Algebra I

wykład z ćwiczeniami dla studentów II roku matematyki

Grzegorz Bobiński

Wydział Matematyki i Informatyki UMK w Toruniu

Toruń 2005

Spis treści

ROZDZIAŁ I

Pierścienie

Dobrze znany fakt z teorii liczb, zwany Zasadniczym Twierdzeniem Arytmetyki, mówi, że każdą liczbę całkowitą większą od 1 można przedstawić jednoznacznie (z dokładnością do porządku czynników) w postaci iloczynu potęg parami różnych liczb pierwszych. Podobnie, każdy unormowany wielomian jednej zmiennej stopnia dodatniego nad ciałem liczb rzeczywistych jest iloczynem unormowanych wielomianów liniowych oraz nierozkładalnych unormowanych wielomianów stopnia 2, przy czym ponownie przedstawienie to jest jednoznaczne z dokładnością do kolejności czynników. Znalezienie wspólnego uzasadnienia obu powyższych faktów oraz uogólnienie ich na nowe sytuacji będzie stanowiło główną motywacją dla rozważań poświęconych pierścieniom.

1.1. Działania w zbiorach

W tym paragrafie rozważymy abstrakcyjne własności działań w zbiorach oraz wprowadzimy oznaczenia przydatne w późniejszych rozważaniach poświęconych pierścieniom i grupom.

1.1.1. *Działaniem w zbiorze* X nazywamy każdą funkcję $* : X \times X \to X$. Obraz pary (a, b) przy działaniu $*$ zapisujemy jako $a * b$, tzn. $a * b = *(a, b)$. Dla oznaczenia iterowanego zastosowania działania stosujemy notację nawiasową, a więc na przykład $a * (b * c) = *(a, *(b, c))$. Działanie $*$ nazywamy *łącznym*, jeśli

$$a * (b * c) = (a * b) * c$$

dla dowolnych $a, b, c \in X$. Działanie $*$ nazywamy *przemiennym*, jeśli

$$a * b = b * a$$

dla dowolnych $a, b \in X$. Dodawanie i mnożenie w zbiorze liczb całkowitych są przykładami działań, które są łączne i przemienne. Odejmowanie liczb całkowitych nie jest ani łączne ani przemienne. Przykładem działania, które jest łączne, ale nie jest przemienne, jest mnożenie macierzy kwadratowych stopnia 2. Łączność działania $*$ oznacza w praktyce, że stosowanie nawiasów jest zbędne. Niepusty zbiór X z działaniem $*$, które jest łączne, będziemy nazywać *półgrupą*. Gdy dodatkowo działanie $*$ jest przemienne, to mówimy o *półgrupie abelowej* (*przemiennej*).

1.1.2. Niech X z działaniem $*$ będzie półgrupą. Element $e \in X$ nazywamy *elementem neutralnym dla działania* $*$, jeśli

$$e * a = a = a * e$$

dla dowolnego $a \in X$. Element neutralny, jeśli istnieje, jest wyznaczony jednoznacznie. Istotnie, jeśli e i e' są elementami neutralnymi dla $*$, to

$$e = e * e' = e'.$$

Element neutralny dla działania $*$ będziemy oznaczać 1_*. Półgrupę (abelową), w której istnieje element neutralny, nazywamy *monoidem* (*abelowym*) .

1.1.3. Niech X z działaniem $*$ będzie monoidem. Element $a \in X$ nazywamy *odwracalnym względem* $*$, jeśli istnieje element $a' \in X$ taki, że

$$a' * a = 1_* = a * a'.$$

Element a', jeśli istnieje, jest wyznaczony jednoznacznie przez a. Istotnie, jeśli element $a'' \in X$ jest taki, że $a'' * a = e = a * a''$, to

$$a' = a' * 1_* = a' * a * a'' = 1_* * a'' = a''.$$

Element a' nazywamy *elementem odwrotnym do* a *względem* $*$ i oznaczamy a^{*-}. Z powyższego rachunku wynika, że jeśli element a jest odwracalny oraz $a' * a = 1_*$ lub $a * a' = 1_*$, to $a' = a^{*-}$. W ogólności nie jest jednak prawdą, że jeśli $a \in X$ oraz istnieje element $a' \in X$ taki, że $a' * a = 1_*$, to element a jest odwracalny (patrz Ćwiczenie 1.1.1, porównaj także Ćwiczenie 1.1.4). Zauważmy, że jeśli element a jest odwracalny, to element odwrotny do a też jest odwracalny i $(a^{*-})^{*-} = a$. Ponadto, gdy elementy a i b są odwracalne, to $a * b$ jest elementem odwracalnym oraz $(a * b)^{*-} = b^{*-} * a^{*-}$. Monoid (abelowy), w którym wszystkie elementy są odwracalne nazywamy *grupą* (*abelową*). Szczególną rolę elementów odwracalnych pokazuje następujący fakt.

Stwierdzenie. *Niech X z działaniem $*$ będzie monoidem.*

(1) *Jeśli $a, b, x \in X$, $a * x = b$ oraz a jest elementem odwracalnym, to $x = a^{*-} * b$.*
(2) *Jeśli $a, b, x \in X$, $x * a = b$ oraz a jest elementem odwracalnym, to $x = b * a^{*-}$.*

1.1.4. Niech X z działaniem $*$ będzie półgrupą. Dla $a \in X$ oraz dodatniej liczby całkowitej n przez a^{*n} oznaczać będziemy

$$\underbrace{a * \cdots * a}_{n \text{ razy } a}.$$

W szczególności $a^{*1} = a$. Jeśli X jest monoidem, to definiujemy $a^{*0} = 1_*$. Gdy dodatkowo założymy, że element a jest odwracalny, to definiujemy a^{*n} jako $(a^{*-})^{*(-n)}$ dla $n < 0$. W szczególności $a^{*(-1)} = a^{*-}$.

Łatwo udowodnić, że

$$a^{*n} * a^{*m} = a^{*(n+m)}$$
$$(a^{*n})^{*m} = a^{*(nm)}$$

dla dowolnego $a \in X$ oraz wszystkich liczb całkowitych n i m, dla których powyższe wyrażenia mają sens. Ponadto, gdy działanie $*$ jest przemienne oraz $a, b \in X$, to

$$(a * b)^{*n} = a^{*n} * b^{*n}.$$

1.1.5. Dla oznaczenia działań zwykle używać będziemy symboli $+$ i $\cdot$. W pierwszym przypadku mówimy o notacji *addytywnej*, w drugim o notacji *multiplikatywnej*. Jeśli stosujemy notację addytywną, to element neutralny oznaczamy przez 0, element odwrotny do a przez $-a$ oraz nazywamy go *elementem przeciwnym do* a, natomiast zamiast a^{*n} piszemy na. Ponadto zamiast pisać $a+(-b)$ piszemy $a-b$. Należy przy tym pamiętać, że $a-b-c$ jest równe $(a-b)-c$, nie zaś $a-(b-c)$. W przypadku notacji *multiplikatywnej* odpowiednie oznaczenia to 1, a^{-1} oraz a^n. Ponadto, w tym przypadku piszemy ab zamiast $a \cdot b$.

Ćwiczenia

1.1.1. Niech X będzie zbiorem oraz niech $\mathscr{F}(X)$ będzie zbiorem wszystkich funkcji $f : X \to X$.

(a) Udowodnić, że $\mathscr{F}(X)$ wraz z działaniem $\circ$ składania funkcji jest monoidem (elementem neutralnym jest funkcja identycznościowa $\mathbb{1}_X$).
(b) Udowodnić, że $f \in \mathscr{F}(X)$ jest elementem odwracalnym wtedy i tylko wtedy, gdy f jest bijekcją.
(c) Niech $f \in \mathscr{F}(X)$. Udowodnić, że istnieje funkcja $f' \in \mathscr{F}(X)$ taka, że $f' \circ f = \mathbb{1}_X$ wtedy i tylko wtedy, gdy f jest injekcją.
(d) Niech $f \in \mathscr{F}(X)$. Udowodnić, że istnieje funkcja $f' \in \mathscr{F}(X)$ taka, że $f \circ f' = \mathbb{1}_X$ wtedy i tylko wtedy, gdy f jest surjekcją.

1.1.2. Niech X z działaniem $*$ będzie półgrupą taką, że istnieją elementy e' i e'' takie, że

$$e' * a = a \text{ oraz } a * e'' = a$$

dla dowolnego elementu $a \in X$. Udowodnić, że X jest monoidem.

1.1.3. Niech X z działaniem $*$ będzie monoidem oraz $a \in X$. Udowodnić, że jeśli istnieją elementy $a' \in X$ oraz $a'' \in X$ takie, że

$$a' * a = 1_* = a * a''$$

to element a jest odwracalny.

1.1.4. Niech X z działaniem $*$ będzie półgrupą taką, że spełnione są następujące warunki:

(a) istnieje element $e \in G$ taki, że $e * a = a$ dla dowolnego elementu $a \in G$,

(b) dla każdego elementu $a \in G$ istnieje element $a' \in G$ taki, że $a' * a = e$.

Udowodnić, że X jest grupą.

1.1.5. Niech X z działaniem $*$ będzie półgrupą taką, że dla dowolnych elementów $a, b \in X$ istnieją elementy $x, y \in X$ takie, że $a * x = b$ oraz $y * a = b$. Udowodnić, że X jest grupą.

1.1.6. Niech X z działaniem $*$ będzie półgrupą skończoną taką, że dla dowolnych $a, b, c \in X$ spełnione są warunki:

$$a * b = a * c \Rightarrow b = c \text{ i } b * a = c * a \Rightarrow b = c.$$

Udowodnić, że X jest grupą.

1.1.7. Niech X z działaniem $*$ będzie monoidem. Udowodnić, że jeśli $a^{*2} = 1_*$ dla dowolnego $a \in X$, to X z działaniem $*$ jest grupą abelową.

1.1.8. Który z poniższych zbiorów jest monoidem (grupą) ze względu na działanie dodawania (mnożenia):

(a) zbiór dodatnich liczb całkowitych,
(b) zbiór nieujemnych liczb całkowitych,
(c) zbiór liczb całkowitych,
(d) zbiór liczb wymiernych.

1.2. Pierścienie — podstawowe definicje

Ten paragraf poświęcony będzie wprowadzeniu pojęć z zakresu teorii pierścieni niezbędnych do sformułowania teorii podzielności.

1.2.1. *Pierścieniem* (*przemiennym z jedynką*) nazywamy zbiór R wraz z dwoma działaniami $+$ i $\cdot$ (zwanymi zwykle dodawaniem i mnożeniem) takimi, że R jest grupą abelową ze względu na działanie $+$ oraz monoidem abelowym ze względu na działanie $\cdot$, i spełnione jest prawo rozdzielności mnożenia względem dodawania, tzn.

$$a(b + c) = ab + ac \text{ i } (b + c)a = ba + ca$$

dla dowolnych $a, b, c \in R$. Ważną rolę w matematyce odgrywają pierścienie, w których działanie $\cdot$ nie jest przemienne lub nie posiada elementu neutralnego, ale takie pierścienie nie będą pojawiać się w naszych rozważaniach.

Zbiory liczb całkowitych, wymiernych, rzeczywistych i zespolonych ze zwykłymi działaniami dodawania i mnożenia są przykładami pierścieni z jedynką, które będziemy oznaczać $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$, odpowiednio. Innym ważnym przykładem pierścienia jest zbiór $\mathbb{Z}_m$ reszt z dzielenia przez m z działaniami dodawania i mnożenia modulo m, gdzie m jest ustaloną dodatnią liczbą całkowitą.

Zauważmy, że w wyrażeniach $0a$, $1a$ oraz $(-1)a$ symbole 0, 1 oraz -1 mogą wystąpić w podwójnej roli: jako liczby całkowite oraz jako wyróżnione elementy pierścienia R. Trzeba zatem sprawdzić, czy różne interpretacje nie prowadzą do różnych wyników. Jedynym wyrażeniem,

dla którego nie jest to oczywiste, jest $0a$. Zauważmy jednak, że równość $0 = 0 + 0$ implikuje, iż $0a = (0 + 0)a = 0a + 0a$, co wobec Stwierdzenia 1.1.3 oznacza, że $0a = 0$, co kończy sprawdzenie.

Łatwo udowodnić, że $(-a)b = -ab = a(-b)$ dla dowolnych $a, b \in R$. Powyższa własność przydaje się w dowodzie równości

$$(na)b = n(ab) = a(nb)$$

zachodzącej dla dowolnych $a, b \in R$ oraz liczby całkowitej n.

1.2.2. Niezerowy element a pierścienia R nazywamy *dzielnikiem zera*, jeśli istnieje element $b \in R$ taki, że $b \neq 0$ oraz $ab = 0$. Element a pierścienia z jedynką R nazywamy *odwracalnym*, jeśli jest odwracalny względem $\cdot$. Zauważmy, że jeśli element jest odwracalny, to nie jest dzielnikiem zera. Ponadto, jeśli $0 \neq 1$ (patrz Ćwiczenie 1.2.1, kiedy w pierścieniu możliwe jest $0 = 1$), to każdy element odwracalny jest niezerowy. Pierścień, w którym nie ma dzielników zera oraz $0 \neq 1$, nazywamy *dziedziną* (*całkowitości*). Dziedzinę, w której każdy element różny od 0 jest odwracalny, nazywamy *ciałem*. Oczywiście każde ciało jest dziedziną. Przykładem dziedziny, która nie jest ciałem jest pierścień liczb całkowitych. Poniższa własność elementów niebędących dzielnikami zera będzie przydatna w naszych rozważaniach.

Stwierdzenie. *Jeśli element a pierścienia R nie jest dzielnikiem zera, to z równości $ab = ac$ wynika, że $b = c$.*

Dowód. Zauważmy, że przy naszych założeniach mamy $a(b-c) = 0$, zatem $b - c = 0$, skąd $b = c$. □

1.2.3. Podzbiór I pierścienia R nazywamy *ideałem pierścienia R*, jeśli

(1) $0 \in I$,
(2) jeśli $a \in I$, to $-a \in I$,
(3) jeśli $a, b \in I$, to $a + b \in I$, oraz
(4) jeśli $a \in R$ i $b \in I$, to $ab \in I$.

W każdym pierścieniu R ideałami są R oraz *ideał trywialny* $\{0\}$ oznaczany przez 0. Jeśli R jest ciałem, to są to jedyne ideały pierścienia R (patrz Ćwiczenie 1.2.12). Ideałami pierścienia $\mathbb{Z}$ są $\mathbb{Z}m$, gdzie m liczbą całkowitą nieujemną. Są to jedyne ideały pierścienia $\mathbb{Z}$ (patrz Ćwiczenie 1.2.14).

Wprowadzimy teraz pewne przydatne oznaczenia. Jeśli X i Y są niepustymi podzbiorami pierścienia R oraz $a \in R$, to piszemy

$$\begin{aligned} -X &= \{-a \mid a \in X\}, \\ X + Y &= \{a + b \mid a \in X,\, b \in Y\}, \\ aX &= \{ab \mid b \in X\}, \end{aligned}$$

oraz

$$Xa = \{ba \mid b \in X\},$$

Oczywiście $aX = Xa$. Piszemy $a + Y$ i $Y + a$ zamiast $\{a\} + Y$ i $Y + \{a\}$, odpowiednio. Łatwo dostrzec, że operacja dodawania podzbiorów zdefiniowana powyżej jest łączna. Rodzina ideałów pierścienia R jest zamknięta na zdefiniowane powyżej operacje, tzn. jeśli I i J są ideałami pierścienia R oraz $a \in I$, to $-I$, $I+J$ oraz aI też są ideałami pierścienia R.

