Algebra I

A. Bojanowska P. Traczyk

Istnieje bardzo dużo podręczników algebry o różnym stopniu zaawansowania. Poniższy tekst powstał dla bardzo prostej przyczyny: chcieliśmy dostarczyć studentom WMIM opracowanie dokładnie dopasowane do obecnego programu przedmiotu ALGEBRA I. Stąd znaczna przewaga teorii grup nad teorią pierścieni. Stąd też silne zaakcentowanie teorii działań grup w teorii grup (i jeszcze stąd, że takie akurat ujęcie podoba się autorom skryptu). Skrypt ten zawiera też dużo zadań i pytań testowych. Część z nich oznaczyliśmy symbolem ♡. Te zadania mają szczególne znaczenie, czasem odwołujemy się do nich w dalszym tekście; często przydają się przy rozwiązywaniu innych zadań. Wśród zadań testowych (w których problem polega na ocenie prawdziwości podanego stwierdzenia) jest sporo zdań fałszywych, ilustrujących typowe błędne wyobrażenia.

0. Wstęp

Wiele teorii matematycznych dostarcza naturalnych przykładów zbiorów wyposażonych w różne działania. Najciekawsze są zwykle działania dwuargumentowe. W wielu typowych sytuacjach działania te są łączne (tzn. $x(yz) = (xy)z$). Wyróżnijmy jeden przykład, a właściwie typ przykładów.

Przykład. Składanie przekształceń (dowolnych przekształceń, dowolnych zbiorów) jest łączne.

Szczególnie interesująca jest sytuacja, gdy rozpatrywane odwzorowania są bijekcjami pewnego zbioru. Na przykład

zbiór izometrii płaszczyzny,
zbiór przesunięć płaszczyzny,
zbiór obrotów płaszczyzny o ustalonym środku obrotu,
zbiór obrotów przestrzeni $\mathbb{R}^3$ wokół prostych przechodzących przez początek układu współrzędnych,
zbiór izomorfizmów liniowych przestrzeni $\mathbb{R}^n$,
zbiór izomorfizmów afinicznych przestrzeni $\mathbb{R}^n$,
zbiór podobieństw płaszczyzny,
zbiór premutacji zbioru skończonego,

są zbiorami w których składanie przekształceń jest nie tylko **łączne,** ale ponadto ma **element neutralny** (odwzorowanie identycznościowe) i dla każdego elementu **element odwrotny.**
Wszystkie wyliczone powyżej przykłady, to tak zwane grupy przekształceń. Wymienione trzy własności (łączność, istnienie elementu neutralnego i istnienie elementu odwrotnego) są podstawą teorii grup. Jest to bardzo obszerna i ważna dziedzina algebry. Jej podstawom poświęcamy pierwszych siedem rozdziałów skryptu. Dwa pozostałe zawierają elementarz teorii pierścieni (przemiennych z jedynką).

1. Grupa, podgrupa grupy, homomorfizm grup

1.1. Definicja. **Grupą** *nazywamy zbiór G, wyposażony*[†] *w trzy działania:*
dwuargumentowe — mnożenie $\big((x,y)\mapsto x\cdot y\big)$,
jednoargumentowe — branie elementu odwrotnego $\big(x\mapsto x^{-1}\big)$
i zeroargumentowe — element wyróżniony 1,
takie że spełnione są następujące aksjomaty:

1. $\forall_{x,y,z\in G}\ (x\cdot y)\cdot z = x\cdot(y\cdot z)$,
2. $\forall_{g\in G}\ g\cdot 1 = 1\cdot g = g$,
3. $\forall_{g\in G}\ g\cdot g^{-1} = g^{-1}\cdot g = 1$.

Działanie dwuargumentowe grupy nazywamy zwykle mnożeniem, a element odwrotny odwrotnością. Aksjomaty grupy gwarantują trzy rzeczy:
1. łączność mnożenia,
2. istnienie elementu neutralnego dla mnożenia,
3. istnienie elementu odwrotnego dla mnożenia.

1.2. Definicja. *Jeżeli* $\forall_{x,y\in G}\quad x\cdot y = y\cdot x$, *to grupę nazywamy* **przemienną** *lub* **abelową**.

1.3. Definicja. *Moc zbioru G nazywamy* **rzędem grupy** *G i oznaczamy symbolem* $|G|$.

Z definicji łatwo wynika, że jest tylko jeden element neutralny mnożenia i że dla dowolnego elementu istnieje dokładnie jeden element odwrotny.

Zamiast $x\cdot y$ piszemy często xy. Zwykle mówimy *grupa G*, pomijając wyszczególnianie pozostałych elementów struktury.

W przypadku grup abelowych często działanie dwuargumentowe oznacza się znakiem $+$ ($x+y$ zamiast $x\cdot y$), element odwrotny przez $-$ ($-x$ zamiast x^{-1}), a element neutralny przez 0. Zapis $(G,\cdot,\cdot^{-1},1)$ nazywamy zapisem multiplikatywnym, a zapis $(G,+,-,0)$ zapisem addytywnym. W zapisie multiplikatywnym przyjęte jest odczytywać symbol g^{-1} jako *odwrotność elementu g*; w zapisie addytywnym symbol $-g$ odczytujemy jako *element przeciwny do elementu g*.

1.4. Definicja. **Podgrupą** *grupy G nazywamy podzbiór $H\subseteq G$, taki że*
$\forall_{x,y\in H}\quad x\cdot y\in H$
$\forall_{x\in H}\quad x^{-1}\in H$
$1\in H$.

Zapis $H\leqslant G$ będzie oznaczać, że H jest podgrupą grupy G.

Jest jasne, że $\mathbf{1}=\{1\}\leqslant G$ jest podgrupą. Taką podgrupę będziemy nazywać **podgrupą trywialną**. Oczywiście cała grupa G też jest swoją podgrupą: $G\leqslant G$.

Przykłady, od których rozpoczęliśmy, to oczywiście przykłady grup, w których operacją grupową jest składanie przekształceń, jedynką przekształcenie identycznościowe, a elementem odwrotnym przekształcenie odwrotne. Rozpatrzmy dalsze przykłady.

1.5. Przykłady.

[†] z formalnego punktu widzenia należałoby napisać: czwórkę uporządkowaną $(G,\cdot,^{-1},1)$

0) Grupa **cykliczna** $\mathbb{Z}$ liczb całkowitych z dodawaniem.
1) Niech K będzie ciałem. Symbolem K^+ oznaczamy grupę addytywną tego ciała, symbolem K^* grupę multyplikatywną ciała (zbiorem jej elementów jest $K \setminus \{0\}$).
2) Niech K będzie ciałem. Symbolem $GL(n, K)$ oznaczamy grupę macierzy odwracalnych $n \times n$ o współczynnikach z K. Macierze o wyznaczniku 1 stanowią podgrupę, oznaczaną symbolem $SL(n, K) \leqslant GL(n, K)$.
3) W grupie $GL(n, \mathbb{R})$ zawarte są dwie szczególnie interesujące grupy:
$O(n) \leqslant GL(n, \mathbb{R})$ — podgrupa złożona z macierzy ortogonalnych i
$SO(n) \leqslant O(n) \leqslant GL(n, \mathbb{R})$ — podgrupa złożona z macierzy ortogonalnych o wyznaczniku 1.
4) Grupa dihedralna — podgrupa $D_{2n} \leqslant O(2)$ przekształceń zachowujących n–kąt foremny o środku symetrii w początku układu współrzędnych.

$$D_{2n} = \{1, \rho, \rho^2, \ldots, \rho^{n-1}, \varepsilon, \rho\varepsilon, \rho^2\varepsilon, \ldots, \rho^{n-1}\varepsilon\},$$

gdzie ρ jest obrotem o $\frac{1}{n}$ kąta pełnego, a ε symetrią osiową.

Odnotujmy ważny fakt, że $\varepsilon^2 = 1$, $\rho^n = 1$ i $\varepsilon\rho\varepsilon = \varepsilon\rho\varepsilon^{-1} = \rho^{-1}$. Zauważmy, że powyższe tożsamości wystarczają do skonstruowania tabeli działania dwuargumentowego dla D_{2n}.

Zauważmy, że $J_n = \{1, \rho, \rho^2, \ldots, \rho^{n-1}\} \leqslant D_{2n}$ jest podgrupą. Nazywamy ją podgrupą obrotów grupy dihedralnej.

5) Grupa **cykliczna** $\mathbb{Z}_n = \{1, \exp(\frac{2\pi i}{n}), \ldots, \exp(\frac{2\pi i(n-1)}{n})\}$ pierwiastków z jedynki stopnia n, z mnożeniem jako działaniem dwuargumentowym.

Jeżeli $k \,|\, n$, $n = km$, to $\{1, \exp(\frac{2\pi im}{n}), \ldots, \exp(\frac{2\pi i(k-1)m}{n})\} \leqslant \mathbb{Z}_n$ jest podgrupą cykliczną rzędu k.
6) Niech X będzie zbiorem. Symbolem Σ_X oznaczamy grupę bijekcji zbioru X z działaniem składania jako mnożeniem i identycznością jako elementem neutralnym. Nazywamy ją grupą permutacji zbioru X. Jeżeli X jest zbiorem n – elementowym, to grupę taką oznaczamy symbolem Σ_n.

1.6. Definicja. *Przekształcenie $\varphi : G \longrightarrow H$ nazywamy* **homomorfizmem** *grup wtedy i tylko wtedy, gdy* $\forall_{g_1, g_2 \in G} \quad \varphi(g_1 \cdot g_2) = \varphi(g_1) \cdot \varphi(g_2)$.

Łatwo sprawdzić, że homomorfizm φ przeprowadza element neutralny na element neutralny, a element odwrotny do g na element odwrotny do $\varphi(g)$.

Istnieją różne szczególne typy homomorfizmów. Poniżej wymieniamy ich nazwy, stosowane bardzo szeroko w matematyce, również poza teorią grup, czy nawet algebrą:

Izomorfizm: taki homomorfizm $\varphi : G \longrightarrow H$, dla którego istnieje homomorfizm $\psi : H \longrightarrow G$, taki że $\varphi\psi = id_H$ i $\psi\varphi = id_G$.

1.7. Uwaga. Homomorfizm grup jest izomorfizmem wtedy i tylko wtedy, gdy jest homomorfizmem i bijekcją zbiorów.

Grupy izomorficzne będziemy uważać za *takie same*. Jest jasne, że dla każdego $n \in \mathbb{N}$ istnieje co najmniej jedna grupa rzędu n (np. grupa $\mathbb{Z}_n$) i tylko skończenie wiele klas izomorfizmu grup rzędu n.

Automorfizm: Izomorfizm z grupy G w tę samą grupę G.

Zauważmy, że zbiór wszystkich automorfizmów grupy G tworzy grupę ze składaniem przekształceń jako działaniem dwuargumentowym. Grupę tę oznaczamy symbolem $Aut(G)$.

Monomorfizm: homomorfizm różnowartościowy.
Epimorfizm: homomorfizm, który jest *na*.
Endomorfizm: homomorfizm, którego dziedzina i przeciwdziedzina są identyczne (ale nie żądamy, żeby był *na*).

Produkt grup. Jeżeli G i H są grupami, to iloczyn kartezjański $G \times H$ z działaniami $(g,h)\cdot(g',h') = (g\cdot g', h\cdot h')$, $(g,h)^{-1} = (g^{-1}, h^{-1})$ oraz elementem neutralnym $(1_G, 1_H)$ jest grupą. Zbiory $G \times \mathbf{1}_H = \{(g, 1_H) : g \in G\} \leqslant G \times H$ i $\mathbf{1}_G \times H = \{(1_G, h) : h \in H\} \leqslant G \times H$ są podgrupami — oczywiście pierwsza podgrupa jest izomorficzna z G, a druga z H.

1.8. Uwaga. *Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to $\varphi(G) \leqslant H$ jest podgrupą grupy H. Także dla każdej podgrupy $H' \leqslant H$, $\varphi^{-1}(H') \leqslant G$ jest podgrupą grupy G. Szczególnie ważna jest podgrupa $\varphi^{-1}(\mathbf{1}) = \{g \in G\colon \varphi(g) = 1\} \leqslant G$. Oznaczamy ją symbolem* $\ker\varphi$ *i nazywamy* **jądrem** *homomorfizmu φ.*

1.9. Uwaga. *Homomorfizm φ jest monomorfizmem wtedy i tylko wtedy, gdy* $\ker\varphi = \mathbf{1}$.

Jeżeli homomorfizm $\varphi : G \longrightarrow H$ jest monomorfizmem, to $\varphi : G \longrightarrow \mathrm{im}\,(\varphi)$ jest izomorfizmem ($\mathrm{im}\,(\varphi) = \varphi(G)$).

1.10. Przykłady homomorfizmów.
1) $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\varphi(k) = \exp(\frac{2\pi i k}{n})$
2) $det : GL(n,K) \longrightarrow K^*$
3) $i_G : G \longrightarrow G \times H$, $i_G(g) = (g, 1_H)$ oraz $\pi_G : G \times H \longrightarrow G$, $\pi_G(g,h) = g$ są homomorfizmami; i_G jest monomorfizmem, π_G jest epimorfizmem. Analogicznie określamy homomorfizmy i_H i π_H.
4) Każdy element $g \in G$ 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 homomorfizmu. W przyszłości, po wprowadzeniu pewnych dodatkowych pojęć, homomorfizm ten będziemy nazywać działaniem grupy G na zbiorze jej elementów, poprzez automorfizmy wewnętrzne. Zauważmy, że

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

Tak określona podgrupa ma swoją nazwę:

1.11. Definicja. *Podgrupę*

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

nazywamy **centrum grupy.**

5) 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.

1.12. 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.*

□

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

1.14. 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.

ZADANIA

Z 1.1. Znaleźć wszystkie możliwe tabelki działań grupowych na zbiorze czteroelementowym.

Z 1.2. Udowodnić, że jeżeli dwa spośród elementów x, y, xy grupy G należą do podgrupy $H \leqslant G$, to również trzeci należy do H.

Z 1.3. Udowodnić, że jeżeli $\forall_{g\in G}\ g^2 = 1$, to G jest grupą abelową. Udowodnić, że jeżeli ponadto grupa G jest skończona, to $|G| = 2^m$.

Z 1.4. Udowodnić, że jeżeli G jest grupą, w której $\forall_{x,\,y\in G}\ (xy)^2 = x^2y^2$, to G jest grupą abelową.

Z 1.5. Na zbiorze $\{0, 1, \ldots, n-1\}$ określamy działanie dwuargumentowe $k +_n l = k + l \pmod n$. Pokazać, że działanie to zadaje strukturę grupy, izomorficznej z $\mathbb{Z}_n$ (w przyszłości będziemy również tę grupę oznaczać symbolem $\mathbb{Z}_n$).

Z 1.6. Udowodnić, że wśród grup: $\mathbb{Z}, \mathbb{R}^+, \mathbb{Q}^+$ żadne dwie nie są izomorficzne[†].

Z 1.7. Udowodnić, że jeżeli $G \cong H$ to $Aut\,(G) \cong Aut\,(H)$.

Z 1.8. Udowodnić, że $SO(2) \cong \{z \in \mathbb{C}^* : |z| = 1\}$, gdzie $\mathbb{C}$ oznacza ciało liczb zespolonych.

Z 1.9. Niech $\phi : G \longrightarrow G$ będzie dane wzorem $\phi(g) = g^{-1}$. Udowodnić, że ϕ jest automorfizmem wtedy i tylko wtedy, gdy G jest abelowa.

Z 1.10. Znaleźć $|GL(n, \mathbb{Z}_p)|$ i $|SL(n, \mathbb{Z}_p)|$.

♡ Z 1.11. Skonstruować monomorfizm $\Sigma_n \longrightarrow GL(n, K)$.

Z 1.12. Skonstruować monomorfizm $D_{2n} \longrightarrow \Sigma_n$ (dla $n \geq 3$).

♡ Z 1.13. Niech $Q_8 := \langle\, j, k \,\rangle \leqslant GL(2, \mathbb{C})$, gdzie j, k są macierzami:

$$j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \qquad k = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

Udowodnić, że $|Q_8| = 8$ i sporządzić tabelkę działania dwuargumentowego (grupę Q_8 nazywamy **grupą kwaternionową**).

♡ Z 1.14. Niech $G = \langle\, X \,\rangle$. Niech $f : G \longrightarrow H$, $j : G \longrightarrow H$ będą homomorfizmami, takimi że dla każdego $x \in X$, $f(x) = j(x)$. Udowodnić, że $f = j$.

♡ Z 1.15. Niech K będzie ciałem. Znaleźć centrum grupy $GL(n, K)$.

♡ Z 1.16. Niech $GL(n, \mathbb{Z})$ oznacza grupę odwracalnych macierzy $n \times n$ o wyrazach całkowitych. Znaleźć jej centrum.

TEST

♡ T 1.1. $(xy)^{-1} = y^{-1}x^{-1}$

T 1.2. Elementy x i y grupy G są przemienne wtedy i tylko wtedy, gdy $x^{-1}y^{-1}xy = 1$.

T 1.3. Elementy x i y grupy G są przemienne wtedy i tylko wtedy, gdy $xyx^{-1}y^{-1} = 1$.

T 1.4. Jeżeli elementy x i y grupy G są przemienne, to dowolne ich potęgi też są przemienne.

T 1.5. Jeżeli $g \in G$, to $\langle\, g \,\rangle$ jest grupą przemienną.

T 1.6. $Z(D_{20}) = 1$

♡ T 1.7. $D_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

[†] chodzi o grupy addytywne ciał $\mathbb{R}$ i $\mathbb{Q}$, a nie o liczby rzeczywiste i wymierne dodatnie

♡ T 1.8. $D_6 \cong \Sigma_3$
T 1.9. $D_{12} \cong \Sigma_6$
♡ T 1.10. W grupie dihedralnej D_{2n} zachodzi równość $\rho^i\varepsilon = \varepsilon\rho^{-i}$.
T 1.11. W grupie dihedralnej D_{10} zachodzi równość $\rho^3\varepsilon\rho = \rho^2\varepsilon$.
T 1.12. W grupie dihedralnej D_{10} zachodzi równość $(\rho\varepsilon)^5 = 1$.
T 1.13. W grupie dihedralnej D_{2m} zachodzi równość $\rho^k\varepsilon \cdot \rho^n\varepsilon = \rho^{k-n}$.
T 1.14. Grupa $\mathbb{Q}^+$ jest skończenie generowana.
T 1.15. Grupa $\mathbb{Z}_{125} \times \mathbb{Z}_5$ zawiera podgrupę izomorficzną z grupą $\mathbb{Z}_5 \times \mathbb{Z}_5$.
♡ T 1.16. Jeżeli G jest grupą przemienną, to $Z(G) = G$.
T 1.17. Jeżeli G jest grupą nieprzemienną, to $Z(G) = \mathbf{1}$.
♡ T 1.18. Jeżeli w zbiorze X, $X \subseteq G$ każde dwa elementy są ze sobą przemienne, to $\langle X \rangle$ jest grupą przemienną.
T 1.19. Niech $f, h : G \longrightarrow H$ będą homomorfizmami. Jeżeli $\ker f = \ker h$, to $f = h$.
T 1.20. Obraz epimorficzny grupy nieprzemiennej jest grupą nieprzemienną.
T 1.21. Obraz epimorficzny grupy przemiennej jest grupą przemienną.
T 1.22. Istnieje epimorfizm grupy Z_{140} na grupę D_{70}.

2. Grupa cykliczna, rząd elementu

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

2.2. 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 $\varphi : \mathbb{Z}_n \longrightarrow G$, $\varphi(\exp(\frac{2\pi im}{n})) = g^m$ 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. □

2.3. 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 $k = \frac{n}{l}$.□

2.4. 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 dla każdej liczby całkowitej k, takiej że $g^k = 1$, ma miejsce podzielność: $n \,|\, k$.
3. Jeżeli $\varphi : G \to H$ jest homomorfizmem, to dla każdego elementu $g \in G$ $o(\varphi(g)) \,|\, o(g)$.

2.5. 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 $o(g^k) \,|\, m$. Przypuśćmy, że $(g^k)^r = 1$. Wynika stąd, że $n \,|\, kr$, a zatem $m \,|\, lr$. Wobec $(m,l) = 1$, $m \,|\, r$, 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.

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

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

2.7. 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 $\varphi(p) = p - 1$.*

2.8. 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. □

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

2.10. 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 $\gamma(1) = 3$, $\gamma(2) = 1$, $\gamma(3) = 4$, $\gamma(4) = 2$.

2.11. 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.

2.12. 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.

2.13. 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.

2.14. 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 $NWW(n_1, n_2, \ldots, n_k) \,|\, o(\sigma)$. □

Warstwy grupy względem podgrupy, twierdzenie Lagrange'a

Stwierdzenie, że rząd podgrupy jest dzielnikiem rzędu grupy, które już udowodniliśmy dla grup cyklicznych, jest prawdziwe dla *wszystkich* grup skończonych i nosi nazwę twierdzenia Lagrange'a.

Niech G będzie dowolną (niekoniecznie skończoną) grupą, a $H \leqslant G$ jej podgrupą. Dla dowolnego $g \in G$ rozpatrzmy podzbiór $gH = \{gh;\, h \in H\} \subseteq G$. Łatwo zauważyć, że:

1) zbiór gH jest klasą abstrakcji zawierającą g następującej relacji równoważności w zbiorze elementów G: $x \sim y \iff x^{-1}y \in H$. Zbiór gH nazywamy **warstwą lewostronną elementu** g **względem podgrupy** H.
2) $1H = H$
3) Dowolne dwie warstwy lewostronne są równoliczne, w szczególności każda warstwa jest równoliczna ze zbiorem H (przyporządkowanie $h \mapsto gh$ ustala bijekcję zbioru H i warstwy gH).

Zbiór warstw lewostronnych oznaczamy symbolem G/H, a jego moc nazywamy **indeksem podgrupy** H **w grupie** G i oznaczamy $[G\colon H]$. (Uwaga: analogicznie można zdefiniować warstwy prawostronne grupy G względem podgrupy H — są to podzbiory postaci $Hg = \{hg : h \in H\} \subseteq G$).

Z faktu, że każda warstwa lewostronna ma tyle samo elementów, co podgrupa H wynika natychmiast następujące twierdzenie.

