4. Działanie grupy na zbiorze

Znaczna część poznanych przez nas przykładów grup, to podgrupy grupy bijekcji jakiegoś zbioru. Często taka podgrupa składa się z bijekcji, które zachowują dodatkową strukturę geometryczną, topologiczną lub algebraiczną, zdefiniowaną na rozpatrywanym zbiorze.

4.1. Definicja. **Działaniem grupy** *G na zbiorze X nazywamy homomorfizm $\phi\colon G \longrightarrow \Sigma_X$. Działanie nazywamy wiernym, jeżeli ϕ jest monomorfizmem.*

Jeżeli zadane jest działanie grupy G na zbiorze X, to mówimy że X jest G – zbiorem. Zamiast oznaczenia $\phi(g)(x)$ będziemy na ogół używać bardziej czytelnego symbolu $\phi_g(x)$. W tym zapisie ϕ_g jest nazwą pewnej bijekcji zbioru X—bijekcji, którą homomorfizm ϕ przypisuje elementowi g z grupy G. Natomiast $\phi_g(x)$ oznacza wartość tej bijekcji dla argumentu x. Czasem stosuje się jeszcze bardziej uproszczony zapis: $g(x)$ zamiast $\phi_g(x)$.

4.2. Przykład. Dla dowolnej grupy G, niech $\psi_g : G \longrightarrow G$ będzie zadane wzorem $\psi_g(x) = gx$ (poza przypadkiem $g = 1$, ψ_g nie jest automorfizmem G lecz tylko bijekcją zbioru elementów). Przekształcenie $\psi : G \longrightarrow \Sigma_G$, $\psi(g) = \psi_g$ jest oczywiście monomorfizmem grup. Wobec tego prawdziwe jest następujące twierdzenie.

4.3. Twierdzenie Cayleya. *Każda grupa G jest izomorficzna z pewną podgrupą grupy bijekcji zbioru G. W szczególności każda grupa rzędu n jest izomorficzna z pewną podgrupą grupy Σ_n.*

4.4. Definicja. *Każdy element $g \in G$ grupy G wyznacza pewien automorfizm $\phi_g : G \longrightarrow G$, zadany wzorem $\phi_g(x) = gxg^{-1}$. Nazywamy go* **automorfizmem wewnętrznym** *grupy G wyznaczonym przez element g.*

Otrzymujemy homomorfizm $\phi : G \longrightarrow Aut(G)$, $\phi(g) = \phi_g$. Jest to ważny przykład działania grupy G na zbiorze jej elementów - nazywamu go działaniem poprzez automorfizmy wewnętrzne. Zauważmy, że

$$\ker \phi = \{g \in G : \forall_{x\in G}\ gx = xg\}.$$

Tak określona podgrupa ma swoją nazwę:

4.5. Definicja. *Podgrupę*

$$Z(G) = \{g \in G : \forall_{x\in G}\ gx = xg\} \leqslant G$$

nazywamy **centrum grupy.**

Przyjrzyjmy się bliżej strukturze dowolnego G—zbioru X.

4.6. Definicja.
Orbitą *punktu $x \in X$ nazywamy zbiór*

$$G(x) = \{g(x)\colon\ g \in G\} \subseteq X.$$

Punktem stałym *działania grupy G na zbiorze X nazywamy każdy punkt spełniający warunek $G(x) = \{x\}$ lub równoważnie $\forall_{g\in G}\ g(x) = x$. Zbiór punktów stałych oznaczamy symbolem X^G.*
Grupą izotropii *punktu $x \in X$ nazywamy podgrupę*

$$G_x = \{g \in G\colon g(x) = x\} \leqslant G.$$

4.7. Uwaga. *Jeżeli punkt $x' \in G(x)$, to $x' = g(x)$ dla pewnego $g \in G$ i wówczas $G_{x'} = g(G_x)g^{-1}$.*

Rozpatrzmy na zbiorze X relację zadaną wzorem

$$x \sim y \iff \exists_{g\in G} \quad y = g(x).$$

Bez trudu sprawdzimy, że relacja ta jest relacją równoważności, a klasą abstrakcji zawierającą punkt $x \in X$ jest orbita tego punktu $G(x)$. Zatem niepusty G–zbiór X jest sumą parami rozłącznych orbit.

4.8. Definicja. *Działanie grupy G na zbiorze X nazywamy* **tranzytywnym** *(inaczej: przechodnim) wtedy i tylko wtedy, gdy*

$$\forall_{x,\,y\in X}\ \exists_{g\in G}\ g(x) = y.$$

Zauważmy, że działanie na niepustym zbiorze jest tranzytywne wtedy i tylko wtedy, gdy ma dokładnie jedną orbitę.

