(4)

(11) Циклични групи

Опр: Група, която се поражда от един свой елемент, се нарича циклична група.

$$G = \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$$

$$a^k = \underbrace{aa \dots a}_{k}, \quad k > 0$$

$$a^0 = e$$

$$a^k = \underbrace{a^{-1}a^{-1} \dots a^{-1}}_{|k|}, \quad k < 0$$

в адитивен запис

$$G = \langle a \rangle = \{ ka \mid k \in \mathbb{Z} \}$$

$$ka = \underbrace{a + a + \dots + a}_{k}, \quad k > 0$$

$$ka = \underbrace{(-a) + (-a) + \dots + (-a)}_{|k|}, \quad k < 0$$

примери за числови групи:

Сш; $\mathbb{Z}^* = G$; $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

G - мултипл.

$a \in G$

$\langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \} < G$

Всеки всякои една поражена група има множество от циклични групи, които я съставят

Опр: (Ред на елемент) (при мултипл. група) Елементът $a \in G$ е от ред k, ако k е *най* естествено число, за което $a^k = e$.

Ако такова естествено число не съществува a има ред ∞ : $o(a) = |a| = k \neq$
$|a| = \infty$

Пример: $C_4 = \{1, i, -1, -i\}$

$$|1| = 1 \; ; \; |i| = 4; \; |-1| = 2; \; |-i| = 4$$

Опр: (Ред на елемент при адитивна група)

най k: $ka = \underbrace{a + a + \dots + a}_{k} = 0$

$\mathbb{Z}$: $|0| = 1$
$|1| = \infty$

Ако $s \neq 0$: $|s| = \infty$

(ТВ) Нека в група G елемент $a \in G$; $|a| = k$

Тогава:

1) $a^n = e \Leftrightarrow k \mid n$

2) $a^s = a^t \Leftrightarrow s \equiv t \pmod{n}$

Д-во:

1) $\Rightarrow$ $a^n = e$ $\quad n = qk + r, \quad 0 \leq r < k$

$e = a^n = a^{qk+r} = a^{qk} \cdot a^r = (a^k)^q \cdot a^r = a^r$

$\Rightarrow e = a^r$ и $0 \leq r < k$ ⇒ $r = 0$ ⇒ $k \mid n$

k е най-ест. число, за което $a^k = e$

2) Ако $a^s = a^t \mid \cdot a^{-t} \Leftrightarrow a^{s-t} = e \Leftrightarrow k \mid (s-t) \Leftrightarrow s \equiv t \pmod{k}$

Следствие: $a \in G$, $|a| = k$

$\langle a \rangle = \{ e, a, a^2, a^3, \ldots, a^{k-1} \}$

a^k — възможни остатъци при деление на k

$a^s = e \Rightarrow k \mid s$

a^m, $m \in \mathbb{Z}$, $m = kq + r$, $0 \le r < k$

$a^m = a^{kq+r} = \underbrace{(a^k)^q}_{e} \cdot a^r = a^r$

$\Rightarrow a^m = a^r$, $0 \le r < k$

$|a| = k \Rightarrow |\langle a \rangle| = k$

Пример за цикл. гр.:

$n \in \mathbb{N}$, $n \ge 2$

$\bar{a} = \{ a + kn \mid k \in \mathbb{Z} \}$

$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1} \}$

$\bar{a} + \bar{b} = \overline{a+b}$

$\bar{2} = \bar{1} + \bar{1}$

$\bar{3} = \bar{1} + \bar{1} + \bar{1}$

$\bar{k} = \underbrace{\bar{1} + \bar{1} + \ldots + \bar{1}}_{k}$

$\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, \ldots, (k-1)\cdot\bar{1} \}$ — адитивно циклична група от ред n

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$

$|\bar{0}| = 1$

$|\bar{1}| = 6$

$|\bar{2}| = 3$

$|\bar{3}| = 2$

$|\bar{4}| = 3$

$|\bar{5}| = 6$

$\Rightarrow |\langle \bar{5} \rangle| = 6 \quad : \langle \bar{5} \rangle < \mathbb{Z}_6$

$\Rightarrow \mathbb{Z}_6 = \langle \bar{1} \rangle = \langle \bar{5} \rangle$

$\langle \bar{2} \rangle = \{\bar{0}, \bar{2}, \bar{4}\} = \langle \bar{4} \rangle$

$\langle \bar{3} \rangle = \{\bar{0}, \bar{3}\}$

08.03.2016

$(G, \cdot)$

$H = \langle a \rangle = \{ a^k \mid k \in \mathbb{Z} \}$ - циклична подгрупа на G породена от елемента a

$H < G$

$|a| = k$, ако k е min $\mathbb{N}$: $a^k = e$, ако такова $\mathbb{N}$ число не съществува, то $|a| = \infty$.

