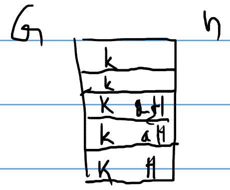
Przypomnienie



$H \leq G$, to $G = \bigcup aH$

$|aH| = |bH| = |H|$

$|H| \mid |G|$

Tw. Lagrange'a.

• Podgrupa generowana przez zbiór.

Lemat. Niech $(G, \cdot)$ grupa $\mathcal{A}$ rodzina podgrup grupy G.
Wtedy $\bigcap \mathcal{A} \leq G$.

D-d. 1. Niech $a, b \in \bigcap \mathcal{A}$.
Wtedy

$$a \in \bigcap \mathcal{A} \iff \forall H \in \mathcal{A} \quad a \in H$$
$$b \in \bigcap \mathcal{A} \iff \forall H \in \mathcal{A} \quad b \in H$$

Więc, $\forall H \in \mathcal{A} \quad H \leq G$

$\forall H \in \mathcal{A} \quad a \cdot b \in H$

$\iff a \cdot b \in \bigcap \mathcal{A}$

2. Niech $a \in \bigcap \mathcal{A}$ ... $a^{-1} \in \bigcap \mathcal{A}$ cbdo.

□

Def. Niech $(G, \cdot)$ grupa $A \subseteq G$.
Podgrupą generowaną przez A nazywamy najmniejszą podgrupę G zawierającą A.

tzn $\langle A \rangle = \bigcap \{ H \leq G : A \subseteq H \}$.

Uwaga. Niech $A \subseteq G$ - grupa. Wtedy:

$$\langle A \rangle = \{ a_1^{n_1} \cdot a_2^{n_2} \cdots a_k^{n_k}, \ k \in \mathbb{N}^+, \ a_i \in A, \ n_i \in \mathbb{Z} \}$$

$$X$$
$$\shortparallel$$

D-d.

1. $\{a_1^{n_1} \cdots a_k^{n_k} : k \in \mathbb{N}^+ \; a_i \in A_i \; n_i \in \mathbb{Z}\} \subseteq \langle A \rangle$

Niech $h \in X$, tzn $h = a_1^{n_1} \cdot a_2^{n_2} \cdots a_k^{n_k}$

Niech $H \leq G$, $H \supseteq A$.

Wtedy $a_1 \ldots a_k \in A \subseteq H$

Więc $h = a_1^{n_1} a_2^{n_2} \cdots a_k^{n_k} \in H$

Więc $\forall H \in \{H \leq G : A \subseteq H\} \quad h \in H$

Więc

$$h \in \bigcap \{H \leq G : A \subseteq H\} = \langle A \rangle.$$

$\langle A \rangle \subseteq X$ ćw. $\square$

Przykład. $G = (\mathbb{Z}, +)$, $A = \{12, 15\}$

Uwaga $\langle A \rangle = \{12k + 15l : k, l \in \mathbb{Z}\} = 3\mathbb{Z}$.

bo $\forall z \quad 3 | z \to \exists k, l \quad 12k + 15l = z$.

- Podgrupa generowana przez jeden element:

$(G, \cdot)$ grupa $g \in G$.

Wtedy $\langle g \rangle \overset{u}{=} \{g^n : n \in \mathbb{Z}\} = \{\ldots g^{-2}, g^{-1}, e, g, g^2, g^3, g^4 \ldots\}$

I $ord(g) = k$ to $\langle g \rangle = \{ \quad , g, g^2, g^3, \ldots, \underset{\underset{g^{-1}}{\shortparallel}}{g^{k-1}}, e, g, \ldots\}$

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

Obserwacja • Niech $(G, \cdot)$ grupa, $g \in G$

$|\langle g \rangle| = ord(g)$

• $g^{ord\, g} = e$.

Fakt. Niech $(G, \cdot)$ grupa skończona, $g \in G$

Wtedy $g^{|G|} = e$.

D-d. Z tw. Lagrange'a: $|\langle g \rangle| \mid |G|$.
tzn. $\exists k \in \mathbb{N}$ $|G| = k |\langle g \rangle| = k \cdot \operatorname{ord}(g)$

Więc $g^{|G|} = g^{\operatorname{ord}(g) \cdot k} = \left(g^{\operatorname{ord}(g)}\right)^k = e^k = e$ $\square$.

- Grupa $\mathbb{Z}_n^*$:

- Wiemy $(\mathbb{Z}_n, +_n, \cdot_n)$ pierścień przemienny.

- Niech $(P, +, \cdot)$ pierścień z 1, $a \in P$ nazywamy elementem odwracalnym gdy $\exists b \in P$ $a \cdot b = 1$

- $P^* = \{a \in P : a \text{ odwracalny}\}$
- Fakt $(P^*, \cdot)$ jest grupą.

- Grupa $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \text{ odwracalny}\}$

$\{a \in \{0, 1, \ldots n-1\} \text{ a odwracalny}\}$.

