7. Klasyfikacja skończenie generowanych grup przemiennych

W tym rozdziale zajmiemy się skończenie generowanymi grupami przemiennymi. Zgodnie z tradycją będziemy się posługiwać zapisem addytywnym. Działanie dwuargumentowe oznaczamy przez $+$ ($x+y$ zamiast $x\cdot y$), działanie jednoargumentowe przez $-$ ($-x$ zamiast x^{-1}), element neutralny przez 0 (zamiast 1), a podgrupę trywialną przez $\mathbf{0}$ (zamiast $\mathbf{1}$). Piszemy także nx zamiast x^n.
Przypomnijmy, że grupę nazywamy grupą **skończenie generowaną**, jeżeli posiada skończony zbiór generatorów. Oczywiście skończenie generowane są wszystkie grupy skończone, grupy cykliczne (w tym $\mathbb{Z}$ — grupa cykliczna nieskończona) i skończone produkty grup skończenie generowanych. Nie są grupami skończenie generowanymi na przykład grupy $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Zacznijmy od przypomnienia pewnych faktów dotyczących grup cyklicznych.

7.1. Stwierdzenie. *Grupa cykliczna nieskończona $\mathbb{Z}$ jest nierozkładalna, Każda podgrupa grupy $\mathbb{Z}$ jest postaci $m\mathbb{Z}$, gdzie $m \in \mathbb{N}\cup\{0\}$.*

7.2. Stwierdzenie. *Jeżeli p jest liczbą pierwszą, to grupa cykliczna $\mathbb{Z}_{p^k}$ jest nierozkładalna.*

7.3. Stwierdzenie. *Jeżeli $n = {p_1}^{k_1}\dots{p_m}^{k_m}$, jest rozkładem liczby n na czynniki pierwsze ($p_i \neq p_j$ dla $i \neq j$), to*

$$\mathbb{Z}_n \cong \mathbb{Z}_{{p_1}^{k_1}} \times \mathbb{Z}_{{p_2}^{k_2}} \times \dots \times \mathbb{Z}_{{p_m}^{k_m}},$$

a zatem $\mathbb{Z}_n$ rozkłada się na produkt p–grup[†] cyklicznych nierozkładalnych.

Oznaczenie: Produkt l egzemplarzy tej samej grupy H będziemy dla skrócenia zapisu oznaczać symbolem H^l. Przyjmujemy konwencję, że dla $l = 0$, H^l jest grupą trywialną.

Następujące twierdzenie rozstrzyga całkowicie problem klasyfikacji skończenie generowanych grup przemiennych.

7.4. Twierdzenie (o klasyfikacji grup przemiennych skończenie generowanych). *Każda skończenie generowana grupa przemienna jest izomorficzna ze skończonym produktem (nierozkładalnych) p–grup cyklicznych i grup izomorficznych z (nierozkładalną) grupą cykliczną nieskończoną $\mathbb{Z}$*

$$(\bigstar) \qquad (\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times (\mathbb{Z}_{{p_2}^{k_2}})^{v_2} \times \dots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \times \mathbb{Z}^l,$$

gdzie ${p_1}^{k_1}, {p_2}^{k_2}, \dots, {p_n}^{k_n}$ są parami różnymi potęgami liczb pierwszych (niekoniecznie różnych), $l \in \mathbb{N}\cup\{0\}$, zaś $k_1, k_2, \dots, k_n, v_1, v_2, \dots, v_n \in \mathbb{N}\setminus\{0\}$.
Ponadto, czynniki produktu są wyznaczone jednoznacznie, z dokładnością do kolejności.

Na sformułowane powyżej **Twierdzenie o klasyfikacji** składają się dwie dość odrębne rzeczy:
1. możliwość przedstawienia grupy w postaci ($\bigstar$),

[†] sformułowanie p–grupa oznacza tutaj *grupę, której rząd jest potęgą liczby pierwszej* i tylko tyle; por. Uwaga 6.3.

2. jednoznaczność zapisu w postaci (★).

Twierdzenie to pozostawimy bez dowodu. Ograniczymy się do kilku uwag. Zaczniemy od uwagi dotyczącej jednoznaczności zapisu (★). Zobaczmy, że w dowodzie jednoznaczności można *rozdzielić* przypadek produktu p–grup cyklicznych skończonych od przypadku produktu grup cyklicznych izomorficznych z $\mathbb{Z}$. Poniższe twierdzenie wyjaśnia dokładnie sens tego sformułowania.