2.15. Twierdzenie Lagrange'a. *Jeżeli G jest grupą skończoną i $H \leqslant G$, to $|G| = |H| \cdot [G\colon H]$.*

To proste twierdzenie ma szereg oczywistych, ale ważnych, konsekwencji:

2.16. Wniosek. *Rząd elementu jest dzielnikiem rzędu grupy.*

2.17. Wniosek. *Każda grupa rzędu p, gdzie p jest liczbą pierwszą, jest izomorficzna z $\mathbb{Z}_p$.*

Dowód. Z twierdzenia Lagrange'a wynika, że podgrupa cykliczna generowana przez dowolny element różny od neutralnego musi być rzędu p, a więc musi być równa całej rozpatrywanej grupie. □

2.18. Uwaga. *Grupa skończona G rzędu n jest cykliczna wtedy i tylko wtedy, gdy dla każdego $k \mid n$ zawiera co najwyżej jedną podgrupę rzędu k.*

Dowód. Wystarczy pokazać, że w grupie G istnieje element rzędu n. Niech $\nu(k)$ oznacza liczbę elementów rzędu k w grupie G. Z założenia wynika, że

$$\nu(k) \leq \varphi(k),$$

gdzie φ jest funkcją Eulera.Z twierdzenia Lagrange'a wnioskujemy że $\nu(k)$ ma szansę być niezerowe tylko wtedy, gdy $k \mid n$. Zatem

$$n = \sum_{k \mid n} \nu(k) \leq \sum_{k \mid n} \varphi(k) = n,$$

a więc dla każdego $k \mid n$ zachodzi równość $\nu(k) = \varphi(k)$. W szczególności $\nu(n) = \varphi(n) > 0$, co kończy dowód. □

W związku z twierdzeniem Lagrange'a nasuwa się pytanie o możliwość jego odwrócenia. Załóżmy, że k jest dzielnikiem $|G|$. Czy istnieje podgrupa rzędu k grupy G i ile jest takich podgrup? Częściową odpowiedzią na to pytanie będzie twierdzenie Cauchy'ego, które mówi, że jeżeli liczba pierwsza p jest dzielnikiem $|G|$, to w G istnieje element rzędu p, a więc i cykliczna podgrupa rzędu p. Udowodnimy je w następnym rozdziale.

ZADANIA

Z 2.1. Niech $\mathbb{Z}_{12} = \{1, g, g^2, \ldots, g^{10}, g^{11}\}$. Znaleźć rzędy wszystkich elementów.

♡ Z 2.2. Znaleźć rzędy elementów w grupie D_{2n}.

Z 2.3. Pokazać, że w grupie rzędu parzystego istnieje element rzędu dwa.

Z 2.4. Pokazać, że w grupie rzędu parzystego liczba elementów rzędu dwa jest zawsze nieparzysta.

Z 2.5. Ile elementów rzędu 6 jest w grupie $\mathbb{C}^*$?

♡ Z 2.6. Niech x, $y \in G$, przy czym $\langle x \rangle \cap \langle y \rangle = \mathbf{1}$. Pokazać, że jeżeli x i y są przemienne, to $\langle x, y \rangle \cong \langle x \rangle \times \langle y \rangle$.

♡ Z 2.7. Niech x, $y \in G$, przy czym $o(x) = n < \infty$, a $o(y) = m < \infty$. Pokazać, że jeżeli $(n, m) = 1$ oraz x i y są przemienne, to $o(xy) = mn$.

Z 2.8. Niech G będzie grupą abelową, która zawiera pewien element rzędu m i pewien element rzędu n. Pokazać, że G zawiera element, którego rząd jest równy $NWW(n, m)$.

Z 2.9. Pokazać, że jeżeli $\varphi : G \longrightarrow H$ jest monomorfizmem, to dla każdego elementu $x \in G$, $o(x) = o(\varphi(x))$.

♡ Z 2.10. Udowodnić, że dla dowolnych elementów a i x dowolnej grupy G zachodzi równość $o(a) = o(xax^{-1})$. Wywnioskować, że w dowolnej grupie G, dla dowolnych dwóch elementów x, $y \in G$, $o(xy) = o(yx)$.

Z 2.11. Sprawdzić, że macierze postaci $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, $a, b, c \in \mathbb{R}$, $ac \neq 0$, tworzą podgrupę w $GL(2, \mathbb{R})$ i znaleźć w niej elementy rzędu 2. Wskazać dwa elementy rzędu dwa, których iloczyn ma rząd nieskończony.

Z 2.12. Pokazać, że podgrupa dowolnej grupy skończonej generowana przez dwa nieprzemienne elementy rzędu dwa jest izomorficzna z grupą dihedralną.

Z 2.13. Podać przykład grupy nieskończonej, której każdy element jest rzędu skończonego.

♡ Z 2.14. Niech $|G| < \infty$. Udowodnić, że liczba elementów rzędu p, gdzie p jest liczbą pierwszą, jest wielokrotnością liczby $p - 1$.

♡ Z 2.15. Niech $|G| < \infty$. Udowodnić, że liczba elementów rzędu n jest wielokrotnością $\varphi(n)$, gdzie φ jest funkcją Eulera.

Z 2.16. Udowodnić, że w skończonej grupie abelowej iloczyn wszystkich elementów jest równy iloczynowi elementów rzędu 2. Zastosować to stwierdzenie do grupy $\mathbb{Z}_p^*$ i wykazać Tw. Wilsona: $(p-1)! \equiv -1 \pmod{p}$.

Z 2.17. Niech $a, b \in G$, $b \neq 1$ i niech $a^5 = 1$, $aba^{-1} = b^2$. Znaleźć rząd b.

Z 2.18. Niech G będzie taką grupą, że część wspólna wszystkich podgrup nietrywialnych jest podgrupą nietrywialną. Pokazać, że każdy element G jest skończonego rzędu.

Z 2.19. *Definicja: Podgrupę właściwą H grupy G nazywamy maksymalną, jeżeli nie istnieje właściwa podgrupa $K \leq G$, $K \neq H$ taka, że $H \leq K \leq G$.*

Pokazać, że jeżeli grupa skończona G ma dokładnie jedną podgrupę maksymalną, to G jest grupą cykliczną i $|G| = p^m$, gdzie p jest liczbą pierwszą i $m > 0$.

♡ Z 2.20. Udowodnić, że $|Aut(\mathbb{Z}_n)| = \varphi(n)$, gdzie φ jest funkcją Eulera.

♡ Z 2.21. Jeżeli $\varphi : G \longrightarrow H$ jest epimorfizmem, a $K \leqslant H$ dowolną podgrupą, to $[G : \varphi^{-1}(K)] = [H : K]$.

Z 2.22. Permutację $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 6 & 3 & 1 & 7 & 5 \end{pmatrix}$ rozłożyć na cykle rozłączne.

Z 2.23. W Σ_6 policzyć złożenie $(123)(546)(231)(46)$ przedstawiając je w postaci iloczynu cykli rozłącznych. Znaleźć jego rząd.

♡ Z 2.24. Udowodnić, że każda permutacja może być przedstawiona w postaci iloczynu transpozycji.

♡ Z 2.25. Udowodnić, że każda permutacja może być przedstawiona w postaci iloczynu transpozycji elementów sąsiednich (tzn. transpozycji postaci $(i, i+1)$).

Z 2.26. Przedstawić w postaci iloczynu transpozycji elementów sąsiednich permutację $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 4 & 2 & 5 \end{pmatrix}$.

Z 2.27. Przedstawić w postaci iloczynu transpozycji elementów sąsiednich permutację $(173)(2456)$.

Z 2.28. Udowodnić, że zbiór złożony z transpozycji (12) i cyklu $(1, 2, \ldots, n)$ generuje całą grupę Σ_n.

Z 2.29. Pokazać, że jeżeli p jest liczbą pierwszą, to Σ_p jest generowane przez dowolną transpozycję i dowolny cykl długości p. Pokazać, rozważając Σ_4, że założenie iż p jest liczbą pierwszą jest istotne.

Z 2.30. Pokazać, że nie istnieje monomorfizm $Q_8 \to \Sigma_4$.

TEST

♡ T 2.1. Niech $x, y \in G$ będą elementami pewnej grupy G. Jeżeli $xy = yx$, to $o(xy) = NWW((o(x), o(y)))$.

♡ T 2.2. Niech $x, y \in G$ będą elementami pewnej grupy G. Jeżeli $\langle x \rangle \cap \langle y \rangle = \mathbf{1}$, to $o(xy) = NWW(o(x), o(y)))$.

♡ T 2.3. Niech (x, y) będzie elementem produktu grup $G \times H$. Jeżeli x i y są elementami rzędów skończonych, to $o(x, y) = NWW(o(x), o(y)))$.

T 2.4. Niech $x, y \in G$. Załóżmy, że $o(x) = k,\ o(y) = n$. Wówczas istnieje w grupie G pewien element rzędu $NWW(n, k)$.

T 2.5. $D_8 \cong Q_8$.

♡ T 2.6. Jeżeli $(|H|, |G|) = 1$, to każdy homomorfizm $H \longrightarrow G$ jest trywialny.

T 2.7. Niech γ będzie generatorem grupy cyklicznej rzędu 30. Wówczas $o(\gamma^{20}) =$ ☐ .

T 2.8. Niech G będzie grupą rzędu 2001. Niech $x \in G$. Wówczas $o(x^{29}) =$ ☐ lub ☐ lub ☐ lub ☐ .

T 2.9. W grupie cyklicznej $\mathbb{Z}_{2001}$ jest ☐ elementów rzędu 2001.

T 2.10. W grupie $\mathbb{Z}_{15}$ elementów rzędu 15 jest: ☐ .

T 2.11. W grupie $\mathbb{Z}_9 \times \mathbb{Z}_9$ jest jeden element rzędu 1, ☐ elementów rzędu 3 i ☐ elementów rzędu 9.

T 2.12. W grupie $\mathbb{Z}_{15} \times \mathbb{Z}_{15}$ jest ☐ podgrup izomorficznych z $\mathbb{Z}_{15}$.

T 2.13. W grupie $\mathbb{Z}_7 \times \mathbb{Z}_5$ elementów rzędu 35 jest dokładnie ☐ .

T 2.14. $\mathbb{Z}_7 \times \mathbb{Z}_5 \cong \mathbb{Z}_{35}$.

T 2.15. Liczba elementów rzędu 12 w dowolnej grupie G jest podzielna przez 11.

T 2.16. Liczba elementów rzędu 12 w dowolnej grupie G jest podzielna przez 4.

T 2.17. Istnieją takie grupy $H, K \leq G$, że $H, K \cong \mathbb{Z}_{15}$ i $H \cap K$ zawiera dokładnie 3 elementy.

T 2.18. Istnieją takie grupy $H, K \leq G$, że $H, K \cong \mathbb{Z}_{15}$ i $H \cap K$ zawiera dokładnie 5 elementów.
T 2.19. Istnieją takie grupy $H, K \leq G$, że $H, K \cong \mathbb{Z}_{15}$ i $H \cap K$ zawiera dokładnie 7 elementów.
T 2.20. Grupa przemienna rzędu 35 jest izomorficzna z $\mathbb{Z}_{35}$.
T 2.21. Istnieje grupa skończona, w której elementów rzędu 5 jest dokładnie 24.
T 2.22. Istnieje grupa przemienna, w której elementów rzędu 7 jest dokładnie 18.
T 2.23. Istnieje grupa rzędu 70, która zawiera nie mniej niż 24 wzajemnie przemienne elementy rzędu 5.
T 2.24. Niech $f : G \to H$ będzie homomorfizmem grup. Niech $g, h \in G$. Załóżmy, że $o(g) = o(h)$. Wówczas $o(f(g)) = o(f(h))$.
T 2.25. Niech $f : G \to H$ będzie homomorfizmem grup. Niech g_1, g_2 będą takimi elementami grupy G, że $\langle g_1 \rangle = \langle g_2 \rangle$. Wówczas $o(f(g_1)) = o(f(g_2))$.
T 2.26. Niech $f : G \to H$ będzie homomorfizmem grup. Jeżeli dla każdego $g \in G$ $o(g) = o(f(g))$, to f jest monomorfizmem.
T 2.27. $\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{10}$.
T 2.28. Niech $\mathbb{Z}_{12} = \langle \gamma \rangle$. Wówczas zbiór $\{\gamma, \gamma^4, \gamma^7, \gamma^{10}\}$ jest warstwą względem pewnej podgrupy.
T 2.29. Niech zbiór elementów $X = \{x_1, \ldots x_n\}$ w grupie G będzie warstwą lewostronną tej grupy względem pewnej podgrupy H. Wynika stąd, że $H = \{1, x_1 \cdot (x_2)^{-1}, \ldots, x_1 \cdot (x_n)^{-1}\}$.
T 2.30. Liczba homomorfizmów grupy $\mathbb{Z}_{120}$ w grupę $\mathbb{Z}$ wynosi $\square$.
T 2.31. Niech $\sigma \in \Sigma_7$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 4 & 2 & 3 & 5 & 1 & 7 \end{pmatrix}$. Wówczas podgrupy $\langle \sigma \rangle \leqslant \Sigma_7$ i $\langle (1\,2\,3\,4\,5\,6) \rangle \leqslant \Sigma_7$ są izomorficzne.
T 2.32. Niech $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 1 & 8 & 2 & 4 & 7 & 6 \end{pmatrix}$. Wówczas $o(\sigma^4) = \square$.
T 2.33. Jeżeli $k_1 + \cdots + k_l \leq n$, to Σ_n zawiera podgrupę izomorficzną z $\mathbb{Z}_{k_1} \times \cdots \times \mathbb{Z}_{k_l}$.
T 2.34. Jeżeli $k_1 + \cdots + k_l \leq n$, to Σ_n zawiera podgrupę izomorficzną z $\Sigma_{k_1} \times \cdots \times \Sigma_{k_l}$.
T 2.35. Jeżeli Σ_n zawiera podgrupę izomorficzną z $\mathbb{Z}_k$, to $k \leq n$.
T 2.36. Rząd permutacji $(1\,3\,4\,6\,7)(2\,3\,5)$ jest równy 15

3. 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, topologiczą lub algebraiczną, zdefiniowaną na rozpatrywanym zbiorze. Poznaliśmy twierdzenie Cayleya, które mówi że, z dokładnością do izomorfizmu, każda grupa po prostu *jest* pewną podgrupą jakiejś grupy bijekcji. Dowód polegał na wskazaniu *monomorfizmu* $\psi : G \to \Sigma_G$.

Zetknęliśmy się jednak także z następującym przykładem: każdy element grupy G wyznacza automorfizm wewnętrzny (a więc bijekcję) $\phi_g : G \longrightarrow G$, określony wzorem $\phi_g(x) = gxg^{-1}$, przy czym iloczynowi elementów odpowiada złożenie automorfizmów. Oznacza to, że przekształcenie $\phi : G \to Aut(G) \leqslant \Sigma_G$ zadane wzorem $\phi(g) = \phi_g$ jest homomorfizmem (choć na ogół nie jest monomorfizmem). Opisana sytuacja jest przykładem *działania grupy G na zbiorze* – tutaj na zbiorze jej elementów.

3.1. 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 $\phi_g(x)$.

Przyjrzyjmy się bliżej strukturze dowolnego G—zbioru X.

3.2. 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*

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

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.

3.3. 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:

3.4. Przykład. Niech G będzie dowolną grupą, a H jej podgrupą. Zdefiniujemy działanie $\phi : G \longrightarrow \Sigma_{G/H}$, 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 $\phi : G \longrightarrow \Sigma_G$ jest monomorfizmem.

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

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

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

Zauważmy, że zachodzi łatwe, ale ważne stwierdzenie:

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

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

jest G–izomorfizmem G–zbiorów.

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

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

Podsumowując: każdy G–zbiór jest rozłączną suma orbit, a każda orbita jest G–izomorficzna z dobrze znanym G–zbiorem (postaci G/H).

Zauważmy, że wybór punktu $x \in X$ zadaje przekształcenie $f : G/G_x \longrightarrow G(x)$, $f(g'G_x) = g'(x)$. Przekształcenie to jest dobrze określone i jest bijekcją zbiorów, co więcej taką, która 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. W szczególności moc orbity jest równa indeksowi $[G : G_x]$. Zbiór X jest rozłączną sumą orbit, więc moc skończonego G–zbioru X jest równa sumie długości orbit rozpatrywanego działania. Uwzględniając wzór na długość orbity podany we Wniosku 3.7 możemy to stwierdzenie zapisać w postaci następującego wzoru.

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

$$|X| = [G : G_{x_1}] + [G : G_{x_2}] + \cdots + [G : G_{x_n}], \tag{3.9}$$

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:

3.10. 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 3.7 wynika zatem, że suma mocy pozostałych orbit jest podzielna przez p. □

Stwierdzenie 3.8 i Wniosek 3.10 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 (3.9), 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 3.10 pozwala także na udowodnienie ważnego, a wcale nie oczywistego twierdzenia:

3.11. 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 3.10

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

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.

3.12. 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 $\{gxg^{-1}\colon g \in G\}$ elementu x nazywamy **klasą sprzężoności** elementu x;
grupę izotropii elementu x nazywamy **centralizatorem** elementu x w G i oznaczamy symbolem $C_G(x)$. Zatem

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

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 (3.9) występująca w Stwierdzeniu 3.8 nazywa się **równaniem klas** i przybiera postać:

$$|G| = |Z(G)| + [G : C_G(g_1)] + [G : C_G(g_2)] + \cdots + [G : C_G(g_k)], \tag{3.13}$$

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

Zanotujmy ważny wniosek z równości 3.13.

3.14. 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. □

3.15. 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. □

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 $H \longrightarrow \Sigma_2$. Homomorfizm ten jest trywialny (por. T2.6).Wynika stąd, że automorfizmy wewnętrzne wyznaczone przez elementy grupy H zachowują podgrupę K, a więc grupa H działa na grupie K i mamy homomorfizm $H \longrightarrow Aut(K)$. 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.

3.16. 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.*

3.17. 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.

ZADANIA

Z 3.1. Znaleźć klasy sprzężoności elementów grupy dihedralnej D_{2n}.

Z 3.2. Znaleźć orbity działania podgrupy obrotów $J \leqslant D_{2n}$ na D_{2n} przez automorfizmy wewnętrzne.

♡ Z 3.3. Korzystając z twierdzenia Cauchy'ego pokazać, że każda grupa rzędu 6 jest izomorficzna z grupą cykliczną $\mathbb{Z}_6$ lub z grupą dihedralną D_6.

Z 3.4. Niech $H \leqslant G$ będzie podgrupą. Sprawdzić, że wzór $\varphi_h(g) = gh^{-1}$ definiuje homomorfizm $\varphi : H \longrightarrow \Sigma_G$, $\varphi_h(g) = gh^{-1}$, a więc działanie grupy H na grupie G. Sprawdzić, że działanie to jest wierne a jego orbitami są warstwy lewostronne G względem H.

Z 3.5. Udowodnić, że nie istnieje grupa, w której elementów rzędu 7 jest dokładnie 18.

Z 3.6. Niech $k(G)$ oznacza liczbę klas sprzężoności elementów grupy G. Udowodnić, że jeżeli G jest skończoną grupą nieprzemienną to $k(G) > |Z(G)| + 1$.

Z 3.7. Udowodnić, że jeżeli G jest grupą skończoną i $k(G)$ jest liczbą parzystą, to $|G|$ jest także liczbą parzystą.

Z 3.8. Niech G będzie grupą skończoną i niech $H \leq G$, $|G : H| = 2$. Pokazać, że jeżeli dla każdego $h \in H$, $h \neq 1$, $C_G(h) \leq H$, to elementy $G \setminus H$ tworzą jedną klasę sprzężoności elementów G.

♡ Z 3.9. Niech $\phi : G \to \Sigma_G$ będzie monomorfizmem określonym w Przykładzie 3.4. Niech $g \in G$ będzie elementem rzędu n. Znaleźć rozkład na cykle rozłączne permutacji $\phi(g)$.

Z 3.10. Niech grupa skończona G działa na skończonym zbiorze X. Udowodnić wzór Burnside'a:

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

gdzie $|X/G|$ oznacza liczbę orbit działania G na X, a $|X^g|$ liczbę punktów stałych przekształcenia wyznaczonego przez $g \in G$.

⋆ Z 3.11. Dla każdego elementu $g \in SO(3)$ zdefiniujmy zbiór biegunów $B(g) = \{x \in S^2 : g(x) = x\}$. Niech G będzie skończoną podgrupą $SO(3)$ i niech $B(G) = \bigcup_{g \in G, g \neq 1} B(g)$. Sprawdzić, że $B(G)$ jest skończonym podzbiorem S^2, zachowywanym przez naturalne działanie G na S^2. Korzystając ze wzoru Burnside'a dla działania G na $B(G)$ wykazać, że jedynymi skończonymi podgrupami grupy $SO(3)$ są: grupy cykliczne $\mathbb{Z}_n$, $n \in N$, grupa symetrii czworościanu, sześcianu i dwunastościanu foremnego.

⋆ Z 3.12. Pokazać, że jeżeli $H \leqslant G$ jest właściwą podgrupą skończonego indeksu, to zbiór $\bigcup_{g \in G} gHg^{-1}$ jest właściwym podzbiorem zbioru elementów grupy G.

Z 3.13. Niech $\sigma \in \Sigma_6 \leqslant \Sigma_7$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 2 & 3 & 5 & 1 \end{pmatrix}$. Znaleźć $|C_{\Sigma_6}(\sigma)|$ oraz $|C_{\Sigma_7}(\sigma)|$.

TEST

T 3.1. Działanie grupy rzędu 27 na zbiorze 35 elementowym ma co najmniej jeden punkt stały.

♡ T 3.2. W klasie sprzężoności elementu $x \in G$ jest dokładnie $[G : C_G(x))]$ elementów.

♡ T 3.3. Dla każdego elementu x dowolnej grupy G zachodzi zawieranie $Z(G) \leqslant C_G(x)$.

T 3.4. Istnieje grupa rzędu 125 i tranzytywne działanie tej grupy na zbiorze mocy 30.

T 3.5. Dla każdej grupy rzędu 125 istnieje działanie tej grupy na zbiorze mocy 30 bez punktu stałego.

T 3.6. Dla każdej grupy rzędu 125 istnieje tranzytywne działanie tej grupy na zbiorze mocy 30.

T 3.7. Istnieje działanie grupy Σ_5 bez punktów stałych na zbiorze 20–elementowym.

♡ T 3.8. Dla dowolnej grupy G i dowolnego $x \in G$, $x \in C_G(x)$.

T 3.9. Istnieje działanie grupy D_{12} na zbiorze siedmioelementowym, które ma dokładnie dwie orbity.

T 3.10. Istnieje działanie grupy D_{12} na zbiorze siedmioelementowym, które ma dokładnie trzy orbity.

T 3.11. Istnieje co najmniej pięć działań grupy D_{12} na zbiorze siedmioelementowym, które mają dokładnie po trzy orbity i z których żadne dwa nie są D_{12}– izomorficzne.

T 3.12. W grupie $GL(2, \mathbb{Z}_7)$ macierzy odwracalnych o współczynnikach z ciała $\mathbb{Z}_7$ istnieje podgrupa indeksu 2.

T 3.13. W grupie $GL(2, \mathbb{Z}_7)$ macierzy odwracalnych o współczynnikach z ciała $\mathbb{Z}_7$ istnieje podgrupa indeksu 3.

♡ T 3.14. Grupa przemienna rzędu 15 jest cykliczna.

T 3.15. Grupa przemienna rzędu 20 jest cykliczna.

T 3.16. Grupa rzędu 10 jest cykliczna.

♡ T 3.17. Grupa przemienna rzędu 2001 jest cykliczna.

T 3.18. Jeżeli $f : G \to H$ jest homomorfizmem i elementy $x, y \in G$ są sprzężone w grupie G, to elementy $f(x), f(y)$ są sprzężone w H.