Ideał I pierścienia R nazywamy *właściwym*, jeśli $I \neq R$. Ideał I jest właściwy wtedy i tylko wtedy, gdy $1 \notin I$. Ideał właściwy I nazywamy *maksymalnym*, jeśli dla dowolnego ideału właściwego J z warunku $I \subset J$ wynika $J = I$. Ideał właściwy I nazywamy *pierwszym*, jeśli dla dowolnych $a, b \in R$, z warunku $ab \in I$ wynika, że $a \in I$ lub $b \in I$. Zauważmy, że każdy ideał maksymalny jest pierwszy. Istotnie, załóżmy, że I jest ideałem maksymalnym w pierścieniu R, $ab \in I$ oraz $a \notin I$. Wtedy $J = I + Ra$ jest ideałem pierścienia R takim, że $I \subset J$ oraz $I \neq J$, więc $J = R$. W szczególności istnieją elementy $x \in I$ oraz $y \in R$ takie, że $1 = x + ya$, więc $b = xb + yab$. Ponieważ $ab \in I$ oznacza to, że $b \in I$.

1.2.4. Poniższe rozumowania prowadzące do definicji ideału generowanego przez podzbiór pojawia się w matematyce wielokrotnie w różnych kontekstach (porównaj na przykład Ćwiczenie 1.6.1 oraz paragraf 2.4).

Lemat. *Jeśli I_α, $\alpha \in A$, $A \neq \varnothing$, są ideałami pierścienia R, to $\bigcap_{\alpha\in A} I_\alpha$ też jest ideałem pierścienia R.*

Dowód. Wynika bezpośrednio z definicji. □

Wniosek. *Jeśli X jest podzbiorem pierścienia R, to istnieje najmniejszy (w sensie zawierania zbiorów) ideał pierścienia R zawierający zbiór X.*

Dowód. Szukanym ideałem jest przekrój wszystkich ideałów zawierających zbiór X. Rozważana rodzina jest niepusta, gdyż $X \subset R$. □

Jeśli X jest podzbiorem pierścienia R, to najmniejszy ideał pierścienia R zawierający zbiór X będziemy oznaczać (X). Gdy $X = \{a_1, \ldots, a_n\}$, to zamiast (X) piszemy $(a_1, \ldots, a_n)$. Jeśli $I = (X)$, to mówimy, że *ideał I jest generowany przez zbiór X*. Ideał I pierścienia R nazywamy *głównym*, gdy istnieje element $a \in R$ taki, że $I = (a)$. Pierścień R, w którym każdy ideał jest główny, nazywamy *pierścieniem ideałów głównych*. Gdy dodatkowo R jest dziedziną, to mówimy o *dziedzinie ideałów głównych*. Zauważmy, że $R = (1)$.

1.2.5. W niedalekiej przyszłości przydatny będzie bardziej konkretny opis ideału generowanego przez podzbiór. Ze względu na prostotę oraz późniejsze zastosowania ograniczymy się do sytuacji ideałów skończenie generowanych (tzn. generowanych przez skończone zbiory).

STWIERDZENIE. *Jeśli $a_1, \ldots, a_n$ są elementami pierścienia R, to $(a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n$. W szczególności, gdy $a \in R$, to $(a) = Ra$.*

DOWÓD. Niech $I = (a_1, \ldots, a_n)$ oraz $J = Ra_1 + \cdots + Ra_n$. Wiemy, że J jest ideałem. Ponadto z definicji ideału wynika, że $J \subset I$. Ponieważ $a_i = 0a_1 + \cdots + 0a_{i-1} + 1a_i + 0a_{i+1} + \cdots + 0a_n \in J$ dla każdego i, więc otrzymujemy tezę. □

1.2.6. Ważna rolę w matematyce odgrywa możliwości porównywania dwóch struktur i, w szczególności, pojęcie izomorfizmu. Funkcję $\varphi : R \to S$ pomiędzy pierścieniami R i S nazywamy *homomorfizmem pierścieni*, jeśli

$$\varphi(a + b) = \varphi(a) + \varphi(b) \text{ oraz } \varphi(ab) = \varphi(a)\varphi(b)$$

dla dowolnych $a, b \in R$. Powyższe warunki implikują, że $\varphi(0) = 0$ oraz $\varphi(-a) = -\varphi(a)$, nie musi być natomiast prawdą, że $\varphi(1) = 1$ (patrz Ćwiczenia 1.2.20, 1.2.22, 1.2.23 oraz 1.2.24).

Jeśli R jest pierścieniem, to funkcja identycznościowa $\mathbb{1}_R$ jest homomorfizmem. Jeśli $\varphi : R \to S$ oraz $\psi : S \to T$ są homomorfizmami pierścieni, to $\psi\varphi : R \to T$ też jest homomorfizmem pierścieni. Mniej trywialnym przykładem homomorfizmu jest funkcja

$$\mathbb{Z} \ni n \mapsto na \in R,$$

gdzie a jest ustalonym elementem pierścienia R takim, że $a^2 = a$ (np. możemy wziąć $a = 1$).

Homomorfizm, który jest injekcją, nazywamy *monomorfizmem*, zaś homomorfizm surjektywny *epimorfizmem*. *Izomorfizmem pierścieni* nazywamy homomorfizm, który jest funkcją odwracalną. Homomorfizm postaci $R \to R$ nazywamy *endomorfizmem* pierścienia R, zaś endomorfizm, który jest izomorfizmem, będziemy nazywać *automorfizmem*. Bardzo często będziemy utożsamiać izomorficzne pierścienie. Więcej o izomorfizmach pierścieni powiemy w paragrafie 1.6. Jeśli $\varphi : R \to S$ jest izomorfizmem, to funkcja odwrotna do φ też jest homomorfizmem (a więc także izomorfizmem) pierścieni, i mówimy, że *pierścienie R i S są izomorficzne* oraz piszemy $R \simeq S$.

Ćwiczenia

1.2.1. Udowodnić, że jeśli $0 = 1$ w pierścieniu R, to $R = 0$.

1.2.2. Niech S będzie zbiorem wszystkich podzbiorów ustalonego zbioru X. W S definiujemy działania $+$ i $\cdot$ wzorami $A + B = (A - B) \cup (B - A)$ oraz $A \cdot B = A \cap B$. Udowodnić, że S z powyższymi działaniami jest pierścieniem.

1.2.3. Niech q będzie liczbą zespoloną taką, że $q^2 \in \mathbb{Z} + q\mathbb{Z}$. Wtedy zbiór $\mathbb{Z}[q] = \{a + bq \mid a, b \in \mathbb{Z}\}$ wraz ze zwykłymi działaniami dodawania i mnożenia jest dziedziną (ważnym elementem rozwiązania jest pokazanie, że jeśli $x, y \in \mathbb{Z}[q]$, to $x + y, xy \in \mathbb{Z}[q]$).

1.2.4. Niech R będzie takim pierścieniem, że $a^2 = a$ dla dowolnego $a \in R$. Udowodnić, że $a + a = 0$ dla dowolnego $a \in R$. Ponadto R jest dziedziną wtedy i tylko wtedy, gdy $R \simeq \mathbb{Z}_2$.

1.2.5. Udowodnić, że każda skończona dziedzina jest ciałem.

1.2.6. Niech R będzie pierścieniem z co najmniej dwoma elementami oraz takim, że dla każdego elementu $a \in R$, $a \neq 0$, istnieje jedyny element $b \in R$ taki, że $a^2 b = a$. Udowodnić, że R jest ciałem.

1.2.7. Udowodnić, że pierścień $\mathbb{Z}_m$ jest dziedziną wtedy i tylko wtedy, gdy m jest liczbą pierwszą.

1.2.8. *Charakterystyką pierścienia* R nazywamy najmniejszą liczbę całkowitą dodatnią n taką, że $na = 0$ dla wszystkich $a \in R$, jeśli taka liczba istnieje, lub 0 w przeciwnym wypadku. Charakterystykę pierścienia R oznaczamy $\operatorname{char} R$.

(a) Udowodnić, że charakterystyka pierścienia R jest najmniejszą liczbą całkowitą dodatnią n taką, $n1 = 0$, jeśli taka liczba istnieje, lub 0 w przeciwnym wypadku.
(b) Udowodnić, że $\operatorname{char} \mathbb{Z} = 0$ oraz $\operatorname{char} \mathbb{Z}_m = m$ dla dowolnej liczby całkowitej dodatniej m.
(c) Udowodnić, że jeśli R jest dziedziną i $\operatorname{char} R \neq 0$, to $\operatorname{char} R$ jest liczbą pierwszą.
(d) Udowodnić, że jeśli charakterystyka pierścienia R jest liczbą pierwszą p, to $(a + b)^p = a^p + b^p$ dla dowolnych $a, b \in R$.

1.2.9. Element a pierścienia R nazywamy *nilpotentnym*, jeśli istnieje liczba całkowita dodatnia n taka, że $a^n = 0$. Udowodnić, że jeśli elementy a i b są nilpotentne, to $a + b$ też jest elementem nilpotentnym.

1.2.10. Udowodnić, że jeśli w pierścieniu nie istnieje element a różny od 0 taki, że $a^2 = 0$, to w pierścieniu nie ma elementów nilpotentnych różnych od 0.

1.2.11. Udowodnij, że podzbiór I pierścienia R jest ideałem wtedy i tylko wtedy, gdy $I \neq \varnothing$, jeśli $a, b \in I$, to $a - b \in I$, oraz jeśli $a \in R$ i $b \in I$, to $ab \in I$.

1.2.12. Udowodnić, że pierścień R jest ciałem, wtedy i tylko wtedy, gdy 0 i R są jedynymi ideałami pierścienia R .

1.2.13. Udowodnić, że ideał trywialny jest ideałem pierwszym pierścienia R, wtedy i tylko wtedy, gdy R jest dziedziną.

1.2.14. Udowodnić, że $\mathbb{Z}$ jest dziedziną ideałów głównych.

1.2.15. Udowodnić, że wszystkie elementy nilpotentne pierścienia R tworzą ideał.

1.2.16. Niech I będzie ideałem pierścienia R. Udowodnić, że zbiór $J = \{a \in R \mid a^n \in I \text{ dla pewnego } n > 0\}$ jest ideałem.

1.2.17. Niech X będzie podzbiorem pierścienia R. Udowodnić, że zbiór $J = \{a \in R \mid ax = 0 \text{ dla każdego } x \in X\}$ jest ideałem.

1.2.18. Niech I', I'' będą ideałem pierścienia R takimi, że $I' \subset I''$. Udowodnić, że zbiór $J = \{a \in R \mid ab \in I' \text{ dla każdego } b \in I''\}$ jest ideałem pierścienia R.

1.2.19. Niech m będzie dodatnią liczbą całkowitą. Udowodnić, że funkcja $\mathbb{Z} \to \mathbb{Z}_m$ przyporządkowująca liczbie całkowitej n jej resztę z dzielenia przez m jest homomorfizmem pierścieni.

1.2.20. Udowodnić, że funkcja $\varphi : \mathbb{Z}_2 \to \mathbb{Z}_4$ dana wzorem $\varphi(k) = 2k$ jest homomorfizmem pierścieni. (Zauważmy, że $\varphi(1) = 2$).

1.2.21. Niech p będzie liczbą pierwszą oraz niech R będzie pierścieniem charakterystyki p. Udowodnić, że funkcja $R \ni a \mapsto a^p \in R$ jest homomorfizmem pierścieni.

1.2.22. Udowodnić, że jeśli $\varphi : R \to S$ jest epimorfizmem pierścieni, to $\varphi(1) = 1$.

1.2.23. Udowodnić, że jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni takim, że istnieje element odwracalny $a \in R$ taki, że $\varphi(a)$ jest elementem odwracalny, to $\varphi(1) = 1$ oraz $\varphi(b^{-1}) = \varphi(b)^{-1}$ dla każdego elementu odwracalnego $b \in R$.

1.2.24. Udowodnić, że jeśli R i S są dziedzinami oraz $\varphi : R \to S$ jest homomorfizmem pierścieni takim, że $\varphi(1) \neq 0$, to $\varphi(1) = 1$.

1.2.25. Udowodnić, że jeśli K i L są ciałami oraz $\varphi : K \to L$ jest homomorfizmem pierścieni takim, że $\varphi(1) \neq 0$, to φ jest monomorfizmem.

1.3. Teoria podzielności w dziedzinach całkowitości

Zgodnie z poczynioną na początku rozdziału zapowiedzią przedstawimy teraz abstrakcyjną wersję Zasadniczego Twierdzenia Arytmetyki. Przez cały paragraf będziemy zakładać, że R jest dziedziną.

1.3.1. Niech $a, b \in R$. Mówimy, że *element a dzieli element b*, jeśli istnieje element $c \in R$ taki, że $b = ac$. Piszemy wtedy $a \mid b$. Elementy a i b nazywamy *stowarzyszonymi*, jeśli $a \mid b$ i $b \mid a$. Jeśli elementy a i b są stowarzyszone, to piszemy $a \approx b$. Relacje podzielności oraz stowarzyszenia mają bezpośrednie przeniesienie na język ideałów generowanych przez odpowiednie elementy.

Stwierdzenie. *Niech R będzie dziedziną całkowitości.*

(1) *$a \mid b$ wtedy i tylko wtedy, gdy $(b) \subset (a)$.*
(2) *$a \approx b$ wtedy i tylko wtedy, gdy $(a) = (b)$.*
(3) *Element a jest odwracalny wtedy i tylko wtedy, gdy $a \mid c$ dla dowolnego $c \in R$.*

(4) *Element a jest odwracalny wtedy i tylko wtedy, gdy $(a) = R$.*
(5) *$\approx$ jest relacją równoważności.*
(6) *$a \approx b$ wtedy i tylko wtedy, gdy istnieje element odwracalny $c \in R$ taki, że $a = cb$.*

Dowód. Jest to bezpośrednia konsekwencja odpowiednich definicji oraz Stwierdzenia 1.2.5. □

1.3.2. Niech R będzie dziedziną całkowitości. Element $a \in R$ nazywamy *nierozkładalnym* jeśli $a \neq 0$, a nie jest elementem odwracalnym oraz jeśli z faktu, że $b \mid a$ wynika, że b jest elementem odwracalnym lub $b \approx a$. Innymi słowy, niezerowy i nieodwracalny element a pierścienia R jest nierozkładalny wtedy i tylko wtedy, gdy z równości $a = bc$ wynika, że $a \approx b$ lub $a \approx c$. Element $a \in R$ nazywamy *pierwszym* jeśli $a \neq 0$, a nie jest elementem odwracalnym oraz z faktu, że $a \mid bc$ wynika, że $a \mid b$ lub $a \mid c$. Zauważmy, że w pierścieniu $\mathbb{Z}$ element jest nierozkładalny, wtedy i tylko wtedy, gdy jest pierwszy, i wtedy i tylko wtedy, gdy jest postaci $\pm p$ dla pewnej liczby pierwszej p. Pierwsza cześć powyższej obserwacji wynika z bardziej ogólnego faktu, która jest częścią poniższego stwierdzenia.

Stwierdzenie. *Niech R będzie dziedziną całkowitości i $a \in R$, $a \neq 0$.*

(1) *Element a jest pierwszy wtedy i tylko wtedy, gdy ideał (a) jest pierwszy.*
(2) *Element a jest nierozkładalny wtedy i tylko wtedy, gdy ideał (a) jest maksymalny w zbiorze wszystkich właściwych ideałów głównych pierścienia R.*
(3) *Każdy element pierwszy jest nierozkładalny.*
(4) *Jeśli R jest dziedziną ideałów głównych, to każdy element nierozkładalny jest pierwszy.*
(5) *Element stowarzyszony z elementem pierwszym jest pierwszy.*
(6) *Element stowarzyszony z elementem nierozkładalnym jest nierozkładalny.*

Dowód. (1) Wynika bezpośrednio z odpowiednich definicji oraz Stwierdzenia 1.2.5.

(2) Przypuśćmy, że element a jest nierozkładalny. Wtedy $(a) \neq R$, gdyż element a nie jest odwracalny. Ponadto, jeśli $(a) \subset (b)$, to $b \mid a$, więc element b jest odwracalny i $(b) = R$, lub $b \approx a$ i $(b) = (a)$.