7.5. Twierdzenie. *Jeżeli*

$$(\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times \cdots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \times \mathbb{Z}^l \cong (\mathbb{Z}_{{q_1}^{m_1}})^{w_1} \times \cdots \times (\mathbb{Z}_{{q_s}^{m_s}})^{w_s} \times \mathbb{Z}^t,$$

to

$$\mathbb{Z}^l \cong \mathbb{Z}^t$$

oraz

$$(\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times \cdots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \cong (\mathbb{Z}_{{q_1}^{m_1}})^{w_1} \times \cdots \times (\mathbb{Z}_{{q_s}^{m_s}})^{w_s}.$$

Dowód. Niech $S(G)$ będzie podgrupą grupy przemiennej G złożoną ze wszystkich elementów skończonego rzędu (dla grupy przemiennej jest to istotnie podgrupa). Jeżeli $G_1 \cong G_2$, to oczywiście

$$\checkmark \qquad S(G_1) \cong S(G_2),$$
$$\checkmark\checkmark \qquad G_1/S(G_1) \cong G_2/S(G_2).$$

Stąd natychmiast wynika, że

$$\underline{\checkmark} \qquad (\mathbb{Z}_{{p_1}^{k_1}})^{v_1} \times \cdots \times (\mathbb{Z}_{{p_n}^{k_n}})^{v_n} \cong (\mathbb{Z}_{{q_1}^{m_1}})^{w_1} \times \cdots \times (\mathbb{Z}_{{q_s}^{m_s}})^{w_s},$$
$$\underline{\checkmark}\,\underline{\checkmark} \qquad \mathbb{Z}^l \cong \mathbb{Z}^t.$$

□

Przypadek produktu grup cyklicznych izomorficznych z $\mathbb{Z}$ jest bardzo prosty:

7.6. Twierdzenie. *Grupy $\mathbb{Z}^l$ i $\mathbb{Z}^t$ są izomorficzne wtedy i tylko wtedy, gdy $l = t$.*

Dowód. Zauważmy, że dla dowolnej grupy przemiennej G, zbiór $2G = \{2g\colon\ g \in G\}$ jest podgrupą. Ponadto, jeżeli $\varphi : G \to H$ jest izomorfizmem, to $\varphi|_{2G} : 2G \to 2H$ i $\tilde{\varphi} : G/2G \to H/2H$ są izomorfizmami.
Oczywiście $\mathbb{Z}^i/2\mathbb{Z}^i \cong (\mathbb{Z}_2)^i$. Zatem, jeżeli $\mathbb{Z}^l \cong \mathbb{Z}^t$, to $(\mathbb{Z}_2)^l \cong (\mathbb{Z}_2)^t$, a wobec tego $l = t$ (bo już sam warunek równoliczności grup $(\mathbb{Z}_2)^l$ i $(\mathbb{Z}_2)^t$ implikuje $l = t$). □

Przypadek produktu p–grup cyklicznych skończonych nietrudno zredukować do sytuacji, gdy rzędy rozpatrywanych p–grup są potęgami *jednej* ustalonej liczby pierwszej p. i posłużyć się indukcją.

Przechodzimy do uwag dotyczących *możliwości przedstawienia grupy w postaci* (★).
Zauważmy, że na mocy Twierdzenia 7.3 wystarczy udowodnić, że prawdziwe jest następujące twierdzenie.

7.7. Twierdzenie. *Każda skończenie generowana grupa abelowa jest izomorficzna z produktem skończonej liczby grup cyklicznych.*

NastEpujący fakt przyjmijmy na wiarę.

7.8. Lemat. *Jeżeli $H \leqslant \mathbb{Z}^n$, to H jest grupą skończenie generowaną.*

Oznaczenie. Wyróżnijmy w $\mathbb{Z}^n$ wygodny układ generatorów $x_1, \ldots, x_n$ gdzie $x_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (wszystkie współrzędne z wyjątkiem i–tej równe 0).

7.9. Stwierdzenie. *Niech $a_1, \ldots, a_n$ będą dowolnymi elementami przemiennej grupy H. Wówczas istnieje dokładnie jeden homomorfizm $f : \mathbb{Z}^n \longrightarrow H$, taki że $f(x_i) = a_i$ dla $i = 1, \ldots, n$.*