T 3.19. Jeżeli $x, y \in H \leqslant G$ i elementy x i y są sprzężone w grupie G, to są też sprzężone w grupie H.

♡ T 3.20. Permutacje (12654)(235) i (1324)(56) są sprzężone w Σ_6.

T 3.21. W grupie Σ_{10} istnieją dwa nie sprzężone ze sobą elementy rzędu 12.

T 3.22. W grupie Σ_{10} istnieją dwa nie sprzężone ze sobą elementy rzędu $n = 9$.

T 3.23. Niech $\sigma, \tau \in \Sigma_n \leqslant \Sigma_{n+k}$, gdzie $\Sigma_n \leqslant \Sigma_{n+k}$ jest naturalnym włożeniem grup permutacji. Jeżeli σ i τ są sprzężone w Σ_{n+k}, to σ i τ są sprzężone w Σ_n.

T 3.24. W grupie Σ_7 każde dwa elementy rzędu 10 są sprzężone.

4. Podgrupy normalne i grupy ilorazowe

Niech $\varphi : G \longrightarrow H$ będzie homomorfizmem. Rozpatrzmy zbiór warstw lewostronnych $G/\ker\varphi$ grupy G względem podgrupy $\ker\varphi$. Łatwo zauważyć, że

$$\varphi(x) = \varphi(y) \iff x^{-1}y \in \ker\varphi \iff x\ker\varphi = y\ker\varphi$$

— homomorfizm φ przeprowadza dwa elementy grupy G na ten sam element grupy H wtedy i tylko wtedy, gdy te dwa elementy wyznaczają tę samą warstwę lewostronną. Wynika stąd następujący wniosek:

4.1. Wniosek. *Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to*

$$|\mathrm{im}\,\varphi| = [G : \ker\varphi].$$

Załóżmy teraz, że φ jest *epimorfizmem.* Wówczas $\varphi : G \longrightarrow H$ wyznacza bijekcję $\bar{\varphi} : G/\ker\varphi \longrightarrow H$ (określoną wzorem $\bar{\varphi}(x\ker\varphi) = \varphi(x)$) zbioru $G/\ker\varphi$ i zbioru elementów grupy H. Na zbiorze warstw $G/\ker\varphi$ można więc w naturalny sposób zdefiniować działania, tak by bijekcja $\bar{\varphi}$ stała się izomorfizmem grup. Łatwo sprawdzić, że działania te są określone następującymi wzorami:

$$\begin{aligned}(x\ker\varphi)\cdot(y\ker\varphi) &= xy\ker\varphi,\\ (x\ker\varphi)^{-1} &= x^{-1}\ker\varphi,\end{aligned}$$

a elementem neutralnym jest warstwa $1\ker\varphi$ (czyli po prostu $\ker\varphi$).

Uwaga. Jeżeli założymy tylko tyle, że H jest podgrupą grupy G, to wzór $xH\cdot yH = xyH$ na ogół nie ma sensu, bo warstwa występująca po prawej stronie zależy od wyboru reprezentantów warstw występujących po lewej stronie. Można się o tym przekonać rozpatrując na przykład zbiór warstw $D_6/\{1,\varepsilon\}$.

Zdefiniujemy teraz taką klasę podgrup, dla których powyższy wzór *ma* sens.

4.2. Definicja. *Podgrupę $H \leqslant G$ nazywamy* **podgrupą normalną** *(lub* **dzielnikiem normalnym***), co oznaczamy symbolem $H \trianglelefteq G$, wtedy i tylko wtedy, gdy dla każdego $g \in G$, $gHg^{-1} = \{ghg^{-1} : h \in H\} = H$, czyli dla każdego automorfizmu wewnętrznego ϕ_g grupy G zachodzi równośc $\phi_g(H) = H$.*

4.3. Uwaga. *Warunek $\forall_{g\in G}\ gHg^{-1} = H$, jest równoważny warunkowi $\forall_{g\in G}\ gHg^{-1} \subseteq H$.*

Dowód. Wystarczy przeprowadzić łatwy rachunek. Niech $h \in H$. Wówczas $h = (gg^{-1})h(gg^{-1}) = g(g^{-1}hg)g^{-1} \in gHg^{-1}$, a zatem $H \subseteq gHg^{-1}$ (a zawieranie w drugą stronę jest bezpośrednio zagwarantowane w założeniu). □

4.4. Uwaga. *Warunek $H \trianglelefteq G$ jest równoważny warunkowi $\forall_{g\in G}\ gH = Hg$, czyli równości warstw prawostronnych i lewostronnych.*

Przykłady podgrup normalnych.

4.5. Przykład. $\mathbf{1} \trianglelefteq G$, $G \trianglelefteq G$

4.6. Przykład. Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem, to $\ker\varphi \trianglelefteq G$. Ten, jak się okaże uniwersalny, przykład ma wiele ważnych podprzykładów:

a) $Z(G) \trianglelefteq G$, gdzie $Z(G) = \ker\phi$, $\phi : G \longrightarrow Aut(G)$

b) $SO(n) \trianglelefteq O(n)$, gdzie $SO(n) = \ker det$, $det : O(n) \longrightarrow \mathbb{Z}_2$.

4.7. Przykład. Każda podgrupa grupy przemiennej jest normalna. (Ta własność nie charakteryzuje grup przemiennych — mają ją również niektóre grupy nieprzemienne, na przykład Q_8.)

4.8. Przykład. $1 \times K \trianglelefteq H \times K$ i $H \times 1 \trianglelefteq H \times K$.

4.9. Stwierdzenie. *Jeżeli $H \leqslant G$ i $[G : H] = 2$, to $H \trianglelefteq G$.*

Dowód. Oczywiście $\forall_{g\in H}\forall_{h\in H}\ ghg^{-1} \in H$. Pozostaje przypadek, gdy $g \notin H$. Przypuśćmy, że $\exists_{h\in H}\ ghg^{-1} \notin H$. Skoro tak, to $ghg^{-1} \in G \setminus H = gH$. Jak widać, elementy g i ghg^{-1} należą do tej samej warstwy (gH) względem podgrupy H. Ale to oznacza, że $g^{-1} \cdot ghg^{-1} \in H$. Po redukcji otrzymujemy $hg^{-1} \in H$, skąd $g \in H$, a to oznacza sprzeczność. □

4.10. Wniosek. *Podgrupa obrotów $J = \{1, \rho, \ldots, \rho^{n-1}\}$ grupy dihedralnej D_{2n} jest dzielnikiem normalnym.*

Odnotujmy jeszcze następujące, łatwe do udowodnienia, własności podgrup normalnych:

1) Jeżeli $\varphi : G \longrightarrow H$ jest homomorfizmem i $N \trianglelefteq H$, to $\varphi^{-1}(N) \trianglelefteq G$
2) Jeżeli $\varphi : G \longrightarrow H$ jest epimorfizmem i $N \trianglelefteq G$, to $\varphi(N) \trianglelefteq H$.
   Jeżeli o przekształceniu φ zakładamy tylko tyle, że jest homomorfizmem, to w każdym razie możemy twierdzić, że $\varphi(N) \trianglelefteq \mathrm{im}\,(\varphi)$.
3) Jeżeli $N_i \trianglelefteq G$ dla $i \in I$ to $\bigcap\limits_{i\in I} N_i \trianglelefteq G$.
4) Jeżeli $N \trianglelefteq G$ i $K \leqslant G$, to $N \cap K \trianglelefteq K$.

4.11. Przykład. Niech $H \leqslant G$ będzie dowolną podgrupą. Rozpatrzymy znany nam homomorfizm $\phi : G \longrightarrow \Sigma_{G/H}$ zadany wzorem $\phi_g(xH) = gxH$, opisujący działanie G na zbiorze warstw G/H. Wówczas $\ker\phi = \bigcap_{g\in G}\ gHg^{-1} \leqslant H$ jest podgrupą normalną grupy G — jest to *największa ze względu na zawieranie podgrupa normalna grupy G, spośród tych, które są zawarte w H*. Oczywiście jeżeli $H \trianglelefteq G$, to $H = \ker\phi$.

Informacja, że otrzymana podgrupa jest jądrem homomorfizmu ϕ jest użyteczna w dowodzie następującego wniosku.

4.12. Wniosek. *Niech H będzie podgrupą indeksu n w grupie skończonej G. Wówczas istnieje podgrupa normalna $N \trianglelefteq G$, $N \leq H$, taka że $n\big|[G : N]$ i $[G : N]\big|n!$ (tzn. indeks N w G jest wielokrotnością n, a dzielnikiem $n!$).*

Dowód. Szukaną grupą jest właśnie grupa $N = \ker\varphi$ opisana w przykładzie 4.11. Podzielność $n\big|[G : N]$ jest oczywista — indeks mniejszej podgrupy jest wielokrotnością indeksu większej podgrupy. Natomiast podzielność $[G : N]\big|n!$ wynika z faktu, że $|\mathrm{im}\,\varphi| = [G : \ker\phi] = [G : N]$ (Wniosek 4.1), z drugiej zaś strony $|\mathrm{im}\,\phi|\ \big|\ |\Sigma_{G/H}|$ (Twierdzenie Lagrange'a). □

4.13. Przykład. Niech $H \leqslant G$. Zdefiniujmy podgrupę

$$N_G(H) = \{g \in G\colon\ gHg^{-1} = H\}.$$

Oczywiście $H \leqslant N_G(H) \leqslant G$ i $H \trianglelefteq N_G(H)$. Zauważmy, że $N_G(H)$ jest *największą taką podgrupą grupy G zawierającą H, w której H jest normalna.* Jest jasne, że jeżeli $H \trianglelefteq G$, to $N_G(H) = G$. Podgrupę $N_G(H)$ nazywamy **normalizatorem** H w G.

Jeżeli rozpatrzymy działanie grupy G na zbiorze jej podgrup, zadane przez automorfizmy wewnętrzne, to $N_G(H)$ jest grupą izotropii podgrupy H, a punktami stałymi tego działania są podgrupy normalne.

Jeżeli $H \trianglelefteq G$, to z taką parą związana jest ważna konstrukcja grupy ilorazowej.

4.14. Definicja. *Niech $H \trianglelefteq G$.* **Grupą ilorazową** *grupy G przez podgrupę normalną H nazywamy zbiór warstw G/H z warstwą $1H$ jako elementem wyróżnionym i z działaniami:*

$$\begin{aligned} xH \cdot yH &= xyH \\ (xH)^{-1} &= x^{-1}H. \end{aligned}$$

Należy sprawdzić, że działanie jest dobrze zdefiniowane, to znaczy nie zależy od wyboru reprezentantów warstw. Niech $xH = x'H$ i $yH = y'H$. Należy pokazać, że $xyH = x'y'H$. Założyliśmy, że $x^{-1}x' \in H$ i $y^{-1}y' \in H$, a chcemy wykazać że $(xy)^{-1}x'y' \in H$. Rozpatrzmy ciąg równości:

$$(xy)^{-1}x'y' = y^{-1}x^{-1}x'y' = y^{-1}x^{-1}x'yy^{-1}y' = \left(y^{-1}(x^{-1}x')y\right)(y^{-1}y').$$

Założyliśmy, że $H \trianglelefteq G$. Zatem $y^{-1}(x^{-1}x')y \in H$. Również $y^{-1}y' \in H$. Wobec tego $(xy)^{-1}x'y' \in H$. Analogicznie sprawdzamy, że działanie jednoargumentowe jest dobrze określone. Fakt, że tak określone działania spełniają aksjomaty grupy jest oczywisty.

Odnotujmy także stwierdzenie:

4.15. Stwierdzenie. *Jeżeli $H \trianglelefteq G$, to odwzorowanie $\pi : G \longrightarrow G/H$, określone wzorem $\pi(g) = gH$ jest epimorfizmem i* $\ker \pi = H$.

Epimomorfizm π nazywamy rzutowaniem grupy G na grupę ilorazową G/H.

4.16. Przykład. Grupa ilorazowa grupy cyklicznej $G = \langle\, g \,\rangle$ przez podgrupę H jest grupą cykliczną i oczywiście $G/H = \langle\, gH \,\rangle$

Przy pomocy grupy ilorazowej możemy opisać obraz dowolnego homomorfizmu.

4.17. Twierdzenie o homomorfizmie. *Niech $\varphi : G \longrightarrow H$ będzie homomorfizmem, a $\pi : G \longrightarrow G/\ker\varphi$ rzutowaniem. Wówczas istnieje dokładnie jeden monomorfizm $\tilde{\varphi} : G/\ker\varphi \longrightarrow H$, taki że $\tilde{\varphi} \circ \pi = \varphi$. W szczególności $\tilde{\varphi} : G/\ker\varphi \longrightarrow im\,\varphi$ jest izomorfizmem.*

Dowód. Szukanym monomorfizmem jest odwzorowanie ψ, określone wzorem $\psi(g\ker\varphi) = \varphi(g)$. □

Zanotujmy jeszcze przydatny wniosek z powyższego twierdzenia.

4.18. Wniosek. *Niech $\varphi : G \longrightarrow H$ będzie epimorfizmem i niech $K \trianglelefteq H$. Wówczas*

$$G/\varphi^{-1}(K) \cong H/K.$$

Dowód. Złożenie $G \xrightarrow{\varphi} H \xrightarrow{\pi_K} H/K$ (gdzie $\pi_K : H \longrightarrow H/K$ jest rzutowaniem) jest epimorfizmem, a jego jądrem jest $\varphi^{-1}(K)$. □

Spróbujmy teraz znaleźć wszystkie homomorfizmy $G \longrightarrow H$, dla danych grup G i H lub przynajmniej obliczyć ile ich jest.
Umiemy to zadanie rozwiązać, gdy $G = \langle\, g \,\rangle$ jest grupą cykliczną — homomorfizm $\varphi : \langle\, g \,\rangle \longrightarrow H$ jest jednoznacznie wyznaczony przez wskazanie elementu $\varphi(g)$, takiego że $o(\varphi(g)) \,|\, o(g)$. Homomorfizmów jest więc dokładnie tyle ile elementów $h \in H$, takich że $o(h) \,|\, o(g)$.

W przypadku dowolnej grupy G zaczniemy od zbadania liczby epimorfizmów $G \longrightarrow K$ dla ustalonego K. Po pierwsze trzeba znaleźć wszystkich kandydatów na jądro takiego epimorfizmu, czyli wszystkie normalne podgrupy $N \trianglelefteq G$, takie że $G/N \cong K$. Nie ma tu żadnego algorytmu. Dwa epimorfizmy ϕ, ψ o tym samym jądrze N różnią się o automorfizm $\tilde{\phi}(\tilde{\psi})^{-1}$ grupy K — mamy bowiem $\phi = \tilde{\phi}\pi_N = \tilde{\phi}(\tilde{\psi})^{-1}\tilde{\psi}\pi_N = \tilde{\phi}(\tilde{\psi})^{-1}\psi$. Zatem liczba epimorfizmów $G \longrightarrow K$ jest równa $n_K \cdot |Aut(K)|$, gdzie n_K jest liczbą normalnych podgrup G, takich że grupa ilorazowa jest izomorficzna z K. Zanotujmy jeszcze, że $|Aut(\mathbb{Z}_n)| = \varphi(n)$.

Na koniec przytoczymy ważny przykład grupy ilorazowej. Niech A będzie grupą abelową, a $\varphi : G \longrightarrow A$ homomorfizmem. Wówczas $\forall_{x,y \in G}\ x^{-1}y^{-1}xy \in \ker \varphi$. Element $x^{-1}y^{-1}xy$ nazywamy **komutatorem** elementów x i y i oznaczamy symbolem $[x, y]$. **Komutantem** grupy G nazywamy podgrupę

$$[G, G] = \langle\, \{[x, y] :\ x, y \in G\} \,\rangle.$$

Komutant jest podgrupą normalną, a nawet ma pewną własność jeszcze lepszą niż normalność. Niech mianowicie $\phi : G \to G$ będzie dowolnym automorfizmem grupy G. Wówczas $\phi([x, y]) = [\phi(x), \phi(y)]$. Wobec tego $\phi([G, G]) = [G, G]$. Warunek normalności podgrupy $[G, G]$ w grupie G jest słabszy — to ten sam warunek, ale tylko dla ϕ będących automorfizmami wewnętrznymi grupy G.

4.19. Definicja. *Podgrupę $H \leqslant G$ nazywamy podgrupą* **charakterystyczną**, *co oznaczamy symbolem $H \blacktriangleleft G$, wtedy i tylko wtedy, gdy dla każdego automorfizmu ϕ grupy G zachodzi równość $\phi(H) = H$.*

4.20. Przykład. Dla dowolnej grupy G jej centrum $Z(G)$ jest podgrupą charakterystyczną.

Jest jasne, że grupa ilorazowa $G/[G, G]$ jest przemienna i że wśród podgrup normalnych grupy G podgrupa $[G, G]$ jest najmniejszą taką, że grupa ilorazowa jest przemienna. Grupę $G/[G, G]$ nazywamy **abelianizacją grupy** G. Jest to największa przemienna grupa ilorazowa grupy G. Precyzyjnie wyraża to następujące twierdzenie.

4.21. Twierdzenie. *Dla każdego homomorfizmu $\varphi : G \longrightarrow A$, gdzie A jest grupą przemienną, istnieje dokładnie jeden homomorfizm $\psi : G/[G, G] \longrightarrow A$, taki że $\psi \circ \pi = \varphi$ ($\pi : G \longrightarrow G/[G, G]$ jest rzutowaniem).*

Permutacje parzyste

W każdej grupie permutacji Σ_n, $n \geq 2$ istnieje podgrupa normalna indeksu 2, oznaczana symbolem A_n — tak zwana **grupa alternująca** (albo: **grupa permutacji parzystych**). Okaże się, że dla $n \geq 5$ jest to jedyna nietrywialna właściwa podgrupa normalna grupy Σ_n.

Grupy, które mają mało podgrup normalnych są z pewnych względów szczególnie interesujące. Wobec tego odnotujmy w tym miejscu następującą definicję.

4.22. Definicja. *Niech G będzie nietrywialną grupą. Jeżeli jedynymi podgrupami normalnymi grupy G są G i podgrupa trywialna, to mówimy, że grupa G jest* **grupą prostą**.

Oczywistym przykładem grupy prostej jest dowolna grupa $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą. Grupy $\mathbb{Z}_p$ są jedynymi przemiennymi grupami prostymi. Grupy A_n (dla $n \geq 5$) również są proste (to już jest mniej oczywiste; pokażemy to dla $n = 5$).

Przechodzimy do opisu grup alternujących.

Skonstruujemy najpierw monomorfizm $\Psi : \Sigma_n \longrightarrow GL(n, \mathbb{R})$. Wybieramy bazę uporządkowaną $e_1, \ldots, e_n$ w $\mathbb{R}^n$ i określamy $\Psi(\sigma)$ jako przekształcenie liniowe, które permutuje elementy bazy tak jak każe σ, to jest $\Psi(\sigma)(e_i) = e_{\sigma(i)}$. Wyznacznik macierzy takiego przekształcenia jest równy ± 1. Zatem mamy homomorfizm $det \circ \Psi : \Sigma_n \longrightarrow \{-1, 1\} \leqslant \mathbb{R}^*$

4.23. Definicja. *Permutację nazywamy* **permutacją parzystą**, *jeżeli należy do jądra homomorfizmu* $\det \circ \Psi$. *W przeciwnym przypadku permutację nazywamy* **permutacją nieparzystą**. *Podgrupę permutacji parzystych grupy Σ_n oznaczamy symbolem A_n.*

Jako jądro pewnego homomorfizmu podgrupa $A_n \leq \Sigma_n$ jest oczywiście normalna w Σ_n. Z twierdzenia o izomorfizmie wynika, że dla $n \geq 2$, $\Sigma_n / A_n \cong \mathbb{Z}_2$.

Ponadto złożenie

- ✓ dwóch permutacji parzystych jest permutacją parzystą,
- ✓ dwóch permutacji nieparzystych jest permutacją parzystą,
- ✓ permutacji parzystej i permutacji nieparzystej jest permutacją nieparzystą.

Zbadamy parzystość cykli. Jest jasne, że cykl długości 2, czyli transpozycja, jest permutacją nieparzystą — wynika to z algorytmu liczenia wyznacznika. Aby ocenić parzystość cyklu dowolnej długości odnotujmy najpierw następujący fakt.

4.24. Stwierdzenie. *Zachodzi równość:*

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_3)(a_1, a_2).$$

□

4.25. Wniosek. *Cykl długości k jest permutacją parzystą jeżeli k jest liczbą nieparzystą, a permutacją nieparzystą jeżeli k jest liczbą parzystą. Jeżeli permutacja jest iloczynem cykli o długościach $k_1, \ldots, k_s$, to jest ona parzysta wtedy i tylko wtedy, gdy wśród liczb $k_1, \ldots, k_s$ jest parzyście wiele parzystych.* □

Na zakończenie tego rozdziału udowodnimy, że A_5 jest grupą prostą.

Zaczniemy od policzenia ile jest klas sprzężoności elementów A_5 i ile elementów liczy każda klasa. Przypomnijmy, że w dowolnej grupie G moc klasy sprzężoności

elementu x jest równa $[G : C_G(x)]$. W poniższej tabeli przedstawiamy możliwe typy rozkładów na cykle, rzędy centralizatorów, moce klas sprzężoności elementów każdego typu ($conj(x)$), liczby elementów o ustalonym typie rozkładu ($sim(x)$) i liczby klas sprzężoności elementów o danym typie rozkładu.

Tabela

rozkład na cykle	$\lvert C_{A_5}(x)\rvert$	$conj(x)$	$sim(x)$	liczba klas sprzężoności
(.)(.)(.)(.)(.)	60	1	1	1
(..)(..)(.)	4	15	15	1
(...)(.)(.)	3	20	20	1
(.....)	5	12	24	2

4.26. Twierdzenie. *Grupa A_5 jest prosta.*

Dowód. Podgrupa normalna (w każdej grupie) jest zawsze sumą mnogościową pewnych klas sprzężoności — bo jeżeli pewien element należy do tej podgrupy normalnej, to już cała jego klasa sprzężoności musi być w niej zawarta. Zatem rząd podgrupy normalnej musi się dać wyrazić jako suma liczebności pewnych klas sprzężoności. W przypadku podgrupy normalnej N grupy A_5 dochodzimy do wniosku, że $|N| = 1 + b \cdot 15 + c \cdot 20 + d \cdot 12$, przy czym współczynniki b i c mogą przyjmować wartości 0 lub 1, a współczynnik d być może również 2 (bo są dwie klasy sprzężoności cykli długości 5 w grupie A_5 i być może obie są zawarte w N). Z twierdzenia Lagrange'a wiemy, że $|N| \,\big|\, 60$. Łatwo sprawdzić, że jedynymi dzielnikami liczby 60, dającymi się przedstawić w żądany sposób są 1 i 60. Zatem w A_5 nie ma podgrup normalnych innych niż sama grupa A_5 i jej podgrupa trywialna. □

ZADANIA

♡ Z 4.1. Pokazać, że podgrupa $H \leqslant G$ jest normalna wtedy i tylko wtedy, gdy dla każdego elementu $g \in G$, jego warstwa lewostronna względem podgrupy H jest równa jego warstwie prawostronnej względem podgrupy H, to jest $gH = Hg$.