Rozpatrzymy teraz podstawowy i w pewnym sensie uniwersalny przykład działania grupy:

4.9. Przykład. Niech G będzie dowolną grupą, a H jej podgrupą. Zdefiniujemy działanie $\phi : G \to \Sigma_{G/H}$, grupy G na zbiorze warstw lewostronnych G/H, wzorem $\phi_g(xH) = (gx)H$.

Odnotujmy następujące własności powyższego działania:

1. jest ono tranzytywne;
2. $G_{gH} = gHg^{-1}$.
3. jeżeli $H = \mathbf{1}$, to działanie jest wierne, czyli $\phi : G \to \Sigma_G$ jest monomorfizmem.

Zauważmy, że ten ostatni fakt, to znane nam już **Twierdzenie Cayley'a**. Wyjaśnienie, dlaczego powyższe działanie jest uniwersalnym przykładem, poprzedzimy definicją.

4.10. Definicja. *Mówimy, że dwa G–zbiory X i Y są G–izomorficzne, jeżeli istnieje bijekcja $f : X \to Y$, taka że*

$$\forall_{x\in X}\,\forall_{g\in G} \quad f(g(x)) = g(f(x)).$$

Zauważmy, że zachodzi łatwe, ale ważne stwierdzenie:

4.11. Stwierdzenie. *Niech X będzie G–zbiorem i niech $x \in X$. Wówczas przekształcenie $f_x : G/G_x \to G(x)$, zadane wzorem*

$$f_x(gG_x) = g(x),$$

jest G–izomorfizmem G–zbiorów.

Dowód. Zauważmy, że $gG_x = g'G_x$ wtedy i tylko wtedy, gdy $g'g^{-1} \in G_x$ czyli wtedy i tylko wtedy $g'g^{-1}(x) = x$, co jest równoważne $g(x) = g'(x)$. Wynika ztego, że f_x jest dobrze określone i różnowartościowe. To, że f_x jest "na" jest oczywiste. Co więcej f_x zachowuje działanie grupy G, to znaczy $f(g(g'G_x)) = g(f(g'G_x))$ dla każdego $g \in G$ i każdej warstwy w G/G_x. □

4.12. Wniosek. *Jeżeli X jest G–zbiorem, to dla każdego $x \in X$*

$$|G(x)| = [G\colon G_x],$$

gdzie $|G(x)|$ oznacza moc orbity $G(x)$.

Podsumowując: każdy G–zbiór jest rozłączną suma orbit, a każda orbita jest G–izomorficzna z dobrze znanym G–zbiorem (postaci G/H). Jeżeli X jest skończonym G–zbiorem, to moc X jest równa sumie długości orbit rozpatrywanego działania. Uwzględniając wzór na długość orbity podany we Wniosku 4.11 możemy to stwierdzenie zapisać w postaci następującego wzoru.

4.13. Stwierdzenie. *Jeżeli X jest skończonym niepustym G–zbiorem, to*

$$|X| = [G : G_{x_1}] + [G : G_{x_2}] + \cdots + [G : G_{x_n}], \tag{4.14}$$

gdzie $G(x_1)$, $G(x_2), \ldots, G(x_n)$ są wszystkimi orbitami działania G na X.

Zanotujmy jeszcze wniosek wypływający z powyższego stwierdzenia:

4.15. Wniosek. *Jeżeli X jest skończonym G–zbiorem i $|G| = p^k$, gdzie p jest liczbą pierwszą, to*

$$|X^G| \equiv |X| \pmod{p}.$$

Dowód. Suma długości orbit jednoelementowych jest oczywiście równa mocy zbioru punktów stałych. Z twierdzenia Lagrange'a i Wniosku 4.12 wynika zatem, że suma mocy pozostałych orbit jest podzielna przez p. □

Stwierdzenie 4.12 i Wniosek 4.13 są często używane w taki sposób, że dowodzi się iż grupa G nie może działać na zbiorze mocy n bez punktów stałych, bo liczba n nie daje się przedstawić w postaci sumy, takiej jak we wzorze (4.14), chyba że co najmniej jednym ze składników jest jedynka. Oczywiście dopuszczalne składniki muszą nie tylko być dzielnikami liczby $|G|$ ale muszą to być liczby wyrażające indeksy podgrup grupy G (wkrótce będziemy potrafili pokazać, że np. w grupie Σ_5, która jest rzędu 120, nie ma podgrupy indeksu 8, chociaż $120 = 8 \cdot 15$).

