2. Zbiór generatorów grupy. Grupa cykliczna, rząd elementu

Teorię grup zacznijmy od następującego oczywistego stwierdzenia.

2.1. Stwierdzenie. *Jeżeli $\{H_i\}_{i\in I}$ jest rodziną podgrup grupy G, to zbiór $\bigcap_{i\in I} H_i \leqslant G$ jest podgrupą grupy G.*

Wobec tego, dla dowolnego podzbioru $X \subseteq G$ istnieje najmniejsza podgrupa grupy G zawierająca X. Nazywamy ją **podgrupą generowaną** przez X i oznaczamy symbolem $\langle X \rangle$.

Oczywiście $\langle \emptyset \rangle = \mathbf{1}$.

2.2. Stwierdzenie. *Jeżeli $X \neq \emptyset$, to*

$$\langle X \rangle = \{g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_k^{\varepsilon_k} \colon k \in \mathbb{N},\ \varepsilon_i = \pm 1,\ g_i \in X\}.$$

Dowód. Jest jasne, że zbiór elementów tej postaci tworzy podgrupę grupy G i jest zawarty w każdej podgrupie grupy G zawierającej X. □

Jeżeli $\langle X \rangle = G$, to X nazywamy zbiorem generatorów G. Mówimy, że grupa jest skończenie generowana jeżeli posiada skończony zbiór generatorów.

2.3. Definicja. *Grupę G nazywamy* **cykliczną** *jeżeli istnieje element $g \in G$, taki że $\langle g \rangle = G$.*

2.4. Twierdzenie. *Grupy $\mathbb{Z}_n$ i $\mathbb{Z}$ są cykliczne. Każda grupa cykliczna jest izomorficzna z jedną z nich.*

Dowód. $\mathbb{Z} = \langle 1 \rangle$, $\mathbb{Z}_n = \langle \exp(\frac{2\pi i}{n}) \rangle$, zatem grupy te są cykliczne.

Niech $G = \langle g \rangle$, czyli $G = \{g^i, i \in \mathbb{Z}\}$.

Przypuśćmy, że istnieje $n \in \mathbb{N}$, takie że $g^n = 1$ i załóżmy, że n jest najmniejszą liczbą naturalną o tej własności. Każda liczba całkowita $k \in \mathbb{Z}$ może być przedstawiona w postaci $k = ln + r$, gdzie $r \in \{0, 1, \ldots, n-1\}$, a zatem $g^k = g^r$. Wynika stąd, że $G = \{1, g, \ldots, g^{n-1}\}$. Wszystkie te elementy są różne (z równości $g^i = g^j$ wynika bowiem $g^{i-j} = 1$). Zatem $|G| = n$ i przekształcenie $\varphi : \mathbb{Z}_n \longrightarrow G$, $\varphi(\exp(\frac{2\pi i m}{n})) = g^m$ jest izomorfizmem.

Jeżeli nie istnieje $n \in \mathbb{N}$, takie że $g^n = 1$, to wszystkie elementy $\{g^i, i \in \mathbb{Z}\}$ są różne, $|G| = \infty$, a odwzorowanie $\varphi : \mathbb{Z} \longrightarrow G$, zadane wzorem $\varphi(m) = g^m$ jest izomorfizmem. □

2.5. Twierdzenie. *Niech G będzie grupą cykliczną. Wówczas:*

1) Jeżeli $H \leqslant G$, to H jest grupą cykliczną.

2) Jeżeli $H \leqslant G$ i $|G| < \infty$, to $|H| \,\big|\, |G|$.

3) Jeżeli $|G| < \infty$, to dla każdego $l \,\big|\, |G|$ istnieje dokładnie jedna podgrupa $H \leqslant G$, taka że $|H| = l$.

Dowód. Niech $G = \langle g \rangle$. Niech k będzie najmniejszą liczbą całkowitą i dodatnią, taką że $g^k \in H$. Jest jasne, że $\langle g^k \rangle \leqslant H$. Jeżeli $g^m \in H$, $m = ks + r$, $0 \leq r < k$, to $g^m = (g^k)^s g^r$, więc $g^r \in H$. Z minimalności k wynika, że $r = 0$, wobec czego $g^m = (g^k)^s \in \langle g^k \rangle$. Zatem $H = \langle g^k \rangle$, co kończy dowód 1).