♡ Z 4.2. Pokazać, że jeżeli $H \trianglelefteq G$, to każda podgrupa grupy G/H jest postaci K/H, gdzie $K \leqslant G$ jest podgrupą zawierającą H. Ponadto udowodnić, że $K/H \trianglelefteq G/H$ wtedy i tylko wtedy, gdy $K \trianglelefteq G$, i że wówczas

$$G/H \Big/ K/H \cong G/K.$$

♡ Z 4.3. Niech $H \trianglelefteq G$. Niech $\pi : G \longrightarrow G/H$ będzie rzutowaniem, a $K \leqslant G$ podgrupą. Udowodnić, że

a) $\pi^{-1}(\pi(K)) = K \cdot H = \{k \cdot h\colon\ k \in K, h \in H\} \leqslant G$. Ponadto $K \cdot H = H \cdot K = \langle\, K \cup H \,\rangle$

b) $K/(K \cap H) \cong (K \cdot H)/H$.

c) podać przykłady podgrup $H \leqslant G$ i $K \leqslant G$, takich że $K \cdot H$ nie jest podgrupą grupy G.

Z 4.4. Znaleźć abelianizację grupy D_{2n}.

Z 4.5. Niech $H \trianglelefteq G$. Udowodnić, że $\forall_{x,\, y \in G}\ xy \in H \Rightarrow yx \in H$. Podać przykład, że jeżeli zakładamy tylko $H \leqslant G$, to wynikanie nie ma miejsca.

Z 4.6. Pokazać, że każda podgrupa w Q_8 jest normalna, choć Q_8 nie jest abelowa.

Z 4.7. Niech $K \trianglelefteq G$ i $\mid G/K \mid = n < \infty$. Pokazać, że:

a) dla każdego $g \in G$, $g^n \in K$.

b) jeżeli $g \in G$ i $g^m \in K$ oraz $(n, m) = 1$, to $g \in K$.

Z 4.8. Załóżmy, że $K \trianglelefteq G$ i $\mid K \mid = m < \infty$. Niech $n \in N$ i $(n, m) = 1$ i niech $g \in G$. Udowodnić, że:

a) jeżeli $o(g) = n$, to $o(gK) = n$.

b) jeżeli w grupie ilorazowej G/K zachodzi $o(gK) = n$, to istnieje element $g' \in G$, taki że $o(g') = n$ oraz $gK = g'K$.

Z 4.9. Niech $H \trianglelefteq G$ i $K \trianglelefteq G$. Pokazać, że jeżeli G/K, G/H są grupami abelowymi, to $G/H \cap K$ jest grupą abelową.

♡ Z 4.10. Niech $N \trianglelefteq G$ będzie podgrupą normalną, a $\pi : G \longrightarrow G/N$ rzutowaniem. Niech $S \subset G$ będzie zbiorem elementów G, takim że $\langle\, \pi(S) \,\rangle = G/N$. Udowodnić, że jeżeli $X \subset N$ i $\langle\, X \,\rangle = N$ to $\langle\, S \cup X \,\rangle = G$.

♡ Z 4.11. Pokazać, że jeżeli $K \blacktriangleleft H$ i $H \trianglelefteq G$ to $K \trianglelefteq G$. Podać przykład takich podgrup $K \trianglelefteq H$ i $H \trianglelefteq G$, że $K \not\trianglelefteq G$.

Z 4.12. Udowodnić, że jeżeli $n \geq 3$, to $J_n \blacktriangleleft D_{2n}$.

Z 4.13. Udowodnić, że jeżeli $K \trianglelefteq G$ to $Z(K) \trianglelefteq G$.

Z 4.14. Udowodnić, że jeżeli $[G, G] \leqslant H \leqslant G$, to $H \trianglelefteq G$.

Z 4.15. Niech $n \geq 3$. Udowodnić, że jeżeli n jest nieparzyste, to $Z(D_{2n}) = 1$, a jeżeli n jest parzyste to $D_{2n}/Z(D_{2n}) \cong D_n$.

Z 4.16. Pokazać, że podgrupa grupy obrotów grupy dihedralnej jest normalna. Pokazać, że jeżeli $k \cdot l = n$, to $D_{2n}/\langle\, \rho^k \,\rangle \cong D_{2k}$.

Z 4.17. Wykazać, że jeżeli w grupie G istnieje podgrupa skończonego indeksu, to istnieje zawarta w niej podgrupa normalna skończonego indeksu.

♡ Z 4.18. Pokazać, że jeżeli p jest najmniejszą liczbą pierwszą dzielącą $|G|$ i $H \leqslant G$, $|G : H| = p$, to $H \trianglelefteq G$.

Z 4.19. (Hölder) Niech $H \trianglelefteq G$, gdzie G jest grupą skończoną a H grupa prostą. Pokazać, że jeżeli $|H|^2$ nie dzieli $|G|$, to H jest jedyną podgrupą G izomorficzną z H.

Z 4.20. Udowodnić, że $GL(2,\mathbb{Z}_3)/Z(GL(2,\mathbb{Z}_3))$ jest izomorficzne z Σ_4.

Z 4.21. Jeżeli G jest skończoną grupą przemienną i $n \mid |G|$, to w grupie G istnieje podgrupa rzędu n i podgrupa indeksu n.

Z 4.22. Niech G będzie grupą skończoną. Pokazać, że G zawiera podgrupę normalną indeksu p, gdzie p jest liczbą pierwszą, wtedy i tylko wtedy, gdy $p \mid |G/[G,G]|$.

Z 4.23. Udowodnić, że jeżeli $|G| = 2r$, $r > 1$ i $\neg(2 \mid r)$, to G nie jest grupą prostą (wskazówka: patrz zadanie 3.9).

4.24. Definicja. *Grupę G nazywamy* **doskonałą**, *jeżeli* $[G,G] = G$.

Z 4.25. Niech G będzie grupą doskonałą, a $K \trianglelefteq G$ podgrupą cykliczną normalną. Pokazać, że $K \leqslant Z(G)$.

Z 4.26. Które z następujących permutacji w Σ_6 są parzyste: (123456), (12345), (123)(45), (23)(46)?

Z 4.27. Niech $H \leqslant \Sigma_n$, $n > 1$. Udowodnić, że jeżeli H zawiera permutację nieparzystą, to H zawiera podgrupę indeksu 2.

Z 4.28. W A_n, $n \geq 3$ znaleźć podgrupę generowaną przez 3-cykle.

♡ Z 4.29. Udowodnić, że dla $n \geq 3$, $Z(\Sigma_n) = 1$.

⋆ Z 4.30. Udowodnić, że dla $n \neq 6$ każdy automorfizm grupy Σ_n, $n > 2$ jest wewnętrzny.

Z 4.31. Rozpatrzmy grupy Σ_4 oraz A_4.

a) Wyznaczyć klasy sprzężoności elementów Σ_4 oraz A_4 .
b) Wskazać dwa elementy A_4, które są sprzężone w Σ_4, a nie są sprzężone w A_4.
c) Znaleźć $Z(A_4)$.
d) Wykazać, że w A_4 istnieje tylko jedna podgrupa rzędu 4, więc jest ona charakterystyczna.
e) Udowodnić, że w A_4 nie istnieje podgrupa rzędu 6.
f) Znaleźć $[A_4, A_4]$.

Z 4.32. Niech $H \leqslant \Sigma_n$. Pokazać, że jeżeli $H \not\subseteq A_n$, to $H \cdot A_n = \Sigma_n$ i $|H| = 2|H \cap A_n|$.

♡ Z 4.33. Niech $\sigma \in A_n$. Pokazać, że klasa sprzężoności w Σ_n elementu σ jest równa jego klasie sprzężoności w A_n jeżeli $C_{\Sigma_n}(\sigma) \not\subseteq A_n$ lub jest sumą dwóch różnych równolicznych klas sprzężoności w A_n jeżeli $C_{\Sigma_n}(\sigma) \subseteq A_n$.

Z 4.34. Niech σ będzie elementem rzędu 5 w grupie A_5. Wówczas $|C_{A_5}(\sigma)| = \square$ (gdzie $C_G(x)$ oznacza zbiór elementów przemiennych z x w grupie G).

Z 4.35. Udowodnić, że grupa zachowujących orientację R^3 izometrii sześcianu jest izomorficzna z grupą Σ_4 (patrz P.C.Aleksandrow: Wwiedienije w teoriu grup).

⋆ Z 4.36. Udowodnić, że grupa zachowujących orientację R^3 izometrii dwudziestościanu foremnego jest izomorficzna z grupą A_5 (patrz P.C.Aleksandrow: Wwiedienije w teoriu grup).

♡ Z 4.37. Niech $\Phi : G \to Aut(G)$ będzie działaniem przez automorfizmy wewnętrzne. Niech $\Re$ będzie zbiorem podgrup grupy G i rozpatrzmy na nim działanie grupy G wyznaczone przez Φ. Wówczas:

a) Podgrupa $H \in \Re$ jest punktem stałym rozpatrywanego działania wtedy i tylko wtedy, gdy $H \trianglelefteq G$.
b) Grupą izotropii podgrupy $H \in \Re$ jest jej normalizator

$$N_G(H) = \{g \in G : gHg^{-1} = H\} \leqslant G.$$

c) Liczba podgrup G sprzężonych z H, czyli moc orbity H, jest równa indeksowi $[G : N_G(H)]$ i dzieli indeks $[G : H]$.

♡ Z 4.38. Niech $H \leqslant G$. Rozpatrzmy działanie G na zbiorze warstw G/H opisane w Przykładzie 3.4 i ograniczmy je do podgrupy $K \leqslant G$. Pokazać, że warstwa gH jest punktem stałym działania grupy K wtedy i tylko wtedy, gdy $K \leqslant gHg^{-1}$. W szczególności, jeżeli $K = H$, to $(G/H)^H = N_G(H)/H$

TEST

♡ T 4.1. Jeżeli $f : G \to H$ jest izomorfizmem i $N \trianglelefteq G$, to $G/N \cong H/f(N))$.

T 4.2. Cykle $(1, 2, 3, 4, 5)$ i $(1, 3, 5, 2, 4)$ są sprzężone w A_5.

T 4.3. Cykle $(1, 2, 3, 4, 5)$ i $(1, 3, 5, 2, 4)$ są sprzężone w Σ_5.

T 4.4. Podgrupa rzędu 2 w Q_8 jest charakterystyczna.

T 4.5. Podgrupa indeksu 2 w Q_8 jest charakterystyczna.

T 4.6. Jeżeli $\langle X \rangle = H \leqslant G$ i dla każdego $g \in G$, $gXg^{-1} = X$, to $H \trianglelefteq G$.

T 4.7. Jeżeli $\langle X \rangle = H \leqslant G$ i dla każdego $g \in G$, $gXg^{-1} \subseteq X$, to $H \trianglelefteq G$.

T 4.8. Jeżeli $\langle X \rangle = H \leqslant G$ i dla każdego $\phi \in Aut(G)$, $\phi(X) = X$, to $H \blacktriangleleft G$.

T 4.9. Jeżeli $\langle X \rangle = H \leqslant G$ i dla każdego $\phi \in Aut(G)$, $\phi(X) \subseteq X$, to $H \blacktriangleleft G$.

T 4.10. Jeżeli $H \trianglelefteq K$ i $K \trianglelefteq G$, to $H \trianglelefteq G$.

T 4.11. Jeżeli $H \trianglelefteq K$ i $K \blacktriangleleft G$, to $H \trianglelefteq G$.

T 4.12. Jeżeli $H \blacktriangleleft K$ i $K \blacktriangleleft G$, to $H \trianglelefteq G$.

T 4.13. Jeżeli $H \blacktriangleleft K$ i $K \blacktriangleleft G$, to $H \blacktriangleleft G$.

T 4.14. Jeżeli $K \leqslant G$, to $Z(K) = K \cap Z(G)$.

T 4.15. Dla dowolnej grupy G i jej elementów $g_1, g_2, \ldots, g_k$ iloczyn $g_1 g_2 \cdots g_k g_1^{-1} g_2^{-1} \cdots g_k^{-1} \in [G, G]$.

T 4.16. Niech H będzie podgrupą normalną w grupie G. Jeżeli $H \nsubseteq Z(G)$, to istnieje nietrywialny homomorfizm $G \longrightarrow Aut(H)$.

T 4.17. Grupa G może zawierać podgrupę właściwą normalną z nią izomorficzną.

T 4.18. Jeżeli $x \in H \leq G$, to klasa sprzężoności elementu x w grupie H jest zawarta w klasie sprzężoności elementu x w grupie G.

T 4.19. Jeżeli grupa rzędu 2000 zawiera dokładnie 4 elementy rzędu 5, to posiada właściwą nietrywialną podgrupę normalną (czyli nie jest prosta).

T 4.20. Jeżeli w dowolnej grupie podgrupa rzędu trzy jest normalna, to jest zawarta w centrum grupy.

T 4.21. Jeżeli w grupie rzędu nieparzystego podgrupa rzędu trzy jest normalna, to jest zawarta w centrum grupy.

T 4.22. Jeżeli $A \trianglelefteq G$ jest abelową podgrupą normalną, to $Z(G) \leq A$.

T 4.23. Istnieje n, takie że $[D_{2n}, D_{2n}] = D_{2n}$

T 4.24. Niech $H \leq G$, $K \leq G$ będą podgrupami. Jeżeli zbiór $HK = \{hk : h \in H, k \in K\}$ jest podgrupą G to $HK = KH$.

T 4.25. Niech $H \leq G$, $K \leq G$ będą podgrupami.Jeżeli $HK = KH$ to HK jest podgrupą G

T 4.26. Jeżeli zbiór $HK = \{hk : h \in H, k \in K\}$ jest podgrupą G to $H \trianglelefteq G$ lub $K \trianglelefteq G$.

T 4.27. Jeżeli HK jest podgrupą G to $|HK| = |K||H|$.

T 4.28. Jeżeli $[G : H] = 2$ i $K \trianglelefteq H$, to $K \trianglelefteq G$.

T 4.29. Podgrupa grupy obrotów grupy D_{2n} jest normalna w D_{2n}.

T 4.30. Podgrupa indeksu 2 jest zawsze podgrupą charakterystyczną.

T 4.31. Niech σ będzie elementem rzędu 5 w grupie A_5. Wówczas σ i σ^2 są sprzężone w A_5.

T 4.32. Niech σ będzie elementem rzędu 5 w grupie A_5. Wówczas σ i σ^{-1} są sprzężone w A_5.

T 4.33. W grupie A_5 każde dwa elementy rzędu 5 są sprzężone.

T 4.34. W grupie A_5 każde dwa elementy rzędu 2 są sprzężone.

T 4.35. Jeżeli G jest grupą skończoną i $[G : [G, G]] = 10$ to istnieje podgrupa $K \leqslant G$ izomorficzna z $\mathbb{Z}_{10}$.

♡ T 4.36. Jeżeli G jest grupą skończoną i $[G : [G, G]] = 10$ to istnieje podgrupa normalna $K \trianglelefteq G$ indeksu 5.

♡ T 4.37. Jeżeli $H \trianglelefteq G$, to $[H, H] \trianglelefteq G$.

T 4.38. Jeżeli G jest nieprzemienną grupą rzędu 125, to $G/Z(G)$ jest izomorficzne z

---

T 4.39. Jeżeli G jest nieprzemienną grupą rzędu 125, to $[G, G] = Z(G)$.

T 4.40. $A_n \trianglelefteq \Sigma_n$ jest podgrupą charakterystyczną.

T 4.41. W grupie Σ_7 każde dwa elementy rzędu 10 są sprzężone.

T 4.42. Istnieje działanie grupy Σ_5 bez punktów stałych na zbiorze 20–elementowym.

T 4.43. Permutacja $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix}$ jest parzysta.

T 4.44. Niech $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 1 & 8 & 2 & 4 & 7 & 6 \end{pmatrix}$. Wówczas σ^4 jest permutacją parzystą.

5. Rozszerzenia. Produkt i produkt półprosty

W rozdziale czwartym zdefiniowaliśmy pojęcie podgrupy normalnej. Jeżeli $N \trianglelefteq G$, to zdefiniowana jest grupa ilorazowa i rzutowanie $\pi : G \longrightarrow G/N$. Powstaje pytanie, do jakiego stopnia struktura grupy G jest zdeterminowana przez grupy N i G/N. Czy klasa izomorfizmu grupy G jest wyznaczona jednoznacznie przez N i G/N? Czy może jest tak przy jakichś jeszcze dodatkowych założeniach o położeniu podgrupy N w grupie G? A może przy jeszcze jakichś dodatkowych informacjach?

W związku z tym będziemy obecnie rozważać różne sytuacje związane z istnieniem w grupie G podgrupy normalnej. Przypomnijmy definicję grupy prostej.

5.1. Definicja. *Niech G będzie nietrywialną grupą. Jeżeli jedynymi podgrupami normalnymi grupy G są sama grupa G i podgrupa trywialna, to mówimy, że grupa G jest* **grupą prostą**.

W rozdziale czwartym pokazaliśmy, że A_5 jest grupą prostą i wspomnieliśmy, że wszystkie grupy alternujące A_n, $n \geq 5$, są proste. Jedynymi przemiennymi grupami prostymi są grupy cykliczne $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą. Grupy proste są jakby "nierozkładalnymi cegiełkami, z których zbudowane są inne grupy". Skończone grupy proste zostały sklasyfikowane. Dowód twierdzenia o klasyfikacji grup prostych był jednym z największych przedsięwzięć w historii matematyki i został zakończony w kwietniu 1981 roku. Jednym z najważniejszych jego kroków było twierdzenie Feita i Thompsona, z którego wynika, że rząd skończonej nieabelowej grupy prostej jest liczbą parzystą. Dowód tego twierdzenia, opublikowany w 1963 roku w pracy *Solvability of groups of odd order,* zajmuje 225 stron.

Przejdziemy do sytuacji, gdy grupa G *posiada* podgrupę normalną N, o której na razie nic więcej nie zakładamy. Wówczas N jest oczywiście jądrem rzutowania π grupy G na iloraz G/N. Możemy to zapisać w następującej postaci:

$$N \longrightarrow G \xrightarrow{\pi} G/N.$$

Bardziej ogólnie:

5.2. Definicja. *Mówimy, że grupa G jest* **rozszerzeniem grupy N za pośrednictwem grupy** H, *jeżeli istnieją: monomorfizm i oraz epimorfizm π, $N \xrightarrow{i} G \xrightarrow{\pi} H$, takie że* $\ker \pi = \operatorname{im} i$.

Jak można się spodziewać, informacja że G jest rozszerzeniem grupy N za pośrednictwem grupy H nie wystarczy do zidentyfikowania typu izomorficznego grupy G.

5.3. Przykład. Niech G będzie rozszerzeniem $\mathbb{Z}_2 \to G \to \mathbb{Z}_2$. Wówczas grupa G może równie dobrze być izomorficzna z $\mathbb{Z}_4$, jak i z $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Definicja dopuszcza możliwości $N = 1$ i $N = G$. Rozszerzenia $G \xrightarrow{id} G \longrightarrow 1$ i $1 \longrightarrow G \xrightarrow{id} G$ są jednak mało interesujące.

Czasami podgrupa normalna jest położona w rozpatrywanej grupie w szczególnie dobry sposób, opisany w następującej definicji.

5.4. Definicja. *Niech $N \trianglelefteq G$. Podgrupę $D \leqslant G$ nazywamy* **dopełnieniem normalnym** *podgrupy N wtedy i tylko wtedy, gdy $N \cap D = 1$ i $N \cdot D = G$,*
gdzie $N \cdot D = \{ax : a \in N,\ x \in D\}$.

Grupę G nazywamy wówczas **produktem półprostym wewnętrznym** *podgrupy normalnej N i jej dopełnienia normalnego D.*

Produkt półprosty wewnętrzny ma ważną własność jednoznaczności przedstawienia elementu w postaci iloczynu. Jest to zresztą prawdą nawet w sytuacji nieco ogólniejszej, opisanej poniżej.

5.5. Stwierdzenie. *Jeżeli $H, K \leqslant G$, $H \cap K = 1$ i $ax = by,\ a, b \in H,\ x, y \in K$, to $a = b$ i $x = y$. Zatem $|HK| = |H| \cdot |K|$.*

Uwaga: Zauważmy, że zbiór HK to tylko podzbiór grupy G, a niekoniecznie podgrupa.

Dowód. $ax = by \Leftrightarrow b^{-1}a = yx^{-1}$. Skoro $b^{-1}a \in H$, a $yx^{-1} \in K$, to $b^{-1}a,\ yx^{-1} \in H \cap K = \mathbf{1}$, czyli $a = b$ i $x = y$. □

Odnotujmy jeszcze przydatny wniosek dla grup skończonych.

5.6. Wniosek. *Jeżeli $N \trianglelefteq G$, $D \leqslant G$, $N \cap D = 1$ i $|N| \cdot |D| = |G| < \infty$, to $ND = G$, czyli G jest produktem półprostym wewnętrznym N i D.*

Dowód. Na mocy Stwierdzenia 5.5 zbiór ND ma $|N| \cdot |D| = |G|$ elementów, czyli rzeczywiście $ND = G$. □

Zwróćmy uwagę na to, że wbrew nazwie, dopełnienie normalne nie musi być podgrupą normalną. Jeżeli jednak *jest* podgrupą normalną, to jest to sytuacja już nam znana:

5.7. Definicja. *Jeżeli $M, N \trianglelefteq G$, $N \cap M = 1$ i $N \cdot M = G$, to grupę G nazywamy* **produktem prostym wewnętrznym** *podgrup N i M.*

Pojęcie produktu prostego wewnętrznego jest bardzo zbliżone do pojęcia produktu grup, zdefiniowanego w rozdziale 1.

