4. Wykład 4: Rząd elementu grupy. Grupy cykliczne.

Definicja 4.1. *Niech $(G, \cdot)$ będzie grupą, $a \in G$. Podgrupę $\langle a \rangle$ nazywamy* **podgrupą cykliczną generowaną przez element** *a. Mówimy, że grupa G jest* **cykliczna**, *gdy istnieje element $g \in G$ taki, że $G = \langle g \rangle$. Element g nazywamy* **generatorem** *grupy G.*

Przykłady:

(1) Niech $G = \mathbb{Z}$. Wtedy $\langle 1 \rangle = \mathbb{Z}$.
(2) Niech $G = \mathbb{Z}_n$. Wtedy $\langle 1 \rangle = \mathbb{Z}_n$.

Twierdzenie 4.1. *Jeśli rząd grupy G jest liczbą pierwszą, to G jest cykliczna i nie zawiera podgrup właściwych.*

Dowód. Rozważmy grupę $(G, \cdot)$ i niech $|G| = p$, $p \in \mathbb{P}$. Pokażemy, że G jest cykliczna. Ustalmy $1_G \neq a \in G$. Wówczas $\langle a \rangle < G$ oraz $\langle a \rangle \neq \{1\}$. Wobec twierdzenia Lagrange'a, $|\langle a \rangle| | p$. Zatem $|\langle a \rangle| = p$, czyli $\langle a \rangle = G$.

Pokażemy, że G nie zawiera podgrup właściwych. Ustalmy $H < G$. Z twierdzenia Lagrange'a wynika, że $|H| | p$. Zatem $|H| = 1$ lub $|H| = p$, czyli $H = \{1\}$ lub $H = G$. □

Uwaga 4.1. *Jeśli G jest grupą cykliczną, to rząd G nie musi być liczbą pierwszą – na przykład rozważmy $\mathbb{Z}_6$.*

Definicja 4.2. *Niech $(G, \cdot)$ będzie grupą, $a \in G$.* **Rzędem elementu** *a nazywamy rząd podgrupy cyklicznej generowanej przez a i oznaczamy $r(a)$.*

Przykłady:

(3) Rozważmy grupę $\mathbb{R}^*$. Wówczas:
- $\langle -1 \rangle = \{-1, 1\}$, więc $r(-1) = 2$;
- $\langle 2 \rangle = \{2^k : k \in \mathbb{Z}\}$, więc $r(2) = \infty$.

(4) Rozważmy grupę $\mathbb{Z}_6$. Wówczas:
- $\langle 2 \rangle = \{0, 2, 4\}$, więc $r(2) = 3$;
- $\langle 1 \rangle = \{0, 1, 2, 3, 4, 5\}$, więc $r(1) = 6$.

(5) Rozważmy grupę $\mathbb{Z}$. Wówczas:
- $\langle 1 \rangle = \mathbb{Z}$, więc $r(1) = \infty$.

(6) Rozważmy grupę $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$. Wówczas:
- $\langle S_1 \rangle = \{I, S_1\}$, więc $r(S_1) = 2$.

Uwaga 4.2. *Niech $(G, \cdot)$ będzie grupą, $a \in G$. Wówczas:*

(1) *$r(a) = 1$ wtedy i tylko wtedy, gdy $a = 1_G$;*
(2) *$r(a) = r(a^{-1})$;*
(3) *jeśli G jest skończona, to*

$$r(a) < \infty \text{ oraz } r(a) | |G|.$$

Dowód. (1) Oczywiste.

(2) Wystarczy zauważyć, że $\langle a \rangle = \langle a^{-1} \rangle$.

(3) Rząd elementu a jest skończony, ponieważ $r(a) = |\langle a \rangle|$ oraz $\langle a \rangle \subset G$, więc $|\langle a \rangle| < \infty$. Dalej, rząd elementu a dzieli rząd grupy G, ponieważ $r(a) = |\langle a \rangle|$ i na mocy twierdzenia Lagrange'a $|\langle a \rangle| | |G|$.