Zakładamy teraz, że $|G| < \infty$. Niech więc $|G| = n$, i $n = kl + r$, $r < k$. Ponieważ $g^n = 1 \in H$, zatem, tak jak poprzednio, z minimalności k wynika, że $k \,|\, n$. Wówczas $H = \{1, g^k, g^{2k}, \ldots, g^{(l-1)k}\}$ i $|H| = \frac{n}{k}$, co kończy dowód punktu 2). Punkt 3) wynika już z tych rozważań – jedyną taką podgrupą jest $H = \langle g^k \rangle$, gdzie $k = \frac{n}{l}$.□

2.6. Definicja. **Rzędem** *elementu $g \in G$ nazywamy liczbę $|\langle g \rangle|$, czyli rząd podgrupy generowanej przez element g. Rząd elementu g oznaczamy symbolem $o(g)$.*

Z poprzednich rozważań wynika jasno, że jeżeli $o(g) < \infty$, to :
1. $o(g)$ jest najmniejszą liczbą naturalną n, taką że $g^n = 1$
2. $o(g) = n$ wtedy i tylko wtedy, gdy $g^n = 1$ i dla każdej liczby całkowitej k, takiej że $g^k = 1$, ma miejsce podzielność: $n \mid k$.
3. Jeżeli $\varphi : G \to H$ jest homomorfizmem, to dla każdego elementu $g \in G$ $o(\varphi(g)) \mid o(g)$.

2.7. Stwierdzenie. *Jeżeli $o(g) = n$, to $o(g^k) = \frac{n}{(n,k)}$.*

Dowód. Mamy $n = (n,k)m$ i $k = (n,k) \cdot l$, gdzie $(m,l) = 1$. Wynika stąd, że $(g^k)^m = g^{(n,k)lm} = g^{nl} = 1$, a zatem $o(g^k) \mid m$. Przypuśćmy, że $(g^k)^r = 1$. Wynika stąd, że $n \mid kr$, a zatem $m \mid lr$. Wobec $(m,l) = 1$, $m \mid r$, co dowodzi, że $o(g^k) = m$.□

Z poprzedniego stwierdzenia wynika, że jeżeli $G = \langle g \rangle$ i $|G| = n$, to generatorami G, czyli elementami rzędu n są elementy g^k, gdzie $(k,n) = 1$. Liczbę tych generatorów, to jest ilość takich liczb naturalnych nie większych od n, które są względnie pierwsze z n, oznaczamy symbolem $\varphi(n)$. Funkcję φ nazywamy funkcją Eulera.

2.8. Uwaga. *Jeżeli $k \mid n$, to w grupie cyklicznej rzędu n jest $\varphi(k)$ elementów rzędu k. Mamy więc*

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

2.9. Wniosek. *Jeżeli p jest liczbą pierwszą, to grupa $\mathbb{Z}_p$ nie posiada nietrywialnych podgrup właściwych, każdy element różny od neutralnego jest rzędu p i $\varphi(p) = p - 1$.*

2.10. Stwierdzenie. *Jeżeli $(k,n) = 1$, to $\mathbb{Z}_k \times \mathbb{Z}_n \cong \mathbb{Z}_{kn}$. W przeciwnym przypadku ten produkt nie jest grupą cykliczną.*

Dowód. Niech $g \in \mathbb{Z}_k$ i $h \in \mathbb{Z}_n$ będą generatorami. Element $(g,h)^l = (g^l, h^l)$ jest elementem neutralnym wtedy i tylko wtedy, gdy $n \mid l$ oraz $k \mid l$. Jeżeli $(k,n) = 1$, jest to równoważne $kn \mid l$, a zatem $o((g,h)) = kn = |\mathbb{Z}_k \times \mathbb{Z}_n|$ i grupa jest cykliczna. Jeżeli $(k,n) > 1$, to z tych rozważań wynika, że w $\mathbb{Z}_k \times \mathbb{Z}_n$ nie ma elementu rzędu kn. □

