сл. $\varphi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ i_1 & i_2 & i_3 & \dots & i_n \end{pmatrix}$ $i_s = \varphi(s)$ – пермутация на числата от 1 до n.

$\forall$ пермутация има обратна $\Rightarrow$ броя на елементите в S_n е толкова колкото са всичките пермутации на числата от 1 до n.

$|S_n| = n!$

$S_2 < S_3 < S_4 < \dots$

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \varphi \circ \psi \longrightarrow \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad (1)$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

В общия случай операцията композиция (∘) е некомутативна!! (само на 2 и 1 елемент е комутативна)

4. Ред на елемент. Циклични групи

Дефиниция Група която се поражда от един свой елемент a, т.е $G = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ – циклична група

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

$a^0 = e$

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

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

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

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

Примери за циклични групи:

$\mathbb{Z}_n$, $\mathbb{Z}^+ = \mathbb{Z}_2$, $\mathbb{Z}$ – циклична група породена от 1 или -1.

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

тъй

Деф: Ред на елемента: Казваме че елемента a е от ред k, ако k е минимално естествено число за което a^k е единичен ел. ($a^k = e$) Ако такова число не съществува казваме че a има ред ∞. Записване: $o(a) = |a| = k$; $|a| = \infty$ $\underbrace{\Rightarrow}_{k} \langle a \rangle = \{e, a, a^2, \dots, a^{k-1}\}$

Пр: $C_4 = \{1, i, -1, -i\}$ $|1| = 1$; $|-1| = 2$; $|-i| = 4$; $|i| = 4$.

Опред. за ред на елемент при адитивна група: min k за което k кратното на елемент a ра е равно на 0 ($\underbrace{a + a + \dots + a}_{k} = 0$)

Пр: $\mathbb{Z}$: $|0| = 1$ $|1| = \infty$ $s \neq 0$: $|s| = \infty$ (ред от s е ∞)

Т6: Нека G е група G и елем $a \in G$, ред $|a| = k$ Тогава:

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

2) $a^s = a^t \iff s \equiv t \pmod k$

Док-во: 1) $a^n = e$ $n = qk + r$ r-остатък с k $r \geq 0$

тогава $e = a^n = a^{qk+r} = a^{qk} \cdot a^r = (a^k)^q \cdot a^r = a^r \Rightarrow e = a^r$ и $0 \leq r < k$

k - min естествено число за което $a^k = e \Rightarrow r = 0 \Rightarrow k \mid n$

2) $a^s = a^t \mid \cdot \bar{a}^t \Rightarrow a^{s-t} = e \iff k \mid (s-t) \Rightarrow s \equiv t \pmod k$

Следствие: $a \in G$, $|a| = k$ Цикл. ел. $\langle a \rangle = \{e, a, a^2, a^3, \dots a^{k-1}\}$

a^k - единичен ел. $a^s = e \Rightarrow k \mid s$

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

$a^m = a^{kq+r} = (a^k)^q \cdot a^r = \overset{e}{a^r}$, $a^m = a^r$, $0 \leq r < k$ $|a| = k \Rightarrow |\langle a \rangle| = k$

Пр. примери за циклична група:

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

$\bar{a} = \{a + kn \mid x \in \mathbb{Z}\}$ $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ - класове (остатъци)

$\bar{a} + \bar{b} = \overline{a+b}$, $\bar{2} = \bar{1} + \bar{1}$, $\bar{3} = \bar{1} + \bar{1} + \bar{1}$, $\bar{k} = \underbrace{\bar{1} + \dots + \bar{1}}_{k} = k\bar{1}$

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, 2\cdot\bar{1}, \dots (k-1)\bar{1}\}$ ↪ кратно на $\bar{1}$.

$\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \dots \bar{5}\}$ $|\bar{0}| = 1$, $|\bar{1}| = 6$

$|\langle \bar{5} \rangle| = 6$ $\langle \bar{5} \rangle < \mathbb{Z}_6 \Rightarrow \mathbb{Z}_6 = \langle \bar{1} \rangle = \langle \bar{5} \rangle$

Опред: Циклична група с операцията "$\cdot$" $(G, \cdot)$

$H = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$ Цикличната подгрупа пораждана от своя елемент $H < G$ H подгрупа на G.

