Циклични групи

Циклична група - група, която се поражда от един свой елемент

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

$a^k = a.a.a.\ldots.a, \; k>0$
$a^0 = e \quad k=0$
$a^k = a^{-1}.\ldots.a^{-1}, \; k<0$
} мултипликативен запис

$ka = a+\ldots+a$
$ka = (-a)+\ldots+(-a)$
} адитивен запис

$\mathbb{C}_n$ - пример за циклична група

$\hookrightarrow \mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$

Казваме, че елементът a е от ред k, ако k е най-малкото естествено число, за което $a^k = e$. Ако такова число не съществува, казваме, че a има ред ∞: $O(a) = |a| = k$

$O(a) = |a| = \infty$

При адитивна група, дефиницията е за $ka = e$

Тв Нека в група G, a е елемент от ред k. Тогава:

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

2) $a^s = a^t \Leftrightarrow s \equiv t \,(k)$

Доказателство:

1) $a^n = e \rightarrow n = qk + r, \; 0 \le r < k$

$a^n = a^{qk+r} = a^{kq}.a^r = (a^k)^q a^r = a^r.e \Rightarrow$ ↯ $\Rightarrow r = 0 \Rightarrow k \mid n$

2) $a^s = a^t \mid .a^{-t} \Rightarrow a^{s-t} = e \Leftrightarrow k \mid s-t \Leftrightarrow s \equiv t \,(k)$

Следствие: $a \in G; \; |a| = k \Rightarrow \langle a \rangle = \{e, a, a^2 \ldots a^{k-1}\}$

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

$\hookrightarrow |\langle a \rangle| = k \rightarrow$ важи и за $k = \infty$

$a^m, \; m \in \mathbb{Z}, \; m = qk + r, \; 0 \le r < k \Rightarrow a^m = a^{kq+r} = (a^k)^q a^r = a^r$

$\Rightarrow \forall m \in \mathbb{Z} \Rightarrow a^m = a^r, \; 0 \le r < k$

Пример за циклична група:

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

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

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

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

$\bar{k} = \underbrace{\bar{1} + \ldots + \bar{1}}_{k} = k\bar{1} \Rightarrow \mathbb{Z}_n = \langle \bar{1} \rangle$ - адитивна, циклична, крайна

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

$|\bar{0}| = 1 \quad |\bar{2}| = 3 \quad |\bar{4}| = 3$

$|\bar{1}| = 6 \quad |\bar{3}| = 2 \quad |\bar{5}| = 6 \Rightarrow |\langle \bar{5} \rangle| = 6$

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

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

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

Опр. Изоморфизъм на групи: $(G_1, \circ)$ и $(G_2, *)$. Казваме, че G_1 е изоморфна на G_2, ако $\exists \varphi: G_1 \to G_2$: 1) φ - биекция;

2) $\varphi(a_1 \circ b_1) = \varphi(a_1) * \varphi(b_1), \forall a_1, b_1 \in G_1$.

Записваме $G_1 \cong G_2$.

Т Нека G е циклична група и $G = \langle g \rangle$. Тогава:

1) ако $|G| = n$, то $G \cong C_n = \{1, \omega_1, \omega_1^2, \ldots, \omega_1^{n-1} \mid \omega_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\}$

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

Доказателство:

1. $|G| = n \Rightarrow G = \langle g \rangle \Rightarrow |g| = n \Rightarrow G = \{e, g, g^2 \ldots g^{n-1}\}$
   $\hookrightarrow g^n = e, \omega_1^n = 1$

$\varphi: C_n \to G : \varphi(\omega_1^k) = g^k \to$ **φ - биекция**

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

$k+s = qn+r$

$\Rightarrow \varphi(\omega_1^k \circ \omega_1^s) = \varphi(\omega_1^k) \cdot \varphi(\omega_1^s) \to$ **φ - хомоморфизъм**