5.8. Twierdzenie. *Jeżeli grupa G jest produktem prostym wewnętrznym podgrup $M, N \trianglelefteq G$, to G jest izomorficzna z produktem $M \times N$. Odwzorowanie $f : M \times N \to G$ zadane wzorem $f(m, n) = mn$ jest izomorfizmem.*

Dowód. Zaczniemy od wykazania, że $\forall_{x \in M} \forall_{y \in N}\ xy = yx$. Oczywiście $xy = yx \Leftrightarrow xyx^{-1}y^{-1} = 1$. Zauważmy, że

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1}.$$

Ale $xyx^{-1} \in N$, bo N jest podgrupą normalną. Również $y^{-1} \in N$. Zatem

$$xyx^{-1}y^{-1} \in N. \tag{1}$$

Analogicznie, wykorzystując normalność M, pokazujemy, że

$$xyx^{-1}y^{-1} \in M. \tag{2}$$

Zestawiając fakty (1) i (2) wnioskujemy, że $xyx^{-1}y^{-1} \in M \cap N = \mathbf{1}$, czyli $xyx^{-1}y^{-1} = 1$, a więc istotnie $xy = yx$. Teraz już łatwo sprawdzić, że
$f((m_1, n_1)(m_2, n_2)) = f(m_1m_2, n_1n_2) = m_1m_2n_1n_2 = (m_1n_1)(m_2n_2) = f(m_1, n_1)f(m_2, n_2)$, co dowodzi, że f jest homomorfizmem. Zatem jest też izomorfizmem, bo oczywiście jest bijekcją (różnowartościowość wynika ze Stwierdzenia 5.5). □

Zauważmy, że dla grup skończonych mamy następujące użyteczne kryterium:

5.9. Wniosek. *Jeżeli $N \trianglelefteq G$, $D \trianglelefteq G$, $N \cap D = 1$ i $|N| \cdot |D| = |G| < \infty$, to G jest produktem prostym wewnętrznym N i D.*

Wróćmy do sytuacji ogólniejszej. Pokażemy, że jeżeli $N \trianglelefteq G$ i $D \leqslant G$, to zbiór ND *jest* podgrupą grupy G (patrz też zadanie 4.3). Przypomnijmy następujące oznaczenie: φ_x jest automorfizmem wewnętrznym grupy G zadany wzorem $\varphi_x(a) = xax^{-1}$.

5.10. Stwierdzenie. *Jeżeli $N \trianglelefteq G$ i $D \leqslant G$, to zbiór ND jest podgrupą grupy G. W szczególności*

$$\checkmark \qquad ax \cdot by = a\varphi_x(b) \cdot xy,$$

$$\checkmark\checkmark \qquad (a \cdot x)^{-1} = \varphi_{x^{-1}}(a^{-1}) \cdot x^{-1}.$$

Dowód. Mamy dowieść, że zbiór ND jest zamknięty ze względu na działania grupowe. Oczywiście wystarczy udowodnić prawdziwość wzorów ✓ i ✓✓. W tym celu wykonujemy następujące rachunki.

$$ax \cdot by = axb(x^{-1}x)y = a(xbx^{-1})xy = a\varphi_x(b) \cdot xy,$$

$$(a \cdot x)^{-1} = x^{-1}a^{-1} = x^{-1}a^{-1}(xx^{-1}) = (x^{-1}a^{-1}x)x^{-1} = \varphi_{x^{-1}}(a^{-1}) \cdot x^{-1}. \qquad \square$$

Z powyższych wzorów natychmiast wynika następujący wniosek.

5.11. Wniosek. *Jeżeli grupa G jest produktem półprostym podgrup $N \trianglelefteq G$ i $D \leqslant G$, to odwzorowanie $p : G \longrightarrow D$ zadane wzorem $p(ax) = x$ jest epimorfizmem grupy G na grupę D. Oczywiście* $\ker f = N$. *Tak więc produkt półprosty jest szczególnym przypadkiem rozszerzenia: $N \hookrightarrow G \xrightarrow{p} D$*

Opiszemy teraz bardzo użyteczną konstrukcję produktu półprostego zewnętrznego.

5.12. Definicja. *Niech N i D będą grupami, a $\varphi : D \longrightarrow Aut(N)$ homomorfizmem. Wówczas na iloczynie kartezjańskim $N \times D$ można określić strukturę grupy, definiując działania w następujący sposób.*

$$1 = (1_N, 1_D)$$

$$\underline{\checkmark} \qquad (a, x)(b, y) = (a\varphi_x(b), xy)$$

$$\underline{\checkmark}\,\underline{\checkmark} \qquad (a, x)^{-1} = (\varphi_{x^{-1}}(a^{-1}), x^{-1}).$$

Tak skonstruowaną grupę nazywamy **produktem półprostym** *grup N i D i oznaczamy $N \rtimes_\varphi D$ lub po prostu $N \rtimes D$.*

5.13. Uwaga. *Jeżeli $\varphi : D \longrightarrow Aut(N)$ jest homorfizmem trywialnym, to zdefiniowane działania są identyczne z działaniami*

$$(a, x)(b, y) = (ab, xy)$$

$$(a, x)^{-1} = (a^{-1}, x^{-1}),$$

czyli produkt półprosty jest w tej sytuacji tożsamy z produktem prostym.

5.14. Uwaga. *W produkcie półprostym $N \rtimes D$ są spełnione równości*

$$\begin{gathered}(a,1)(b,1) = (ab,1)\\ (1,x)(1,y) = (1,xy)\\ (1,x)(a,1)(1,x)^{-1} = (\varphi_x(a),1)\\ (a,1)(1,x) = (a,x)\end{gathered} \tag{3}$$

Oznacza to, że elementy postaci $(a,1)$ stanowią podgrupę normalną $\bar{N}$ izomorficzną z grupą N, elementy postaci $(1,x)$ stanowią podgrupę $\bar{D}$ izomorficzną z grupą D, a cała grupa $N \rtimes D$ jest produktem półprostym wewnętrznym podgrup $\bar{N}$ i $\bar{D}$.

Podobnie jak w przypadku produktu, pojęcie produktu półprostego wewnętrznego jest bardzo zbliżone do pojęcia produktu półprostego grup.

5.15. Twierdzenie. *Jeżeli grupa G jest produktem półprostym wewnętrznym podgrup $N \trianglelefteq G$ i $D \leqslant G$, to G jest izomorficzna z produktem półprostym $N \rtimes_\varphi D$, gdzie $\varphi : D \longrightarrow Aut(N)$ jest zadane wzorem $\varphi_x(a) = axa^{-1}$. Odwzorowanie $f : N \rtimes_\varphi D \to G$ zadane wzorem $f(a,x) = ax$ jest izomorfizmem.*

Dowód. Łatwo sprawdzić, że

$$f((a,x)(b,y)) = f(a\varphi_x(b), xy) = a\varphi_x(b)xy = axbx^{-1}xy = axby = f(a,x)f(b,y),$$

co dowodzi, że f jest homomorfizmem. Zatem f jest izomorfizmem, bo oczywiście jest bijekcją (różnowartościowość wynika ze Stwierdzenia 5.5). □

5.16. Przykłady.

1) Grupa $O(n)$ jest produktem półprostym wewnętrznym $SO(n) \trianglelefteq O(n)$ i $\mathbb{Z}_2$. Dla nieparzystej liczby n jest to produkt prosty (bo wówczas $-I \notin SO(n)$, a przy tym $-I \in Z(O(n))$).
2) Grupa $Aff(n)$ izomorfizmów afinicznych przestrzeni $\mathbb{R}^n$ jest produktem półprostym wewnętrznym grupy przesunięć przestrzeni $\mathbb{R}^n$ i grupy $GL(n,\mathbb{R}^n)$.
3) Grupa $Iso(n)$ izometrii przestrzeni $\mathbb{R}^n$ (wyposażonej w iloczyn skalarny) jest produktem półprostym wewnętrznym grupy przesunięć $\mathbb{R}^n$ i $O(n)$.
4) Grupa permutacji Σ_n jest produktem półprostym wewnętrznym grupy A_n i grupy $\mathbb{Z}_2$.

W powyższych przykładach obserwowaliśmy istnienie struktury produktu półprostego w znanych nam skądinąd grupach. Dzięki produktowi półprostemu możemy także konstruować różne *nowe* przykłady grup — jeżeli mamy jakąś wiedzę na temat automorfizmów znanych już grup. Dlatego najpierw udowodnimy następujące stwierdzenie.

5.17. Stwierdzenie. *Jeżeli p jest liczbą pierwszą, to $Aut(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.*

Dowód. Łatwo się przekonać, że każdy automorfizm f grupy $\mathbb{Z}_p = \{e, \gamma, \gamma^2, \ldots, \gamma^{p-1}\}$ jest postaci

$$f(x) = x^s,$$

gdzie $s = 1, 2, \ldots, p-1$. Oznaczmy taki automorfizm symbolem φ_s. Łatwo zauważyć, że $\varphi_s \circ \varphi_r = \varphi_{sr(modp)}$. Z tego natychmiast widać, że $Aut(\mathbb{Z}_p)$ jest izomorficzna z grupą niezerowych reszt z dzielenia przez p z mnożeniem modulo p jako działaniem dwuargumentowym. Ale to jest po prostu grupa multiplikatywna ciała F_p. W ciele F_p jest nie więcej niż k elementów x spełniających równanie $x^k = 1$ (bo wielomian stopnia k nie może mieć więcej niż k pierwiastków). Elementy dowolnej podgrupy rzędu k grupy multiplikatywnej ciała F_p spełniają powyższe równanie, a zatem o ile istnieje podgrupa rzędu k, to tylko jedna. Z Uwagi 2.18 wynika zatem, że grupa $Aut(\mathbb{Z}_p)$ jest cykliczna. □

5.18. Stwierdzenie. *Jeżeli p jest liczbą pierwszą i $(q, p-1) > 1$, to istnieje nieprzemienna grupa rzędu $p \cdot q$.*

Oczywiście istnieje nietrywialny homomorfizm $\varphi : \mathbb{Z}_q \longrightarrow Aut(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$. Wobec tego produkt półprosty $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ jest grupą nieprzemienną, na mocy poniższego lematu.

5.19. Lemat. *Produkt półprosty $N \rtimes_\varphi D$ jest grupą przemienną wtedy i tylko wtedy, gdy grupy N i D są przemienne, a homomorfizm φ jest trywialny.*

Dowód. $\Rightarrow$ Wiemy, że grupa $N \rtimes_\varphi D$ zawiera podgrupę izomorficzną z N i podgrupę izomorficzną z D. Skoro więc grupa $N \rtimes_\varphi D$ jest przemienna, to N i D muszą być przemienne. Pozostaje pokazanie, że φ jest homomorfizmem trywialnym. Załóżmy, że nie. Oznacza to, że $\exists_{x \in D} \exists_{a \in N}\ \varphi_x(a) \neq a$. Wówczas $(1, x)(a, 1)(1, x)^{-1} = (\varphi_x(a), 1) \neq (a, 1)$, co przeczy założeniu o przemienności grupy $N \rtimes_\varphi D$.
$\Leftarrow$ Skoro φ jest homomorfizmem trywialnym, to zgodnie z Uwagą 5.13 mamy do czynienia z produktem prostym, a produkt prosty grup przemiennych jest grupą przemienną. □

Zilustrujemy to dokładniej na bardziej konkretnym przykładzie.

5.20. Przykład. Istnieje nieprzemienna grupa rzędu 21 :
Niech $\mathbb{Z}_7 = \langle\, \alpha \,\rangle$, $\mathbb{Z}_3 = \langle\, \beta \,\rangle$.
Rozpatrzmy homomorfizm $\varphi : \mathbb{Z}_3 \longrightarrow Aut(\mathbb{Z}_7)$ zadany wzorami $\varphi_\beta(x) = x^2$, $\varphi_{\beta^2}(x) = x^4$ i oczywiście $\varphi_1 = id$. Łatwo sprawdzić, że jest to rzeczywiście homomorfizm. Na przykład $\varphi_{\beta^2} = \varphi_\beta \circ \varphi_\beta$, bo $\varphi_\beta(\varphi_\beta(x)) = \varphi_\beta(x^2) = (x^2)^2 = x^4 = \varphi_{\beta^2}(x)$. Homomorfizm φ można też opisać jednym wzorem:

$$\varphi_{_{\beta^j}}(\alpha^k) = \alpha^{2^j k}$$

Niech $a = (\alpha, 1)$, $b = (1, \beta)$. Wówczas w grupie $\mathbb{Z}_7 \rtimes_\varphi \mathbb{Z}_3$ zachodzą następujące równości (przyładowe).
Przede wszystkim, zgodnie ze wzorem (3) w Uwadze 5.14 mamy

$$b^j a^k b^{-j} = a^{2^j k}$$

Stąd konkretne wyliczenia:
$abab = a(bab^{-1})(bb) = aa^2b^2 = a^3b^2$,
$a^4b^2a^2b = a^4(b^2a^2b^{-2})(b^2b) = a^4a^8b^3 = a^{12}b^3 = a^5$.
I ogólnie:

$$a^i b^j a^k b^l = a^i(b^j a^k b^{-j})(b^j b^l) = a^i a^{2^j k} b^{j+l} = a^{i+2^j k} b^{j+l}.$$

$$(a^i b^j)^{-1} = a^{2^{-j}(-i)} b^{-j}$$

5.21. Przykład. Istnieje nieprzemienna grupa rzędu 27.
Łatwo sprawdzić, że odwzorowanie $f : \mathbb{Z}_3 \times \mathbb{Z}_3 \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_3$ zadane wzorem $f(x, y) = (x, xy)$ jest automorfizmem grupy $\mathbb{Z}_3 \times \mathbb{Z}_3$. Jest to oczywiście automorfizm nietrywialny. $f \circ f(x, y) = (x, x^2y)$, a $f \circ f \circ f(x, y) = f(f \circ f(x, y)) = f(x, x^2y) = (x, x^3y) = (x, y)$, czyli $f \circ f \circ f = id$. Zatem f jest elementem stopnia 3 w $Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$. W takim razie istnieje nietrywialny homomorfizm
$\varphi : \mathbb{Z}_3 \longrightarrow \langle f \rangle \leqslant Aut(\mathbb{Z}_3 \times \mathbb{Z}_3)$, taki że $\varphi_\gamma = f$ (gdzie γ jest generatorem $\mathbb{Z}_3$). Wynika stąd, że grupa G zdefiniowana jako produkt półprosty $G = (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\varphi \mathbb{Z}_3$ jest grupą nieprzemienną. Grupa ta ma następującą interesującą własność: $\forall_{g \in G}\ g^3 = 1$. Przypomnijmy, że jeżeli w grupie G jest spełniony warunek $\forall_{g \in G}\ g^2 = 1$, to grupa G jest przemienna.
5.22. Przykład. Jeżeli p jest liczbą pierwszą, to istnieje grupa nieprzemienna rzędu p^3.
Wiemy, że $|Aut(\mathbb{Z}_p \times \mathbb{Z}_p)| = (p^2 - 1)(p^2 - p)$. Liczba ta jest podzielna przez p, zatem na mocy Twierdzenia Cauchy'ego w grupie $Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$ istnieje element rzędu p. Skoro tak, to istnieje nietrywialny homomorfizm $\varphi : \mathbb{Z}_p \longrightarrow Aut(\mathbb{Z}_p \times \mathbb{Z}_p)$. Wobec tego produkt półprosty $(\mathbb{Z}_p \times \mathbb{Z}_p) \rtimes_\varphi \mathbb{Z}_p$ jest nieprzemienny.

ZADANIA

Z 5.1. Pokazać, że A_4 jest produktem półprostym wewnętrznym podgrupy normalnej izomorficznej z $\mathbb{Z}_2 \times \mathbb{Z}_2$ i jej dopełnienia normalnego izomorficznego z $\mathbb{Z}_3$.
Z 5.2. Niech $n > 3$. Udowodnić, że jeżeli $n = 2m$ i m jest liczbą nieparzystą to $D_{2n} \cong D_n \times \mathbb{Z}_2$. Pokazać, że we wszystkich pozostałych przypadkach D_{2n} nie jest izomorficzne z produktem swoich podgrup właściwych.
Z 5.3. Podać przykład grupy G i jej podgrup $K \trianglelefteq G$, $H \trianglelefteq G$ takich, że $K \cong H$ ale $G/K \ncong G/H$.
Z 5.4. Podać przykład grupy G i jej podgrup $K \trianglelefteq G$, $H \trianglelefteq G$ takich, że $G/K \cong G/H$ ale $K \ncong H$.
Z 5.5. Pokazać, że jeżeli $H \trianglelefteq G$ ma w G dokładnie jedno dopełnienie normalne, to H jest składnikiem prostym w G. Podać przykład $H \trianglelefteq G$ będącego składnikiem prostym i posiadającego więcej niż jedno dopełnienie normalne.

Definicja. *Grupę G nazywamy grupą metacykliczną jeżeli posiada cykliczną podgrupę normalną L, taką że G/L jest cykliczna.*

Z 5.6. Podać przykład grupy metacyklicznej, która nie jest cykliczna. Udowodnić, że każda podgrupa i każda grupa ilorazowa grupy metacyklicznej jest metacykliczna
⋆ Z 5.7. Podać przykład nietrywialnej grupy doskonałej, która nie jest grupą prostą.
Z 5.8. Wskazać cztery nie izomorficzne produkty półproste $\mathbb{Z}_7 \rtimes \mathbb{Z}_6$.
Z 5.9. Jeżeli $H, K \in G$ są podgrupami skończonego indeksu w grupie G i $([G : H], [G : K]) = 1$, to $HK = G$.

TEST

♡ T 5.1. Jeżeli N i H są grupami skończenie generowanymi, a $N \to G \to H$ jest rozszerzeniem, to G jest grupą skończenie generowaną.
T 5.2. Istnieje grupa przemienna G, taka że grupa $|Aut(G)| = 15$.
T 5.3. $Aut(\mathbb{Z}_n)$ jest grupą przemienną.
T 5.4. Istnieje taka grupa skończona G, że $G/Z(G) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.
T 5.5. Istnieje taka grupa skończona G, że $G/Z(G) \cong D_{10}$.
T 5.6. Istnieje taka grupa skończona G, że $|G/Z(G)| = 35$.
T 5.7. Produkt grup prostych jest grupą prostą.
T 5.8. Produkt grup doskonałych jest grupą doskonałą.
T 5.9. $D_8 \cong D_4 \times \mathbb{Z}_2$.
T 5.10. $D_{36} \cong D_{18} \times \mathbb{Z}_2$.
T 5.11. Jeżeli $H, K \leqslant G$ i $HK = G$, to co najmniej jedna z grup H i K jest podgrupą normalną.
T 5.12. Jeżeli $H, K \leqslant G$ i każdy element g w grupie G ma jednoznaczne przedstawienie w postaci $g = xy,\ x \in H,\ y \in K$, to co najmniej jedna z grup H i K jest podgrupą normalną.
T 5.13. Jeżeli $H, K \leq G$, $H \cap K = 1$ i $HK = G$, to co najmniej jedna z podgrup H, K jest podgrupą normalną w G.
T 5.14. Jeżeli H jest grupą prostą nieprzemienną, to istnieje grupa $G \ncong H$ taka że $G/Z(G) \cong H$.
T 5.15. Jeżeli G jest grupą skończoną, to $G/Z(G)$ jest grupą prostą.
T 5.16. $\mathbb{Z}_{10} \times \mathbb{Z}_{15} \cong \mathbb{Z}_{150}$.
T 5.17. Niech p będzie liczbą pierwszą. Jeżeli $N \trianglelefteq G$ i $[G : N] = p,\ (p, |N|) = 1$, to w grupie G istnieje dopełnienie normalne podgrupy N.

6. p–grupy. Twierdzenie Sylowa

6.1. Definicja. *Niech p będzie liczbą pierwszą. Grupę, której rząd jest równy p^n nazywamy* p**–grupą**.

6.2. Uwaga. Nie będziemy już powtarzać założenia, że p jest liczbą pierwszą. Zawsze wtedy, gdy jest mowa o p–grupie, założenie takie jest automatycznie przyjmowane.

6.3. Uwaga. Sformułowanie p–grupa będziemy czasem rozumieć w następujący sposób: *grupa, której rząd jest potęgą jakiejś liczby pierwszej.* Znak p nie musi więc koniecznie wskazywać o jaką konkretnie liczbę pierwszą chodzi. Potrzeba taka powstaje niekiedy, gdy musimy rozpatrywać różne liczby pierwsze jednocześnie.

Przypominamy kilka już dowiedzionych faktów:
1. Nietrywialna p–grupa ma nietrywialne centrum.
2. Każda grupa rzędu p^2 jest przemienna.
3. Istnieje grupa nieprzemienna rzędu p^3.

Z nietrywialności centrum p–grupy wynikają następujące mocne twierdzenia o p-grupach.

6.4. Twierdzenie. *Jeżeli G jest p-grupą i $|G| = p^m$, to istnieje ciąg podgrup*

$$\mathbf{1} = G_0 \leqslant G_1 \leqslant \cdots \leqslant G_{m-1} \leqslant G_m = G,$$

taki że $G_i \trianglelefteq G$ i $|G_i| = p^i$.

Dowód. Zastosujemy indukcję ze względu na m. Teza jest oczywista dla $m = 0$. Załóżmy, że teza jest prawdziwa dla $m-1$, gdzie $m > 0$. Niech z będzie nietrywialnym elementem rzędu p w centrum grupy G (istnienie takiego elementu wynika z nietrywialności $Z(G)$ i z twierdzenia Cauchy'ego (3.11)). Niech $G_1 = \langle z \rangle$. Oczywiście $G_1 \trianglelefteq G$, bo $G_1 \leqslant Z(G)$. Grupa G/G_1 jest rzędu p^{m-1}, zatem na mocy założenia indukcyjnego istnieje ciąg podgrup normalnych $H_0 \leqslant H_1 \leqslant \cdots \leqslant H_{m-2} \leqslant H_{m-1} = G/G_1$. Przyjmując $G_0 = \mathbf{1}$, a dla $i \geq 1$, $G_i = \pi^{-1}(H_{i-1})$, gdzie $\pi : G \longrightarrow G/G_1$, otrzymujemy szukany ciąg podgrup grupy G. □

6.5. Twierdzenie. *Jeżeli G jest p–grupą i $[G : H] = p$, to $H \trianglelefteq G$.*

Dowód. Stosujemy podobne rozumowanie indukcyjne, jak w dowodzie poprzedniego twierdzenia. W centrum grupy G wybieramy element z rzędu p i jak poprzednio mamy $\langle z \rangle \trianglelefteq G$.
Jeżeli $z \in H$, to $H/\langle z \rangle \leqslant G/\langle z \rangle$ jest podgrupą indeksu p, a więc z założenia indukcyjnego normalną w $G/\langle z \rangle$. Zatem H jest podgrupą normalną w G, jako przeciwobraz podgrupy normalnej.
Jeżeli natomiast $z \notin H$, to zauważamy, że $H \leqslant N_G(H)$, $z \in N_G(H)$, zatem $\langle H \cup \{z\} \rangle \leqslant N_G(H)$. Ale $G = \langle H \cup \{z\} \rangle \leqslant N_G(H)$. Zatem $N_G(H) = G$, czyli $H \trianglelefteq G$. □

Twierdzenie Sylowa

Udowodnimy 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.

6.6. 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 $|H| = p^k$.*

6.7. 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 $s_p \,|\, r$ i $s_p \equiv 1 \pmod p$.

