3) $\tilde{a}' \in G_1$, jei $\tilde{a} \in G_1$. $a' = a^{-1} \in G_1$ $(a^m)' = (a')^m$

G_1 žymėsime (a) ir vadinsime

cikline grupe, generuota elemento a.

Pagal apibr.

$$a^{-m} = (a')^m \Rightarrow a^m \circ (a')^m = a^m \circ a^{-m} = a^0 = e$$

...ciklinės grupės gali būti baigtinės
ir begalinės

(Apibrėžimas tinka bet kokiai grupai)

Def. Mažiausias natūrinis skaičius
$d \in \mathbb{N}$, kurį imant $a^d = e$
vadinamas elemento a eile, žymime $E(a)$

Čia a yra bet kuris grupės elementas

(jei d neegzistuoja baigtinis, tai elemento eilė yra begalinė)

Pvz. $E(e) = 1$

(žr. 5A.4 Toliau tik ciklinėms grupėms)

T. Baigtinės ciklinės grupės generuojančio elemento a eilė sutampa su grupės $(a) = G$ eile

$$E(a) = E(G)$$ (Lemma teorema)

◁ $E(a) \leq E(G)$, nes priešingu atveju grupėje būtų daugiau skirtingų elemento laipsnių negu grupėje yra elementų. $E(a)$ negali būti ir mažesnė už $E(G)$, nes ciklinę grupę sudaro tik elemento a laipsniai. ▷

-5A-

(klasės)

Rasti elementų eilę $2+13\mathbb{Z}$ ciklinės grupės $(\mathbb{Z}/13\mathbb{Z}, \cdot)$

k	0	1	2	3	4	5	6	7	8	9	10	11	12
$2^k \bmod 13$	1	2	4	8	3	6	12	11	9	5	10	7	(1)
$4^k \bmod 13$	1	4	3	12	9	10	(1)						

Elemento $2+13\mathbb{Z}$ eilė yra 12, ji sutampa su grupės $(\mathbb{Z}/13\mathbb{Z}, \cdot)$ eile.

Elemento $4+13\mathbb{Z}$ eilė yra 6.

$(\mathbb{Z}/13\mathbb{Z}, \cdot)$ elementų skaičius sutampa su skaičiaus n

$\gcd(n, 13) = 1$

Jų yra 12 $(1, 2, \dots, 12)$

Elemento $2+13\mathbb{Z}$ eilė yra 12.

Šis elementas generuoja ciklinę grupę $(2+13\mathbb{Z})$ sutampančią su $(\mathbb{Z}/13\mathbb{Z}, \cdot)$

...vyzdžiai (~~[illegible]~~ baigtinėms ciklinėms grupėms)

a- generuojantis elementas

... Bet kurį neigiamą laipsnį galima keisti tokiu ... teigiamu laipsniu.

$$a^{-s} = a^{m} \quad S, m > 0$$

$E(a) = d$

$S = dt + r, \quad 0 \le r < d.$

$$a^{-s} = a^{-dt-r} = a^{-dt} a^{-r}$$

$$= (a^{-d})^t a^{-r} = (e^{-1})^t a^{-r} = a^{-r}$$

$a^{-d} \circ a^d = a^0 = e$ $\quad a^d = e \quad$ pagal apibrėžimą eilės

$$a^{-r} = e\, a^{-r} = a^{d} a^{-r} = a^{d-r}.$$

$$\boxed{a^{-s} = a^{d-r}}$$

S2.

Jeigu generuojančio elemento a eilė yra n, tai

$$(a) = \{a^0 = e, a^1, \dots, a^{n-1}\}.$$

$$\{e, a, \dots, a^{n-1}\}$$

2. Baigtinėje ciklinėje grupėje (a)

$a^d = e$

$a^m = e \iff m = E(a)t$.

$d = E(a)$

◁ Užtenka parodyti būtinumą.

Tarkime priešingai, kad m - nedalinis iš d.

$m = dt + r, \quad 0 < r < d$.

$e = a^m = a^{dt} \circ a^r = (a^d)^t \circ a^r = a^r$ (čia $a^d = e$)

Bet tai prieštarauja teiginiui, kad d - yra elemento a eilė ▷

S4. Ciklinės grupės yra Abelio (komutatyvios)

◁ $a^m \circ a^n = a^{m+n} = a^{n+m} = a^n \circ a^m$ ▷ (aritmetika)

S5. Visos tos pačios eilės baigtinės ir begalinės ciklinės grupės yra izomorfiškos. (su operac. $\circ_1$ ir $\circ_2$)

◁ (a) ir (b) dvi ciklinės grupės. Imkime tokią f:

$f(a^m) = b^m$. Parodysime, kad tai yra izomorfizmas (bijekcija ir)

↓ cikl. gr.

$$f(a^n \circ_1 a^k) = f(a^{n+k}) = b^{n+k}$$

$$= b^n \circ_2 b^k = f(a^n) \circ_2 f(a^k).$$

↑ cikl. grupė

§6. Ciklinės grupės ~~kiekviena pogrupis~~

yra ciklinis

Nagrinėkime ciklinę grupę (a) ~~ir~~ pogrupį $G_2 = (A, \circ)$

~~Tarkime~~ $A = \{a^m, m \in M\} \subset \mathbb{Z}\}$

Tarkime, kad mažiausias teigiamas laipsnis $k > 0$, $b = a^k$ (Neigiamo laipsnio elem. galima atvaizduoti teig. laipsnio elementu). — jis atitinka elementą

Tada parodysime, kad $m = kt \in M$, $t \in \mathbb{Z}$, ir b yra generuojantis elementas pogrupio $G_2 = (b)$.

Jeigu $\exists s = kt + r$, $0 < r < k$, tai turėtume ($s \in M$)

$$((a^s \in A) \wedge (a^k \in A)) \Rightarrow ((a^s \in A) \wedge (a^{kt} \in A))$$

$$\Rightarrow ((a^s \in A) \wedge (a^{-kt} \in A)) \Rightarrow a^{s-kt} \in A$$

$\Rightarrow a^r \in A$, bet tai prieštarauja teig., kad k yra mažiausias.