Teoria grup
Ćwiczenia i zadania domowe

Jan Dereziński

Katedra Metod Matematycznych Fizyki
Uniwersytet Warszawski
Pasteura 5, 02-093, Warszawa
e-mail jan.derezinski@fuw.edu.pl

27 października 2014

rok 2014/15

1 Przykłady

(1) Pokazać, że wszystkie grupy rzędu 2 są izomorficzne z $\mathbb{Z}_2$.

(2) Pokazać, że wszystkie grupy rzędu 3 są izomorficzne z $\mathbb{Z}_3$.

(3) Pokazać, że wszystkie grupy rzędu 4 są izomorficzne z $\mathbb{Z}_4$ lub $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(4) Pokazać, że wszystkie grupy rzędu 5 są izomorficzne z $\mathbb{Z}_5$.

(5) Pokazać, że wszystkie grupy rzędu 6 są izomorficzne z $\mathbb{Z}_6$ lub S_3.

(6) Znaleźć wszystkie podgrupy S_3

(7) Pokazać, że $\mathrm{Aut}(S_3) \simeq \mathrm{Inn}(S_3) \simeq S_3$

2 Grupy abelowe

Stwierdzenie 2.1 *Wszystkie podgrupy $\mathbb{Z}$ są postaci $m\mathbb{Z}$ dla $m \in \mathbb{N}$.*

Dowód. Niech m będzie najmniejszym dodatnim elementem w podgrupie G. Oczywiście, $m\mathbb{Z} \subset G$.

Pokażmy inkluzję odwrotną. Nech $n \in G \backslash m\mathbb{Z}$. Wtedy $n = mk + r$, $0 < r < m$. Zatem $r \in G$, co jest sprzecznością. □

Stwierdzenie 2.2 *Jeśli n, m są liczbami względnie pierwszymi, to*

$$\mathbb{Z}_m \times \mathbb{Z}_n \ni ([i], [j]) \mapsto [in + jm] \in \mathbb{Z}_{mn}$$

jest izomorfizmem.

Dowód. Najpierw sprawdzamy, że dla dowolnych $m, n \in \mathbb{N}$ powyższe odwzorowanie jest dobrze określone i jest homomorfizmem. Aby dowieść, że jest on surjektywny korzystamy z faktu, że dla względnie pierwszych m, n istnieją $i, j \in \mathbb{Z}$ takie, że $in + jm = 1$. □

Lemat 2.3 *Niech G będzie skończoną grupą abelową. Wtedy istnieją $n_1, \ldots, n_k$ takie, że*

$$G \simeq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \tag{2.1}$$

Dowód. Niech $\{a_1, \ldots, a_t\}$ będą generatorami grupy G. Zdefiniujmy

$$R(a_1, \ldots, a_t) := \left\{(m_1, \ldots, m_t) \in \{0, 1, \ldots\}^t \ : \ m_1 a_1 + \ldots + m_t a_t = 0\right\}.$$

Dążymy do tego, by znaleźć generatory $\{b_1, \ldots, b_s\}$ dla których $R(b_1, \ldots, b_s) := \{k_1 n_1, \ldots k_1 n_s \ : k_i \in \{0, 1, \ldots\}\}$. Wtedy (2.1) jest spełnione.

Dowód przebiega przez indukcję względem liczby generatorów. Załóżmy, że dla $t-1$ generatorów teza jest prawdziwa. Pokażmy dla t.

Niech m będzie najmniejszą dodatnią liczbą występującą wśród elementów ciągów w R. Możemy przyjąć, że $m = m_1$ dla $(m_1, \ldots, m_t)$. Najpierw pokazujemy, że jeśli $(n_1, \ldots, n_t) \in R$, $(n_1, \ldots, n_t) \neq (m_1, \ldots, m_t)$, to m dzieli n_1. Zatem G jest generowana przez relację a $m_1 a_1 + \cdots m_t a_t = 0$i relacje między $a_2 \ldots, a_t$.

Następnie pokazjemy, że m dzieli wszystkie m_j. Zatem $m_j = m q_j$. Kładziemy

$$\tilde{a}_1 := a_1 + q_2 a_2 + \cdots + q_t a_t.$$

Wtedy G jest generowana przez $\tilde{a}_1$, relację $m\tilde{a}_1 = e$ i $a_2, \ldots, a_t$ i relacje między nimi. Stosujemy założenie indukcyjne i dostajemy, że G jest generowana przez $\tilde{a}_1, \tilde{a}_2, \ldots, \tilde{a}_t$ i relacje

$$m\tilde{a}_1 = 0, \ \tilde{m}_2 \tilde{a}_2 = 0, \ldots, \tilde{m}_2 \tilde{a}_2 = 0.$$

□

Niech p będzie liczbą pierwszą. Mówimy, Że G jst p-grupą, jeśli $\#G = p^k$.

