Egzamin I $11^{15} - 13$ 28.06
II $11^{15} - 13$ 05 07 sala 30, D1.

Grupy cykliczne.

Def. Grupę $(G, \cdot)$ nazywamy cykliczną, gdy

$$\exists g \in G \quad \langle g \rangle = G.$$

Przykłady $(\mathbb{Z}, +) = \langle 1 \rangle$

$n = 1, 2, 3, \ldots \quad C_n = (\{0, \ldots, n-1\}, +_n)$

Obserwacja.
Niech $G = \langle g \rangle$, $\operatorname{ord}(g) = n$, wtedy

$$G = \{g, g^2, g^3, \ldots, g^{n-1}, g^n = e\}$$

$$g^k \cdot g^l = g^{k+l} \cdot g^{m \cdot n} = g^{k+l \pmod n} = g^{k +_n l}$$

Tw. Niech $(G, \cdot)$ grupa cykliczna.
1. $|G| = n < \infty$ to $G \cong C_n$
2. $|G| = \aleph_0$ to $G \cong (\mathbb{Z}, +)$.

D-d. 1. Niech $|G| = n$, Niech $\langle g \rangle = G$.

Wtedy $G = \{g, g^2, \ldots, g^{n-1}, g^0 = e\}$

Funkcja $\varphi(k) = g^k : C_n \to G$ jest izomorfizmem:

- φ jest homomorfizmem:

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

- φ jest na:
Niech $x \in G$, wtedy ist $k \in \{0, \dots n-1\}$ $x = g^k$
i wtedy
$$\varphi(k) = g^k = x, \quad \varphi \text{ jest na}.$$

- φ jest 1-1.

Zatem φ jest izomorfizm □

Wniosek. Jeśli G, H grupy cykliczne, $|G| = |H|$
$G \cong H$

D-d. Oznaczmy $|G| = |H| = n$.
Wtedy $\left.\begin{matrix} G \cong C_n \\ H \cong C_n \end{matrix}\right\} \to G \cong H.$ □

Lemat. Niech $\varphi : G \to H$ homomorfizm, $A \leq H$.
Wtedy $\varphi^{-1}(A) \leq G$

D-d ćw.

Fakt. Podgrupa grupy cyklicznej jest cykliczna.

- D-d.
Wiemy: każda podgrupa grupy $(\mathbb{Z}, +)$ jest cykliczna.

Wystarczy pokazać dla grup C_n:

Rozważmy homomorfizm $\varphi_n : \mathbb{Z} \to C_n$

$$\varphi_n(k) = k \pmod n.$$

Niech $A \leq C_n$, Cel: A jest cykliczna.
Wtedy $\varphi_n^{-1}(A) \leq \mathbb{Z}$.

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi_n} & C_n \\ \varphi_n^{-1}(A) & & A \\ g & & \varphi_n(g) \end{array}$$

Lista: $\varphi_n^{-1}(A)$ jest grupa cyklicza.

tzn $\exists g \in \varphi_n^{-1}(A) : \langle g \rangle = \varphi_n^{-1}(A)$.

Wtedy $\langle \varphi(g) \rangle = A$. ... □

Fakt Niech $(G, \cdot)$ grupa cykliczna $\langle g \rangle = G$, $\operatorname{ord} g = n$.
Wtedy dla $k \in \{0, \dots n-1\}$

$$\langle g^k \rangle = \langle g^{NWD(n,k)} \rangle.$$

D-d. Należy pokazać $\supseteq, \subseteq$:

$\langle g^k \rangle \subseteq \langle g^{NWD(n,k)} \rangle$:
Niech $x \in \langle g^k \rangle$ tzn $x = (g^k)^l$ $l \in \mathbb{N}$.

Wiemy, że $NWD(n,k) \mid k$ więc $\exists t \in \mathbb{N}$ $k = t \cdot NWD(n,k)$.

Wtedy $x = g^{kl} = g^{NWD(n,k) \cdot t \cdot l} = \left(g^{NWD(n,k)}\right)^{t \cdot l} \in \langle g^{NWD(n,k)} \rangle$

$\supseteq$ ćwiczenie. □

- Podgrupy n-elementowej grupy cyklicznej. $G = \langle g \rangle$

- Podgrupy grupy cyklicznej są cykliczne, więc są postaci

$$H = \langle x \rangle = \langle g^k \rangle.$$

- Podgrupy są postaci $\langle g^k \rangle$: $k \mid n$.

$\langle g^k \rangle = \langle g^{NWD(n,k)} \rangle$ ponieważ $NWD(n,k) \mid n$

- Jeśli $k \mid n$ to $|\langle g^k \rangle| = \frac{n}{k}$.

Zbiór podgrup $G = \langle g \rangle$ jest równy

$$\{ \langle g^k \rangle : k \mid n \}$$

- Niech $H_1, H_2 \leq G$. Jeśli $|H_1| = |H_2| \Rightarrow H_1 = H_2$.

bo jeśli $|H_1| = |H_2| = m$ to

$$H_1 = \langle g^{\frac{n}{m}} \rangle$$
$$\| $$
$$H_2 = \langle g^{\frac{n}{m}} \rangle$$

□

Rzędy elementów w grupie cyklicznej n-elementowej.