Załóżmy teraz, że ideał (a) jest maksymalny w zbiorze wszystkich właściwych ideałów głównych. Jeśli $b \mid a$, to $(a) \subset (b)$, a więc $(b) = (a)$ i $b \approx a$, lub $(b) = R$ i element b jest odwracalny.

(3) Przypuśćmy, że element a jest pierwszy oraz $b \mid a$. Wtedy $a = bc$ dla pewnego $c \in R$. W szczególności $a \mid bc$, skąd $a \mid b$ lub $a \mid c$. W pierwszym przypadku $a \approx b$. W drugim $a \approx c$, a więc b musi być elementem odwracalnym.

(4) Przypuśćmy, że element a jest nierozkładalny. Na mocy punktu (2) ideał (a) jest maksymalny w zbiorze wszystkich właściwych ideałów głównych. Ponieważ R jest dziedziną ideałów głównych, zatem (a) jest ideałem maksymalnym, a więc pierwszym, co kończy dowód wobec punktu (1).

(5), (6) Jest to natychmiastowa konsekwencja punktów (1) i (2) wykorzystująca własność, że jeśli $a \approx b$, to $(a) = (b)$. □

1.3.3. Następująca definicja opisuje sytuację, z którą mamy do czynienia w pierścieniu liczb całkowitych. Dziedzinę R nazywamy *dziedziną z jednoznacznością rozkładu*, jeśli:

(1) dla każdego niezerowego i nieodwracalnego elementu $a \in R$ istnieją nierozkładalne elementy $c_1, \ldots, c_n$ takie, że $a = c_1 \cdots c_n$,
(2) jeśli $c_1, \ldots, c_n, d_1, \ldots, d_m$ są elementami nierozkładalny mi oraz $c_1 \cdots c_n = d_1 \cdots d_m$, to $n = m$ oraz istnieje permutacja σ zbioru $\{1, \ldots, n\}$ taka, że $c_i \approx d_{\sigma(i)}$ dla każdego $i = 1, \ldots, n$.

Zauważmy w szczególności, że jeśli R jest dziedziną z jednoznacznością rozkładu, $a \in R$, $a \neq 0$, oraz $c_1, \ldots, c_m$ są parami niestowarzyszonymi elementami nierozkładalnymi pierścienia R takimi, że dla każdego elementu nierozkładalnego c pierścienia R takiego, że $c \mid a$, istnieje i takie, że $c \approx c_i$, to $a = bc_1^{k_1} \ldots c_m^{k_m}$ dla pewnego elementu odwracalnego b oraz pewnych nieujemnych liczb całkowitych $k_1, \ldots, k_m$.

Zauważmy, że jeśli R jest dziedziną z jednoznacznością rozkładu, to każdy element nierozkładalny jest pierwszy.

1.3.4. Naszym celem będzie udowodnienie, że dziedziny ideałów głównych są dziedzinami z jednoznacznością rozkładu. Zauważmy, że na mocy Ćwiczenia 1.2.14 twierdzenie to będzie stanowiło uogólnienie Zasadniczego Twierdzenia Arytmetyki. Rozpoczniemy od następującej pomocniczej obserwacji.

LEMAT. *Niech R będzie dziedziną ideałów głównych. Jeśli a_1, a_2, ... są elementami pierścienia R takimi, że $(a_i) \subset (a_j)$ dla wszystkich $i \leq j$, to istnieje dodatnia liczba całkowita n taka, że $(a_i) = (a_n)$ dla wszystkich $i \geq n$.*

DOWÓD. Niech $I = \bigcup_{i=1}^{\infty}(a_i)$. Zauważmy, że I jest ideałem. Jedyną trudność stanowi uzasadnienie, że jeśli $x, y \in I$, to $x + y \in I$. Wiemy jednak, że w powyższej sytuacji istnieją i oraz j takie, że $x \in (a_i)$ i $y \in (a_j)$. Jeśli $i \leq j$, to $x \in (a_j)$, więc $x + y \in (a_j) \subset I$. Podobnie postępujemy, gdy $j \leq i$. Ponieważ R jest dziedziną ideałów głównych, więc istnieje element $a \in R$ taki, że $I = (a)$. Z definicji ideału I wynika, że istnieje dodatnia liczba całkowita n taka, że $a \in (a_n)$. Dla $i \geq n$ mamy wtedy ciąg inkluzji $I = (a) \subset (a_n) \subset (a_i) \subset I$, co kończy dowód. □

1.3.5. Udowodnimy teraz zapowiadane twierdzenie.

TWIERDZENIE. *Każda dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu.*

DOWÓD. Niech R będzie dziedziną ideałów głównych. Pokażemy najpierw, że każdy niezerowy i nieodwracalny element $a \in R$ ma przedstawienie w postaci iloczynu elementów nierozkładalnych. Niech S będzie zbiorem tych niezerowych i nieodwracalnych elementów pierścienia R, dla których takie przedstawienie nie istnieje. Zauważmy najpierw, że jeśli dla niezerowych i nieodwracalnych elementów b i c mamy $b, c \notin S$, to $bc \notin S$. Ponadto, jeśli $a \in S$, to istnieje element $d_a \in S$ taki, że $(a) \subset (d_a)$ oraz $(a) \neq (d_a)$. Istotnie, element a nie jest nierozkładalny, zatem istnieją elementy $b, c \in R$ takie, że $a = bc$ oraz $a \not\approx b$ i $a \not\approx c$. Oczywiście $b \neq 0$ i $c \neq 0$. Ponadto elementy b i c są nieodwracalne. Z powyższej uwagi wynika też, że $b \in S$ lub $c \in S$, więc możemy wziąć $d_a = b$ w pierwszym przypadku i $d_a = c$ w drugim przypadku. Z powyższej obserwacji wynika zatem, że jeśli $S \neq \varnothing$, to istnieje ciąg a_1, a_2, ... elementów zbioru S taki, że $(a_i) \subset (a_{i+1})$ oraz $(a_i) \neq (a_{i+1})$ dla $i \geq 1$. Przeczy to poprzedniemu lematowi, a więc mamy równość $S = \varnothing$, co kończy dowód pierwszej części twierdzenia.

Drugą część twierdzenia udowodnimy przez indukcję ze względu na $\min(n, m)$, przy czym bez straty ogólności możemy założyć, że $n \leq m$. Przypuśćmy najpierw, że $c = d_1 \cdots d_m$, $m \geq 1$, gdzie c, d_1, ..., d_m są nierozkładalne. Jeśli $m = 1$, to teza jest oczywista. Załóżmy zatem, że $m > 1$. Ponieważ R jest dziedziną ideałów głównych, więc na mocy Stwierdzenia 1.3.2(4) element c jest pierwszy. Stąd istnieje indeks $i \in \{1, \ldots, m\}$ taki, że $c \mid d_i$, a więc $c \approx d_i$, gdyż element d_i jest nierozkładalny. Bez straty ogólności możemy założyć, że $i = m$. Wtedy $c = ud_m$ dla pewnego elementu odwracalnego u, skąd $d_1 \cdots d_{m-1} = u$, co jest niemożliwe gdyż elementy d_1, ..., d_{m-1} są nieodwracalne.

Załóżmy teraz, że $n > 1$ oraz przypuśćmy, że elementy $c_1, \ldots, c_n, d_1, \ldots, d_m$ są nierozkładalne i $c_1 \cdots c_n = d_1 \cdots d_m$. Podobnie jak poprzednio możemy założyć, że $c_n = ud_m$ dla pewnego elementu odwracalnego u. Wtedy elementy $uc_1, c_2, \ldots, c_{n-1}, d_1, \ldots, d_{m-1}$ są nierozkładalne oraz $(uc_1)c_2 \cdots c_{n-1} = d_1 \cdots d_{m-1}$. Z założenia indukcyjnego wynika, że $n - 1 = m - 1$ oraz istnieje permutacja τ zbioru $\{1, \ldots, n-1\}$ taka, że $uc_1 \approx d_{\tau(1)}$ oraz $c_i \approx d_{\tau(i)}$, $i = 2, \ldots, n-1$. Wtedy permutacja σ zbioru $\{1, \ldots, n\}$ dana wzorem $\sigma(i) = \tau(i)$ dla $i \in \{1, \ldots, n-1\}$ oraz $\sigma(n) = m$, jest szukaną permutacją (zauważmy, że $c_1 \approx uc_1$). □

1.3.6. Bezpośrednie sprawdzanie, że dziedzina jest dziedziną ideałów głównych może być czasami pracochłonne. Dowód tego faktu w przypadku pierścienia liczb całkowitych po raz kolejny sugeruje, w jakich sytuacjach sprawdzenie tej własności nie powinno nastręczać kłopotów. Dziedzinę całkowitości R nazywamy *dziedziną pre-Euklidesa* jeśli istnieje funkcja $\varphi : R \setminus \{0\} \to \mathbb{Z}$ taka, że:

(1) $\varphi(a) \geq 0$ dla wszystkich $a \in R$, $a \neq 0$,
(2) jeśli $a, b \in R$ oraz $b \neq 0$, to istnieją elementy $q, r \in R$ takie, że $a = qb + r$ oraz $r = 0$ lub $\varphi(r) < \varphi(b)$.

Jeśli dodatkowo, $\varphi(a) \leq \varphi(ab)$ dla wszystkich $a, b \in R$, $a, b \neq 0$, to mówimy, że R jest *dziedziną Euklidesa*. Zauważmy, że $\mathbb{Z}$ jest dziedziną Euklidesa z funkcją $\varphi(n) = |n|$. Innych przykładów dziedzin Euklidesa dostarcza Ćwiczenie 1.3.5 oraz Wniosek 1.5.1.

Twierdzenie. *Jeśli R jest dziedziną pre-Euklidesa, to R jest dziedziną ideałów głównych.*

Dowód. Niech I będzie ideałem w R. Możemy założyć, że $I \neq 0$. Niech $a \in I$ będzie takim elementem, że $\varphi(a) = \min\{\varphi(b) \mid b \in I, b \neq 0\}$. Jeśli $b \in I$, to istnieją elementy $q, r \in R$ takie, że $b = qa + r$ oraz $r = 0$ lub $\varphi(r) < \varphi(a)$. Ponieważ $r \in I$, więc z wyboru elementy a wynika, że $r = 0$, a więc $b \in Ra = (a)$. Stąd $I = (a)$, co kończy dowód. □

Natychmiastową konsekwencją powyższego twierdzenia oraz Twierdzenia 1.3.5 jest następujący fakt.

Wniosek. *Jeśli R jest dziedziną pre-Euklidesa, to R jest dziedziną z jednoznacznością rozkładu.* □

1.3.7. Na zakończenie tego paragrafu wprowadzimy pojęcie największego wspólnego dzielnika. Niech $a_1, \ldots a_n \in R$. Element $d \in R$ nazywamy *największym wspólnym dzielnikiem elementów $a_1, \ldots, a_n$*, jeśli

(1) $d \mid a_i$ dla wszystkich $i = 1, \ldots, n$, oraz
(2) jeśli $c \mid a_i$ dla wszystkich $i = 1, \ldots, n$, to $c \mid d$.

Zauważmy, że największy wspólny dzielnik, jeśli istnieje, jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia. Z tego powodu fakt, że d jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_n$ zapisujemy $\gcd(a_1, \ldots, a_n) \approx d$. Z drugiej strony, jeśli $a_1 \approx b_1$, $\ldots$, $a_n \approx b_n$, to $\gcd(a_1, \ldots, a_n) \approx \gcd(b_1, \ldots, b_n)$. Formalnie więc operację brania największego wspólnego dzielnika należałoby zdefiniować w zbiorze klas abstrakcji pierścienia R względem relacji $\approx$.

Dla przykładu $\gcd(a, a) \approx a$, $\gcd(1, a) \approx 1$ oraz $\gcd(0, a) \approx a$ dla dowolnego $a \in R$. Łatwo zauważyć, że operacja brania największego wspólnego dzielnika jest łączna, tzn.

$$\gcd(\gcd(a_{1,1}, \ldots, a_{1,i_1}), \ldots, \gcd(a_{j,1}, \ldots, a_{j,i_j})) \approx \gcd(a_{1,1}, \ldots, a_{1,i_1}, \ldots, a_{j,1}, \ldots, a_{j,i_j})$$

dla dowolnych $a_{1,1}, \ldots, a_{1,i_1}, \ldots, a_{j,1}, \ldots, a_{j,i_j} \in R$. Elementy $a_1, \ldots, a_n$ pierścienia z jedynką R nazywamy *względnie pierwszymi*, jeśli 1 jest ich największym wspólnym dzielnikiem.

W przyszłości przydatne będą następujące mniej elementarne własności operacji gcd.

TWIERDZENIE.

(1) *Jeśli R jest dziedziną z jednoznacznością rozkładu, to dla dowolnych elementów $a_1, \ldots, a_n$ pierścienia R istnieje największy wspólny dzielnik.*

(2) *Jeśli dodatkowo R jest dziedziną ideałów głównych, to d jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_n$ wtedy i tylko wtedy, gdy $(d) = (a_1) + \cdots + (a_n)$. W szczególności, jeśli $d \approx \gcd(a_1, \ldots, a_n)$, to istnieją elementy $r_1, \ldots, r_n \in R$ takie, że $d = r_1 a_1 + \cdots + r_n a_n$.*

DOWÓD. (1) Bez straty ogólności możemy założyć, że elementy $a_1, \ldots, a_n$ są niezerowe. Jeśli $a_i = b_i c_1^{k_{i,1}} \cdots c_m^{k_{i,m}}$ jest przedstawieniem elementu a_i jako iloczynu elementu odwracalnego b_i oraz potęg parami niestowarzyszonych elementów nierozkładalnych $c_1, \ldots, c_m$ (dopuszczamy możliwość $k_{i,j} = 0$), to

$$\gcd(a_1, \ldots, a_n) \approx c_1^{k_1} \cdots c_m^{k_m},$$

gdzie $k_j = \min(k_{1,j}, \ldots, k_{n,j})$.

(2) Wynika bezpośrednio z odpowiednich definicji. □

Wykorzystując wzór na największy wspólny dzielnik dwóch elementów zawarty w powyższym dowodzie można pokazać, że jeśli R jest dziedziną z jednoznacznością rozkładu, $c \mid ab$ oraz $(a, c) \approx 1$, to $c \mid b$. Z powyższego wzoru wynika też, jeśli $c \in R$ oraz dla każdego i, $a_i = cb_i$ dla pewnego b_i, to $\gcd(a_1, \ldots, a_n) \approx c \gcd(b_1, \ldots, b_n)$.

Ćwiczenia

1.3.1. Udowodnić, że jeśli R jest dziedziną z jednoznacznością rozkładu, to każdy element pierwszy dziedziny R jest nierozkładalny.

1.3.2. Udowodnić, że dziedzina R jest dziedziną z jednoznacznością rozkładu wtedy i tylko wtedy, gdy każdy niezerowy ideał pierwszy pierścienia R zawiera niezerowy ideał główny, który jest pierwszy.

1.3.3. Niech R będzie dziedziną ideałów głównych.

(a) Udowodnić, że każdy ideał pierwszy jest maksymalny.

(b) Ideał właściwy P pierścienia R nazywamy *prymarnym*, jeśli z faktu, że $ab \in P$ oraz $a \notin P$ wynika, że $b^n \in P$ dla pewnego $n > 0$. Udowodnić, że niezerowy ideał P jest prymarny wtedy i tylko wtedy, gdy istnieje liczba dodatnia n oraz element pierwszy p taki, że $P = (p^n)$.

(c) Udowodnić, że każdy ideał właściwy w R może być przedstawiony (jednoznacznie z dokładnością do porządku) jako przekrój skończonej ilości ideałów prymarnych.

1.3.4. Niech $R = \mathbb{Z}[\sqrt{10}]$ (patrz Ćwiczenie 1.2.3) oraz niech $N : R \to \mathbb{Z}$ dane będzie wzorem $N(a + b\sqrt{10}) = a^2 - 10b^2$ dla $a, b \in \mathbb{Z}$.