□

Twierdzenie 4.2. *Niech $(G, \cdot)$ będzie grupą, $a \in G$.*

(1) *Jeśli nie istnieje* $n \in \mathbb{N}$ *takie, że* $a^n = 1_G$, *to* $r(a) = \infty$.
(2) *Jeśli istnieje* $n \in \mathbb{N}$ *takie, że* $a^n = 1_G$, *to*

$$r(a) = \min\{n \in \mathbb{N} : a^n = 1_G\}.$$

Dowód. (1) Zgodnie z definicją, $r(a) = |\langle a\rangle|$ oraz $\langle a\rangle = \{a^k : k \in \mathbb{Z}\}$. Pokażemy, że jeśli $i \neq j$, to $a^i \neq a^j$. Ustalmy i, j, $i > j$ oraz przypuśćmy, że $a^i = a^j$. Wówczas $a^{i-j} = 1_G$ oraz $i - j \in \mathbb{N}$, co jest sprzeczne z założeniem o nieistnieniu $n \in \mathbb{N}$ takiego, że $a^n = 1_G$.

Tym samym $\langle a\rangle$ zawiera nieskończenie wiele parami różnych elementów, czyli $r(a) = \infty$.

(2) Tak jak poprzednio, $r(a) = |\langle a\rangle|$ oraz $\langle a\rangle = \{a^k : k \in \mathbb{Z}\}$. Niech $k = \min\{n \in \mathbb{N} : a^n = 1_G\}$. Pokażemy, że $|\langle a\rangle| = \{1_G, a^1, a^2, \ldots, a^{k-1}\}$. Inkluzja ($\supset$) jest oczywista, a dla dowodu inkluzji ($\subset$) ustalmy $g \in |\langle a\rangle|$. Wówczas $g = a^m$, dla pewnego $m \in \mathbb{Z}$. Dzieląc z resztą m przez k otrzymujemy istnieje $q, r \in \mathbb{Z}$ takich, że

$$m = kq + r \text{ oraz } 0 \leq r < k.$$

Dalej, $a^m = a^{kq+r} = (a^k)^q a^r = a^r \in \{1, a^1, a^2, \ldots, a^{k-1}\}$.

Pozostaje pokazać, że zbiór $\{1, a^1, a^2, \ldots, a^{k-1}\}$ zawiera k elementów. Przypuśćmy bowiem, że istnieją $i, j \in \{0, 1, \ldots, k-1\}$, $i > j$, takie, że $a^i = a^j$. Wówczas $a^{i-j} = 1_G$, ale $0 < i - j < k$, co jest sprzeczne z wyborem k.

□

Przykłady:

(7) Rozważmy grupę $U(\mathbb{Z}_{10}) = \{1, 3, 7, 9\}$. Wówczas $r(3) = 4$.
(8) Rozważmy grupę $D(3) = \{ID_3, O_1, O_2, S_1, S_2, S_3\}$. Wówczas $r(O_2) = 3$.

Wniosek 4.1. *Niech* $(G, \cdot)$ *będzie grupą.*

(1) *Jeżeli* G *jest skończona i* $|G| = n$, *to* $\forall a \in G(a^n = 1_G)$.
(2) *Jeżeli* $a \in G$ *i* $r(a) = k$, *to* $a^k = 1_G$.
(3) *Jeżeli* $a \in G$, $r(a) = k$ *i* $a^m = 1_G$, *to* $k \leq m$.

Przykład:

(9) Rozważmy grupę $U(\mathbb{Z}_8) = \{1, 3, 5, 7\}$. Wówczas $3^4 = 1$, ale $r(3) = 2$.

Twierdzenie 4.3. *Niech* $(G, \cdot)$ *będzie grupą,* $a \in G$. *Jeżeli* $a^m = 1_G$, *to wówczas* $r(a)|m$.

Dowód. Niech $r(a) = k$. Przypuśćmy, że $k \nmid m$. Dzieląc z resztą m przez k otrzymujemy istnieje liczb całkowitych $q, r \in \mathbb{Z}$ takich, że

$$m = kq + r \text{ oraz } 0 < r < k.$$

Dalej, $1_G = a^m = a^{kq+r} = (a^k)^q a^r = a^r$, co daje sprzeczność z Twierdzeniem 4.2. □

Wniosek 4.2. *Niech* $(G, \cdot)$ *będzie grupą skończoną. Wówczas* G *jest cykliczna wtedy i tylko wtedy, gdy istnieje* $a \in G$ *taki, że* $r(a) = |G|$.