Wniosek 4.15 pozwala także na udowodnienie ważnego, a wcale nie oczywistego twierdzenia:

4.16. Twierdzenie Cauchy'ego. *Jeżeli G jest grupą skończoną i liczba pierwsza p jest dzielnikiem rzędu grupy G, to w G istnieje element rzędu p.*

Dowód. Niech $X = \{(g_1, g_2, \ldots, g_p) \in G \times G \times \cdots \times G\colon\ g_1 \cdot g_2 \cdot \ldots \cdot g_p = 1\}$. Zbiór X ma $|G|^{p-1}$ elementów, w szczególności

$$|X| \equiv 0 \pmod{p}.$$

Niech $f \in \Sigma_X$, $f(g_1, g_2, \ldots, g_p) = (g_p, g_1, g_2, \ldots, g_{p-1})$. Łatwo sprawdzić, że $o(f) = p$, a więc $\langle f \rangle \cong \mathbb{Z}_p$. Zauważmy, że

$$X^{\langle f \rangle} = \{(g, g, \ldots, g) \in G \times G \times \cdots \times G\colon\ g^p = 1\}.$$

Zgodnie z Wnioskiem 4.15

$$|X^{\langle f \rangle}| \equiv |X| \equiv 0 \pmod{p}.$$

Moc zbioru $X^{\langle f \rangle}$ jest na pewno różna od zera, bo na pewno $(1, 1, \ldots, 1) \in X^{\mathbb{Z}_p}$. Wobec faktu, że $p \,\big|\, |X^{\langle f \rangle}|$, zbiór $X^{\langle f \rangle}$ musi zawierać jeszcze co najmniej $p-1$ innych ciągów $(g, g, \ldots, g) \in X$, teraz już takich, że $g \neq 1$. Oczywiście z tego, że $g \neq 1$ i $g^p = 1$, gdzie p jest liczbą pierwszą, wynika że $o(g) = p$. □

Wróćmy do przykładu, od którego rozpoczęliśmy ten rozdział.

4.17. Przykład. Niech grupa G działa na zbiorze jej elementów przez automorfizmy wewnętrzne, $\phi : G \longrightarrow Aut(G)$. O automorfizmie wewnętrznym ϕ_g mówimy także, że jest sprzężeniem wyznaczonym przez element g. Jak się przekonamy, analiza tego działania odgrywa ważną rolę w badaniu struktury grupy i dlatego jego orbity i grupy izotropii mają odrębne nazwy:

orbitę $\{gxg^{-1} : g \in G\}$ elementu x nazywamy **klasą sprzężoności** elementu x;

grupę izotropii elementu x nazywamy **centralizatorem** elementu x w G i oznaczamy symbolem $C_G(x)$. Zatem

$$C_G(x) = \{g \in G : \, gxg^{-1} = x\},$$

a moc klasy sprzężoności elementu x jest równa $[G : C_G(x)]$.

Zbiór punktów stałych działania przez automorfizmy wewnętrzne ma już swoją nazwę — jest to **centrum** $Z(G)$ grupy G.

Jeżeli G jest grupą skończoną, to równość (4.14) występująca w Stwierdzeniu 4.13 nazywa się **równaniem klas** i przybiera postać:

$$|G| = |Z(G)| + [G : C_G(g_1)] + [G : C_G(g_2)] + \cdots + [G : C_G(g_k)], \tag{4.18}$$

gdzie $g_1, g_2, \ldots, g_k$ jest listą reprezentantów wszystkich nie jednoelementowych klas sprzężoności.

Zanotujmy ważny wniosek z równości 4.18.

4.19. Wniosek. *Jeżeli $|G| = p^k$, gdzie p jest liczbą pierwszą, $k > 0$, to centrum $Z(G)$ grupy G jest nietrywialne.*

Dowód. Z równości 3.13 wynika, że $|G| \equiv |Z(G)| \equiv 0 \pmod{p}$. Ponieważ $|Z(G)| \geq 1$ i $p \,\big|\, |Z(G)|$, to $|Z(G)| \geq p$, a więc centrum jest nietrywialne. □

4.20. Wniosek. *Jeżeli p jest liczbą pierwszą, to każda grupa G rzędu p^2 jest przemienna.*

Dowód. Mamy udowodnić, że $G = Z(G)$. Z poprzedniego wniosku wiemy, że w $Z(G)$ jest jakiś element nietrywialny x.

Jeżeli $\langle x \rangle = G$, to grupa G jest cykliczna, a więc przemienna.