(a) Udowodnić, że $N(xy) = N(x)N(y)$ dla dowolnych $x, y \in R$ oraz $N(x) = 0$ wtedy i tylko wtedy, gdy $x = 0$.
(b) Udowodnić, że element $x \in R$ jest odwracalny wtedy i tylko wtedy, gdy $N(x) = \pm 1$.
(c) Udowodnić, że elementy 2, 3, $4 + \sqrt{10}$, $4 - \sqrt{10}$ są nierozkładalne i parami niestowarzyszone, ale $2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$. W szczególności elementy te nie są pierwsze.
(d) Udowodnić, że każdy element w pierścieniu R może być przedstawiony w postaci iloczynu elementów nierozkładalnych.

1.3.5. Udowodnić, że pierścień $\mathbb{Z}[i]$ wraz z funkcją $a + bi \mapsto |a + bi|^2 = a^2 + b^2$ jest dziedziną Euklidesa. (*Wskazówka*: Niech $x, y \in \mathbb{Z}[i]$, $x \neq 0$ i $y\overline{x} = a + bi$. Istnieją liczby $c, d \in \mathbb{Z}$ takie, że $|a - c|x||, |b - d|x|| \leq \frac{1}{2}|x|$. Wtedy $|r| < |x|$ dla $r = y - qx$, gdzie $q = c + di$.)

1.3.6. Wyznaczyć wszystkie elementy odwracalne w pierścieniu $\mathbb{Z}[i]$.

1.3.7. Udowodnić, że $\mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ jest dziedziną ideałów głównych.

1.3.8. Udowodnić, że jeśli R jest dziedziną z jednoznacznością rozkładu oraz d jest niezerowym elementem pierścienia R, to istnieje skończenie wiele ideałów głównych zawierających ideał (d) (*Wskazówka*: Wykorzystać fakt, że jeśli $(d) \subset (c)$, to $c \mid d$).

1.3.9. Udowodnić, że jeśli R wraz z funkcją φ jest dziedziną Euklidesa, to element $a \in R$ jest odwracalny wtedy i tylko wtedy, gdy $\varphi(a) = \varphi(1)$.

1.4. Pierścienie wielomianów oraz ciała ułamków

W tym paragrafie wprowadzimy formalizm związany z pierścieniami wielomianów. Ze względu na większą prostotę prezentacji rozpoczniemy od szczególnej sytuacji pierścienia wielomianów jednej zmiennej.

1.4.1. Niech R będzie pierścieniem. *Pierścieniem wielomianów jednej zmiennej nad R* nazywamy zbiór $R^{(\mathbb{N})}$ wszystkich ciągów o wyrazach z R takich, że tylko skończona ilość wyrazów ciągu jest różna od 0. Działania w zbiorze $R^{(\mathbb{N})}$ definiujemy wzorami

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots),$$
$$(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = (a_0 \cdot b_0, a_1 b_0 + a_0 b_1, \ldots, \sum_{k+l=m} a_k b_l, \ldots).$$

Jako ćwiczenie pozostawiamy sprawdzenie, że działania te są dobrze określone oraz że definiują w zbiorze $R^{(\mathbb{N})}$ strukturę pierścienia. Elementem neutralnym dla działania dodawania jest ciąg $(0, 0, \ldots)$, zaś dla mnożenia $(1, 0, 0, \ldots)$. Zauważmy, że jeśli R jest dziedziną, to $R^{(\mathbb{N})}$ też jest dziedziną.

Niech X oznacza element $(0, 1, 0, 0, \ldots)$ pierścienia $R^{(\mathbb{N})}$. Prosta indukcja pokazuje, że $X^n = (0, \ldots, 0, 1, 0, 0, \ldots)$, gdzie 1 pojawia się na

$n+1$ miejscu, dla dowolnej nieujemnej liczby całkowitej n. Zauważmy, że funkcja

$$R \ni r \mapsto (r, 0, 0, \ldots) \in R^{(\mathbb{N})}$$

jest monomorfizmem pierścieni, w związku z czym dla dowolnego elementu a pierścienia R ciąg $(a, 0, 0, \ldots)$ będziemy oznaczać przez a. Łatwo sprawdzić, że $aX^n = (0, \ldots, 0, a, 0, 0, \ldots)$, gdzie ponownie a występuje na $n+1$ miejscu. W konsekwencji każdy wielomian można przedstawić w postaci $a_0 + a_1X + \cdots + a_nX^n$ dla pewnych elementów a_0, $\ldots$, a_n pierścienia R oraz liczby całkowitej nieujemnej n. Jeśli założymy, że $a_n \neq 0$ (w szczególności $f \neq 0$), to powyższe przedstawienie jest jednoznaczne. W związku z powyższym, jeśli R jest pierścieniem z jedynką, to przez $R[X]$ oznaczać będziemy pierścień wielomianów jednej zmiennej nad R, w którym ciąg $(0, 1, 0, 0, \ldots)$ oznaczony został przez X.

Niech R będzie pierścieniem i $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Jeśli $a_n \neq 0$, to n nazywamy *stopniem wielomianu* f i oznaczamy $\deg f$, elementy a_0, $\ldots$, a_n nazywamy *współczynnikami wielomianu* f, a_n *współczynnikiem wiodącym wielomianu* f, zaś a_0 *wyrazem wolnym*. W przypadku, gdy $f = 0$, to $\deg f = -\infty$. Wielomiany stopnia nie większego niż 0 nazywamy *wielomianami stałymi*. Łatwo sprawdzić, że $\deg(f+g) \leq \max(\deg f, \deg g)$ i $\deg(fg) \leq \deg f + \deg g$. Jeśli dodatkowo założymy, że R jest dziedziną, to ostatnia nierówność jest równością. Niezerowy wielomian, którego współczynnik wiodący jest równy 1, nazywamy nazywamy *wielomianem unormowanym*.

1.4.2. Niech R będzie pierścieniem oraz niech n będzie dodatnią liczbą całkowitą. Podobnie jak powyżej definiujemy *pierścień wielomianów n-zmiennych nad R* jako zbiór $R^{(\mathbb{N}^n)}$ wszystkich funkcji $f : \mathbb{N}^n \to R$ takich, że $f(u) \neq 0$ dla skończenie wielu u, z działaniami zdefiniowanymi wzorami

$$(f+g)(u) = f(u) + g(u),$$
$$(f \cdot g)(u) = \sum_{v+w=u} f(v)g(w).$$

Elementem neutralnym dla dodawania jest funkcja $0 : \mathbb{N}^n \to R$ dana wzorem $0(u) = 0$ dla każdego u, zaś elementem neutralnym dla mnożenia funkcja $1 : \mathbb{N}^n \to R$ dana wzorem

$$1(u) = \begin{cases} 1 & u = (0, \ldots, 0), \\ 0 & u \neq (0, \ldots, 0). \end{cases}$$

Podobnie jak powyżej funkcja $R \to R^{(\mathbb{N}^n)}$, $a \mapsto f_a$, gdzie

$$f_a(u) = \begin{cases} a & u = (0, \ldots, 0), \\ 0 & u \neq (0, \ldots, 0), \end{cases}$$

jest monomorfizmem pierścieni, w związku z czym będziemy pisać a zamiast f_a.

Dla $i = 1, \dots, n$ niech $X_i : \mathbb{N}^n \to R$ będzie funkcją daną wzorem

$$X_i(u) = \begin{cases} 1 & u = (0, \dots, 0, \underbrace{1}_{i\text{-te miejsce}}, 0, \dots, 0), \\ 0 & \text{w przeciwnym wypadku.} \end{cases}$$

W powyższej sytuacji pierścień wielomianów n-zmiennych nad R oznaczamy przez $R[X_1, \dots, X_n]$. Jeśli R jest dziedziną, to $R[X_1, \dots, X_n]$ też jest dziedziną. Jeśli $f \in R[X_1, \dots, X_n]$, to

$$f = \sum_{(u_1,\dots,u_n)\in\mathbb{N}^n} a_{u_1,\dots,u_n} X_1^{u_1} \cdots X_n^{u_n}.$$

dla pewnych $a_{u_1,\dots,u_n} \in R$. Elementy $a_{u_1,\dots,u_n}$ nazywamy *współczynnikami wielomianu f*. *Stopniem wielomianu f* nazywamy $\max\{u_1 + \cdots u_n \mid (u_1, \dots, u_n) \in \mathbb{N}^n, a_{u_1,\dots,u_n} \neq 0\}$, lub $-\infty$ gdy $f = 0$. Stopień wielomianu f oznaczamy $\deg f$. Ponownie $\deg(f + g) \leq \max(\deg f, \deg g)$, $\deg(fg) \leq \deg f + \deg g$, oraz jeśli R jest dziedziną, to $\deg(fg) = \deg f + \deg g$. Wielomiany postaci $aX_1^{v_1} \cdots X_n^{v_n}$ dla $a \in R$, $a \neq 0$, nazywamy *jednomianami*.

1.4.3. Ważną własnością pierścieni wielomianów jest możliwość definiowania ich etapami, a mianowicie bezpośrednio z definicji można pokazać, że pierścienie

$$R[X_1] \cdots [X_n] \text{ oraz } R[X_1, \dots, X_n]$$

są izomorficzne.

Inną cechę pierścieni wielomianów opisuje poniższe stwierdzenie.

Stwierdzenie. *Jeśli R jest pierścieniem, $\varphi : R \to S$ jest homomorfizmem pierścieni oraz $s_1, \dots, s_n \in S$, to istnieje jedyny homomorfizm pierścieni $\phi : R[X_1, \dots, X_n] \to S$ taki, że $\phi(r) = \varphi(r)$ dla wszystkich $r \in R$ oraz $\phi(X_i) = s_i$ dla wszystkich $i = 1, \dots, n$.*

Homomorfizm ϕ, o którym mowa w powyższym stwierdzeniu nazywamy *podstawieniem $s_1, \dots, s_n$ za $X_1, \dots, X_n$*. Powyższa własność charakteryzuje jednoznacznie pierścień wielomianów n zmiennych (patrz Ćwiczenie 1.4.1). Szczególny i najczęściej stosowany przypadek to sytuacja, gdy $\varphi = \mathbb{1}_R$. W tej sytuacji piszemy $f(s_1, \dots, s_n)$ (lub $f(s)$, gdy $s = (s_1, \dots, s_n)$) zamiast $\phi(f)$ dla $f \in R$.

Dowód. Łatwo sprawdzić, że szukany homomorfizm musi i jest zdefiniowany wzorem

$$\phi(\sum a_{u_1,\dots,u_n} X_1^{u_1} \cdots X_n^{u_n}) = \sum \varphi(a_{u_1,\dots,u_n}) s_1^{u_1} \cdots s_n^{u_n}. \qquad \square$$

1.4.4. Uogólnimy teraz na przypadek dowolnej dziedziny znaną konstrukcję ciała liczb wymiernych z pierścienia liczb całkowitych. W tym celu wprowadzimy najpierw pojęcia kongruencji oraz struktury ilorazowej. Niech R będzie półpierścieniem, tzn. zbiorem z dwoma działaniami $+$ i $\cdot$, który jest monoidem ze względu na każde z tych działań i w którym zachodzi prawo rozdzielności. *Kongruencją w półpierścieniu* R nazywamy każdą relację równoważności $\sim$ taką, że

$$\text{jeśli } a \sim b, c \sim d, \text{ to } a + c \sim b + d, ac \sim bd.$$

Zauważmy, że z warunków tych wynika, że jeśli R jest pierścieniem oraz $a \sim b$, to $-a \sim -b$. Istotnie, jeśli $a \sim b$, to otrzymujemy, że $0 \sim b - a$, ponieważ $-a \sim -a$. Wykorzystując teraz fakt, że $-b \sim -b$ otrzymujemy, że $-b \sim -a$. Podobnie, jeśli R jest pierścieniem, a i b są elementami odwracalnymi oraz $a \sim b$, to $a^{-1} \sim b^{-1}$. Nie musi być natomiast prawdą, że jeśli element a jest odwracalny oraz $a \sim b$, to element b też jest odwracalny. Trywialnymi przykładami kongruencji są relacja równości oraz relacja totalna $R \times R$ utożsamiająca wszystkie elementy. Innym przykładem kongruencji jest relacja $\equiv_m$ przystawania modulo m w pierścieniu liczb całkowitych. Więcej informacji na temat kongruencji, w szczególności ich związek z ideałami pierścienia, będzie podanych w paragrafie 1.6.

Niech $\sim$ będzie relacją kongruencji w półpierścieniu R. W zbiorze klas abstrakcji $R/\sim$ definiujemy działania dodawania i mnożenia wzorami

$$[a]_\sim + [b]_\sim = [a+b]_\sim$$
$$[a]_\sim [b]_\sim = [ab]_\sim.$$

Łatwo sprawdzić, że działania te są poprawnie określone oraz zbiór $R/\sim$ wraz z tymi działaniami jest półpierścieniem, który nazywamy *półpierścieniem ilorazowym pierścienia R względem relacji $\sim$*. Elementem neutralnym dla dodawania jest $[0]_\sim$, zaś elementem neutralnym dla mnożenia jest $[1]_\sim$. Gdy dodatkowo R jest pierścieniem, to $R/\sim$ też jest pierścienie oraz elementem przeciwnym do $[a]_\sim$ jest $[-a]_\sim$. Dla przykładu mamy, że $R/ =\simeq R$ oraz $R/R \times R \simeq 0$. Ponadto $\mathbb{Z}/\equiv_m \simeq \mathbb{Z}_m$. Zauważmy, że funkcja

$$R \ni a \to [a]_\sim \in R/\sim$$

jest epimorfizmem pierścieni, który nazywamy *naturalnym rzutowaniem*.

1.4.5. Niech R będzie dziedziną. Niech S będzie zbiorem wszystkich par (a, b) takich, że $a, b \in R$ oraz $b \neq 0$. Elementy zbioru S nazywamy *ułamkami* oraz zapisujemy $\frac{a}{b}$. W zbiorze S wprowadzamy

działania dodawania i mnożenia wzorami

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},$$
$$\frac{a}{b}\frac{c}{d}=\frac{ac}{bd}.$$

Ponieważ R jest dziedziną, więc działania te są poprawie określone. Łatwo sprawdzić, że określają one w S strukturę dziedziny z elementami neutralnymi $\frac{0}{1}$ oraz $\frac{1}{1}$.

Niech $\sim$ będzie relacją w zbiorze S daną wzorem

$$\frac{a}{b}\sim\frac{c}{d} \text{ wtedy i tylko wtedy, gdy } ad=bc.$$

Łatwo sprawdzić, że relacja $\sim$ jest kongruencją, oraz że pierścień ilorazowy $S/\sim$ jest ciałem, które nazywamy *ciałem ułamków dziedziny* R. Elementy pierścienia $S/\sim$ będziemy oznaczać $\frac{a}{b}$ zamiast $[\frac{a}{b}]_\sim$, ale należy pamiętać, że są one klasami abstrakcji, a więc na przykład funkcja „mianownika" $S/\sim\ \frac{a}{b}\mapsto a\in R$ nie jest poprawnie określona. Zauważmy, że funkcja

$$R\ni a\mapsto\frac{a}{1}\in S/\sim$$

jest monomorfizmem pierścieni, który jest izomorfizmem, gdy R jest ciałem. Powyższy monomorfizm pozwala nam utożsamiać element $a\in R$ z elementem $\frac{a}{1}$ ciała ułamków oraz mówić, że „ciało ułamków zawiera dziedzinę R". Ćwiczenie 1.4.3 pokazuje, że ciało ułamków jest najmniejszym ciałem o tej własności. Inną charakteryzację ciała ułamków przedstawia Ćwiczenie 1.4.4

Ćwiczenia

1.4.1. Niech R będzie pierścieniem oraz niech $\psi:R\to R'$ będzie homomorfizmem pierścieni. Jeśli istnieją elementy $x_1,\ldots,x_n\in R'$ takie, że dla każdego homomorfizmu pierścieni $\varphi:R\to S$ oraz elementów $s_1,\ldots,s_n\in S$ istnieje dokładnie jeden homomorfizm $\phi:R'\to S$ taki, że $\varphi=\phi\psi$ oraz $\phi(x_i)=s_i$ dla wszystkich i, to $R'\simeq R[X_1,\ldots,X_n]$.