$\Rightarrow$ **φ - изоморфизъм** $\Rightarrow C_n \cong G$

2. $|G| = \infty, G = \langle g \rangle \Rightarrow |g| = \infty \Rightarrow G = \{g^k \mid k \in \mathbb{Z}\}$

$\varphi: \mathbb{Z} \to G : \varphi(k) = g^k$

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

$\varphi(k+s) = g^{k+s} = g^k \cdot g^s = \varphi(k) \cdot \varphi(s) \Rightarrow$ **φ - хомоморфизъм**

$\Rightarrow$ **φ - изоморфизъм** $\Rightarrow \mathbb{Z} \cong G$

Т G - циклична група и $H < G \Rightarrow H$ - циклична

Доказателство:

1) $|G| = \infty \Rightarrow G \cong \mathbb{Z}$

$H < G$. Нека $g^d \in H$ и d е $\min$ $\mathbb{N}$ число, за което $g^d \in H$.

$g^s \in H \Rightarrow s = qd + r,\ 0 \le r < d$

$\Rightarrow g^s = g^{qd+r} = \underbrace{(g^d)^q}_{\in H} \cdot g^r \in H \Rightarrow g^r = g^{s-dq} \Rightarrow g^r \in H \Rightarrow$ т.к. d е $\min \mathbb{N}$ число: $g^d \in H \Rightarrow r = 0 \Rightarrow g^s = g^{dq} \Rightarrow \langle g^d \rangle \Rightarrow H \le \langle g^d \rangle,\ g^d \in H \Rightarrow$

$\Rightarrow (g^d)^k \in H \Rightarrow \langle g^d \rangle \le H \Rightarrow H = \langle g^d \rangle \Rightarrow H$ - циклична

2) $|G| = n \Rightarrow G = \langle g \rangle$ и $\langle g \rangle = n$

$H < G$ и $g^d \in H$, d е $\min \mathbb{N}$, за което $g^d \in H$.

s - произволно, $g^s \in H$

... (аналогично на 1)) $\Rightarrow H \le \langle g^d \rangle$ и $H = \langle g \rangle$.

Ако приложим това за $e = g^n$, ще получим, че $n = qd + r_1,\ 0 \le r_1 < d \Rightarrow$

$\Rightarrow e = (g^d)^{q_1} \cdot r_1 \Rightarrow g^{r_1} \in H \Rightarrow r_1 = 0$. Така получаваме условие какви могат да бъдат подгрупите на крайна циклична група $\Rightarrow d / n$.

Симетрични групи

D $M \neq \emptyset$; $S(M) = \{\varphi \mid \varphi : M \to M$ - биекция$\}$

$\varphi \circ \psi (x) = \varphi(\psi(x))$

- некомутативна

$|M| = n \to M = \{1, 2, 3, \dots, n\}$

$S(M) = S_n$ - симетрична група от степен n

$\varphi \in S_n \Rightarrow \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$, $i_k = \varphi(k)$

↳ пермутация на $\overline{1,n}$ $\Rightarrow |S_n| = n! = P_n$

Представяне на елементите чрез цикли

$\sigma = (i_1, i_2 \dots i_k)$ - цикъл с дължина k

$\{i_1 \dots i_k\} \subset \{1 \dots n\}$

$i_1 \xrightarrow{\sigma} i_2 \xrightarrow{\sigma} \dots \to i_{k-1} \xrightarrow{\sigma} i_k \xrightarrow{\sigma} i_1$ ⟶ За всички останали елементи е изпълнено, че не се променят под действие на σ.

$S_8 \to (2,4,6,8) \to \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 2 \end{pmatrix}$

D Циклите $(i_1 \dots i_k)$ и $(j_1 \dots j_s)$ са независими, ако подмножествата от точки, които преместват, нямат общ елемент.

Свойство: Ако σ и τ са независими цикли, то те комутират.

!Забележка: Това не важи за зависими цикли!