Fakt. g^k jest generatorem $G = \langle g \rangle \iff$

$$NWD(n,k) = 1$$

$\leftarrow$:

D-d: Jeśli $NWD(n,k) = 1$ to

$$\langle g^k \rangle = \langle g^{NWD(n,k)} \rangle = \langle g^1 \rangle = \langle g \rangle = G.$$

$\rightarrow$: Niewprost Niech $NWD(n,k) = m > 1$

Wtedy $\langle g^k \rangle = \langle g^{NWD(n,k)} \rangle = \langle g^m \rangle = \{e, g^m, g^{2m} \dots g^{\frac{n}{m}-1}\}$

$|\langle g^k \rangle| = \frac{n}{m} < n$, $\langle g^k \rangle \neq G$. $\square$

Fakt. Liczba generatorów grupy G. jest równa $\varphi(|G|)$.

$|\{k \in \{1, \dots, n-1\} : \langle g^k \rangle = G\}| = |\{k \in \{1 \dots, n-1\} : NWD(n,k) = 1\}|$

$= \varphi(n)$ $\square$

Fakt Niech $G = \langle g \rangle$, $ord(g) = n$. , $k \in \mathbb{N}$

1. $k \nmid n$: $|\{x \in G : ord\, x = k\}| = 0$

2. $k | n$ $|\{x \in G : ord\, x = k\}| = \varphi(k)$

D-d: Niech $x, y \in G$ $ord\, x = ord\, y = k$.
Wtedy $\langle x \rangle = n = \langle y \rangle$
Więc $\langle x \rangle = \langle y \rangle$.
Niech $x \in G$ $ord\, x = k$, wtedy wszystkie
elementy rzędu k należą do $\langle x \rangle$
Dokładnie, elementy rzędu k są generatorami $\langle x \rangle$.
$\langle x \rangle$ - k-elementowa grupa cykliczna.

Więc $|\{x \in G : ord\, x = k\}| = |\{y \in \langle x \rangle : y - \text{generator } \langle x \rangle\}| = \varphi(k)$ $\square$

Przykład. $G = C_{12}$: elementy rzędu 5 $\rightarrow$ 0 sztuk bo $5 \nmid 12$.
elementy rzędu 3 $\rightarrow$ $\varphi(3) = 2$

Wniosek. Niech $n \in \mathbb{N}^+$. Wtedy

$$\sum_{k|n} \varphi(k) = n.$$

D-d. Niech $G = \langle g \rangle$, $|G| = n$.
Dla $k \in \mathbb{N}^+$ oznaczmy $A_k = \{x \in G : \operatorname{ord} x = k\}$
Wiemy:

(1) $k \nmid n$ $\quad A_k = \emptyset$.
(2) $k \neq l$ $\quad A_k \cap A_l = \emptyset$.

Wtedy $G = \bigcup_{k \in \mathbb{N}} A_k \overset{1}{=} \bigcup_{k|n} A_k$.

$$n = |G| = \left|\bigcup_{k|n} A_k\right| \overset{2}{=} \sum_{k|n} |A_k| = \sum_{k|n} \varphi(k) \quad \square$$

TW. Niech p liczba pierwsza.
Wtedy grupa $\mathbb{Z}_p^* = (\{1, \dots, p-1\}, \cdot_p)$ jest cykliczna.

D-d. Wystarczy pokazać, że w $\mathbb{Z}_p^*$ istnieje element rzędu $p-1$.
($\mathbb{Z}_p$ $+_p$, $\cdot_p$) ciało
Niech $k \in \mathbb{N}$. Liczba elementów rzędu k w $\mathbb{Z}_p^*$

- $k \nmid p-1$ to nie ma elementów rzędu k.

- $k \mid p-1$:
Liczba elementów rzędu k jest równa 0 lub $\varphi(k)$:

bo: Niech $x \in G$ element rzędu k.
$B_k = \{y \in G : \operatorname{ord} y = k\} \neq \emptyset$.

Każdy $y \in B_k$ spełnia równanie $y^k = 1$

B_k

- $|\{y \in \mathbb{Z}_p : y^k = 1\}| \leq k$.
- Wszystkie $x^1, x^2, x^3, \ldots, x^{k-1}, x^k = 1$. są różnymi rozwiązaniami równania $y^k = 1$

$$|\{y \in \mathbb{Z}_p : y^k = 1\}| = k.$$

$(\{y \in \mathbb{Z}_p : y^k = 1\}, \cdot_p)$ - jest grupą cyklliczną.

Liczba elementów rzędu k w $\mathbb{Z}_p^*$ jest równa $\varphi(k)$ □

Niech $a_k \in \mathbb{N}$ liczba elementów rzędu k w $\mathbb{Z}_p^*$

$k \nmid p-1$ $\quad a_k = 0$

$k \mid p-1$ $\quad a_k = 0$ v $a_k = \varphi(k)$.

Niech $A_k = \{x \in \mathbb{Z}_p^* : \operatorname{ord} x = k\}$ $\quad |A_k| = a_k$

$$\mathbb{Z}_p^* = \bigcup_{k \in \mathbb{N}} A_k$$

$$p-1 = |\mathbb{Z}_p^*| = \left|\bigcup_{k \in \mathbb{N}} A_k\right| = \left|\dot{\bigcup_{k \mid p-1}} A_k\right| = \sum_{k \mid p-1} |A_k| = \sum_{k \mid p-1} a_k$$

$$\leq \sum_{k \mid p-1} \varphi(k) = p-1$$

równość gdy

$\forall k \mid p-1 \quad a_k = \varphi(k)$

Zatem dla $k = p-1$: $\quad a_{p-1} = \varphi(p-1) > 0$

$$|A_{p-1}| > 0$$

Zatem istnieje element rzędu $p-1$ w $\mathbb{Z}_p^*$. Jest to generator $\mathbb{Z}_{p-1}$ □