1.4.2. Niech R będzie pierścieniem. Jeśli $a_nX^n+\ldots+a_0$ jest dzielnikiem zera w $R[X]$, to istnieje niezerowy element $b\in R$ taki, że $ba_i=0$ dla wszystkich i.

1.4.3. Niech R będzie dziedziną, niech K będzie ciałem ułamków dziedziny R, niech L będzie ciałem oraz niech $\varphi:R\to L$ będzie monomorfizmem pierścieni. Udowodnić, że istnieje jedyny monomorfizm $\psi:K\to L$ taki, że $\psi(\frac{r}{1})=\varphi(r)$ dla wszystkich $r\in R$.

1.4.4. Niech R i K będą dziedzinami oraz niech $\psi:R\to K$ będzie homomorfizmem pierścieni takim, że $\psi(r)$ jest elementem odwracalnym dla każdego $r\in R$. Udowodnić, że jeśli dla każdej dziedziny S oraz każdego homomorfizmu pierścieni $\varphi:R\to S$ takiego, że $\varphi(r)$ jest elementem odwracalnym w S, istnieje dokładnie jeden homomorfizm $\phi:K\to S$ taki, że $\varphi=\phi\psi$, to dziedzina K jest izomorficzna z ciałem ułamków dziedziny R.

1.4.5. Niech R i S będą dziedzinami oraz niech K będzie ciałem ułamków dziedziny R. Jeśli istnieją monomorfizmy pierścieni $R \to S$ i $S \to K$, to ciało ułamków dziedziny S jest izomorficzne z K.

1.4.6. Pierścień R nazywamy lokalnym, jeśli posiada dokładnie jeden ideał maksymalny. Udowodnić, że R jest pierścieniem lokalnym wtedy i tylko wtedy, gdy wszystkie elementy nierozkładalne pierścienia R tworzą ideał.

1.4.7. Udowodnić, że pierścień R w którym $0 \neq 1$ jest lokalny wtedy i tylko wtedy, gdy z warunku $a + b = 1$ wynika, że jeden z elementów a lub b jest odwracalny.

1.4.8. Udowodnić, że jeśli $\varphi : R \to S$ jest epimorfizmem pierścieni oraz pierścień R jest lokalny, to S też jest pierścieniem lokalnym.

1.4.9. Niech R będzie dziedziną oraz niech K będzie ciałem ułamków dziedziny R. Dla ideału pierwszego P niech $R_P = \{\frac{a}{b} \in K \mid b \in P\}$ (bardziej precyzyjnie, R_P jest zbiorem tych $x \in K$ dla istnieje przedstawienie w postaci ułamka $\frac{a}{b}$ z $b \in P$). Udowodnić, że R_P jest pierścieniem lokalnym.

1.4.10. Niech R będzie dziedziną oraz niech K będzie ciałem ułamków dziedziny R. Udowodnić, że jeśli utożsamimy R z podzbiorem $\{\frac{a}{1} \mid a \in R$, to $R = \bigcap_{M \text{ ideał maksymalny}} R_M$.

1.5. Teoria podzielności w pierścieniach wielomianów

Cytowane na początku rozdziału twierdzenie o strukturze wielomianów nad ciałem liczb rzeczywistych można zawrzeć w zdaniu, że $\mathbb{R}[X]$ jest dziedziną z jednoznacznością rozkładu. Naszym celem w tym paragrafie będzie udowodnieniem uogólnienia tego faktu mówiącego, że jeśli R jest dziedziną z jednoznacznością rozkładu, to $R[X_1, \ldots, X_n]$ też jest dziedziną z jednoznacznością rozkładu. Ze względu na indukcyjny charakter tego procesu dużo uwagi poświęcimy rozważaniom dotyczącym wielomianów jednej zmiennej.

1.5.1. Następujący fakt, zwany algorytmem dzielenia, ma kluczowe znaczenie przy badaniu podzielności wielomianów nad ciałem.

Twierdzenie. *Niech R będzie dziedziną oraz $f, g \in R[X]$. Jeśli $g \neq 0$ oraz współczynnik wiodący wielomianu g jest odwracalny w R, to istnieją jedyne wielomiany $q, r \in R[X]$ takie, że*

$$f = qg + r \text{ oraz } \deg r < \deg g.$$

Zauważmy, że jeśli $g = X - c$, $c \in R$, to $r = f(c)$. Istotnie, warunek $\deg r < \deg g$ implikuje, że r jest wielomianem stałym, a więc $r = r(c) = f(c) - q(c)g(c) = f(c)$, gdyż $g(c) = 0$.

Dowód. Dowód istnienia wielomianów q i r będzie indukcyjny ze względu na $\deg f$. Jeśli $\deg f < \deg g$, to wystarczy wziąć $q = 0$ i $r = f$. Załóżmy teraz, że $n = \deg f \geq \deg g = m$ oraz niech a i b będą współczynnikami wiodącymi wielomianów f i g odpowiednio. Ponieważ b jest elementem odwracalnym, więc istnieje element $c \in R$ taki, że $a =$

bc. Wtedy $h = f - cX^{n-m}g$ jest wielomianem stopnia mniejszego niż f, więc na mocy założenia indukcyjnego istnieją wielomiany $p, r \in R[X]$ takie, że $h = pg + r$ i $\deg r < \deg g$. Łatwo sprawdzić, że wielomiany $q = cX^{n-m} + p$ oraz r maja żądane własności.

Dla dowodu jednoznaczności załóżmy, że $q_1 g + r_1 = q_2 g + r_2$ dla pewnych wielomianów $q_1, q_2, r_1, r_2 \in R[X]$ takich, że $\deg r_1, \deg r_2 < \deg g$. Wtedy $(q_1 - q_2)g = r_2 - r_1$, więc $\deg(q_1 - q_2) + \deg g = \deg(r_2 - r_1) < \deg g$, skąd $\deg(q_1 - q_2) = -\infty$, tzn. $q_1 = q_2$, zatem także $r_1 = r_2$. □

Ważną konsekwencją powyższego twierdzenia jest następujący fakt.

Wniosek. *Jeśli K jest ciałem, to $K[X]$ jest dziedziną Euklidesa. W szczególności, $K[X]$ jest dziedziną ideałów głównych oraz dziedziną z jednoznacznością rozkładu. Wielomian $f \in K[X]$ jest odwracalny wtedy i tylko wtedy, gdy f jest niezerowym wielomianem stałym.*

Dowód. Z poprzedniego twierdzenia wynika natychmiast, że $K[X]$ wraz z funkcja $f \mapsto \deg f$ jest dziedziną Euklidesa. Druga część twierdzenia jest konsekwencją równości $\deg(fg) = \deg(f) + \deg(g)$. □

1.5.2. Nie jest prawdą, że pierścień wielomianów n zmiennej nad ciałem jest pierścieniem ideałów głównych, gdy $n > 1$ (patrz Ćwiczenie 1.5.1). Zatem dowód zapowiadanego twierdzenia w tym przypadku musi korzystać z innych technik. Najpierw jednak zbadamy dokładniej czynniki stopnia 1 w pierścieniu wielomianów jednej zmiennej. Przydatne do tego celu będzie pojęcie pierwiastka, które wprowadzimy w ogólnej sytuacji pierścienia wielomianów n zmiennych.

Niech R będzie dziedziną oraz $f \in R[X_1, \ldots, X_n]$. Element $c \in R^n$ nazywamy *pierwiastkiem wielomianu f*, jeśli $f(c) = 0$. Bezpośrednio z definicji oraz Twierdzenia 1.5.1 wynika, że jeśli $f \in R[X]$, to element $c \in R$ jest pierwiastkiem wielomianu f wtedy i tylko wtedy, gdy $X - c \mid f$.

Konsekwencją tej obserwacji jest następujący fakt.

Stwierdzenie. *Jeśli R jest dziedziną oraz $f \in R[X]$ jest niezerowym wielomianem stopnia n, to f ma co najwyżej n pierwiastków.*

Dowód. Niech $c_1, \ldots, c_m$ będą parami różnymi pierwiastkami wielomianu f. Przez indukcję ze względu m pokażemy, że $m \leq n$. Jeśli $m = 0$, to teza jest oczywista, załóżmy zatem, że $m > 0$. Z obserwacji poprzedzającej stwierdzenie wiemy, że istnieje wielomian g taki, że $f = (X - c_m)g$. Oczywiście $g \neq 0$. Ponieważ $0 = f(c_i) = g(c_i)(c_i - c_m)$, $c_i \neq c_m$ oraz R jest dziedziną, więc dla każdego $i = 1, \ldots, m-1$, c_i jest pierwiastkiem wielomianu g. Z założenia indukcyjnego wiemy, że $m - 1 \leq \deg g = n - 1$, co kończy dowód. □

1.5.3. Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K. Ponieważ pierścień R możemy traktować jako podzbiór ciała K, więc każdy wielomian jednej zmiennej nad R możemy traktować jako element pierścienia $K[X]$. Mamy następujące uogólnienie metody poszukiwania pierwiastków wymiernych dla wielomianów o współczynnikach całkowitych.

STWIERDZENIE. *Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K oraz $f \in R[X]$ niezerowym wielomianem. Niech a jest będzie współczynnikiem wiodącym wielomianu f oraz niech b będzie wyrazem wolnym wielomianu b. Jeśli $u = \frac{x}{y} \in K$ jest pierwiastkiem wielomianu f oraz $(x, y) = 1$, to $x \mid b$ oraz $y \mid a$.*

DOWÓD. Niech $n = \deg f$ oraz $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ (w szczególności $a_0 = b$ oraz $a_n = a$). Przy pomocy bezpośredniego rachunku można sprawdzić, że warunek $f(u) = 0$ implikuje, iż

$$ay^n = -x(a_n x^{n-1}y^0 + a_{n-1}x^{n-2}y^1 + \cdots + a_1 x^0 y^{n-1})$$

oraz

$$bx^n = -y(a_{n-1}x^{n-1}y^0 + a_{n-2}x^{n-2}y^1 + \cdots + a_0 x^0 y^{n-1}).$$

Pierwsza równość implikuje, że $x \mid ay^n$, co wobec warunku $(x, y) = 1$ oznacza, że $x \mid a$. Podobnie druga równość implikuje, że $y \mid b$. □

1.5.4. Niech R będzie dziedziną i $f \in R[X]$. Pierwiastek $c \in R$ nazywamy *m-krotnym*, jeśli $(X - c)^m \mid f$ i $(X - c)^{m+1} \nmid f$. Pierwiastki 1-krotne nazywamy *prostymi*, zaś pierwiastki m-krotne, dla $m \geq 2$, *wielokrotnymi*. Liczbę m nazywamy *krotnością pierwiastka*. Jeśli c nie jest pierwiastkiem wielomianu f, to będziemy też mówić, że c jest pierwiastkiem krotności 0.

Krotność pierwiastka można badać wykorzystując pochodną. Jeśli $f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$, to definiujemy $f' = na_n X^{n-1} + (n - 1)a_{n-1}X^{n-2} + \cdots + a_1$. Wielomian f' nazywamy *pochodną* wielomianu f. Łatwo sprawdzić, że $(f + g)' = f' + g'$ oraz $(fg)' = f'g + fg'$.

STWIERDZENIE. *Niech R będzie dziedziną oraz $f \in R[X]$.*

(1) *Element $c \in R$ jest pierwiastkiem wielokrotnym wielomianu f wtedy i tylko wtedy, gdy $f(c) = 0 = f'(c)$.*
(2) *Jeśli R jest ciałem i $(f, f') = 1$, to f nie ma pierwiastków wielokrotnych.*

DOWÓD. (1) Niech m będzie krotnością c jako pierwiastka wielomianu f. Wtedy $f = (X - c)^m g$ dla $g \in R[X]$ takiego, że $g(c) \neq 0$, więc $f' = m(X-c)^{m-1}g+(X-c)^m g'$. Łatwo sprawdzić, że gdy $m = 0$, to $f(c) \neq 0$, gdy $m = 1$, to $f(c) = 0$, ale $f'(c) \neq 0$, zaś gdy $m \geq 2$, to $f(c) = 0 = f'(c)$.

(2) Ponieważ $R[X]$ jest dziedziną ideałów głównych, więc na mocy Twierdzenia 1.3.7(2) wiemy, że istnieją wielomiany $g, h \in R[X]$ takie,

że $1 = gf + hf'$. Zatem jeśli $f(c) = 0$, to $1 = h(c)f'(c)$, więc $f'(c) \neq 0$, co kończy dowód na mocy poprzedniego punktu. □

1.5.5. Niech R będzie dziedziną z jednoznacznością rozkładu oraz $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$. Największy wspólny dzielnik współczynników $a_n, \ldots, a_0$ nazywamy *zawartością wielomianu* f oraz oznaczamy $C(f)$. Zauważmy, że zawartość wielomianu f jest wyznaczona z dokładnością do stowarzyszenia elementów w R oraz $C(f) \approx 0$ wtedy i tylko wtedy, gdy $f = 0$. Jeśli $a \in R$, to $C(af) \approx aC(f)$. Wielomian f nazywamy *prymitywnym*, gdy $C(f) \approx 1$. Każdy wielomian f możemy zapisać w postaci $f = C(f)g$, gdzie g jest wielomianem prymitywnym.

Lemat (Gauss). *Jeśli R jest dziedziną z jednoznacznością rozkładu oraz $f, g \in R[X]$, to $C(fg) \approx C(f)C(g)$. W szczególności, iloczyn wielomianów prymitywnych jest wielomianem prymitywnym.*

Dowód. Z uwagi poprzedzającej lemat wynika, że wystarczy pokazać, iż iloczyn wielomianów prymitywnych jest wielomianem prymitywnym. Niech $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0$ oraz $g = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_0$ będą wielomianami prymitywnymi, oraz niech $fg = c_{n+m}X^{n+m} + c_{n+m-1}X^{n+m-1} + \cdots + c_0$. Ustalmy nierozkładalny element $p \in R$. Z założenia prymitywności wielomianów f i g wynika, że istnieją nieujemne liczby całkowite s i t takie, że $p \mid a_i$ dla $i = 0, \ldots, s-1$, $p \nmid a_s$, $p \mid b_i$ dla $i = 0, \ldots, t-1$ i $p \nmid b_t$. Z bezpośredniego rachunku wynika, że $p \nmid c_{s+t}$, co wobec dowolności elementu p oznacza, że $C(fg) \approx 1$. □

1.5.6. Przypomnijmy (Wniosek 1.5.1), że jeśli K jest ciałem, to wielomian $f \in K[X]$ jest odwracalny wtedy i tylko wtedy, gdy $f \in K$ (tzn. f jest wielomianem stałym) oraz $f \neq 0$. Ogólniej, jeśli R jest dziedziną, to wielomian $f \in R[X]$ jest elementem odwracalnym wtedy i tylko wtedy, gdy $f \in R$ oraz f jest odwracalny w R. Powyższa obserwacja będzie przydatna w dowodzie poniższego faktu.