Stwierdzenie 2.4 *Każda abelowa p-grupa jest postaci*

$$\mathbb{Z}_p^{a_1} \times \cdots \mathbb{Z}_{p^k}^{a_k}.$$

Liczby $a_1, \ldots, a_k$ są jednoznacznie wyznaczone.

Dowód. Istnienie takiego rozkładu wynika z Lematu 2.3 i indukcji.

Aby pokazać jednoznaczność, sprawdzamy, że dla $m = 1, \ldots, k$,

$$\#\{b \in G \ : \ p^m b = 0\} = p^{a_1} p^{2a_2} \cdots p^{m a_m} \cdots p^{k a_k}.$$

Czyli dla $m = 1, \ldots, k$,

$$a_1 + 2a_2 + \cdots + m a_m + \cdots + k a_k$$

są wyznaczone jednoznacznie. Stąd $a_1, \ldots, a_k$ są jednoznacznie wyznaczone. □

Twierdzenie 2.5 *Niech G będzie skończoną grupą abelową. Wtedy wszystkie elementy rzędu p^k dla pewnego k tworzą p-grupę G_p. Mamy*

$$G \simeq G_{p_1} \times \cdots \times G_{p_k}.$$

$\mathbb{Z}_n$ jest pierścieniem.

$$\mathbb{Z}_n^\times := \{k \in \mathbb{Z}_n \ : \ k \text{ względnie pierwsze z } \ n\}$$

stanowi grupę. Definiujemy funkcję Eulera

$$\phi(n) := \#\mathbb{Z}_n^\times$$

Jeśli $n = p$ jest pierwsze, to $\phi(p) = p - 1$ i $\mathbb{Z}_p^\times \simeq \mathbb{Z}_{p-1}$ i wtedy $\mathbb{Z}_p$ jest ciałem.

Przykłady:

$$\mathbb{Z}_8^\times \simeq \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_{10}^\times \simeq \mathbb{Z}_4.$$

Stwierdzenie 2.6 *Wszystkie podgrupy $\mathbb{Z}_n$ są postaci $\mathbb{Z}_m$ gdzie m dzieli n.*

Dowód. Niech m będzie najmniejszym elementem podgrupy G. Wtedy $g \simeq \mathbb{Z}_m$. □

Mamy $\mathbb{Z}_n/\mathbb{Z}_m \simeq \mathbb{Z}_{n/m}$, czyli

$$0 \to \mathbb{Z}_m \to \mathbb{Z}_n \to \mathbb{Z}_{n/m} \to 0. \tag{2.2}$$

Zadanie 1 *Niech p będzie pierwsze. Jakie grupy przemienne mogą występować na miejscu G w ciągu dokładnym*

$$0 \to \mathbb{Z}_p \to G \to \mathbb{Z}_p \to 0.$$

Odpowiedź: $G = \mathbb{Z}_p^2$ lub $G = \mathbb{Z}_{p^2}$.

Stwierdzenie 2.7 *Niech dla pewnej grupy abelowej G*

$$0 \to \mathbb{Z}_m \to G \to \mathbb{Z}_k \to 0. \tag{2.3}$$

(2.3) się rozszczepia $\Leftrightarrow$ m i k są względnie pierwsze $\Leftrightarrow$ $G = \mathbb{Z}_m \times \mathbb{Z}_k = \mathbb{Z}_{mk}$.

Dowód. Jeśli nie są względnie piewsze, to mają wspólny dielnik pierwszy p. Załóżmy, że p^a dzieli m, ale p^{a+1} nie dzieli m, oraz p^b dzieli k ale p^{b+1} nie dzieli k. Wtedy rzędy elementów $\mathbb{Z}_m \times \mathbb{Z}_k$ nie dzielą się przez $p^{\max(a,b)+1}$. Natomiast w $\mathbb{Z}_{mk}$ istnieją elementy o rzędzie p^{a+b}. □

3 Iloczyn półprosty grup $\mathbb{Z}_n$

Zadanie 2 *Jak wyglądają automorfizmy $\mathbb{Z}_n$?*

Każdy automorfizm jest zadany jednoznacznie przez obraz 1, który oznaczamy przez k. Każdy automorfizm zachowuje $\mathbb{Z}_n^\times$, zatem $k \in \mathbb{Z}_n^\times$. Oznaczmy taki automorfizm przez ρ_k. Wtedy $\rho_k(j) = jk$. Oczywiście, $\rho_k^m(j) = k^m j$.