Jeżeli $\langle x \rangle$ jest podgrupą właściwą, to istnieje jakiś element $y \in G$, taki że $y \notin \langle x \rangle$. Oczywiście $xy = yx$. Zatem $\langle x, y \rangle$ jest grupą przemienną. Ale $\langle x, y \rangle$, to już na pewno jest cała grupa G. □

Zastanówmy się jeszcze nad związkiem liczby klas sprzężoności grupy skończonej z jej rzędem - czy jeżeli grupa ma k klas sprzężoności, to jej rząd może być dowolnie duży? Okazuje się, że nie i że prawdziwy jest następujący fakt.

4.21. Stwierdzenie. *Dla liczby naturalnej $k \in \mathbb{N}$ istnieje liczba naturalna $B(k) \in \mathbb{N}$, taka że jeżeli grupa skończona G ma dokładnie k klas sprzężoności, to $|G| \leq B(k)$.*

Skorzystamy z łatwego lematu, którego dowód pozostawiamy czytelnikowi.

4.22. Lemat. *Dla ustalonej liczby naturalnej k i dodatniej liczby rzeczywistej a równanie*

$$\frac{1}{x_1} + \cdots + \frac{1}{x_k} = a$$

ma skończoną liczbę rozwiązań w zbiorze liczb naturalnych.

Dowód Stwierdzenia 4.21 Rozpatrzmy równanie klas:

$$|G| = [G : C_G(g_1)] + [G : C_G(g_2)] + \cdots + [G : C_G(g_k)],$$

gdzie $g_1, g_2, \ldots, g_k$ są reprezentantami wszystkich (także tych jednoelementowych) klas sprzężoności grupy G. Możemy założyć, że $g_1 = 1$. Korzystając z twierdzenia Lagrange'a i dzieląc obie strony równości przez $|G|$ otrzymujemy

$$1 = \frac{1}{|C_G(g_1)|} + \cdots + \frac{1}{|C_G(g_k)|}.$$

Ponieważ liczba rozwiązań równania $\frac{1}{x_1} + \cdots + \frac{1}{x_k} = 1$ jest skończona, to istnieje $B(k) \in \mathbb{N}$, zależne tylko od k i takie że dla każdego i, $|C_G(g_i)| \leq B(k)$. W szczególności dla $g_1 = 1$, $|C_G(g_1)| = |G| \leq B(k)$. □

Na zakończenie tych rozważań zobaczymy jak można skorzystać z wprowadzonych pojęć odpowiadając na pytanie: Czy istnieje grupa, która ma dokładnie osiem elementów rzędu 5?

Pokażemy, że nie. Przypuśćmy, że jednak istnieje. Wówczas taka grupa G ma dokładnie dwie podgrupy cykliczne rzędu 5, $H = \langle x \rangle \leqslant G$ i $K = \langle y \rangle \leqslant G$. Działanie grupy H na grupie G przez automorfizmy wewnętrzne wyznacza działanie H na zbiorze podgrup grupy G. Działanie to zachowuje dwuelementowy zbiór podgrup 5–cio elementowych. Mamy więc homomorfizm $H \to \Sigma_2$. Homomorfizm ten jest trywialny Wynika stąd, że automorfizmy wewnętrzne wyznaczone przez elementy grupy H zachowują podgrupę K, a więc grupa H działa na grupie K i mamy homomorfizm $H \to Aut(K)$. Ponieważ $|Aut(K)| = \varphi(5) = 4$, to analogiczne rozumowanie jak poprzednio dowodzi, że działanie to jest trywialne. Oznacza to w szczególności, że $xyx^{-1} = y$. Spełnione są założenia zadania 2.6, a więc $\langle x, y \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. Wobec tego w grupie G są co najmniej 24 elementy rzędu 5. Dochodzimy do sprzeczności z założeniem, że jest ich dokładnie 8.

Klasy sprzężoności w grupach permutacji

Niech $\sigma = (c_1, \ldots, c_s)$ będzie pewnym cyklem, a γ pewną permutacją w Σ_n. Wówczas $\gamma\sigma\gamma^{-1} = (\gamma(c_1), \ldots, \gamma(c_s))$ — łatwo to sprawdzić w drodze bezpośredniego rachunku. Korzystając (wielokrotnie) z równości $axya^{-1} = (axa^{-1})(aya^{-1})$ otrzymujemy następujący wniosek.

4.23. Wniosek. *Dwie permutacje są sprzężone wtedy i tylko wtedy, gdy mają podobne rozkłady na iloczyn cykli rozłącznych, tzn. w obydwu rozkładach występuje po tyle samo cykli tej samej długości.*

4.24. Przykład. Permutacje (126)(347)(58)(9) i (6)(345)(29)(178) są sprzężone w Σ_9, bo mają po jednym cyklu długości jeden, po jednej transpozycji i po dwa cykle długości trzy w rozkładzie na iloczyn cykli rozłącznych.