Dowód.

a) Niech $\mathcal{P}$ będzie rodziną wszystkich p^k–elementowych podzbiorów grupy G. Na rodzinie $\mathcal{P}$ określamy działanie grupy G przez domnażanie z lewej strony, to znaczy dla $X \in \mathcal{P}$ (czyli dla p^k–elementowego podzbioru grupy G) $g(X) = \{g \cdot x : x \in X\}$. Pokażemy, że istnieje w rodzinie $\mathcal{P}$ taki element X, którego podgrupa izotropii ma p^k elementów, czyli jest szukaną p–podgrupą Sylowa .
Moc rodziny $\mathcal{P}$ wynosi $\binom{n}{p^k}$, co nie jest podzielne przez p. Istnieje więc orbita, której liczba elementów nie jest podzielna przez p. Okazuje się, że za X wystarczy przyjąć dowolny element tej orbity. Niech mianowicie X należy do rozpatrywanej orbity i niech $H = G_X \leqslant G$ będzie jego grupą izotropii. Liczba elementów w rozpatrywanej orbicie jest równa $[G : H]$, a ponieważ moc orbity nie jest podzielna przez p, to i liczba $[G : H] = \frac{|G|}{|H|}$ nie jest podzielna przez p. W takim razie $p^k \,\big|\, |H|$. Mogłoby się jeszcze zdarzyć, że $|H| > p^k$. Wykluczamy tę ewentualność w następujący sposób: Niech $x_0 \in X$. Jeżeli $G_X = H$, to w szczególności $\forall_{h \in H}\ hx_0 \in X$. Jednak elementy postaci $hx_0 \in X$ są parami różne, więc $|H| \leq |X| = p^k$.
Mamy zatem $p^k \,\big|\, |H|$ i $|H| \leq p^k$ czyli $|H| = p^k$.

b) Niech H będzie p–podgrupą Sylowa w G, a $K \leqslant G$, $|K| = p^l$ pewną p–podgrupą. Rozważmy działanie K na zbiorze warstw lewostronnych G/H przez domnażanie z lewej strony. Podgrupa K jest p–grupą, zatem na mocy Wniosku 3.10

$$|(G/H)^K| \equiv |G/H| \pmod p.$$

Ponadto $|G/H| = [G : H] = r$, $(p, r) = 1$, więc istnieje warstwa gH będąca punktem stałym rozpatrywanego działania. Oznacza to, że dla każdego elementu $k \in K$, $kgH = gH$, czyli dla każdego elementu $k \in K$, $g^{-1}kg \in H$. Zatem $g^{-1}Kg \leqslant H$ lub równoważnie $K \leqslant gHg^{-1}$. Oczywiście gHg^{-1} też jest p–podgrupą Sylowa.

c) Wynika natychmiast z b).

d) Rozpatrzmy działanie grupy G na s_p– elementowym zbiorze p–podgrup Sylowa, wyznaczone przez automorfizmy wewnętrzne. Z punktu b) wynika, że jest ono tranzytywne. Niech H będzie jedną z podgrup Sylowa — jej grupą izotropii jest $N_G(H)$, a jej orbitą zbiór wszystkich p–podgrup Sylowa. Zatem $s_p = [G : N_G(H)]$ i $s_p \mid r$ (bo $H \leqslant N_G(H) \leqslant G$, a $[G : H] = r$).
Ograniczmy teraz rozpatrywane działanie (na s_p–elementowym zbiorze p–podgrup Sylowa) do ustalonej p–podgrupy Sylowa H. Podgrupa H jest oczywiście punktem stałym tego działania. Pokażemy, że jest to jedyny punkt stały. Z tego będzie już łatwo wywnioskować, że $s_p \equiv 1 \pmod p$ — wystarczy skorzystać z Wniosku 3.10.

Pozostaje dowieść, że H jest jedynym punktem stałym. Załóżmy, że podgrupa Sylowa K jest także punktem stałym. Chcemy udowodnić, że

$$H = K.$$

Skoro K jest punktem stałym rozpatrywanego działania, to $H \leqslant N_G(K)$. Wówczas K i H są p–podgrupami Sylowa grupy $N_G(K)$ i zgodnie z punktem c) są w niej sprzężone — istnieje element $g \in N_G(K)$, taki że $gKg^{-1} = H$. Ale $gKg^{-1} = K$, więc istotnie $K = H$. □

Odnotujmy oczywisty, ale bardzo przydatny, wniosek z twierdzenia Sylowa.

6.8. Wniosek. *Niech $H \leqslant G$ będzie p–podgrupą Sylowa w G. Podgrupa H jest normalna wtedy i tylko wtedy, gdy jest jedyną p–podgrupą Sylowa grupy G.*

Z twierdzenia Sylowa i Twierdzenia 6.4 wynika także natychmiast:

6.9. Wniosek. *Jeżeli p jest liczbą pierwszą i $p^k \,\big|\, |G|$, to w G istnieje podgrupa rzędu p^k.*

Zastosowania twierdzenia Sylowa

6.10. Stwierdzenie. *Jeżeli p i q są liczbami pierwszymi, $(p-1, q) = 1$ i $|G| = pq$, to q–podgrupa Sylowa grupy G jest normalna.*

Dowód. Wiemy, że $s_q \,|\, p$, czyli $s_q = 1$ lub $s_q = p$. Ale mamy także warunek $s_q \equiv 1 \pmod{q}$ (równoważnie: $q \,|\, s_q - 1$), którego nie spełnia liczba p. Pozostaje tylko możliwość $s_q = 1$. W takim razie q–podgrupa Sylowa jest normalna. □

6.11. Wniosek. *Jeżeli p i q są różnymi liczbami pierwszymi i $|G| = pq$, $(p-1, q) = (p, q-1) = 1$, to $G \cong \mathbb{Z}_{pq}$.*

Dowód. Na mocy Stwierdzenia 6.10 zarówno p–podgrupa jak i q–podgrupa Sylowa są normalne. Są one ponadto izomorficzne, odpowiednio, z $\mathbb{Z}_p$ i $\mathbb{Z}_q$, a ich część wspólna jest podgrupą trywialną (bo $p \neq q$). Zatem $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. □

6.12. Stwierdzenie. *Jeżeli p i q są różnymi liczbami pierwszymi i $|G| = p^2 q$, to p–podgrupa lub q–podgrupa Sylowa grupy G jest normalna.*

Dowód (nie wprost). Przypuśćmy, że $s_p > 1$ i $s_q > 1$. Wówczas $s_p = q$ i $p \mid (s_p - 1)$, a zatem $p \mid q - 1$, więc $q > p$.
Z kolei $s_q \mid p^2$, co wobec założenia $s_q > 1$ pozostawia możliwości $s_q = p$ i $s_q = p^2$. Jednak możliwość $s_q = p$ jest wykluczona przez obserwację, że $q > p$ i warunek z twierdzenia Sylowa $q \mid (s_q - 1)$. Pozostaje więc tylko możliwość $s_q = p^2$.
Dla dokończenia dowodu zastosujemy teraz charakterystyczny chwyt, tzw. zliczanie elementów. W grupie G mamy $p^2 \cdot (q-1)$ elementów rzędu q (bo q–podgrup Sylowa jest p^2 i są one izomorficzne z $\mathbb{Z}_q$ — a więc każde dwie mają w części wspólnej tylko element neutralny). Postaje p^2 elementów rzędu różnego od q, a zatem wszystkie one muszą wchodzić w skład p^2–elementowej p–podgrupy Sylowa. Wobec tego p–podgrupa Sylowa jest tylko jedna, wbrew założeniu, że $s_p, s_q > 1$. □

Uwaga. Można na pierwszy rzut oka odnieść wrażenie, że udowodniliśmy iż w grupie rzędu $p^2 q$ to właśnie p–podgrupa Sylowa musi być normalna. Tak jednak nie jest — samo założenie $s_p > 1$ nie wystarczało do dojścia do sprzeczności. Korzystaliśmy z obydwu części założenia $s_p, s_q > 1$. Na przykład grupa D_{20} jest rzędu $2^2 \cdot 5$, a 2–podgrupa Sylowa nie jest w niej normalna.

6.13. Stwierdzenie. *Jeżeli $|G| = pqr$, gdzie p, q, r są różnymi liczbami pierwszymi, to p–podgrupa lub q–podgrupa lub r–podgrupa Sylowa jest normalna.*

Dowód. Załóżmy, że $p > q > r$. Mamy

$$|G| = pqr \geq s_p(p-1) + s_q(q-1) + s_r(r-1) + 1.$$

Przypuśćmy, że żadna z rozpatrywanych podgrup Sylowa nie jest normalna. Mamy zatem $s_p > 1$, $s_q > 1$ i $s_r > 1$. Wykorzystując punkt 4) twierdzenia Sylowa (i założone uporządkowanie liczb p, q, r) wnioskujemy, że
$s_p = qr$,
$s_q = p$ lub $s_q = pr$, a więc w każdym razie $s_q \geq p$,
$s_r \geq q$.
Zatem $pqr \geq s_p(p-1)+s_q(q-1)+s_r(r-1)+1 \geq qr(p-1)+p(q-1)+q(r-1)+1 = pqr + (p-1)(q-1)$, czyli ostatecznie

$$pqr \geq pqr + (p-1)(q-1)$$

To oczywiście jest niemożliwe, zatem założenie $s_p, s_q, s_r > 1$ doprowadziło do sprzeczności. □

6.14. Wniosek. *Jeżeli p, q, r są różnymi liczbami pierwszymi i żadna z nich nie jest dzielnikiem żadnej innej pomniejszonej o 1 (tzn. $\neg(p \mid q-1)$, i.t.d.), to każda grupa rzędu pqr jest cykliczna.*

Dowód. Niech N, K, L będą (odpowiednio) p, q, r–podgrupami Sylowa (nie zakładamy żadnego ich uporządkowania). Wiemy, ze Stwierdzenia 6.13, że co najmniej jedna z tych podgrup jest normalna. Dla ustalenia uwagi załóżmy, że $N \trianglelefteq G$. Wówczas NK jest grupą rzędu pq. Na mocy Wniosku 6.11 grupa ta jest izomorficzna z $\mathbb{Z}_{pq}$. W szczególności, $NK \leqslant N_G(K)$, zatem $|N_G(K)| \geq pq$. Wobec tego $s_q \leq \frac{pqr}{pq} = r$. Pozostawia to już tylko dwie możliwości: $s_q = 1$ lub $s_q = r$. Ale $s_q = r$ jest wykluczone przez warunek z twierdzenia Sylowa: $q \mid s_q - 1$. Wobec tego $s_q = 1$, czyli $K \trianglelefteq G$. Analogicznie dowodzimy, że $L \trianglelefteq G$. Ustaliliśmy zatem, że $N, K, L \trianglelefteq G$. Oczywiście przecięcia każdych dwóch z tych podgrup są trywialne (bo rzędy są względnie pierwsze). Zatem $G \cong N \times K \times L \cong \mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r \cong \mathbb{Z}_{pqr}$. □

Jak pokazują powyższe przykłady, wiele algebraicznych własności grupy skończonej wynika wyłącznie z tego ile ta grupa ma elementów, a twierdzenie Sylowa jest bardzo pomocnym narzędziem w dowodzeniu tego typu stwierdzeń. Jest ono także przydatne przy rozstrzyganiu, czy grupa danego rzędu może być prosta. Przykład poprzedzimy użytecznymi uwagami o grupach prostych.

6.15. Uwaga. *Grupa Σ_4 nie zawiera podgrupy prostej nieprzemiennej.*

Dowód. Oczywiście sama grupa Σ_4 nie jest prosta. Jej podgrupy właściwe mogą być rzędu $1, 2, 3, 4, 6, 8, 12$. Nie wnikając w to jakie to są podgrupy (a nie jest to trudne) widzimy od razu, że Stwierdzenia 6.10 i 6.12 wykluczają prostotę grup rzędu 6 i 12. Grupy rzędu $1, 2, 3, 4, 8$ nie mogą być nieprzemiennymi grupami prostymi, bo są p–grupami. □

Zauważmy, że z powyższego łatwego faktu wynika ciekawe spostrzeżenie, że grupy proste nie mogą mieć "dużych" podgrup.

6.16. Wniosek. *Jeżeli G jest nieprzemienną grupą prostą, a $H \leqslant G$ podgrupą, to $|G:H| \geq 5$.*

Dowód. Homomorfizm, którego dziedzina jest grupą prostą, musi być albo monomorfizmem albo homomorfizmem trywialnym. Ale dobrze nam znany homomorfizm $\phi : G \longrightarrow \Sigma_{[G:H]}$ nie jest trywialny. Zatem $\phi(G)$ jest nieprzemienną prostą podgrupą w $\Sigma_{[G:H]}$. Wobec tego $[G:H] \geq 5$. □

I jeszcze jedna, podobna obserwacja:

6.17. Stwierdzenie. *Jeżeli nieprzemienna grupa G prosta zawiera podgrupę H, to $|G|$ jest dzielnikiem liczby $[G:H]!$.*

Dowód. Tak jak w poprzednim dowodzie stwierdzamy, że istnieje monomorfizm $\phi : G \longrightarrow \Sigma_{[G:H]}$. Wobec tego grupa $\Sigma_{[G:H]}$ zawiera podgrupę rzędu $|G|$, i teza wynika z twierdzenia Lagrange'a. □

6.18. Przykład. Nie istnieje grupa prosta rzędu 144.

Dowód. Przypuśćmy, że istnieje grupa prosta G rzędu $144 = 2^4 3^2$. Z założenia, że G jest grupą prostą wynika, że $s_3 \neq 1$. Twierdzenie Sylowa dopuszcza możliwości $s_3 = 4$, $s_3 = 16$. Możemy wykluczyć $s_3 = 4$, bo $s_3 = [G : N_G(H_3)]$, a jako grupa prosta, grupa G nie może mieć podgrupy indeksu 4 (Wniosek 6.16). Wobec tego $s_3 = 16$. Niech U i V będą dwiema różnymi 3–podgrupami Sylowa grupy G. Zbadamy, jaki może być rząd podgrupy $M = \langle U \cup V \rangle$. Z Twierdzenia Lagrange'a oraz zawierań $U < M \leqslant G$ wynika, że $|M| = 18, 36, 72$ lub 144. Wartości 36 i 72 musimy odrzucić, bo jako grupa prosta nieprzemienna G nie ma podgrup indeksu 2 ani 4. Wartość 18 również odrzucamy, bo z twierdzenia Sylowa łatwo wywnioskować, że w grupie rzędu 18 jest tylko jedna 3–podgrupa Sylowa (a w M co najmniej dwie). Zatem $M = G$. Zauważmy, że oczywiście $U \cap V \trianglelefteq M$, a nawet $U \cap V \leqslant Z(M)$, bo grupy U i V są przemienne. Zatem $U \cap V = 1$ — w przeciwnym razie $U \cap V$ byłoby nietrywialną podgrupą normalną w grupie prostej $M = G$. Wobec tego mamy 16 3–podgrup Sylowa i każde dwie mają trywialną część wspólną. W takim razie 3–podgrupy Sylowa zawierają łącznie $16 \cdot 8 = 128$ elementów nietrywialnych. Pozostaje 16 elementów i wszystkie one składają się na jedyną możliwą 2–podgrupę Sylowa. 2–podgrupa Sylowa jest więc normalna, wbrew założeniu o prostocie grupy G. □

ZADANIA

♡ Z 6.1. Niech G będzie p – grupą. Pokazać, że dowolna właściwa podgrupa $H \leqslant G$ jest właściwą podgrupą swojego normalizatora $N_G(H)$. Zauważyć, że z tego faktu natychmiast wynika Twierdzenie 6.5.

Z 6.2. Pokazać, że jeżeli G jest nieabelową grupą rzędu p^3 to $k(G) = p^2 + p - 1$, gdzie $k(G)$ oznacza liczbę klas sprzężoności elementów grupy G.

♡ Z 6.3. Pokazać, że jeżeli G jest p-grupą skończoną a $H \trianglelefteq G$ nietrywialnym dzielnikiem normalnym, to $H \cap Z(G) \neq \mathbf{1}$.

Z 6.4. Znaleźć podgrupy Sylowa w D_{2n}. Wyznaczyć ich liczbę.

Z 6.5. Znaleźć 2-podgrupę Sylowa w Σ_4. Udowodnić, że jest ona izomorficzna z D_8. Ile różnych 2-podgrup Sylowa zawiera Σ_4?

Z 6.6. Udowodnić, że każda grupa rzędu 85 jest cykliczna.

♡ Z 6.7. Niech G będzie grupą prostą rzędu 60.

a) znaleźć liczbę podgrup rzędu 5 i pokazać, że G ma 24 elementy rzędu 5.

b) wykazać, że G nie ma podgrupy rzędu 15.

c) wykazać, że G ma dokładnie 20 elementów rzędu 3.

⋆ Z 6.8. Udowodnić, że grupa prosta rzędu 60 jest izomorficzna z A_5.

Z 6.9. Udowodnić, że jeżeli $|G| = p^2q$, gdzie p, q są różnymi liczbami pierwszymi oraz $p^2 \not\equiv 1 \pmod{q}$ i $q \not\equiv 1 \pmod{p}$ to G jest grupą abelową.

Z 6.10. Udowodnić, że nie ma grupy prostej rzędu 56.

Z 6.11. Udowodnić, że nie ma grupy prostej rzędu 132.

Z 6.12. Udowodnić, że nie ma grupy prostej rzędu 300.

Z 6.13. Udowodnić, że nie ma grupy prostej rzędu 90.

Z 6.14. Udowodnić, że nie istnieje grupa prosta rzędu $351 = 27 \cdot 13$.

Z 6.15. Udowodnić, że nie istnieje grupa prosta rzędu $992 = 32 \cdot 31$.

♡ Z 6.16. Niech $n = p^m r$, gdzie m i r są liczbami naturalnymi, p jest liczbą pierwszą, $r > 1$, $\neg(p \mid r)$. Pokazać, że jeżeli istnieje grupa prosta rzędu $n = p^m r$, to $p^m \mid (r-1)!$. Wywnioskować, że dla $m \geq 4$ nie istnieje grupa prosta rzędu $2^m 5$.

Z 6.17. Udowodnić, że nie ma grupy prostej rzędu 80.

⋆ Z 6.18. Zbadać, czy każda grupa rzędu $17 \cdot 5 \cdot 7$ jest cykliczna.

Z 6.19. Załóżmy, że grupa G jest produktem prostym wewnętrznym swoich podgrup Sylowa. Udowodnić, że dowolna właściwa podgrupa $H \leqslant G$ jest właściwą podgrupą swojego normalizatora $N_G(H)$ (porównaj z zadaniem 6.1).

♡ Z 6.20. Niech G będzie grupą skończoną, a $H \leqslant G$ jej p–podgrupą Sylowa. Niech $K \trianglelefteq G$ będzie podgrupą normalną i niech $\pi : G \longrightarrow G/K$ będzie epimorfizmem na grupę ilorazową. Udowodnić, że

a) $H \cap K$ jest p–podgrupą Sylowa grupy K i każda p–podgrupa Sylowa grupy K jest postaci $H' \cap K$, gdzie H' jest pewną p–podgrupą Sylowa grupy G.

b) grupa $\pi(H)$ jest p–podgrupą Sylowa grupy ilorazowej G/K i każda p–podgrupa Sylowa grupy G/K jest postaci $\pi(H')$ gdzie H' jest p–podgrupą Sylowa grupy G.

TEST

T 6.1. Dla każdej nietrywialnej skończonej p–grupy G istnieje epimorfizm $G \longrightarrow \mathbb{Z}_p$.

♡ T 6.2. Jeżeli $H \trianglelefteq G$ jest normalną p–podgrupą, to H jest zawarte w każdej p–podgrupie Sylowa grupy G.

T 6.3. Niech $H \leqslant G$ będzie podgrupą Sylowa grupy skończonej G. Załóżmy, że istnieje podgrupa normalna $K \trianglelefteq G$, taka że $H \trianglelefteq K$. Wówczas $H \trianglelefteq G$ jest normalną podgrupą grupy G.

T 6.4. Istnieje tylko jedna (z dokładnością do izomorfizmu) grupa rzędu 55.

T 6.5. Jeżeli grupa G rzędu 55 ma podgrupę normalną rzędu 5, to G jest cykliczna.

T 6.6. Każda grupa rzędu $5^2 7^2$ jest przemienna.

T 6.7. Każda grupa rzędu $3^2 5^2$ jest przemienna.

T 6.8. Każda grupa rzędu 35 jest cykliczna.

T 6.9. Każda grupa rzędu 105 jest cykliczna.

T 6.10. Każda grupa rzędu $5 \cdot 7 \cdot 13$ jest cykliczna.

T 6.11. Jeżeli $G = K \times H$ i S jest p–podgrupą Sylowa grupy G, to S jest postaci $H_1 \times H_2$, gdzie H_1 i H_2 są podgrupami Sylowa odpowiednio podgrup K i H.

T 6.12. Jeżeli $G = K \times H$ i M jest podgrupą grupy G, to M jest postaci $H_1 \times H_2$, gdzie H_1 i H_2 są p–podgrupami odpowiednio podgrup K i H.

♡ T 6.13. Każde działanie grupy A_5 na zbiorze 7–elementowym ma punkt stały.

T 6.14. Część wspólna wszystkich 2–podgrup Sylowa grupy D_{2n}, $n \geq 3$ jest zawarta w podgrupie obrotów.

T 6.15. Każda grupa rzędu $3^2 \cdot 13$ ma nietrywialne centrum.

T 6.16. Każda grupa rzędu $3^2 \cdot 19$ ma nietrywialne centrum.

T 6.17. W grupie Σ_5, 2–podgrupa Sylowa jest izomorficzna z _____.

T 6.18. Część wspólna wszystkich 2–podgrup Sylowa grupy Σ_4 jest izomorficzna z _____.

T 6.19. Część wspólna wszystkich 2–podgrup Sylowa grupy Σ_5 jest izomorficzna z _____.

T 6.20. Część wspólna wszystkich p–podgrup Sylowa grupy prostej jest trywialna.

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, to znaczy nie jest izomorficzna z produktem swoich podgrup właściwych nietrywialnych. Każda podgrupa grupy $\mathbb{Z}$ jest postaci $m\mathbb{Z}$, gdzie $m \in \mathbb{N}\cup\{0\}$.*

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

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.

Naszym celem jest następujące twierdzenie, które rozstrzyga całkowicie problem klasyfikacji skończenie generowanych grup przemiennych.

7.3. 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 (★).

Zaczniemy od udowodnienia jednoznaczności zapisu (★). Dowód rozbijemy na kilka prostych kroków. Najpierw pokażemy, 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.

7.4. 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

✓ $$S(G_1) \cong S(G_2),$$

✓✓ $$G_1/S(G_1) \cong G_2/S(G_2).$$

Stąd natychmiast wynika, że

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

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

□

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

7.5. 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 redukujemy do sytuacji, gdy rzędy rozpatrywanych p–grup są potęgami *jednej* ustalonej liczby pierwszej p. Jest to możliwe dzięki następującemu wnioskowi z twierdzenia Sylowa.

7.6. Wniosek z twierdzenia Sylowa. *Skończona grupa przemienna jest izomorficzna z produktem swoich podgrup Sylowa. Zatem dwie grupy skończone przemienne są izomorficzne wtedy i tylko wtedy, gdy izomorficzne są ich podgrupy Sylowa.*

□

Dla zakończenia dowodu jednoznaczności zapisu (★) pozostaje pogrupować w rozpatrywanym zapisie czynniki odpowiadające poszczególnym liczbom pierwszym i rozpatrywać je osobno. Sprowadza się to do rozpatrzenia przypadku, gdy w zapisie tym występują tylko skończone p–grupy cykliczne, przy ustalonej liczbie pierwszej p.