Lemat. *Niech R będzie dziedziną z jednoznaczności rozkładu z ciałem ułamków K oraz $f, g \in R[X]$ będą wielomianami prymitywnymi. Wtedy wielomiany f i g są stowarzyszone w $R[X]$ wtedy i tylko wtedy, gdy są stowarzyszone w $K[X]$.*

Dowód. Z uwagi poprzedzającej lemat wynika, że jeśli wielomiany są stowarzyszone w $R[X]$, to są stowarzyszone w $K[X]$. Załóżmy teraz, że istnieje element odwracalny $u \in K[X]$ taki, że $f = ug$. Wiemy, że $u \in K$, więc $u = \frac{a}{b}$ dla niezerowych elementów $a, b \in R$. Wtedy $bf = ag$. Wykorzystując fakt, że $C(f)$ i $C(g)$ są elementami odwracalnymi otrzymujemy

$$b \approx bC(f) \approx C(bf) \approx C(ag) \approx aC(g) \approx a,$$

więc istnieje element odwracalny $v \in R$ taki, że $a = vb$. Wtedy $u = \frac{v}{1} = v$, co kończy dowód. □

1.5.7. Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K oraz niech $f \in K[X]$ będzie niezerowym wielomianem. Wtedy istnieją niezerowe elementy $a, b \in R$ oraz wielomian prymitywny $g \in R[X]$ takie, $bf = ag$. Istotnie, niech $f = \frac{a_n}{b_n}X^n + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + \cdots + \frac{a_0}{b_0}$. Jeśli $b = b_n b_{n-1} \cdots b_0$, to $bf \in R[X]$, zatem $bf = C(bf)g$ dla pewnego wielomianu prymitywnego $g \in R[X]$.

Powyższa uwaga będzie przydatna miedzy innymi w dowodzie poniższego faktu.

Lemat. *Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K oraz niech $f \in R[X]$ będzie wielomianem prymitywnym dodatniego stopnia. Wtedy wielomian f jest nierozkładalny w $R[X]$ wtedy i tylko wtedy, gdy jest nierozkładalny w $K[X]$.*

Dowód. Przypuśćmy najpierw, że wielomian $f \in R[X]$ jest prymitywny oraz nierozkładalny w $R[X]$. Gdyby $\deg f = 0$, to $f \approx C(f)$ byłby elementem odwracalnym w R, a więc także w $R[X]$, co jest niemożliwe. Zatem $\deg f > 0$ i wielomian f nie jest odwracalny w $K[X]$. Niech $f = gh$ dla $g, h \in K[X]$. Z uwagi poprzedzającej lemat wiemy, że istnieją niezerowe elementy $a, b, c, d \in R$ oraz wielomiany prymitywne $g_1, h_1 \in R[X]$ takie, że $bg = ag_1$ oraz $dh = ch_1$. Wtedy $bdf = acg_1h_1$, więc wykorzystując Lemat Gaussa oraz nasze założenia otrzymujemy, że

$$bd \approx C(bdf) \approx C(acg_1h_1) \approx ac.$$

Stąd wynika, że wielomiany f i g_1h_1 są stowarzyszone w $R[X]$. Ponieważ wielomian f jest nierozkładalny, więc albo $\deg g = \deg g_1 = 0$, a więc g jest elementem odwracalnym w $K[X]$, lub $\deg h = \deg h_1 = 0$, i h jest elementem odwracalnym w $K[X]$. W obu przypadkach otrzymujemy, że wielomian f jest nierozkładalny w $K[X]$.

Przypuśćmy teraz, że wielomian $f \in R[X]$ jest prymitywny oraz nierozkładalny w $K[X]$. Oczywiście wtedy $\deg f > 0$, więc wielomian f nie jest odwracalny w $R[X]$. Niech $f = gh$ dla $g, h \in R[X]$. Nierozkładalność wielomianu f w $K[X]$ implikuje, że $\deg g = 0$ lub $\deg h = 0$. Jeśli $\deg g = 0$, to $1 \approx C(f) \approx gC(h)$, więc g jest elementem odwracalnym w R, co oznacza, że wielomian f jest nierozkładalny w $R[X]$. Analogicznie rozumujemy, gdy $\deg h = 0$. □

1.5.8. Udowodnimy teraz zapowiadane twierdzenie.

Twierdzenie. *Jeśli R jest dziedziną z jednoznacznością rozkładu, to $R[X]$ też jest dziedziną z jednoznacznością rozkładu.*

Zauważmy, że powyższe twierdzenie implikuje natychmiast, że jeśli R jest dziedziną z jednoznacznością rozkładu oraz n jest dodatnią liczbą całkowitą, to $R[X_1, \ldots, X_n]$ też jest dziedziną z jednoznacznością

rozkładu. W szczególności, gdy K jest ciałem, to $K[X_1, \ldots, X_n]$ też jest dziedziną z jednoznacznością rozkładu.

Dowód. Niech $f \in R[X]$ będzie niezerowym elementem nieodwracalnym. Udowodnimy najpierw, że f może być przedstawiony w postaci iloczynu elementów nierozkładalnych w $R[X]$. Zauważmy najpierw, że $f = C(f)f_1$, gdzie f_1 jest wielomianem prymitywnym. Ponieważ R jest dziedziną z jednoznacznością rozkładu, więc $C(f)$ jest elementem odwracalnym w R lub może być przedstawiony w postaci iloczynu elementów nierozkładalnych w R. Ponieważ elementy odwracalne (odpowiednio, nierozkładalne) w R są odwracalne (nierozkładalne) w $R[X]$, więc możemy założyć, że f jest wielomianem prymitywnym. Niech K będzie ciałem ułamków dziedziny R. Z Wniosku 1.5.1 wiemy, że istnieją wielomiany $g_1, \ldots, g_n \in K[X]$ nierozkładalne w $K[X]$ takie, że $f = g_1 \cdots g_n$. Wiemy, że dla każdego $i = 1, \ldots, n$, istnieją niezerowe elementy $a_i, b_i \in R$ oraz wielomian prymitywny $h_i \in R[X]$ takie, że $b_i g_i = a_i h_i$. Wtedy $bf = ah_1 \cdots h_n$, gdzie $a = a_1 \cdots a_n$ oraz $b = b_1 \cdots b_n$. Z Lematu Gaussa oraz prymitywności wielomianów f, h_1, $\ldots$, h_n wynika, że $b \approx a$ w R, a co za tym idzie $f \approx h_1 \cdots h_n$ w $R[X]$. Dla zakończenia pierwszej części dowodu wystarczy zatem pokazać, że wielomiany h_1, $\ldots$, h_n są nierozkładalne w $R[X]$. Jest to konsekwencją poprzedniego lematu, gdyż dla każdego $i = 1, \ldots, n$, wielomiany g_i oraz h_i są stowarzyszone w $K[X]$.

Udowodnimy teraz jednoznaczność przedstawienia. Przypuśćmy, że $a_1, \ldots, a_m, b_1, \ldots, b_n, g_1, \ldots, g_k, h_1, \ldots, h_l \in R[X]$ są wielomianami nierozkładalnymi przy czym $\deg a_i = 0 = \deg b_j$ oraz $\deg g_i, \deg h_j > 0$. Nierozkładalność elementów a_1, $\ldots$, a_m, b_1, $\ldots$, b_n jako wielomianów implikuje ich nierozkładalność jako elementów dziedziny R, natomiast nierozkładalność wielomianów g_1, $\ldots$, g_k, h_1, $\ldots$, h_l implikuje ich prymitywność. Stąd elementy $a_1 \cdots a_m$ i $b_1 \cdots b_n$ są stowarzyszone w R, co implikuje, że $n = m$ oraz istnienie permutacji σ zbioru $\{1, \ldots, n\}$ takiej, że $a_i \approx b_{\sigma(i)}$, gdyż R jest dziedziną z jednoznacznością rozkładu. Analogicznie wielomiany $g_1 \cdots g_k$ i $h_1 \cdots h_l$ są stowarzyszone w $R[X]$, a więc także $K[X]$. Ponieważ wielomiany g_1, $\ldots$, g_k, h_1, $\ldots h_l$ są nierozkładalne w $K[X]$ na mocy poprzedniego lematu, więc korzystając ponownie z Wniosku 1.5.1 otrzymujemy, że $k = l$ oraz istnienie permutacji τ zbioru $\{1, \ldots, k\}$ takiej, że wielomiany g_i oraz $h_{\tau(i)}$ są stowarzyszone w $K[X]$. To kończy dowód wobec Lematu 1.5.6. □

1.5.9. Mamy następującą metodę testowania nierozkładalności wielomianów (przykłady zastosowania poniższego twierdzenia można znaleźć w Ćwiczeniach 1.5.7, 1.5.8 i 1.5.10).

Twierdzenie (Kryterium Eisenteina). *Niech R będzie dziedziną z jednoznacznością rozkładu oraz ciałem ułamków K i niech $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0 \in R[X]$ będzie wielomianem stopnia dodatniego.*

Jeśli istnieje element nierozkładalny $p \in R$ taki, że

$$p \nmid a_n,\ p \mid a_{n-1},\ \ldots, p \mid a_0, p^2 \nmid a_0,$$

to wielomian f jest nierozkładalny w $K[X]$. Jeśli dodatkowo wielomian f jest prymitywny, to jest nierozkładalny w $R[X]$.

Dowód. Wiemy, że $f = C(f)f_1$ dla pewnego wielomianu prymitywnego $f_1 \in R[X]$. Ponieważ $C(f)$ jest elementem odwracalnym w $K[X]$ oraz $p \nmid C(f)$ (gdyż $p \nmid a_n$), więc możemy założyć, że wielomian f jest prymitywny. Wobec Lematu 1.5.7 wystarczy udowodnić, że wielomian f jest nierozkładalny w $R[X]$.

Przypuśćmy, że $f = gh$ dla $g, h \in R[X]$. Na mocy Lematu Gaussa wiemy, że $C(f) \approx C(g)C(h)$, zatem wielomiany g i h są prymitywne. Niech $k = \deg g$, $l = \deg h$, $g = b_kX^k + b_{k-1}X^{k-1} + \cdots + b_0$ oraz $h = c_lX^l + c_{l-1}X^{l-1} + \cdots + c_0$. Ponieważ $a_0 = b_0c_0$, więc nasze założenia implikują, że $p \mid b_0$ lub $p \mid c_0$. Bez straty ogólności możemy założyć, że miejsce ma pierwsza możliwość. Ponieważ $p^2 \nmid a_0$, więc wtedy $p \nmid c_0$. Ponieważ wielomian g jest prymitywny, więc istnieje i takie, że $p \nmid b_i$. Niech $m = \min\{i \mid p \nmid b_i\}$. Ponieważ $a_m = b_mc_0 + b_{m-1}c_1 + \cdots + b_0c_m$, więc otrzymujemy, że $p \nmid a_m$, co oznacza, że $m = n$. W szczególności $k = n$ i $l = 0$. Ponieważ g jest wielomianem prymitywnym stopnia zero, jest to element odwracalny w $R[X]$, co kończy dowód. □

Ćwiczenia

1.5.1. Niech R będzie dziedziną. Jeśli w dziedzinie R istnieje element nierozkładalny, to $R[X]$ nie jest dziedziną ideałów głównych. (*Wskazówka*: Niech $a \in R$ będzie elementem nierozkładalnym. Wtedy ideał (X, c) nie jest główny w $R[X]$.) W szczególności dziedziny $\mathbb{Z}[X]$ oraz $K[X_1, \ldots, X_n]$, gdzie K jest ciałem oraz $n > 1$, nie są dziedzinami ideałów głównych.

1.5.2. Niech K będzie ciałem oraz $f, g \in K[X]$, przy czym $\deg g \geq 1$. Udowodnić, że istnieje liczba całkowita nieujemna r oraz wielomiany $f_0, \ldots, f_r \in K[X]$ takie, że $\deg f_i < \deg g$ dla każdego i oraz

$$f = f_0 + f_1g + \cdots + f_rg^r.$$

1.5.3. Niech R będzie dziedziną oraz niech $f \in R[X]$ będzie wielomianem stopnia dodatniego.

(a) Udowodnić, że jeśli $\operatorname{char} R = 0$, to $f' \neq 0$.
(b) Udowodnić, że jeśli $\operatorname{char} R = p$ dla liczby pierwszej p, to $f' = 0$ wtedy i tylko wtedy, gdy $f = g(X^p)$ dla pewnego $g \in R[X]$ (tzn. $f = a_nX^{np} + a_{n-1}X^{(n-1)p} + \cdots + a_0$ dla pewnych $a_n, a_{n-1}, \ldots, a_0 \in R$).

1.5.4. Niech R będzie pierścieniem oraz $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in R[X]$. Udowodnić, że f jest elementem odwracalnym w $R[X]$ wtedy i tylko wtedy, gdy a_0 jest elementem odwracalnym w R oraz $a_1, \ldots, a_n$ są elementami nilpotentnymi.

1.5.5. Niech p będzie liczbą pierwszą oraz niech $\varphi : \mathbb{Z}[X] \to \mathbb{Z}_p[X]$ będzie homomorfizmem indukowanym przez homomorfizm $\mathbb{Z} \to \mathbb{Z}_p$ opisany w Ćwiczeniu 1.2.19.

(a) Udowodnić, że jeśli $f \in \mathbb{Z}[X]$ jest wielomianem unormowanym oraz $\varphi(f)$ jest nierozkładalny w $\mathbb{Z}[X]$, to f jest nierozkładalny w $\mathbb{Z}[X]$.
(b) Znaleźć przykład nieunormowanego wielomianu $f \in \mathbb{Z}[X]$, dla którego powyższy fakt nie jest prawdziwy.

1.5.6. Niech $f = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$ będzie wielomianem stopnia n. Przypuśćmy, że istnieją liczba całkowita k oraz liczba pierwsza p takie $0 < k < n$, $p \nmid a_n$, $p \nmid a_k$, $p \mid a_{k-1}$, $\ldots$, $p \mid a_0$ oraz $p^2 \nmid a_0$. Udowodnić, że istnieje wielomian nierozkładalny w $\mathbb{Z}[X]$ stopnia co najmniej k, który dzieli f.

1.5.7. Udowodnić, że wielomian $2X^3 - 6X^2 + 9X - 15$ jest nierozkładalny w $\mathbb{Z}[X]$ i $\mathbb{Q}[X]$.

1.5.8. Niech R będzie dziedziną z jednoznacznością rozkładu. Udowodnić, że wielomian $Y^3 + X^2Y^2 + X^3Y + X$ jest nierozkładalny w $R[X, Y]$.

1.5.9. Niech R będzie dziedziną oraz $c \in R$. Udowodnić, że wielomian f jest nierozkładalny w $R[X]$ wtedy i tylko wtedy, gdy wielomian $f(X - c)$ jest nierozkładalny w $R[X]$.

1.5.10. Niech p będzie liczbą pierwszą. Udowodnić, że wielomian $f = X^{p-1} + X^{p-2} + \cdots + 1$ jest nierozkładalny w $\mathbb{Z}[X]$. (*Wskazówka*: Rozważyć wielomian $f(X + 1)$.)

1.5.11. Udowodnić, że jeśli $c_0, c_1, \ldots, c_n$ są parami różnymi elementami dziedziny R oraz $d_0, d_1, \ldots, d_n$ są elementami dziedziny R, to w $R[X]$ istnieje co najwyżej jeden wielomian f stopnia nie większego niż $n + 1$ taki, że $f(c_i) = d_i$ dla każdego i.

1.5.12. Niech K będzie ciałem. Udowodnić, że jeśli $c_0, c_1, \ldots, c_n$ są parami różnymi elementami ciała K oraz $d_0, d_1, \ldots, d_n$ są elementami ciała K, to wielomian

$$f = \sum_{i=0}^{n} \frac{(X - c_0) \cdots (X - c_{i-1})(X - c_{i+1}) \cdots (X - c_n)}{(c_i - c_0) \cdots (c_i - c_{i-1})(c_i - c_{i+1}) \cdots (c_n - c_n)} d_i$$

jest jedynym wielomianem stopnia nie większego niż $n + 1$ takim, że $f(c_i) = d_i$ dla wszystkich i.

1.5.13. Niech R będzie pierścieniem.

(a) Udowodnić, że dla dowolnych elementów $a, b \in R$ takich, że a jest elementem odwracalnym w R, przyporządkowanie $X \mapsto aX + b$ indukuje automorfizm pierścienia R, który jest identycznością na R. Znaleźć funkcję odwrotną.
(b) Udowodnić, że jeśli R jest dziedziną z jednoznacznością rozkładu, to każdy automorfizm pierścienia $R[X]$, który jest identycznością na R, ma postać opisaną w poprzednim punkcie.