2.11. Wniosek. *Jeżeli $(k,n) = 1$, to $\varphi(kn) = \varphi(k)\varphi(n)$*

2.12. Wniosek. *Jeżeli p jest liczbą pierwszą, to w grupie $\mathbb{Z}_{p^n}$ jest dokładnie $\varphi(p^n) = p^n - p^{n-1}$ elementów rzędu p^n.*

Rzędy elementów w grupach permutacji

Znamy już grupy permutacji. Wiemy, że każda grupa jest, z dokładnością do izomorfizmu, podgrupą pewnej grupy permutacji. Teraz przyjrzymy się dokładniej grupom permutacji zbiorów skończonych. Dla ustalenia uwagi, załóżmy, że n–elementowy zbiór składa się z liczb $\{1, 2, \ldots, n\}$. Permutację $\sigma \in \Sigma_n$ możemy zapisać w postaci macierzowej:

$$\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

W górnym wierszu macierzy piszemy permutowane elementy, a w dolnym ich obrazy. Na przykład: $\gamma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ oznacza permutację γ, taką że $\gamma(1) = 3$, $\gamma(2) = 1$, $\gamma(3) = 4$, $\gamma(4) = 2$.

2.13. Definicja. *Permutację $\gamma \in \Sigma_n$ nazywamy* **cyklem** *długości k, jeżeli istnieją takie elementy $c_1, c_2, \ldots c_k$, że*

$$\gamma(c_i) = \begin{cases} c_{i+1} & gdy\ i < k \\ c_1 & gdy\ i = k, \end{cases}$$

przy czym dla każdego elementu x spoza tej listy zachodzi $\gamma(x) = x$.

Cykl taki będziemy oznaczać symbolem $\gamma = (c_1, \ldots, c_k)$. Oczywiście zapis ten ma sens tylko wtedy, gdy dobrze wiemy, na jakim zbiorze jest określona cała permutacja. Na przykład pytanie o to, czy permutacja $\sigma = (1, 4, 3, 2)$ ma punkty stałe jest bez sensu, jeżeli nie mamy zewnętrznej informacji o tym, na jakim zbiorze ta permutacja jest określona. Warto też zwrócić uwagę na fakt, że zapis ten nie jest jednoznaczny — równie dobrze można by napisać na przykład $\sigma = (2, 1, 4, 3)$.
Cykl długości dwa, (a, b), nazywamy **transpozycją** elementów a i b.

2.14. Definicja. *Cykle $\sigma = (b_1, b_2, \ldots, b_r) \in \Sigma_n$ i $\tau = (c_1, c_2, \ldots, c_s) \in \Sigma_n$ są rozłączne jeżeli $\{b_1, b_2, \ldots, b_r\} \cap \{c_1, c_2, \ldots, c_s\} = \emptyset$.*

Jest jasne, że dwa cykle rozłączne są przemienne.

2.15. Twierdzenie. *Każdą permutację można przedstawić jako iloczyn rozłącznych cykli. Przedstawienie to jest jednoznaczne z dokładnością do kolejności cykli.*

Dowód tego faktu przeprowadza się przez indukcję ze względu na moc permutowanego zbioru — jest on bardzo łatwy i pomijamy go. Ideę dowodu można łatwo zrozumieć analizując przykład.

Rozkład na cykle rozłączne permutacji:

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

W rozkładzie permutacji na cykle rozłączne często opuszcza się cykle długości jeden.

2.16. Stwierdzenie. *Jeżeli permutacja σ jest iloczynem cykli rozłącznych długości $n_1, n_2, \ldots, n_k$, to $o(\sigma) = NWW(n_1, n_2, \ldots, n_k)$*

Dowód. Cykle rozłączne są przemienne, zatem $o(\sigma) \,|\, NWW(n_1, n_2, \ldots, n_k)$. Z drugiej strony, skoro $\sigma^l = id$, to $l-$ ta potęga każdego cyklu jest identycznością (korzystamy tu z rozłączności cykli). Zatem dla każdego $1 \leq i \leq k$ mamy $n_i \,|\, l$, więc $NWW(n_1, n_2, \ldots, n_k) \,|\, o(\sigma)$. □