7.7. Twierdzenie. *Jeżeli p jest liczbą pierwszą, to grupy*

$$G_1 = \prod_{i=1}^{n} \left(\mathbb{Z}_{p^i}\right)^{w_i} \quad oraz \quad G_2 = \prod_{i=1}^{n} \left(\mathbb{Z}_{p^i}\right)^{v_i}$$

są izomorficzne wtedy i tylko wtedy, gdy

$$\forall_{1 \leq i \leq n}\ w_i = v_i$$

Uwaga: w tym zapisie, dla uproszczenia, dopuszczamy zerowe wykładniki, by mieć tę samą indeksację obydwu produktów.

Dowód.
$\Leftarrow$ Przy jednakowych wykładnikach grupy G_1 i G_2 są po prostu identyczne.
$\Rightarrow$ Dowód indukcyjny ze względu na n.
Dla $n = 1$ teza jest oczywiście prawdziwa.
Załóżmy, że jest prawdziwa dla $n-1$, wykażemy że jest prawdziwa dla n. Niech $P(G) = \{x \in G : px = 0\}$. Łatwo sprawdzić, że jeżeli $G_1 \cong G_2$, to $G_1/P(G_1) \cong G_2/P(G_2)$ i $P(G_1) \cong P(G_2)$.
Ale $G_1/P(G_1) \cong \prod_{i=1}^{n-1} \left(\mathbb{Z}_{p^i}\right)^{w_{i+1}}$ i $G_2/P(G_2) \cong \prod_{i=1}^{n-1} \left(\mathbb{Z}_{p^i}\right)^{v_{i+1}}$. Na mocy zasady indukcji izomorficzność tych dwóch grup oznacza, że $w_2 = v_2, \ldots, w_n = v_n$. Pozostaje pokazać, że $w_1 = v_1$. W tym celu zauważmy, że $|P(G_1)| = p^s$, gdzie $s = \sum_{i=1}^{n} w_i$ i analogicznie $|P(G_2)| = p^t$, gdzie $t = \sum_{i=1}^{n} v_i$. Skoro więc $P(G_1) \cong P(G_2)$, to te dwie sumy muszą być równe. Mamy więc $w_1 = v_1$, bo już stwierdziliśmy, że wyrazy o wyższych numerach są, odpowiednio, takie same. □
Kończy to dowód *jednoznaczności zapisu w postaci* (★).

Przechodzimy do dowodu *możliwości przedstawienia grupy w postaci* (★).
Zauważmy, że na mocy Twierdzenia 7.2 wystarczy udowodnić, że prawdziwe jest następujące twierdzenie.

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

Dowód Twierdzenia 7.8 poprzedzimy dłuższymi przygotowaniami.

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

Dowód. Zastosujemy indukcję ze względu na n.
Dla $n = 1$ podgrupa H musi być cykliczna (a więc skończenie generowana).
Przypuśćmy, że teza jest prawdziwa dla $n - 1$.
Niech $H \leqslant \mathbb{Z}^n$.
Niech $N = (\mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbf{0}) \cap H$. Na mocy założenia indukcyjnego grupa N jest skończenie generowana. Oczywiście $N \trianglelefteq H$ i $K = H/N$ jest grupą cykliczną. W takim razie H jest rozszerzeniem postaci $N \to H \to K$, gdzie N i K są grupami skończenie generowanymi. Zatem H jest grupą skończenie generowaną (por. zadania Z.4.10 i T.5.1). □

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).

7.10. 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. □

Zauważmy, że układu generatorów o tak dobrych własnościach nie da się znaleźć już na przykład w nietrywialnej skończonej grupie cyklicznej. Z Twierdzenia 7.3 wyniknie łatwo, że każda skończenie generowana grupa abelowa, która posiada zbiór generatorów spełniający tezę Stwierdzenia 7.10 jest izomorficzna z grupą $\mathbb{Z}^k$, dla pewnego $k \in \mathbb{N} \cup \{0\}$.

7.11. 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 7.10 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

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

7.12. 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 7.9 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 nad 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.

7.13. 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.

7.14. 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 $\mathbb{Z}_1 = \mathbf{0}$, $\mathbb{Z}_0 = \mathbb{Z}$).*

Przystępujemy do dowodu Twierdzenia 7.5. 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.

7.15. 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): w Przykładzie 7.11 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 i–tej kolumny dodano j–tą kolumnę pomnożoną przez stałą c). □

Pozostaje pokazać, że dopuszczalne na mocy Lematu 7.15 operacje pozwalają od dowolnej macierzy przejść do macierzy diagonalnej.

7.16. 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 7.16. □
Kończy to dowód *możliwości przedstawienia grupy w postaci* (★). Tym samym, zakończony jest dowód Twierdzenia 7.3 o klasyfikacji grup przemiennych skończenie generowanych. □

7.17. Przykład. Niech $A = \begin{pmatrix} 1 & 30 & 0 \\ 1 & 15 & 0 \end{pmatrix}$. Zbadamy, jaka jest klasa izomorfizmu grupy $\mathbb{Z}^3/A$. Przekształcamy macierz A w podany poniżej sposób:

$$\begin{pmatrix} 1 & 30 & 0 \\ 1 & 15 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 1 & -15 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & -15 & 0 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 15 & 0 \end{pmatrix} \to$$

$$\to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 15 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Jak widać $\mathbb{Z}^3/A \cong Z_1 \times \mathbb{Z}_{15} \times \mathbb{Z}_0 = \mathbf{0} \times \mathbb{Z}_{15} \times \mathbb{Z} = \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}$.

Warto jeszcze wspomnieć o często stosowanej notacji dotyczącej grup przemiennych skończenie generowanych.

7.18. Przykład. Zapis: grupa przemienna G zadana przez generatory i relacje

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

lub krócej

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

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

ZADANIA

Z 7.1. Niech G i H będą skończonymi grupami przemiennymi. Pokazać, że jeżeli dla każdej liczby naturalnej n grupa G ma tyle samo elementów rzędu n, co grupa H, to G i H są izomorficzne. (Założenie przemienności jest istotne, por. Przykład 5.21).
Z 7.2. Zbadać, czy $\mathbb{Q} \times \mathbb{Q} \cong \mathbb{Q}$.
Z 7.3. Niech $\mathbb{Z} \xrightarrow{f} \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \xrightarrow{g} \mathbb{Z} \times \mathbb{Z}$ będą homomorfizmami zadanymi wzorami $f(x) = (4x, 6x, 2x)$, $g(x, y, z) = (5x - 5y + 5z, 10x - 10y + 10z)$. Sprawdzić, że $g \circ f$ jest homomorfizmem trywialnym i znaleźć $\ker g / \operatorname{im} f$.

TEST

T 7.1. W grupie addytywnej liczb wymiernych $\mathbb{Q}$ istnieje podgrupa właściwa $H \leqslant \mathbb{Q}$, taka że $H \cong \mathbb{Q}$.
T 7.2. Jeżeli w skończonej grupie przemiennej G każda podgrupa właściwa jest cykliczna, to G jest grupą cykliczną.
T 7.3. Jeżeli w grupie przemiennej G rzędu 9 każda podgrupa właściwa jest cykliczna, to G jest grupą cykliczną.
T 7.4. Jeżeli w grupie przemiennej G rzędu 8 każda podgrupa właściwa jest cykliczna, to G jest grupą cykliczną.
T 7.5. Niech H będzie podgrupą grupy $\mathbb{Z} \times \mathbb{Z}$ generowaną przez elementy $(4, 3)$ i $(0, 7)$. Wówczas grupa $\mathbb{Z} \times \mathbb{Z}/H$ jest skończona i jest izomorficzna z _____.
T 7.6. $\mathbb{Z}_{21} \times \mathbb{Z}_{40} \cong \mathbb{Z}_{168} \times \mathbb{Z}_5$
T 7.7. Grupa przemienna, która zawiera więcej niż 20 elementów rzędu 25 musi zawierać podgrupę izomorficzną z $\mathbb{Z}_{25} \times \mathbb{Z}_{25}$.
T 7.8. $\mathbb{Z}_{21} \times \mathbb{Z}_8 \times \mathbb{Z}_5 \cong \mathbb{Z}_{42} \times \mathbb{Z}_{20}$
T 7.9. Jeżeli G i H są grupami przemiennymi rzędu 81 i żadna z tych grup nie zawiera elementów rzędu 9, to grupy te są izomorficzne.
T 7.10. $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_3 \times \mathbb{Z}_{105}$.
T 7.11. $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{315}$.
T 7.12. $(\mathbb{Q}/\mathbb{Z}) \times \mathbb{Z} \cong \mathbb{Q}$.
T 7.13. Niech G, H będą skończenie generowanymi grupami przemiennymi. Jeżeli $G \times \mathbb{Q} \cong H \times \mathbb{Q}$, to $G \cong H$.
T 7.14. Niech G, H będą skończenie generowanymi grupami przemiennymi. Jeżeli $G \times (\mathbb{Q}/\mathbb{Z}) \cong H \times (\mathbb{Q}/\mathbb{Z})$, to $G \cong H$.

8. Pierścienie

Ostatnie dwa rozdziały poświęcamy teorii pierścieni. Ograniczamy się w zasadzie do teorii pierścieni przemiennych z jedynką.

8.1. Definicja. **Pierścieniem** *nazywamy zbiór R wyposażony*[†] *w cztery działania: dwa dwuargumentowe — dodawanie $\big((x,y)\mapsto x+y\big)$ i mnożenie $\big((x,y)\mapsto x\cdot y\big)$, jedno jednoargumentowe — branie elementu przeciwnego $(x\mapsto -x)$, i jedno zeroargumentowe — element wyróżniony 0, takie że $(R,+,-,0)$ jest grupą przemienną, i są spełnione następujące warunki:*
$\forall_{a,b,c\in R}\ a\cdot(b\cdot c)=(a\cdot b)\cdot c$
$\forall_{a,b,c\in R}\ a\cdot(b+c)=a\cdot b+a\cdot c$ *oraz* $\forall_{a,b,c\in R}\ (b+c)\cdot a=b\cdot a+c\cdot a$

Pierścieniem z jedynką *nazywamy pierścień wyposażony*[††] *w jeszcze jedno działanie zeroargumentowe — element wyróżniony 1, taki że*
$\forall_{a\in R}\ 1\cdot a=a\cdot 1=a$.
Jeżeli $\forall_{a,b\in R}\ a\cdot b=b\cdot a$, to mówimy że pierścień jest przemienny.

8.2. Definicja. **Podpierścieniem** *pierścienia z jedynką R nazywamy podzbiór $P\subseteq R$, taki że*
P jest podgrupą grupy addytywnej pierścienia R,
$1\in P$,
$\forall_{a,b\in P}\ a\cdot b\in P$.

W definicji pierścienia z jedynką nie zakładaliśmy, że $0\neq 1$. Jednak istnieje tylko jeden pierścień, w którym $0=1$, tak zwany pierścień zerowy.

8.3. Przykład. Pierścieniem zerowym nazywamy pierścień zawierający tylko jeden element $0=1$.

Uwaga. Jeżeli $0=1$, to w rozpatrywanym pierścieniu R nie ma żadnych innych elementów.

Dowód. Niech $x\in R$. Wówczas $x=x\cdot 1=x\cdot 0=0$. □

8.4. Przykład. Jeżeli R jest niezerowym pierścieniem przemiennym z jedynką, to zbiór macierzy $n\times n$, oznaczany symbolem $M_{n\times n}(R)$, ze zwykłymi działaniami na macierzach, jest pierścieniem z jedynką. Dla $n>1$ pierścień ten jest nieprzemienny.

8.5. Przykład. Jeżeli R jest pierścieniem, a X jest dowolnym niepustym zbiorem, to zbiór R^X, z działaniami określonymi w oczywisty sposób (np. $f\cdot g=h$, gdzie $h(x)=f(x)\cdot g(x)$), jest pierścieniem.

Podajemy jeszcze jeden przykład, dla zilustrowania tego, jak ważne jest precyzyjne określenie rodzaju rozpatrywanych obiektów.

8.6. Przykład. Rozpatrujemy pierścień przemienny z jedynką $\mathbb{Z}_{10}$. Działania dodawania i mnożenia są wykonywane modulo 10, jedynką jest oczywiście liczba 1, a zerem liczba 0. Rozpatrzmy podzbiór $P=\{0,5\}$. Podzbiór ten nie zawiera jedynki pierścienia z jedynką $\mathbb{Z}_{10}$, więc nie jest podpierścieniem pierścienia z jedynką $\mathbb{Z}_{10}$. Zauważmy jednak, że zbiór P jest zamknięty ze względu na mnożenie, dodawanie, branie elementu odwrotnego i zawiera element zerowy. Przyjęty sposób

[†] z formalnego punktu widzenia należałoby napisać: piątkę uporządkowaną $(R,+,\cdot,-,0)$.

[††] z formalnego punktu widzenia należałoby napisać: szóstkę uporządkowaną $(R,+,\cdot,-,0,1)$.

wyrażenia tej sytuacji, to stwierdzenie, że P jest podpierścieniem $\mathbb{Z}_{10}$ w kategorii pierścieni, ale *nie* w kategorii pierścieni przemiennych z jedynką. Zauważmy jeszcze, że w zbiorze P *jest* element neutralny ze względu na mnożenie — liczba 5 ($5 \cdot 5 = 25 = 5$, $5 \cdot 0 = 0$). Ale to nie wystarcza, żeby P uznać za podpierścień pierścienia $\mathbb{Z}_{10}$ w kategorii pierścieni przemiennych z jedynką. Definicja wymaga, żeby do podpierścienia pierścienia przemiennego z jedynką należała jedynka wyjściowego pierścienia.

W dalszym ciągu wykładu ograniczamy się do rozpatrywania pierścieni przemiennych z jedynką.

8.7. Przykład. Ciało jest pierścieniem przemiennym z jedynką.
8.8. Przykład. Pierścień $\mathbb{Z}_n$ liczb całkowitych modulo n z dodawaniem i mnożeniem modulo n.
8.9. Przykład. **Pierścień wielomianów:** Niech R będzie pierścieniem przemiennym z jedynką.
Pierścieniem wielomianów jednej zmiennej nad R nazywamy zbiór ciągów

$$\{(a_0, a_1, \dots)\colon a_i \in R, \quad a_i = 0 \ \text{ dla prawie wszystkich } i\}$$

z działaniami

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots), \quad \text{gdzie } c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

$$-(a_0, a_1, \dots) = (-a_0, -a_1, \dots)$$

oraz elementami: $(0, 0, 0, \dots)$ jako zerem i $(1, 0, 0, \dots)$ jako jedynką.
Oznaczymy przez X ciąg $(0, 1, 0, 0, \dots)$. Ciąg $(a, 0, 0, \dots)$ będziemy w skrócie oznaczać literą a. Wówczas $X^n = (0, 0, \dots, 0, 1, 0, \dots)$ — ciąg z jedynką na n–tym miejscu. Ponadto $(a_0, a_1, \dots, a_n, 0, 0, \dots) = a_0 + a_1 X + \dots + a_n X^n$. W tej konwencji mnożenie wielomianów wyraża się znanym wzorem.
Pierścień wielomianów nad R oznaczamy symbolem $R[X]$.
Konstrukcję pierścienia wielomianów można iterować: $(R[X])[Y]$ oznaczamy symbolem $R[X, Y]$ i nazywamy pierścieniem wielomianów dwóch zmiennych.

W podobny sposób definiujemy też pierścień wielomianów dowolnej skończonej liczby zmiennych.

8.10. Przykład. **Pierścień szeregów formalnych:** Jeżeli w Przykładzie 8.9 opuścimy założenie, że prawie wszystkie współczynniki a_i są równe 0, to z analogicznie określonymi działaniami otrzymamy pierścień szeregów formalnych, który oznaczamy symbolem $R[[X]]$. Tak, jak w przypadku wielomianów, zamiast ciągu $(a_1, a_2, \dots)$ piszemy $\sum_{i=0}^{\infty} a_i X^i$. Działania wyrażają się znanymi wzorami:

$$\sum_{i=0}^{\infty} a_i X^i + \sum_{i=0}^{\infty} b_i X^i = \sum_{i=0}^{\infty} (a_i + b_i) X^i$$

$$\Big(\sum_{i=0}^{\infty} a_i X^i\Big) \cdot \Big(\sum_{i=0}^{\infty} b_i X^i\Big) = \sum_{i=0}^{\infty} c_i X^i, \quad \text{gdzie } c_i = \sum_{j=0}^{i} a_j b_{i-j} \ .$$

Podobnie jak w przypadku wielomianów konstrukcję pierścienia szeregów formalnych można iterować: $(R[[X]])[[Y]]$ oznaczamy $R[[X,Y]]$ i nazywamy pierścieniem szeregów formalnych dwóch zmiennych, itd.

8.11. Przykład. **Produkt pierścieni:** Tak jak w teorii grup, na iloczynie kartezjańskim $P \times R$ pierścieni przemiennych z jedynką można określić działania wzorami $(x,y)(x',y') = (xx', yy')$, $(x,y)+(x',y') = (x+x', y+y')$, $-(x,y) = (-x,-y)$, $1 = (1_P, 1_R)$ i $0 = (0_P, 0_R)$. Zbiór $P \times R$ z tak określonymi działaniami jest pierścieniem przemiennym z jedynką. Nazywamy go produktem pierścieni P i R.

Własności elementów pierścienia

8.12. Definicja. *Element $x \in R$ nazywamy* **dzielnikiem zera** *wtedy i tylko wtedy, gdy istnieje element niezerowy $y \in R$, dla którego $xy = 0$.*
Element $x \in R$ nazywamy **odwracalnym** *wtedy i tylko wtedy, gdy istnieje element $y \in R$, zwany* **odwrotnością** *elementu x, dla którego $xy = 1$.*
Element $x \in R$ nazywamy **nilpotentnym** *jeżeli istnieje liczba całkowita dodatnia n, dla której $x^n = 0$.*

8.13. Uwaga. W pierścieniu niezerowym 0 *jest* dzielnikiem zera. W każdym pierścieniu 0 jest elementem nilpotentnym.

8.14. Uwaga. Można skracać przez elementy, które nie są dzielnikami zera, to znaczy: jeżeli x nie jest dzielnikiem zera i $xy = xz$ to $y = z$.

8.15. Uwaga. Element odwracalny nie jest dzielnikiem zera. Jego odwrotność jest wyznaczona jednoznacznie. Zbiór elementów odwracalnych, z jedynką jako elementem neutralnym, jest grupą ze względu na mnożenie.

8.16. Przykład. W pierścieniu $\mathbb{Z}_n$ dzielnikami zera są te liczby k, dla których $(k,n) > 1$. Pozostałe elementy są odwracalne.

Ten ostatni przykład łatwo uogólnić do następującego stwierdzenia.

8.17. Stwierdzenie. *W pierścieniu skończonym, element nie będący dzielnikiem zera jest odwracalny.*

Dowód. Niech $0, x_1, \ldots, x_n$ będzie listą elementów rozpatrywanego pierścienia. Rozpatrzmy element x, który nie jest dzielnikiem zera. Z założenia o elemencie x i Uwagi 8.14 wynika, że iloczyny $xx_1, \ldots, xx_n$ są parami różne i że żaden z nich nie jest zerem. Zatem rozpatrywane iloczyny, to wszystkie niezerowe elementy pierścienia. Wobec tego któryś z nich *jest* jedynką. □

8.18. Definicja. *Niezerowy pierścień przemienny z jedynką, który nie ma niezerowych dzielników zera, nazywamy* **dziedziną całkowitości**.

Ze Stwierdzenia 8.16 natychmiast wynikają następujące fakty.

8.19. Stwierdzenie. *W dziedzinie całkowitości obowiązuje prawo skracania (przez elementy niezerowe) dla mnożenia.*

8.20. Stwierdzenie. *Skończona dziedzina całkowitości jest ciałem.*

ZADANIA

Wszystkie poniższe zadania dotyczą *pierścieni przemiennych z jedynką*. W związku z tym *podpierścień* musi zawierać jedynkę wyjściowego pierścienia.

Z 8.1. Znaleźć dzielniki zera, elementy odwracalne i elementy nilpotentne w pierścieniach $\mathbb{Z}_{24}$ i $\mathbb{Z}_{16}$.

Z 8.2. W pierścieniach $\mathbb{Z}_9[X]$ i $\mathbb{Z}_{15}[X]$ wskazać elementy odwracalne, dzielniki zera, elementy nilpotentne.

Z 8.3. Czy $\mathbb{Z}_{24}$ zawiera podpierścień izomorficzny z $\mathbb{Z}_8$?

Z 8.4. Znaleźć podpierścienie pierścienia $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

♡ Z 8.5. Wykazać, że jeżeli R jest dziedziną całkowitości, to $R[X]$ oraz $R[[X]]$ także są dziedzinami całkowitości.

Z 8.6. Niech $f = a_0 + a_1x + \cdots + a_nx^n \in R[X]$. Pokazać, że:

a) f jest elementem odwracalnym $\iff$ a_0 jest elementem odwracalnym, a współczynniki $a_1, \ldots, a_n$ są elementami nilpotentymi.

b) f jest nilpotentny $\iff$ $a_0, a_1, \ldots, a_n$ są nilpotentne.

c) f jest dzielnikiem zera $\iff$ istnieje $a \in R$, taki że $af = 0$.

Z 8.7. W pierścieniu szeregów formalnych $R[[X]]$ szereg $\sum_{i=0}^{\infty} a_iX^i$ jest odwracalny wtedy i tylko wtedy, gdy a_0 jest elementem odwracalnym pierścienia R.

♡ Z 8.8. Niech x będzie elementem odwracalnym, a y elementem nilpotentnym. Pokazać, że $x + y$ jest elementem odwracalnym.

TEST

♡ T 8.1. $\forall_{x\in R}\ 0x = x0 = 0$.

♡ T 8.2. $\forall_{x\in R}\ (-1)x = -x$.

T 8.3. Każdy pierścień czteroelementowy jest ciałem.

T 8.4. Każdy pierścień pięcioelementowy jest ciałem.

T 8.5. Produkt dziedzin całkowitości jest dziedziną całkowitości.

T 8.6. Element nieodwracalny jest dzielnikiem zera.

T 8.7. W niezerowym pierścieniu skończonym element nieodwracalny jest dzielnikiem zera.

9. Homomorfizmy i ideały.

9.1. Definicja. *Przekształcenie $\varphi : R \to P$ pierścieni przemiennych z jedynką nazywamy homomorfizmem, jeżeli są spełnione następujące warunki.*
a) φ *jest homomorfizmem grup addytywnych,*
b) $\forall_{a,b\in R}\ \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,
c) $\varphi(1) = 1$.

Określenia izomorfizm, monomorfizm, epimorfizm, automorfizm, endomorfizm są używane w sposób analogiczny, jak w teorii grup. Prawdziwa jest także uwaga analogiczna do Uwagi 1.7.