Przykładem jest

$$\rho_{-1}(j) = -j,$$

które jest automorfizmem rzędu 2. Definiujemy grupę dihedralną

$$D_n = \mathbb{Z}_n \rtimes \mathbb{Z}_2 := \mathbb{Z}_n \rtimes_{\rho_{-1}} \mathbb{Z}_2.$$

Ogólniej, jeśli $k \in \mathbb{Z}_n^\times$ i $k^m \equiv 1 \bmod(n)$, to możemy zdefiniować

$$\mathbb{Z}_n \rtimes_k \mathbb{Z}_m := \mathbb{Z}_n \rtimes_{\rho_k} \mathbb{Z}_m.$$

3.1 Grupa $O(2)$ i jej podgrupy

Grupa $SO(2)$ składa się z obrotów o kąt $\phi \in [0, 2\pi[$, oznaczanych przez C_ϕ. Jest izomorficzna z $\mathbb{R}/2\pi\mathbb{Z}$. Posiada automorfizm $\phi \mapsto -\phi$ rzędu 2, który generuje działanie grupy $\mathbb{Z}_2$.

Grupa $O(2)$ posiada poza tym odbicia w osiach przechodzących przez osie nachylone o kąt ϕ. Mamy $O(2) = SO(2) \rtimes \mathbb{Z}_2$.

$$P_\psi P_\phi = C_{2(\psi-\phi)}, \quad C_{2\psi} = P_{\phi+\psi} P_\phi.$$

Skończone podgrupy $O(2)$ są postaci C_n, $n = 1, 2, \ldots$, D_n, $n = 1, 2 \ldots$.

Grupa dihedralna D_n ma następujące klasy sprzężoności:

n parzyste

identyczność	1
$C_{\frac{2\pi k}{n}}, C_{-\frac{2\pi k}{n}}$, $k = 1, \ldots \frac{n}{2} - 1$	2
C_π	1
odbicie w prostej przechodzącej przez naprzeciwległe wierzchołki	$\frac{n}{2}$
odbicie w prostej przechodzącej przez środki naprzeciwległych boków	$\frac{n}{2}$

n nieparzyste

identyczność	1
$C_{\frac{2\pi k}{n}}, C_{-\frac{2\pi k}{n}},$, $k = 1, \ldots [\frac{n}{2}]$	2
odbicie w prostej przechodzącej przez wierzchołek i środek naprzeciwległego boku	n

Grupa dihedralna $\mathbb{Z}_n \rtimes \mathbb{Z}_2$ jest generowana przez a, b spełniające relacje

$$a^n = e, \quad b^2 = e, \quad abab = e.$$

Jest też generowana przez b, c spełniające relacje

$$b^2 = e, \quad c^2 = e, \quad (bc)^n = e.$$

Można przejść z jednej rodziny generatorów do drugich przez $c = ab$.

$\mathbb{Z}_n \rtimes_k \mathbb{Z}_m$ jest generowane przez a, b spełniające relacje

$$a^n = e, \quad b^m = e, \quad bab^{-1} = a^k.$$

3.2 Grupa afiniczna

Grupa $GL(\mathbb{K}^n)$ działa na $\mathbb{K}^n$ automorfizmami w oczywisty sposób. Można zatem zdefiniować $\mathbb{K}^n \rtimes GL(\mathbb{K}^n)$. Mamy

$$(a, A)(b, B) = (a + Ab, AB).$$

Znaleźć $(a, A)^{-1}$. (Równe $(A^{-1}a, A^{-1})$.)

Zadanie 3 *Pokazać, że*

$$\phi_{(a,A)}x := a + Ax, \quad x \in \mathbb{K}^n$$

jest działaniem grupy $\mathbb{K}^n \rtimes GL(\mathbb{K}^n)$ *na* $\mathbb{K}^n$.

Mamy

$$\phi_{(a,A)}(\phi_{(b,B)}(x)) = \phi_{(a,A)}(b + Bx) = a + Ab + ABx = \phi_{(a,A)(b,B)}(x).$$

Każdy element $\mathbb{R}^2 \rtimes SO(2)$ jest translacją lub obrotem. Klasy sprzężoności są numerowane przez kąt obrotu $\in [0, 2\pi[$ i odległość translacji

Do $\mathbb{R}^2 \rtimes O(2)$ należą jeszcze odbicia z poślizgiem. (Zwykłe odbicia mają zerowy poślizg). Klasy sprzężoności są numerowane dla obrotów przez moduł kąta $\in [0, \pi]$, odległość translacji, długość poślizgu.