$|a| = k \Leftrightarrow |\langle a \rangle| = k \Rightarrow \langle a \rangle = \{ e, a, a, \ldots, a^{k-1} \}$

$|a| = \infty \Leftrightarrow |\langle a \rangle| = \infty$

Опр. (Изоморфизъм)

Нека $(G_1, \cdot)$ и $(G_2, *)$ - групи.

Указваме, че $\boxed{G_1 \cong G_2}$, ако:

$\exists \varphi: G_1 \to G_2$ и

1) φ - биекция;

2) $\varphi(a \cdot b) = \varphi(a) \circledast \varphi(b), \forall a, b \in G_1$.

(операцията на дадената група; операцията на другата група)

Алгебрата не разпознава изоморфните обекти помежду си.

Th. Нека G е циклична група и $G = \langle g \rangle$, тогава

1) ако $|G| = n$, то $G \cong C_n = \{ 1, \omega_1, \omega_1^2, \ldots, \omega_1^{n-1} \}$,

2) ако $|G| = \infty$, то $G \cong \mathbb{Z}$.

където $\omega_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, $\omega_1^n = 1$

Доказателство:

1) $|G| = n$, $G = \langle g \rangle$ и $|g| = n \Rightarrow g^n = e$

$G = \{ e, g, g^2, \ldots, g^{n-1} \}$

$\varphi: C_n \to G$

$\varphi(\omega_1^k) = g^k$

1) φ е биекция;

2) $\varphi(\omega_1^k \cdot \omega_1^s) = \varphi(\omega_1^{k+s}) = \varphi(\omega_1^r) = g^r = g^r \cdot (g^n)^q =$

$k+s = qn+r,\ 0 \le r < n$ (e)

$= g^{r+nq} = g^{k+s} =$

$\Rightarrow \varphi$ е хомоморфизъм $= g^k \cdot g^s = \varphi(\omega_1^k) \cdot \varphi(\omega_1^s)$

$\Rightarrow$ От 1) и 2) $\Rightarrow \varphi$ е изоморфизъм

$\Rightarrow G \cong C_n$

2) $|G| = \infty,\ G = \langle g \rangle$

$\langle g \rangle = G = \{ g^k \mid k \in \mathbb{Z} \}$

$\varphi : \mathbb{Z} \to G$

$\varphi(k) = g^k$

$k \neq s \Rightarrow g^{k-s} \neq e \Rightarrow g^k \neq g^s$

$\Rightarrow \varphi$ е биекция

$\varphi(k+s) = g^{k+s} = g^k \cdot g^s = \varphi(k) \cdot \varphi(s)$

$\Rightarrow \varphi$ е изоморфизъм $\Rightarrow G \cong \mathbb{Z}$

Има една единствена с точност до изоморфизъм безкрайна циклова група.

Идея за разписка: ↙

Th G - циклична група и $H < G$, то H - циклична

Доказателство:

а) $|G| = n \Rightarrow G \cong \mathbb{Z}$

$H < G$

Щем $g^d \in H$ и d е най-малкото, за което $g^d \in H$.

$g^s \in H$

$s = qd + r,\ 0 \le r < d$

$g^s = g^{qd+r} = \underbrace{(g^d)^q}_{\in H} \cdot g^r$

$\underbrace{g^s}_{\in H}$

$g^r = g^s \cdot g^{qd} \in H \overset{\text{об}}{\underset{d\text{-min}}{\Rightarrow}} r = 0$

$\Rightarrow g^s = g^{qd} = (g^d)^q \in \langle g^d \rangle$

$\Rightarrow H \leq \langle g^d \rangle$

$g^d \in H \Rightarrow (g^d)^k \in H$

$\Rightarrow \langle g^d \rangle \leq H$

$\Rightarrow H = \langle g^d \rangle$

$\Rightarrow H$ е циклична подгрупа

б) $|G| = n$ $G = \langle g \rangle$ и $|g| = n$

$H < G$ и $d: \min > 0$, за което $g^d \in H$.

$s: g^s \in H \Rightarrow d \mid s \Rightarrow s = qd \Rightarrow g^s = (g^d)^q \in \langle g^d \rangle$

Да видим по същия начин

$H = \langle g^d \rangle$

$g^n = e \in H : n = q_1 d + r_1,\ 0 \leq r_1 < d$

$\underbrace{e}_{\in H} = \underbrace{(g^d)^{q_1}}_{\in H} \cdot g^{r_1} \Rightarrow g^{r_1} \in H \Rightarrow r_1 = 0 \Rightarrow d \mid n$

~~Характеризиране на циклична група~~