9.2. Uwaga. Homomorfizm pierścieni jest izomorfizmem wtedy i tylko wtedy, gdy jest homomorfizmem *i* bijekcją zbiorów.

9.3. Przykład. Jedynym homomorfizmem $\mathbb{Z} \to \mathbb{Z}$ jest identyczność.
9.4. Przykład. Istnieje dokładnie jeden homomorfizm $f : \mathbb{Z} \to \mathbb{Z}_n$ — określony wzorem $f(x) = x \pmod n$.
9.5. Przykład. Istnieje dokładnie jeden homomorfizm z dowolnego pierścienia w pierścień zerowy.
9.6. Przykład. Dla każdego elementu a pierścienia R wzór

$$\phi_a(a_nX^n + \cdots + a_1X + a_0) = a_na^n + \cdots + a_1a + a_0$$

określa pewien homomorfizm $\phi_a : R[X] \to R$.
9.7. Przykład. Określimy pewien homomorfizm $\Phi : R[X] \to R^R$. Niech $w = a_nX^n + \cdots + a_1X + a_0$. Obraz wielomianu w oznaczamy symbolem Φ_w i zadajemy wzorem:

$$\Phi_w(a) = a_na^n + \cdots + a_1a + a_0.$$

Tak więc $\Phi_w(a)$ to po prostu $w(a)$ — wartość wielomianu w w punkcie a. Elementy zbioru $\Phi(R[X])$ nazywamy funkcjami wielomianowymi.
Dobrze wiadomo, że dla ciał $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ homomorfizm Φ jest monomorfizmem — różne wielomiany wyznaczają różne funkcje. Spójrzmy jednak na następujący przykład: $R = \mathbb{Z}_2$, $w_1 = X^2 + X$, $w_2 = X^3 + X$. Łatwo sprawdzić, że $\Phi_{w_1} = \Phi_{w_2}$ — jest to w obydwu przypadkach funkcja zerowa.

Podobnie jak w przypadku teorii grup, do badania homomorfizmów posłuży nam pojęcie jądra i pierścienia ilorazowego.

9.8. Definicja. *Jądrem homomorfizmu $\varphi : R \to P$ nazywamy zbiór*

$$ker\,\varphi = \{x \in R\colon \varphi(x) = 0\}.$$

Jądro homomorfizmu ma następujące własności:
a) jest podgrupą grupy addytywnej pierścienia R
b) $\forall_{x\in R}\forall_{a\in ker\,\varphi}\ a \cdot x \in ker\,\varphi$.

9.9. Definicja. **Ideałem** *pierścienia R nazywamy taką podgrupę I grupy addytywnej tego pierścienia, która spełnia warunek:*
$\forall_{x\in R\ a\in I}\ a\cdot x\in I$.
Używamy oznaczenia $I \trianglelefteq R$.

9.10. Przykłady.
1) Jądro dowolnego homomorfizmu jest ideałem.
2) $\{0\} \trianglelefteq R$ jest ideałem, który nazywamy ideałem zerowym.
3) Przypomnijmy, że w pierścieniu liczb całkowitych $\mathbb{Z}$, podgrupy grupy addytywnej są postaci, $n\mathbb{Z}$, dla pewnego $n\in\mathbb{N}$. Każda z nich jest ideałem, gdyż jest jądrem homomorfizmu $f:\mathbb{Z}\to\mathbb{Z}_n$, $f(x)=x \pmod n$.
4) $R \trianglelefteq R$ — ten ideał nazywamy niewłaściwym.

Ideał nazywamy **właściwym,** jeżeli jest różny od całego pierścienia. Zanotujmy przydatne, choć oczywiste, stwierdzenie:

9.11. Stwierdzenie. *Ideał jest właściwy wtedy i tylko wtedy, gdy nie zawiera* 1.

Dowód. Jeżeli ideał zawiera 1, to $\forall_{x\in R}\ x\cdot 1 = x\in I$, czyli $I=R$. □
Wobec powyższego, ideał właściwy nie jest podpierścieniem pierścienia przemiennego z jedynką.

Odnotujmy jeszcze następujące, łatwe do udowodnienia, własności ideałów (analogiczne do odpowiednich własności podgrup normalnych):
1) Jeżeli $\varphi : R \longrightarrow P$ jest homomorfizmem i $J \trianglelefteq P$, to $\varphi^{-1}(J) \trianglelefteq R$.
2) Jeżeli $\varphi : R \longrightarrow P$ jest epimorfizmem i $I \trianglelefteq R$, to $\varphi(I) \trianglelefteq P$.
Jeżeli o przekształceniu φ zakładamy tylko tyle, że jest homomorfizmem, to w każdym razie możemy twierdzić, że $\varphi(I) \trianglelefteq \operatorname{im}(\varphi)$.
3) Jeżeli $I_k \trianglelefteq R$ dla $k\in K$ to $\bigcap\limits_{k\in K} I_k \trianglelefteq R$.

Z tej ostatniej własności wynika, że dla każdego podzbioru $A\subseteq R$ istnieje najmniejszy ze względu na zawieranie ideał pierścienia R zawierający zbiór A — oznacza się go przez (A) i nazywa **ideałem generowanym** przez A. Nietrudno znaleźć postać elementów ideału (A).

9.12. Stwierdzenie. *Jeżeli $A\subseteq R,\ A\neq\emptyset$, to*

$$(A)=\{a_1x_1+\cdots+a_jx_j : j\in\mathbb{N},\ a_i\in A,\ x_i\in R\}.$$

Dowód. Łatwo sprawdzić, że każdy ideał zawierający zbiór A zawiera powyższy zbiór i że zbiór ten *jest* ideałem. □

9.13. Definicja. *Ideał $I \trianglelefteq R$ nazywamy* **ideałem głównym** *wtedy i tylko wtedy, gdy istnieje element $a\in R$, taki że $I=(a)=\{ax : x\in R\}$.*

9.14. Stwierdzenie. *W pierścieniu $\mathbb{Z}$ i w pierścieniu $k[X]$ (wielomianów nad ciałem k) każdy ideał jest główny.*

Dowód. Dla niezerowego ideału w pierścieniu $\mathbb{Z}$ generatorem jest liczba całkowita o najmniejszym module spośród liczb różnych od zera należących do ideału. W przypadku pierścienia wielomianów należy wziąć wielomian najmniejszego stopnia spośród niezerowych wielomianów należących do ideału. □

Używając pojęcia ideału można podać wygodną charakteryzację tych pierścieni, które są ciałami.

9.15. Stwierdzenie. *Pierścień jest ciałem wtedy i tylko wtedy, gdy jest niezerowy i jedynymi jego ideałami są ideał zerowy i cały pierścień.*

Dowód. $\Rightarrow$ Jeżeli $\{0\} \neq I \trianglelefteq R$, to istnieje $x \neq 0$, $x \in I$. Wówczas $x \cdot x^{-1} = 1 \in I$, zatem $I = R$.
$\Leftarrow$ Jeżeli $x \neq 0$, to $\{0\} \neq (x)$, więc $(x) = R$ i $1 \in (x)$ — co oznacza, że istnieje y, dla którego $xy = 1$. □

Pierścienie ilorazowe

9.16. Definicja. *Niech $I \trianglelefteq R$ będzie ideałem. Wówczas* **pierścieniem ilorazowym** *nazywamy zbiór warstw R/I z działaniami:*

$$\begin{aligned}(x+I)+(y+I) &= (x+y)+I\\ (x+I)\cdot(y+I) &= x\cdot y+I\\ -(x+I) &= -x+I\end{aligned}$$

i warstwami: $1+I$ jako jedynką, I jako zerem.
Przekształcenie $\pi : R \to R/I$ zadane wzorem $\pi(x) = x + I$ jest epimorfizmem, $ker\,\pi = I$.

Udowodnimy twierdzenie o homomorfizmie, analogiczne do Twierdzenia 4.17 w teorii grup.

9.17. Twierdzenie o homomorfizmie. *Jeżeli $\varphi : R \to P$ jest homomorfizmem, to istnieje dokładnie jeden homomorfizm $\tilde{\varphi} : R/ker\,\varphi \to P$, taki że $\varphi = \tilde{\varphi} \circ \pi$, gdzie $\pi : R \to R/ker\,\varphi$. Homomorfizm $\tilde{\varphi} : R/ker\,\varphi \to \varphi(R)$ jest izomorfizmem i istnieje wzajemnie jednoznaczna odpowiedniość między ideałami pierścienia $\varphi(R)$ a ideałami R zawierającymi $ker\,\varphi$.*

Dowód. Szukanym homomorfizmem jest $\tilde{\varphi}(xker\,\varphi) = \varphi(x)$. Uzasadnienie jest analogiczne jak w przypadku grup. □

W zależności od własności pierścienia ilorazowego będziemy wyróżniać pewne ideały.

9.18. Definicja. *Ideał $I \trianglelefteq R$ nazywamy* **ideałem pierwszym** *wtedy i tylko wtedy, gdy R/I jest dziedziną całkowitości.*
Ideał $I \trianglelefteq R$ nazywamy **ideałem maksymalnym** *wtedy i tylko wtedy, gdy R/I jest ciałem.*

Oczywiście, każdy ideał maksymalny jest pierwszy. Podamy warunki równoważne tym z definicji i wówczas będzie widać dlaczego używa się nazw — pierwszy i maksymalny.

9.19. Stwierdzenie. *Ideał $I \trianglelefteq R$ jest pierwszy wtedy i tylko wtedy, gdy $I \neq R$ oraz dla dowolnych $x, y \in R$, jeżeli $xy \in I$, to $x \in I$ lub $y \in I$.*
Ideał $I \trianglelefteq R$ jest maksymalny wtedy i tylko wtedy, gdy jest elementem maksymalnym, ze względu na zawieranie, w zbiorze właściwych ideałów R (oznacza to, że $I \neq R$ oraz jeżeli $J \trianglelefteq R$ i $I \subseteq J$, to $I = J$ lub $J = R$).

Dowód. W obydwu wypadkach możemy ograniczyć rozważania do sytuacji, gdy I jest ideałem właściwym. W przeciwnym razie iloraz jest pierścieniem zerowym, a więc nie jest ani dziedziną całkowitości, ani ciałem. Zakładamy zatem, że $I \neq R$.

Pierścień R/I jest dziedziną całkowitości wtedy i tylko wtedy, gdy z równości $(x+I)\cdot(y+I) = xy+I = 0+I$ wynika, że $(x+I = 0+I \ \vee \ y+I = 0+I)$, a zatem wtedy i tylko wtedy, gdy z $xy \in I$ wynika, że $(x \in I \ \vee \ y \in I)$.

Pierścień R/I jest ciałem wtedy i tylko wtedy, gdy jego jedynymi ideałami są ideał zerowy oraz cały pierścień R/I, a zatem (wobec wzajemnie jednoznacznej odpowiedniości między ideałami pierścienia ilorazowego R/I a ideałami pierścienia R zawierającymi I) wtedy i tylko wtedy, gdy z $I \subseteq J \trianglelefteq R$ wynika $(I = J \vee J = R)$. □

9.20. Twierdzenie. *Każdy ideał właściwy I jest zawarty w pewnym ideale maksymalnym.*

Dowód. Rozpatrzmy zbiór ideałów właściwych zawierających I, z częściowym porządkiem wyznaczonym przez zawieranie. Łańcuchami† są wówczas wstępujące rodziny ideałów. Każdy łańcuch ma zatem ograniczenie górne, bo suma wstępującej rodziny ideałów właściwych jest ideałem właściwym (nie zawiera jedynki, bo nie zawiera jej żaden z sumowanych składników). Na mocy lematu Zorna w zbiorze tym istnieje więc element maksymalny. □

9.21. Wniosek. *Każdy niezerowy pierścień można odwzorować epimorficznie na pewne ciało.* □

9.22. Przykłady.

1) $\mathbb{Z}/(n) \cong \mathbb{Z}_n$ jest pierścieniem skończonym. Zatem ideał główny (n) jest maksymalny wtedy i tylko wtedy, gdy jest pierwszy, a więc wtedy i tylko wtedy, gdy n jest liczbą pierwszą.
2) Niech X będzie przestrzenią topologiczną, a $C(X)$ pierścieniem funkcji ciągłych o wartościach rzeczywistych. Niech $x_0 \in X$. Ideał $\{f\colon f(x_0) = 0\}$ jest jądrem epimorfizmu $\phi : C(X) \to R$, określonego wzorem $\phi_f(x_0) = f(x_0)$, a więc jest maksymalny.

Następne dwa przykłady ilustrują ważną metodę otrzymywania interesujących ciał jako pierścieni ilorazowych pierścienia wielomianów nad ciałem.

3) Ideał $(x^2+1) \trianglelefteq \mathbb{R}[X]$ jest maksymalny, i $\mathbb{R}[X]/(x^2+1) \cong \mathbb{C}$. Izomorfizm jest wyznaczony przez przyporządkowanie warstwie $x+(x^2+1)$ liczby i.
4) Łatwo sprawdzić, że $\mathbb{Z}_2[X]/(X^2+X+1)$ jest ciałem o czterech elementach, więc ideał (X^2+X+1) jest maksymalny.

Ciało ułamków

Na koniec opiszemy jeszcze jedną często stosowana konstrukcję ciał. Załóżmy, że R jest dziedziną całkowitości. Obowiązuje wówczas, tak jak w ciele, prawo skracania (przez elementy niezerowe) dla mnożenia:

$$\forall_{x\neq 0}\forall_{y,z}\ xy = xz \Leftrightarrow y = z.$$

Jednak, inaczej niż w ciele, niektóre niezerowe elementy mogą nie mieć odwrotności. Okazuje się, że dziedzina R, choć sama nie musi być ciałem, jest zawsze *zawarta* w pewnym ciele. Istnieje prosta konstrukcja, która to gwarantuje, tzw. konstrukcja ciała ułamków $Q(R)$ dziedziny R. W szczególnym przypadku, gdy $R = \mathbb{Z}$ otrzymujemy dobrze znane ciało liczb wymiernych: $Q(\mathbb{Z}) = \mathbb{Q}$.

† tzn. podzbiorami liniowo uporządkowanymi.

Niech R będzie dziedziną całkowitości. Na zbiorze par uporządkowanych $R \times (R \setminus \{0\})$ określamy relację równoważności $\sim$ wzorem
$(x, y) \sim (z, v) \Leftrightarrow xv = yz$. Klasę równoważności tej relacji nazywamy ułamkiem i oznaczamy symbolem $\frac{x}{y}$ (tak więc $\frac{x}{y} = \frac{z}{v} \Leftrightarrow xv = yz$). Zbiór wszystkich ułamków oznaczamy symbolem $Q(R)$.

9.23. Definicja. **Ciałem ułamków** *dziedziny całkowitości R nazywamy zbiór $Q(R)$ z ułamkiem $\frac{0}{1}$ jako zerem, ułamkiem $\frac{1}{1}$ jako jedynką i działaniami określonymi wzorami:*

$$\frac{x}{y} + \frac{p}{q} = \frac{xq + py}{yq}$$
$$\frac{x}{y} \cdot \frac{p}{q} = \frac{xp}{yq}$$
$$-\frac{p}{q} = \frac{-p}{q}$$

Łatwo sprawdzić, że takie działania są dobrze określone i że definiują ciało. Odwzorowanie $i : R \hookrightarrow Q(R)$ zadane wzorem $i(x) = \frac{x}{1}$ jest monomorfizmem pierścieni. Zatem istotnie, każda dziedzina całkowitości jest podpierścieniem pewnego ciała.

9.24. Przykład. Niech $R = k[X]$ będzie pierścieniem wielomianów ciała k. Ciało ułamków $Q(k[X])$ oznaczamy symbolem $k(X)$ i nazywamy **ciałem funkcji wymiernych nad** k. Dla $k = \mathbb{Z}_2$ konstrukcja ta dostarcza przykładu ciała nieskończonego charakterystyki 2.

Konstrukcję ciała ułamków rozumiemy jako operację dodania do dziedziny całkowitości pewnych brakujących elementów. Zauważmy, że oczywiście
9.25. Uwaga. Jeżeli dziedzina całkowitości R jest ciałem, to $Q(R) \cong R$.

ZADANIA

Z 9.1. Pokazać, że pierścień R jest ciałem wtedy i tylko wtedy, gdy każdy homomorfizm określony na R, o wartościach w pierścieniu niezerowym, jest monomorfizmem.
Z 9.2. Znaleźć wszystkie ideały pierścieni $\mathbb{Z}_{15}$ i $\mathbb{Z}_{16}$. Wskazać wśród nich pierwsze i maksymalne. Znaleźć pierścienie ilorazowe.
Z 9.3. Pokazać, że ideał pierścienia skończonego jest pierwszy wtedy i tylko wtedy, gdy jest maksymalny.
Z 9.4. Pokazać, że jeżeli $p|n$, to nie istnieje homomorfizm pierścienia $\mathbb{Z}[\frac{1}{n}] \longrightarrow \mathbb{Z}_p$, gdzie $\mathbb{Z}[\frac{1}{n}]$ jest podpierścieniem $\mathbb{Q}$ generowanym przez $\mathbb{Z}$ i $\frac{1}{n}$.
Z 9.5. Znaleźć wszystkie homomorfizmy pierścieni $\mathbb{Z}[X]/(10X^2 - 6X - 3) \longrightarrow \mathbb{Z}_{11}$.
Z 9.6. Niech I_1 oraz I_2 będą ideałami pierścienia R. Wykazać, że podzbiór R $\{x_1 + x_2 : x_1 \in I_1,\, x_2 \in I_2\}$ jest ideałem generowanym przez $I_1 \cup I_2$.
Z 9.7. Niech R będzie pierścieniem lokalnym, to znaczy takim, że ma on dokładnie jeden ideał maksymalny. Udowodnić, że jeżeli $x \in R$ oraz $x^2 = x$ to $x = 0$ lub $x = 1$.
Z 9.8. Czy pierścień $\mathbb{Z}[X]/(X^n - 1)$ jest dziedziną całkowitości?
Z 9.9. Zbadać, czy ideał główny $(2i)$ pierścienia $\mathbb{Z}[i]$ jest pierwszy.
Z 9.10. Zbadać, czy w pierścieniu $\mathbb{Z}[X]$ ideał $(X^2, X^3 + 6)$ jest główny.
Z 9.11. Pokazać, że $\mathbb{Z}[i]/(3 + i) \cong \mathbb{Z}_{10}$.
Z 9.12. Pokazać, że $\mathbb{R}[X]/(X^2 - 2X + 2) \cong \mathbb{C}$.
Z 9.13. Udowodnić, że jeżeli R jest nieskończoną dziedziną całkowitości, to homomorfizm $\Phi : R[X] \longrightarrow R^R$ dany wzorem $\Phi_f(a) = f(a)$ jest monomorfizmem.
Z 9.14. Udowodnić, że pierścień $R[X]$ jest dziedziną ideałów głównych wtedy i tylko wtedy, gdy R jest ciałem. Podać przykład ideału w $\mathbb{Z}[X]$, który nie jest główny.
♡ Z 9.15. Udowodnić, że w pierścieniu wielomianów $K[X]$, gdzie K jest ciałem, każdy niezerowy ideał pierwszy jest maksymalny.
Z 9.16. Znaleźć wszystkie homomorfizmy pierścieni:
a) $\mathbb{Z}[X]/(X^2) \longrightarrow \mathbb{Z}_{24}$
b) $\mathbb{Z}[X, Y]/(X^2 - Y^3) \longrightarrow \mathbb{Z}$
c) $\mathbb{Z}[X]/(X^n - 1) \longrightarrow \mathbb{Q}$
d) $\mathbb{Z}[X]/(X^n - 1) \longrightarrow C$
Z 9.17. Znaleźć wszystkie homomorfizmy pierścieni $\mathbb{Z}[X]/(15X^2 + 10X - 2) \longrightarrow \mathbb{Z}_7$.

TEST

T 9.1. Pierścień $\mathbb{Z}_8$ jest obrazem homomorficznym pierścienia $\mathbb{Z}_{24}$.
T 9.2. Każdy ideał pierścienia $\mathbb{Z}_n$ jest główny.
T 9.3. Każdy ideał pierwszy pierścienia $\mathbb{Z}$ jest maksymalny.
T 9.4. Jeżeli skończony niezerowy pierścień nie zawiera podpierścienia właściwego, to jest izomorficzny z którymś z pierścieni $\mathbb{Z}_n$.
T 9.5. W produkcie pierścieni $R \times P$ podzbiór $R \times \{0\}$ jest podpierścieniem.
T 9.6. W produkcie pierścieni $R \times P$ podzbiór $R \times \{0\}$ jest ideałem.
T 9.7. Podpierścień dziedziny całkowitości jest dziedziną całkowitości.
T 9.8. W pierścieniu $\mathbb{Z}_n$ każdy ideał jest główny.
T 9.9. W pierścieniu $\mathbb{Z}_n$ każdy ideał pierwszy jest maksymalny.
T 9.10. Jeżeli pierścień ilorazowy pierścienia $K[X]$, gdzie K jest ciałem, jest dziedziną całkowitości, to jest ciałem.
T 9.11. $R[X]/((X - 1)(X + 1)) \cong R[X]/((X - 2)X)$

T 9.12. $\mathbb{C}[X,Y]/(X^2-Y^2) \cong \mathbb{C}[X,Y]/(XY)$
T 9.13. $\mathbb{Z}[X]/(2X(X-1)) \cong \mathbb{Z}[X]/(X(X-1))$.
T 9.14. $\mathbb{Q}[X]/(2X(X-1)) \cong \mathbb{Q}[X]/(X(X-1))$.
T 9.15. $\mathbb{Z}[X]/(X(X-1)) \cong \mathbb{Z}[X]/(X) \times \mathbb{Z}[X]/(X-1)$.
T 9.16. $\mathbb{Z}[X]/(X^2+X+1)$ jest izomorficzny z podpierścieniem $\mathbb{R}$.
T 9.17. $\mathbb{Z}[i]/(1+2i) \cong \mathbb{Z}_5$.
T 9.18. $\mathbb{Z}[i]/(1+2i) \cong \mathbb{Z}_2$.
T 9.19. $\mathbb{Z}[i]/(2+2i)$ ma skończenie wiele elementów.
T 9.20. $\mathbb{Z}[i]/(2+2i)$ jest dziedziną całkowitości.
T 9.21. $\mathbb{Z}[i]/(2+2i)$ jest ciałem.
T 9.22. Pierścień $Z_{15}[X]$ ma nieskończenie wiele dzielników zera.
T 9.23. W pierścieniu $Z[X]$ ideał (X^2, X^4-3) jest główny.
T 9.24. Ideał $((3,5))$ jest ideałem pierwszym w $\mathbb{Z} \times \mathbb{Z}$.
T 9.25. Ideał $((3,5))$ jest ideałem maksymalnym w $\mathbb{Z} \times \mathbb{Z}$.
T 9.26. Niech K będzie ciałem. Ciało funkcji wymiernych dwóch zmiennych $K(X,Y)$ zawiera podciało izomorficzne z ciałem $K(X)$.
T 9.27. Niech R będzie dziedziną całkowitości. Wówczas $Q(R)(X) \cong Q(R[X])$.