Fakt. $a \in \{0, \ldots n-1\}$ jest odwracalny w $\mathbb{Z}_n$
$\iff$
$NWD(a, n) = 1$.

Uwaga Niech $p \in \mathbb{P}$ - pierwsza, $\mathbb{Z}_p^* = \{1, 2, \ldots p-1\}$
Wniosek $p \in \mathbb{P}$
$\mathbb{Z}_p^* = (\{1, 2, \ldots p-1\}, \cdot_p)$ jest grupą.

Przypomnienie: Niech $n \in \mathbb{N}^+$
$\varphi_n(k) = k \bmod (n) : \mathbb{Z} \to \{0, \dots, n-1\}$
jest homomorfizmem pierścieni $(\mathbb{Z}, +, \cdot) \to \mathbb{Z}_n$
$[\varphi_n(a \pm b) = \varphi_n(a) \pm_n \varphi_n(b). \quad \varphi_n(a \cdot b) = \varphi_n(a) \cdot \varphi_n(b)]$

Ozn: $a \equiv b \pmod n \Leftrightarrow n \mid a-b$,
$\cdot\ \varphi_n(a) \equiv a \pmod n$

TW Małe twierdzenie Fermata.

Niech $p \in \mathbb{P}$, $a \in \mathbb{N}$, a i p względnie pierwsze.
Wtedy
$$a^{p-1} \equiv 1 \pmod p$$

D-d $\cdot\ g^{|G|} = e$ stosujemy do grupy $\mathbb{Z}_p^*$.

Niech $p \in \mathbb{P}$, $NWD(a, p) = 1$.
$$\varphi_p(a^{p-1}) = \varphi_p(a)^{p-1} = \underbrace{\varphi_p(a)}_{\in \mathbb{Z}_p^*}{}^{|\mathbb{Z}_p^*|} = 1$$

$$\varphi_p(a^{p-1}) = 1$$
$$a^{p-1} \equiv 1 \bmod p \qquad \square$$

• TW. Eulera - Fermata.

Def. Funkcja Eulera nazywamy funkcję
$$\varphi(n) = |\mathbb{Z}_n^*|$$

Uwaga.

- $\varphi(n) = |\mathbb{Z}_n^*| = |\{a \in \{1,2,\dots,n-1\} : NWD(a,n)=1\}|$
- $\varphi(10) = |\{1\ \cancel{2}\ 3\ \cancel{4}\ \cancel{5}\ \cancel{6}\ 7\ \cancel{8}\ 9\}| = |\{1,3,7,9\}| = 4$
- Niech $p \in \mathbb{P}$ $\quad \varphi(p) = p-1$
- Niech $p \in \mathbb{P}, n \in \mathbb{N}$ $\quad \varphi(p^n) = (p^n - 1) - (p^{n-1} - 1) = p^n - p^{n-1}$

TW Eulera - Fermata

Niech $n \in \mathbb{N}^+$ $a \in \mathbb{N}$ $NWD(a,n) = 1$.

Wtedy:

$$a^{\varphi(n)} \equiv 1 \pmod n$$

D-d Zastosowanie Uwagi: $g^{|G|} = e$ do $\mathbb{Z}_n^*$:

$$\varphi_n(a^{\varphi(n)}) = \underbrace{\varphi_n(a)}_{\mathbb{Z}_n^*}{}^{\varphi(n)} = \varphi_n(a)^{|\mathbb{Z}_n^*|} \overset{u}{=} 1$$

Ozn:

$$a^{\varphi(n)} \equiv 1 \pmod n \qquad \square$$

Zastosowanie TW E-F:

Podaj resztę z dzielenia przez 10 liczby 7^{67}

1 $\varphi(10) = 4$

TW EF: $\quad 7^4 \equiv 1 \bmod 10$

$$7^{67} = 7^{4\cdot 16} \cdot 7^3 = (7^4)^{16} \cdot 7^3 \equiv_{10} (1)^{16} \cdot 7^3 = 7^3 = 49 \cdot 7 \equiv_{10}$$

$$9 \cdot 7 \equiv 63 \equiv 3$$

Reszta z dzielenia przez 10 jest równa

$$\varphi_{10}(7^{67}) = \varphi_{10}\left((7^4)^{16} \cdot 7^3\right) \overset{tw}{=} \varphi_{10}\left((7^4)^{16}\right) \cdot_{10} \varphi_{10}(7^3) =$$

$$\Big(\underbrace{\varphi_{10}(7^4)}_{1}\Big)^{16} \cdot_{10} \left(\varphi_{10}(7)\right)^3 = 1^{16} \cdot_{10} 7^3 = 7^3 \pmod{10}$$

$$= 3. \quad \square$$

TW Jeśli $m, n \in \mathbb{N}^+$ względnie pierwsze, to

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

Wniosek Każda liczba naturalna

$$N = p_1^{k_1} \cdot p_2^{k_2} \cdots p_t^{k_t}$$

$$\varphi(N) = \ldots$$