Dowód. Bezpośrednie sprawdzenie. □

7.10. Przykład. Dla dowolnych $1 \leq i, j \leq n,\ i \neq j,\ c \in \mathbb{Z}$ istnieje automorfizm f grupy $\mathbb{Z}^n$, zadany wzorem

$$f(x_k) = \begin{cases} x_k & k \neq j \\ cx_i + x_j & k = j \end{cases}.$$

Stwierdzenie 7.9 gwarantuje istnienie *homomorfizmu* zadanego na generatorach w taki właśnie sposób. O tym, że jest to *automorfizm* przekonujemy się sprawdzając, że istnieje homomorfizm odwrotny f^{-1}, zadany wzorem

$$f^{-1}(x_k) = \begin{cases} x_k & k \neq j \\ -cx_i + x_j & k = j \end{cases}.$$

7.11. Wniosek. *Każda grupa przemienna skończenie generowana jest obrazem homomorficznym pewnej grupy $\mathbb{Z}^n$.*
Zatem każda grupa przemienna skończenie generowana da się przedstawić w postaci $\mathbb{Z}^n/N$, gdzie $N \leqslant \mathbb{Z}^n$. □

Na mocy Lematu 7.8 podgrupa N grupy $\mathbb{Z}^n$ jest zadana przez podanie skończonego układu generatorów. Każdy z tych generatorów można zapisać w postaci wektora $(a_1, \ldots, a_n)$. Zapisując je jeden pod drugim otrzymamy macierz A. Będziemy używać naturalnego i wygodnego zapisu $\mathbb{Z}^n/A$ na oznaczenie ilorazu grupy $\mathbb{Z}^n$ przez podgrupę generowaną przez wiersze macierzy A.

7.12. Przykład. Niech $A = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ Wówczas $\mathbb{Z}^3/A \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbf{0} \cong \mathbb{Z}_3 \times \mathbb{Z}_2$.

Powyższy przykład jest oczywiście bardzo szczególny — rozpatrujemy macierz diagonalną, co pozwala na łatwe zidentyfikowanie grupy ilorazowej, w postaci takiej, jakiej oczekujemy (tzn. w postaci produktu grup cyklicznych). Odnotujmy oczywiste stwierdzenie ogólne.

7.13. Stwierdzenie. *Jeżeli A jest macierzą diagonalną o wyrazach $a_1, \ldots, a_n$ na przekątnej, to $\mathbb{Z}^n/A$ jest izomorficzne z produktem grup $\mathbb{Z}_{a_i}$ (stosujemy tu konwencję, że $\mathbb{Z}_1 = \mathbf{0}$, $\mathbb{Z}_0 = \mathbb{Z}$).*

Ustaliliśmy, że rozpatrywana grupa przemienna skończenie generowana jest postaci $\mathbb{Z}^n/A$. Chcemy teraz pokazać, że macierz A może być zastąpiona macierzą diagonalną. Jest to możliwe dzięki następującemu lematowi.

7.14. Lemat. *Następujące operacje na macierzy A nie zmieniają klasy izomorfizmu grupy ilorazowej:*
(a) Zamiana dwóch wierszy (albo kolumn) miejscami
(b) Pomnożenie wiersza (lub kolumny) przez -1
(c) Dodanie do i–tego wiersza (kolumny) wielokrotności j–tego wiersza (kolumny), dla $i \neq j$.
(d) Usunięcie/dodanie wiersza zerowego.

Dowód. Dopuszczalność operacji na wierszach jest we wszystkich czterech przypadkach oczywista — wiersze zmodyfikowanej macierzy opisują dokładnie tę samą podgrupę. W przypadku operacji kolumnowych ((a),(b),(c)) wyjaśnienie jest nieco bardziej skomplikowane. Na przykład dla operacji typu (c): rozpatrywaliśmy automorfizm f grupy $\mathbb{Z}^n$, zadany wzorem

$$f(x_k) = \begin{cases} x_k & k \neq j \\ cx_i + x_j & k = j \end{cases} .$$

Jest jasne, że $\mathbb{Z}^n/N \cong \mathbb{Z}^n/f(N)$. Łatwo sprawdzić, że macierz opisująca podgrupę $f(N)$ to właśnie zmodyfikowana macierz A (do j–tej kolumny dodano i–tą kolumnę pomnożoną przez stałą c). □

Pozostaje pokazać, że dopuszczalne operacje pozwalają od dowolnej macierzy przejść do macierzy diagonalnej.