Dowód. ($\Rightarrow$): oczywiste. ($\Leftarrow$): niech $a \in G$ będzie taki, że $r(a) = |G|$; wówczas $|\langle a\rangle| = |G|$ oraz $\langle a\rangle < G$, czyli $\langle a\rangle = G$. □

Przykłady:

(10) $\mathbb{Z}_5$ jest cykliczna, gdyż $r(1) = 5$.
(11) $U(\mathbb{Z}_8)$ nie jest cykliczna, gdyż

$$r(1) = 1, r(3) = 2, r(5) = 2 \text{ oraz } r(7) = 2.$$

(12) $\mathbb{Z}_2 \times \mathbb{Z}_2$ nie jest cykliczna, gdyż

$$r((0,0)) = 1, r((1,0)) = 2, r((0,1)) = 2 \text{ oraz } r((1,1)) = 2.$$

(13) $\mathbb{Z}_2 \times \mathbb{Z}_3$ jest cykliczna, gdyż $r((1,2)) = 6$.

Twierdzenie 4.4. (1) *Dowolna grupa cykliczna jest abelowa.*
(2) *Podgrupa grupy cyklicznej jest cykliczna.*

Dowód. (1) Niech $G = \langle a \rangle$. Ustalmy $x, y \in G$. Wtedy $x = a^k$, $y = a^l$, dla pewnych $k, l \in \mathbb{Z}$. Natenczas

$$xy = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = yx.$$

(2) Niech $G = \langle a \rangle$. Ustalmy $H < G$. Możemy założyć, że $H \neq \{1_G\}$ (oczywiście podgrupa trywialna $\{1_G\}$ jest cykliczna). Ustalmy $c \in H$, $c \neq 1_G$. W szczególności $c = a^k$, dla pewnego $k \in \mathbb{Z}$. Możemy założyć, że $k \in \mathbb{N}$, gdyż jeśli $k < 0$, to $c^{-1} = a^{-k} \in H$. Niech $n = \min\{l \in \mathbb{N} : a^l \in H\}$.

Pokażemy, że $H = \langle a^n \rangle$. Inkluzja ($\supset$) jest oczywista, skupmy się na dowodzie inkluzji ($\subset$). Ustalmy $x \in H$. Wówczas $x = a^m$, dla pewnego $m \in \mathbb{Z}$. Dzieląc z resztą m przez n otrzymujemy istnieje liczb całkowitych $q, r \in \mathbb{Z}$ takich, że

$$m = nq + r \text{ oraz } 0 < r < n.$$

Dalej, $a^m = a^{nq+r} = (a^n)^q a^r$, a więc $a^r = a^m (a^n)^{-q} \in H$. Wobec wyboru n, jedyną możliwością staje się, aby $r = 0$. Wówczas $m = nq$, a stąd $x = a^m = (a^n)^q \in \langle a^n \rangle$.

□

Uwaga 4.3. *Z przeprowadzonego dowodu wynika, że jeśli $(G, \cdot)$ jest grupą cykliczną, $G = \langle a \rangle$ oraz $\{1_G\} \neq H < G$, to $H = \langle a^n \rangle$, gdzie*

$$n = \min\{l \in \mathbb{N} : a^l \in H\}.$$

Przykład:

(14) Rozważmy grupę $\mathbb{Z}$ oraz $H = \langle m, n \rangle < \mathbb{Z}$. H jest cykliczna oraz

$$H = \langle a^d \rangle, d = \min\{l \in \mathbb{N} : 1 \cdot l \in H\}.$$

Ponieważ $H = \{xm + yn : x, y \in \mathbb{Z}\}$, więd d jest najmniejszą z liczb naturalnych postaci $xm + yn$, a więc, wobec algorytmu Euklidesa, $d = NWD(m, n)$.