1.5.14. Niech K będzie ciałem. Udowodnić, że jednomiany X i Y są względnie pierwsze w $K[X, Y]$, ale $(X) + (Y) \neq (1)$.

1.6. Twierdzenia o izomorfizmie

W tym paragrafie omówimy bardziej abstrakcyjne własności pierścieni. Jak zobaczymy w paragrafie 2.3 rozważania te przenoszą się bez wielkich zmian na inne sytuacje spotykane w algebrze.

1.6.1. Rozpoczniemy od omówienia związku między kongruencjami oraz ideałami. Jeśli $\sim$ jest kongruencją w pierścieniu R, to przez $I_\sim$ będziemy oznaczać $[0]_\sim$. Dla przykładu $I_= = 0$ oraz $I_{R\times R} = R$. Gdy $R = \mathbb{Z}$ oraz m jest dodatnią liczbą całkowitą, to $I_{\equiv_m} = \mathbb{Z}m$.

Podobnie, gdy I jest ideałem w pierścieniu R, to przez $\sim_I$ oznaczać będziemy relację w R zadaną przez warunek

$$a \sim_I b \text{ wtedy i tylko wtedy, gdy } a - b \in I.$$

Mamy $\sim_0 ==$, $\sim_R = R \times R$ oraz, gdy $R = \mathbb{Z}$, $\sim_{\mathbb{Z}m} = \equiv_m$. Powyższa zbieżność nie jest przypadkowa jak widać z poniższego stwierdzenia.

Stwierdzenie. *Niech R będzie pierścieniem.*

(1) *Jeśli $\sim$ jest kongruencją w pierścieniu R, to $I_\sim$ jest ideałem oraz $\sim_{I_\sim} = \sim$.*
(2) *Jeśli I jest ideałem pierścienia R, to $\sim_I$ jest kongruencją oraz $I_{\sim_I} = I$. Ponadto $[a]_{\sim_I} = a + I$.*

Dowód. Bezpośrednie sprawdzenie odpowiednich warunków. □

Niech I będzie ideałem pierścienia R. Definiujemy R/I jako $R/\sim_I$. Wobec powyższego stwierdzenia rozważania punktu 1.4.4 prowadzą natychmiast do wniosku, że wzory

$$(a + I) + (b + I) = (a + b) + I,$$
$$(a + I) \cdot (b + I) = ab + I,$$

zadają w R/I strukturę pierścienia. Pierścień R/I nazywamy *pierścieniem ilorazowym*. Przypomnijmy też, że odwzorowanie

$$R \ni a \mapsto a + I \in R/I$$

jest epimorfizmem pierścieni, które nazywamy *naturalnym rzutowaniem*. Wykorzystując pojęcie pierścienia ilorazowego można podać inne charakteryzacje ideałów pierwszych i maksymalnych (patrz Ćwiczenia 1.6.2 i 1.6.3).

Jeśli I jest ideałem pierścienia R, to dla ideału $J \subseteq R$ takiego, że $I \subseteq J$, przez J/I oznaczać będziemy zbiór $\{a + I \mid a \in J\} \subseteq R/I$. Łatwo sprawdzić, że J/I jest ideałem pierścienia R/I oraz, że przyporządkowanie $J \mapsto J/I$ jest zachowującą inkluzje bijekcją pomiędzy ideałami pierścienia R zawierającymi I oraz ideałami pierścienia R/I.

1.6.2. Oprócz ideałów ważną rolę w badaniu pierścieni odgrywają podpierścienie. Podzbiór S pierścienia R nazywamy podpierścieniem, jeśli jest pierścieniem ze względu na działania $+$ i $\cdot$ ograniczone do S, tzn. jeśli spełnione są następujące warunki:

(1) jeśli $a, b \in S$, to $a + b, ab \in S$,
(2) $0 \in S$ oraz jeśli $a \in S$, to $-a \in S$,
(3) istnieje element $e \in S$ taki, że $ea = a$ dla wszystkich $a \in S$.

Element e, o którym mowa w ostatnim warunku, nie musi się pokrywać z jedynką pierścienia R. Dla przykładu wszystkie inkluzje w poniższym ciągu są inkluzjami podpierścieni $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, ale na przykład $\mathbb{Z}_m$ nie jest podpierścieniem pierścienia $\mathbb{Z}$. Jeśli S jest podpierścieniem pierścienia R, to funkcja $a \ni S \mapsto a \in R$ jest monomorfizmem pierścieni, który nazywamy *naturalnym włożeniem.*

Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to zbiór $\operatorname{Im}\varphi = \{\varphi(a) \mid a \in R\}$ jest podpierścieniem pierścienia S. Oczywiście, φ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{Im}\varphi = R$. Z drugiej strony, gdy φ jest monomorfizmem, to indukowane odwzorowanie $R \to \operatorname{Im}\varphi$ jest izomorfizmem. Z uwagi tej korzystaliśmy konstruując zanurzenia pierścienia w pierścień wielomianów bądź dziedziny w pierścień ułamków. Oczywiście, gdy $\varphi : S \to R$ jest naturalnym włożeniem, to $\operatorname{Im}\varphi = S$.

Gdy $\varphi : R \to S$ jest homomorfizmem pierścieni, to zbiór $\operatorname{Ker}\varphi = \{a \in R \mid \varphi(a) = 0\}$ jest ideałem pierścienia R. Bezpośrednim rachunkiem można sprawdzić, że φ jest monomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = 0$. Zauważmy, że gdy $\pi : R \to R/I$ jest naturalnym rzutowaniem, to $\operatorname{Ker}\pi = I$.

1.6.3. Twierdzenia o izomorfizmie, które za chwilę sformułujemy, opierają się na następującej obserwacji.

Twierdzenie. *Niech $\varphi : R \to S$ będzie homomorfizmem pierścieni oraz niech I będzie ideałem pierścienia R takim, że $I \subseteq \operatorname{Ker}\varphi$. Wtedy odwzorowanie $\phi : R/I \to S$ dane wzorem*

$$\phi(a + I) = \varphi(a)$$

jest poprawnie określone oraz jest homomorfizmem. Ponadto $\operatorname{Ker}\phi = \operatorname{Ker}\varphi/I$ *i* $\operatorname{Im}\phi = \operatorname{Im}\varphi$.

Dowód. Bezpośredni rachunek. □

Bezpośrednią konsekwencją powyższego twierdzenia jest poniższy fakt.

Wniosek 1.6.3.1 (Pierwsze Twierdzenie o Izomorfizmie). *Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to funkcja*

$$R/\operatorname{Ker}\varphi \in a + \operatorname{Ker}\varphi \mapsto \varphi(a) \in \operatorname{Im}\varphi$$

jest poprawnie określona oraz jest izomorfizmem pierścieni.

Dowód. Zastosować powyższe twierdzenia dla $I = \operatorname{Ker}\varphi$. □

Przykładem zastosowanie Pierwszego Twierdzenia o Izomorfizmie jest izomorfizm pierścieni $\mathbb{Z}/\mathbb{Z}m$ oraz $\mathbb{Z}_m$. Inny przykład zastosowania tego twierdzenia można znaleźć w Ćwiczeniu 1.6.7.

Łatwo sprawdzić, jeśli S jest podpierścieniem pierścienia R oraz I jest ideałem pierścienia R, to $S \cap I$ jest ideałem pierścienia S. Ponadto, jeśli $1 \in S$, to $S + I$ jest podpierścieniem pierścienia R zawierającym ideał I.

Wniosek 1.6.3.2 (Drugie Twierdzenie o Izomorfizmie). *Jeśli R jest pierścieniem, S jest podpierścieniem pierścienia R oraz I jest ideałem pierścienia R takim, że $S + I$ też jest podpierścieniem pierścienia R, to funkcja*

$$S/(S \cap I) \ni a + (S \cap I) \mapsto a + I \in (S + I)/I$$

jest poprawnie określone oraz jest izomorfizmem pierścieni.

Dowód. Zastosować Pierwsze Twierdzenia o Izomorfizmie do homomorfizmu $S \to R/I$ będącego złożeniem naturalnego włożenia $S \to R$ oraz naturalnego rzutowania $R \to R/I$. □

Przykład zastosowania powyższego twierdzenia można znaleźć w Ćwiczeniu 1.6.8.

Wniosek 1.6.3.3 (Trzecie Twierdzenie o Izomofizmie). *Jeśli I i J są ideałami pierścienia R takimi, że $I \subseteq J$, to funkcja*

$$(R/I)/(J/I) \ni (a + I) + (J/I) \mapsto a + J \in R/J$$

poprawnie określona oraz jest izomorfizmem.

Dowód. Niech $\pi : R \to R/J$ będzie naturalnym rzutowaniem. Wiemy, że funkcja

$$R/I \ni a + I \mapsto a + J \in R/J$$

jest dobrze określona oraz jest homomorfizmem, którego jądrem jest J/I, zaś obrazem R/J. Wystarczy teraz skorzystać z Pierwszego Twierdzenia o Izomorfizmie. □

Ćwiczenia

1.6.1. Niech X będzie podzbiorem pierścienia R. Udowodnić, że istnieje najmniejszy podpierścień pierścienia R zawierający podzbiór X.

1.6.2. Niech R będzie pierścieniem. Udowodnić, że ideał I pierścienia R jest pierwszy wtedy i tylko wtedy, gdy pierścień R/I jest dziedziną.

1.6.3. Niech R będzie pierścieniem. Udowodnić, że ideał I pierścienia R jest maksymalny wtedy i tylko wtedy, gdy pierścień R/I jest ciałem.

1.6.4. Niech $\varphi : R \to S$ będzie homomorfizmem pierścieni. Udowodnić poniższe stwierdzenia.

(a) Jeśli T jest podpierścieniem pierścienia R, to $\varphi(T)$ jest podpierścieniem pierścienia S.

(b) Jeśli T jest podpierścieniem pierścienia S, to $\varphi^{-1}(T)$ jest podpierścieniem pierścienia R.
(c) Jeśli I jest ideałem pierścienia R oraz φ jest epimorfizmem, to $\varphi(I)$ jest ideałem pierścienia S.
(d) Jeśli I jest ideałem pierścienia S, to $\varphi^{-1}(I)$ jest ideałem pierścienia R.

1.6.5. Niech R będzie pierścieniem, w którym $0 \neq 1$. Udowodnić, że pierścień R posiada dokładnie jeden ideał pierwszy wtedy i tylko wtedy, gdy każdy element nieodwracalny jest nilpotentny.

1.6.6. Niech M będzie ideałem maksymalnym pierścienia R. Udowodnić, że pierścień R/M^n posiada dokładnie jeden ideał pierwszy.

1.6.7. Niech K będzie ciałem. Udowodnić, że dla każdego elementu $a \in K$ ideał $(X - a) \in K[X]$ jest maksymalny. (*Wskazówka*: Rozważyć homomorfizm $K[X] \ni f \mapsto f(a) \in K$.)

1.6.8. Niech K będzie ciałem. Udowodnić, że pierścień $K[X, Y]/(X - Y^2)$ jest dziedziną. (*Wskazówka*: Wykorzystując Drugie Twierdzenie o Izomorfizmie udowodnić, że $K[X, Y]/(X - Y^2) \simeq K[Y]$.)

ROZDZIAŁ II

Grupy

Inną ważną strukturą algebraiczną są grupy. Badaniom podstawowych własności grup poświęcony będzie ten rozdział. Naszym celem będzie udowodnienie kilku podstawowych faktów dotyczących struktury grup: twierdzenia Lagrange'a, klasyfikacji grupy cyklicznych oraz twierdzeń Sylowa.

2.1. Twierdzenie Lagrange'a

Ten paragraf poświęcony będzie udowodnieniu twierdzeniu Langrange'a opisującego związek pomiędzy ilością elementów grupy oraz jej podgrupy.

2.1.1. Przypomnijmy, że grupą nazywamy zbiór G wraz z łącznym działaniem $\cdot$, dla którego istnieje element neutralny oraz wszystkie elementy są odwracalne (patrz także Ćwiczenia 1.1.4 oraz 1.1.5). Jeśli działanie $\cdot$ jest przemienne, to grupę nazywamy *abelową*. Zwykle dla oznaczenia działania w grupie będziemy stosować notację multiplikatywną. Zastosowanie notacji addytywnej będzie oznaczało, że rozważane działanie jest przemienne.

Jeśli R jest pierścieniem, to zbiór R jest grupą ze względu na działanie dodawania, którą też oznaczamy R i nazywamy *grupą addytywną pierścienia* R. Ogólniej, gdy I jest ideałem pierścienia R, to I jest też grupą ze względu na dodawanie w pierścieniu, która będziemy oznaczać I. Ponadto zbiór elementów odwracalnych w pierścieniu R tworzy grupę ze względu na mnożenie, oznaczaną R^* i nazywaną *grupą multiplikatywną pierścienia* R. Powyższe przykłady są przykładami grup abelowych. Podstawowym przykładem grupy, która nie jest przemienna, jest zbiór $\mathscr{S}(X)$ funkcji odwracalnych na zbiorze X z działaniem składania funkcji (grupa ta jest abelowa wtedy i tylko wtedy, gdy $|X| \leq 2$). Gdy $X = \{1, 2, \ldots, n\}$, to piszemy $\mathscr{S}_n$ zamiast $\mathscr{S}(\{1, 2, \ldots, n\})$.

2.1.2. Niech G będzie grupą. Podzbiór $H \subseteq G$ nazywamy *podgrupą grupy* G, jeśli spełnione są następujące warunki:

(1) $1 \in H$;
(2) jeśli $a, b \in H$, to $ab \in H$;
(3) jeśli $a \in H$, to $a^{-1} \in H$.

Zauważmy, że podgrupa H grupy G jest grupą ze względu na działanie $\cdot$ obcięte do H. Jeśli K jest podgrupą grupy H oraz H jest podgrupą

grupy G, to K jest podgrupą grupy G. Ponadto, jeśli K jest podgrupą grupy G oraz H jest podgrupą grupy G zawierającą K, to K jest podgrupą grupy H.

Jeśli X i Y są dwoma podzbiorami grupy G, to przez XY oznaczać będziemy zbiór złożony z wszystkich elementów postaci xy, $x \in X$, $y \in Y$. Zamiast $\{a\}Y$ i $X\{a\}$ piszemy aY i Xa odpowiednio. Podobnie przez X^{-1} oznaczać będziemy zbiór wszystkich elementów postaci x^{-1}, $x \in X$. Zauważmy, że $(XY)^{-1} = Y^{-1}X^{-1}$. Ponadto, gdy grupa jest abelowa, to $XY = YX$. W przypadku notacji addytywnej analogicznie wprowadzamy oznaczenie $X + Y$ oraz $-X$. Korzystając z powyższej notacji definicję podgrupy możemy zapisać następująco: podzbiór H grupy G jest podgrupą, jeśli

(1) $1 \in H$;
(2) $HH \subseteq H$;
(3) $H^{-1} \subseteq H$.

Oczywiście w każdej grupie cała grupa oraz grupa trywialna 1 złożona z elementu neutralnego są podgrupami. Jeśli S jest podpierścieniem pierścienia R, to grupa addytywna pierścienia S jest podgrupą grupy addytywnej pierścienia R. Podobnie, gdy I jest ideałem pierścienia R, to I jest podgrupą grupy addytywnej pierścienia R. Innym przykładem jest podgrupa $\mathbb{C}_m$ grupy $\mathbb{C}^*$, gdzie $\mathbb{C}_m$ jest grupą pierwiastków stopnia m z jedynki. Gdy V jest przestrzenią liniową, to zbiór $\mathrm{GL}(V)$ automorfizmów liniowych przestrzeni V jest podgrupą grupy $\mathscr{S}(V)$.