Пр. За безкрайна циклична група - цялите числа - пораждани от $1, -1$.

Опр: За изоморфизам на групи: // Нека имаме 2 групи $(G_1, \circ)$ и $(G_2, *)$ казваме че $G_1 \cong G_2$ (изоморфни) ако $\exists \varphi: G_1 \to G_2$ и
1) φ - биекция 2) $\varphi(a \circ b) = \varphi(a) * \varphi(b)$, $\forall a, b \in G_1$ (хомоморф)

Тн: За коя 2 изоморфни цикл. групи са алгебрично изоморфни декларации:
Нека G - цикл. гр. и $G = \langle g \rangle$ (G - порождена от ел g) тогава:
1) ако $|G| = n$ то $G \cong C_n = \{1, \omega_1, \omega_1^2, \dots, \omega_1^{n-1}\}$
$\omega_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, $\omega_1^n = 1$
2) ако $|G| = \infty$ то $G \cong \mathbb{Z}$

Док-во)
1) $|G| = n$, $G = \langle g \rangle$ и $|g| = n \Rightarrow g^n = e \in G = \{e, g, g^2, \dots g^{n-1}\}$
$\varphi: C_n \to G$ $\varphi(\omega_1^k) = g^k$
(1) φ - биекция
$k+s = gn+2$, $0 \le r < n$
(2) $\varphi(\omega_1^k \cdot \omega_1^s) = \varphi(\omega_1^{k+s}) = \varphi(\omega_1^2) = g^2 = g^2 \cdot (g^n)^q = g^{2+nq} = g^{k+s} =$
$= g^k \cdot g^s = \varphi(\omega_1^k) \cdot \varphi(\omega_1^s) \Rightarrow \varphi$ - хомоморфизам $\Rightarrow$
от 1 и 2 $\Rightarrow \varphi$ - изоморфизам $\Rightarrow G \cong C_n$
2) $|G| = \infty$ - безкр. цикл. група $G = \langle g \rangle$ $\langle g \rangle = G = \{g^k \mid k \in \mathbb{Z}\}$
(1) $\varphi: \mathbb{Z} \to G$ $\varphi(k) = g^k$ $k \ne s \Rightarrow g^{k-s} \ne e \Rightarrow g^k \ne g^s \Rightarrow \varphi$ - биекция
(2) За хомоморфизма: $\varphi(k+s) = g^{k+s} = g^k \cdot g^s = \varphi(k) \cdot \varphi(s) \Rightarrow$
φ - изоморфизам $\Rightarrow G \cong \mathbb{Z}$

Тн: Подгрупа на цикличната група е цикличка. G - цикл. гр.
$H < G$ то H - цикл.
Док-во: а) $|G| = \infty \Rightarrow G \cong \mathbb{Z}$ $H < G$
Нека $g^d \in H$ и d - min естествено число за което $g^d \in H$
$g^s \in H$, $s = qd + r$, $0 \le r < d$
$g^s = g^{qd+r} = (g^d)^q \cdot g^r \Rightarrow g^r = g^s \cdot g^{-qd} \in H \Rightarrow r = 0 \Rightarrow d$ - min
$\Rightarrow g^s = g^{qd} = (g^d)^q \in \langle g^d \rangle \Rightarrow H \subseteq \langle g^d \rangle$;
$g^d \in H \Rightarrow (g^d)^k \in H \Rightarrow \langle g^d \rangle \subseteq H \Rightarrow H = \langle g^d \rangle$ - цикл. подгр.
б) $|G| = n$
$G = \langle g \rangle$ и $|g| = n$, $H < G$ и d - min > 0, за което $g^d \in H$ и нека
(s единствено за което) $s: g^s \in H \Rightarrow d \mid s \Rightarrow s = q \cdot d \Rightarrow$
$\Rightarrow g^s = (g^d)^q \in \langle g^d \rangle$ $H = \langle g^d \rangle$, $g^n = e \in H$; $n = q_1 d + r_1$, $0 \le r_1 < d$
подгр. $e = (g^d)^{q_1} \cdot g^{r_1} \Rightarrow g^{r_1} \in H \Rightarrow r_1 = 0 \Rightarrow d \mid n$