7.15. Lemat. *Każdą macierz całkowitoliczbową można za pomocą operacji (a)–(d) sprowadzić do postaci diagonalnej.*

Dowód (a zarazem opis algorytmu).
Szukamy w macierzy A niezerowego wyrazu c o najmniejszej wartości bezwzględnej. Jeżeli się da, to dodajemy odpowiednio dobraną wielokrotność jego wiersza lub kolumny do innego odpowiednio dobranego wiersza (kolumny), tak aby uzyskać wyraz niezerowy o mniejszej wartości bezwzględnej.
Jeżeli się *nie da*, to oznacza to, że wszystkie wyrazy w kolumnie i wierszu wyrazu c są podzielne przez c. Wówczas dodając wielokrotności wiersza i kolumny wyrazu c do pozostałych wierszy i kolumn doprowadzamy do takiej sytuacji, że w wierszu i kolumnie wyrazu c są same zera (poza wyrazem c.)
Przestawiając wiersze i kolumny doprowadzamy do tego, żeby wyraz c znalazł się w lewym górnym rogu.
Powtarzamy całą procedurą dla mniejszej macierzy, powstałej przez skreślenie pierwszego wiersza i kolumny. Tak naprawdę pracujemy dalej z tą dużą macierzą, tylko że pierwszy wierszy i kolumna nie podlegają już żadnym modyfikacjom. Ostatecznie otrzymujemy macierz diagonalną (być może konieczne będzie dopisanie lub usunięcie pewnej liczby wierszy zerowych), co kończy dowód lematu. □
Kończy to także dowód *możliwości przedstawienia grupy w postaci* (★).

Warto jeszcze wspomnieć o często stosowanej notacji dotyczącej grup przemiennych skończenie generowanych.
7.16. Przykład. Zapis: grupa przemienna G zadana przez generatory i relacje

$$\langle\, x, y, z, w \mid x + 2y - 2z = 0,\ 2x - 5y = 0,\ 3x = 0 \,\rangle$$

lub krócej

$$\langle\, x, y, z, w \mid x + 2y - 2z,\ 2x - 5y,\ 3x \,\rangle$$

jest równoważny naszemu zapisowi $G = \mathbb{Z}^3/A$, gdzie $A = \begin{pmatrix} 1 & 2 & -2 & 0 \\ 2 & -5 & 0 & 0 \\ 3 & 0 & 0 & 0 \end{pmatrix}$.

Zobaczmy, co to za grupa. Przekształcamy macierz A w podany poniżej sposób:

$$\begin{pmatrix} 1 & 2 & -2 & 0 \\ 2 & -5 & 0 & 0 \\ 3 & 0 & 0 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 2 & -2 & 0 \\ 0 & -9 & 4 & 0 \\ 0 & -6 & 6 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -9 & 4 & 0 \\ 0 & -6 & 6 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 6 & 6 & 0 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 4 & 0 \\ 0 & 0 & 30 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 30 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 30 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 30 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Jak widać $\mathbb{Z}^4/A \cong Z_1 \times \mathbb{Z}_1 \times \mathbb{Z}_{30} \times \mathbb{Z}_0 = \mathbf{0} \times \mathbf{0} \times \mathbb{Z}_{30} \times \mathbb{Z} = \mathbb{Z}_{30} \times \mathbb{Z} = \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}$.

Twierdzenie Sylowa

Przytoczymy teraz twierdzenie Sylowa, na które można patrzeć jak na odwrócenie twierdzenia Lagrange'a dla pewnych dzielników rzędu grupy. Jeżeli G jest grupą rzędu n i $n = {p_1}^{k_1} \dots {p_s}^{k_s}$ jest przedstawieniem n w postaci iloczynu potęg różnych liczb pierwszych, to twierdzenie Sylowa mówi, że dla każdego p_i istnieje w G podgrupa rzędu ${p_i}^{k_i}$ i podaje ograniczenia na liczbę takich podgrup.

7.17. Definicja. *Niech $|G| = p^k \cdot r$, gdzie p jest liczbą pierwszą i $(p, r) = 1$. Podgrupę $H \leqslant G$ nazywamy p–**podgrupą Sylowa** grupy G jeżeli $|H| = p^k$.*

7.18. Twierdzenie Sylowa. *Niech $|G| = p^k \cdot r$, gdzie p jest liczbą pierwszą i $(p, r) = 1$. Wówczas:*

a) Istnieje p–podgrupa Sylowa w G.

b) Jeżeli H jest p–podgrupą Sylowa w G, a $K \leqslant G$ dowolną p-podgrupą, to istnieje element $g \in G$ dla którego $K \leqslant gHg^{-1}$. W szczególności, każda p–podgrupa grupy G jest zawarta w pewnej p–podgrupie Sylowa.

c) Każde dwie p–podgrupy Sylowa są sprzężone.

d) Jeżeli s_p oznacza liczbę p–podgrup Sylowa grupy G, to $s_p \mid r$ i $s_p \equiv 1 \pmod{p}$.