Następujące proste do sprawdzenia własności operacji na podzbiorach grupy G będą przydatne w dowodach:

(1) $(\bigcup_{i\in I} X_i)(\bigcup_{j\in J} Y_j) = \bigcup_{i,j} X_iY_j$, $(\bigcup_{i\in I} X_i)^{-1} = \bigcup_{i\in I} X_i^{-1}$,
(2) $(\bigcap_{i\in I} X_i)(\bigcap_{j\in J} Y_j) \subseteq \bigcap_{i,j} X_iY_j$, $(\bigcap_{i\in I} X_i)^{-1} \subseteq \bigcap_{i\in I} X_i^{-1}$.

2.1.3. Jeśli H jest podgrupą grupy G, to przez $\sim_H$ oznaczać będziemy relację w G zdefiniowaną poprzez warunek:

$$a \sim_H b \text{ wtedy i tylko wtedy } a^{-1}b \in H.$$

Stwierdzenie. *Niech H będzie podgrupą grupy G. Relacja $\sim_H$ jest relacją równoważności w G. Klasa abstrakcji elementu $a \in G$ względem $\sim_H$ jest równa aH. Ponadto $|H| = |aH|$ dla każdego $a \in H$.*

Dowód. Bezpośrednio z definicji oraz własności podgrupy wynika, że relacja $\sim_H$ jest zwrotna, symetryczna i przechodnia, zatem istotnie jest relacją równoważności. Z definicji relacji $\sim_H$ wynika, że $a \sim_H b$ wtedy i tylko wtedy, gdy $b = a(a^{-1}b) \in aH$. Ponadto łatwo widać, że funkcja $H \ni b \mapsto ab \in aH$ jest bijekcją – funkcja odwrotna dana jest wzorem $aH \ni b \mapsto a^{-1}b \in H$. □

Zauważmy, że z powyższego stwierdzenia wynika między innymi, że jeśli H jest podgrupą grupy G oraz $a \in H$, to $aH = H$. Istotnie, gdy $a \in H$, to $a \sim_H 1$, a więc $aH = 1H = H$.

Jeśli H jest podgrupą grupy G, to zbiór klas abstrakcji relacji $\sim_H$ oznaczać będziemy G/H, a jego elementy nazywać *warstwami lewostronnymi podgrupy H w G*. Ilość warstw lewostronnych oznaczać będziemy $[G : H]$ oraz nazywać *indeksem podgrupy H w G* (może być to nieskończona liczba kardynalna). Łatwo sprawdzić, że $[G : G] = 1$ i $[G : 1] = |G|$. Łatwy rachunek pokazuje, że $[\mathbb{Z} : \mathbb{Z}_m] = m$.

Analogicznie jak powyżej można zdefiniować warstwy prawostronne grupy G względem H. W ogólności nie jest prawdą, że warstwy prawostronne i lewostronne pokrywają się, nie mniej indeks zdefiniowany przy pomocy warstw prawostronnych pokrywa się z indeksem zdefiniowanym powyżej (patrz Ćwiczenie 2.1.14).

2.1.4. Poniższy lemat będzie odgrywał kluczową rolę w dowodzie twierdzenia Lagrange'a.

Lemat. *Niech H będzie podgrupą grupy G. Wtedy istnieją elementy a_i, $i \in G/H$, takie, że $G = \bigcup_{i\in G/H} a_iH$ oraz $a_iH \cap a_jH = \varnothing$ dla $i \neq j$. Z drugiej strony, jeśli dane są elementy b_k, $k \in I$, takie, że $G = \bigcup_{k\in I} b_kH$ oraz $b_kH \cap b_lH = \varnothing$ dla $k \neq l$, to $|I| = |G/H|$.*

Dowód. Pierwsza część lematu jest sformułowaniem faktu, że jeśli $\sim$ jest relacją równoważności na zbiorze X, to X jest sumą rozłączną wszystkich klas abstrakcji, dla $\sim=\sim_H$ oraz $X = G$. Dla dowodu drugiej części rozważmy funkcję $f : I \to G/H$ daną wzorem $f(k) = b_kH$, $k \in I$. Z założenia $G = \bigcup_{k\in I} b_kH$ wynika, że f jest surjekcją, z faktu, że $b_kH \cap b_lH = \varnothing$ dla $k \neq l$ otrzymujemy, że f jest injekcją. Zatem f jest bijekcją, co kończy dowód. □

2.1.5. *Rzędem grupy G* nazywamy ilość jej elementów. Pierwszym wnioskiem z powyższego lematu, który udowodnimy, jest zapowiadane wcześniej twierdzenia Lagrange'a.

Twierdzenie (Lagrange). *Jeśli H jest podgrupą grupy G, to $|G| = [G : H]|H|$. W szczególności, jeśli grupa G jest skończona, to rząd H dzieli rząd G.*

Dowód. Z Lematu 2.1.4 wiemy, że istnieją elementy a_i, $i \in G/H$, takie, że $G = \bigcup_{i\in G/H} a_iH$ oraz $a_iH \cap a_jH = \varnothing$ dla $i \neq j$. Ponadto ze Stwierdzenia 2.1.3 wynika też, że $|a_iH| = |H|$ dla wszystkich $i \in G/H$, co kończy dowód twierdzenia. □

2.1.6. Inną konsekwencją Lematu 2.1.4 jest multiplikatywność indeksu.

Twierdzenie. *Jeśli K i H są podgrupami grupy G takimi, że $K \subseteq H$, to $[G : K] = [G : H][H : K]$.*

Dowód. Z Lematu 2.1.4 wiemy, że istnieją elementy a_i, $i \in G/H$, takie, że $G = \bigcup_{i\in G/H} a_iH$ oraz $a_iH \cap a_jH = \varnothing$ dla $i \neq j$. Analogicznie istnieją elementy b_k, $k \in H/K$, takie, że $H = \bigcup_{k\in H/K} b_kK$ oraz

$b_kH \cap b_lH = \varnothing$ dla $k \neq l$. Wtedy $aH = \bigcup_{k\in H/K} ab_kK$ dla dowolnego $a \in G$, skąd $G = \bigcup_{i\in G/H}\bigcup_{k\in H/K} a_ib_kK$. Na mocy Lematu 2.1.4 wystarczy udowodnić, że jeśli $(i,k) \neq (j,l)$, to $a_ib_kK \cap a_jb_lK = \varnothing$, co na mocy Stwierdzenia 2.1.3 oraz własności relacji równoważności jest równoważne temu, że $a_ib_kK \neq a_jb_lK$. Przypuśćmy zatem, że $a_ib_kK = a_jb_lK$. Oznacza to, że $b_k^{-1}a_i^{-1}a_jb_l \in K$, skąd wynika, że $a_i^{-1}a_j \in b_kKb_l^{-1}$. Ponieważ $b_k, b_l \in H$ oraz K jest podgrupą grupy H, więc wnioskujemy stąd, że $a_i^{-1}a_j \in H$, a więc $i = j$. Wykorzystując ten fakt otrzymujemy, że $b_k^{-1}b_l \in K$, więc $k = l$, co kończy dowód. □

Ćwiczenia

2.1.1. Udowodnić, że zbiór $\mathbb{R}_+$ dodatnich liczb rzeczywistych z działaniem mnożenia jest grupą abelową.

2.1.2. Niech n będzie liczbą całkowitą dodatnią oraz niech K będzie ciałem. Udowodnić, że zbiór $\mathrm{GL}_n(K)$ $n \times n$-macierzy o współczynnikach w K i niezerowym wyznaczniku jest grupą ze względu na mnożenie macierzy.

2.1.3. Niech X będzie zbiorem i niech G będzie grupą. Definiujemy $\mathscr{F}(X,G) = \{f : X \to G\}$. Udowodnić, że zbiór $\mathscr{F}(X,G)$ jest grupą ze względu na działanie: $(fg)(x) = f(x)g(x)$. Grupa ta jest grupą abelową, jeśli G jest grupą abelową.

2.1.4. Niech G będzie taką grupą, że $(ab)^2 = a^2b^2$ dla dowolnych $a, b \in G$. Udowodnić, że grupa G jest abelowa.

2.1.5. Niech G będzie taką grupą, że $(ab)^{-1} = a^{-1}b^{-1}$ dla dowolnych $a, b \in G$. Udowodnić, że grupa G jest abelowa.

2.1.6. Niech G będzie taką grupą, że istnieje liczba całkowita n taka, że $(ab)^n = a^nb^n$, $(ab)^{n+1} = a^{n+1}b^{n+1}$ i $(ab)^{n+2} = a^{n+2}b^{n+2}$ dla dowolnych $a, b \in G$. Udowodnić, że grupa G jest abelowa.

2.1.7. Niech G będzie grupą oraz niech $a, b \in G$ będą takie, że $bab^{-1} = a^n$ dla pewnego $n > 0$. Udowodnić, że $b^mab^{-m} = a^{n^m}$ dla dowolnego $m > 0$.

2.1.8. Niech G będzie grupą skończoną rzędu parzystego. Udowodnić, że istnieje element $a \in G$ taki, że $a \neq 1$ oraz $a^2 = 1$.

2.1.9. Niech G będzie grupą. Udowodnić, że podzbiór $H \subseteq G$ jest podgrupą wtedy i tylko wtedy, gdy $H \neq \varnothing$ oraz jeśli $a, b \in H$, to $ab^{-1} \in H$.

2.1.10. Niech H będzie niepustym i skończonym podzbiorem grupy G. Udowodnić, że H jest podgrupą grupy G wtedy i tylko wtedy, gdy $ab \in H$ dla dowolnych $a, b \in H$.

2.1.11. Niech p będzie liczbą pierwszą i niech R_p będzie zbiorem tych liczb wymiernych, których mianownik jest względnie pierwszy z p. Udowodnić, że R_p jest podgrupą grupy $\mathbb{Q}$.

2.1.12. Niech p będzie liczbą pierwszą i niech R^p będzie zbiorem tych liczb wymiernych, których mianownik jest potęgą liczby p. Udowodnić, że R^p jest podgrupą grupy $\mathbb{Q}$.

2.1.13. Niech S będzie niepustym podzbiorem grupy G. Definiujemy relacje $\sim_S$ w grupie G wzorem: $a \sim_S b$ wtedy i tylko wtedy, gdy $ab^{-1} \in S$. Udowodnić, że S jest relacją równoważności wtedy i tylko wtedy, gdy S jest podgrupą grupy G.

2.1.14. Niech H będzie podgrupą grupy G. Definiujemy relację $\sim^H$ w G wzorem

$$a \sim^H b \text{ wtedy i tylko wtedy, gdy } ab^{-1} \in H.$$

(a) Udowodnić, że $\sim^H$ jest relacją równoważności oraz że $[a]_{\sim^H} = Ha$ i $|Ha| = H$ dla dowolnego $a \in G$.
(b) Udowodnić, że ilość klas abstrakcji relacji $\sim^H$ jest równa $[G : H]$.
(c) Niech $G = \mathscr{S}_3$ oraz $H = \{\mathbb{1}, \sigma\}$, gdzie

$$\sigma(1) = 2,\ \sigma(2) = 1,\ \sigma(3) = 3.$$

Udowodnić, że H jest podgrupą grupy G. Niech $\tau \in \mathscr{S}(X)$ będzie dane wzorem

$$\tau(1) = 1,\ \tau(2) = 3,\ \tau(3) = 2.$$

Udowodnić, że $\tau H \neq H\tau$.

2.1.15. Niech

$$H = \{\sigma \in \mathscr{S}_n \mid \sigma(n) = n\}.$$

Udowodnić, że H jest podgrupą grupy $\mathscr{S}_n$.

2.1.16. Niech H i K będą skończonymi podgrupami grupy G. Udowodnić, że $|HK| = |H||K|/|H \cap K|$.

2.1.17. Niech H i K będą podgrupami grupy G.

(a) Udowodnić, że $[H : H \cap K] \leq [G : K]$.
(b) Przypuśćmy, że $[G : K] < \infty$. Udowodnić, że $[H : H \cap K] = [G : K]$ wtedy i tylko wtedy, gdy $G = KH$.

2.1.18. Niech H i K będą podgrupami grupy G takimi, że $[G : H], [G : K] < \infty$.

(a) Udowodnić, że $[G : H \cap K] \leq [G : H][G : K]$.
(b) Udowodnić, że $[G : H \cap K] = [G : H][G : K]$ wtedy i tylko wtedy, gdy $G = HK$.

2.1.19. Niech H i K będą podgrupami grupy G. Udowodnić, że HK jest podgrupą grupy G wtedy i tylko wtedy, gdy $HK = KH$.

2.1.20. Niech p będzie liczbą pierwszą oraz niech G będzie grupą rzędu $p^k m$, gdzie $k \geq 0$ oraz $(p, m) = 1$. Jeśli H jest podgrupą grupy G rzędu p^k oraz K jest podgrupą grupy G rzędu p^l dla pewnego l taką, że $K \not\subseteq H$, to HK nie jest podgrupą grupy G.

2.1.21. Niech H i K będą podgrupami grupy G takimi, że $[G : H]$ i $[G : K]$ są skończone oraz względnie pierwsze. Udowodnić, że $G = HK$.

2.1.22. Niech H, K i N będą podgrupami grupy G takimi, że $H \subseteq N$. Udowodnić, że $HK \cap N = H(K \cap N)$.

2.1.23. Niech H, K i N będą podgrupami grupy G takimi, że $H \subseteq K$, $H \cap N = K \cap N$ oraz $HN = KN$. Udowodnić, że $H = K$.

2.2. Grupy ilorazowe

Omówimy teraz pojęcie grupy ilorazowej. Omawiane poniżej pojęcia są analogiczne do tych zdefiniowanych w przypadku pierścieniu.

2.2.1. Niech G będzie grupą. Relację równoważności $\sim$ w G nazywamy *kongruencją w* G, jeśli dla dowolnych $a, b, c, d \in G$, z faktu, że $a \sim b$ oraz $c \sim d$ wynika, że $ac \sim bd$. Zauważmy, że jeśli $\sim$ jest kongruencją w grupie G oraz $a \sim b$, to $a^{-1} \sim b^{-1}$. Istotnie, ponieważ $a \sim b$ oraz $a^{-1} \sim a^{-1}$, więc $1 = aa^{-1} \sim ba^{-1}$. Wykorzystując dodatkowo fakt, że $1 = bb^{-1}$ oraz, że $b^{-1} \sim b^{-1}$, otrzymujemy, że $b^{-1} = b^{-1}bb^{-1} \sim b^{-1}ba^{-1} = a^{-1}$. Jeśli $\sim$ jest kongruencją w grupie G, to przez $N_\sim$ oznaczać będziemy klasę abstrakcji 1.

Podobnie jak w pierścieniu relacje $=$ i $G \times G$ są kongruencjami oraz $N_= = 1$ i $N_{G\times G} = G$. Jeśli R jest pierścieniem oraz $\sim$ jest kongruencją w pierścieniu R, to $\sim$ jest też kongruencją w grupie addytywnej pierścienia R oraz $N_\sim = I_\sim$. Mamy też następujący przykład kongruencji w grupie, która nie jest abelowa. Niech V będzie skończenie wymiarową przestrzenią liniową nad ciałem K. Przypomnijmy, że mamy funkcję wyznacznika $\det : \mathrm{GL}(V) \to K^*$. Relacja $\sim$ w $\mathrm{GL}(V)$ zadana poprzez warunek $f \sim g$ wtedy i tylko wtedy, gdy $\det f = \det g$, jest kongruencją oraz $N_\sim = \mathrm{SL}(V) = \{f \in \mathrm{GL}(V) \mid \det f = 1\}$.

2.2.2. Zauważmy, że we wszystkich powyższych przykładach $N_\sim$ jest podgrupą. Nie jest to przypadkiem, ale nie każda podgrupą może być otrzymana w ten sposób.

Stwierdzenie. *Jeśli $\sim$ jest kongruencją w grupie G, to $N_\sim$ jest podgrupą grupy G oraz $aN_\sim a^{-1} \subseteq N_\sim$ dla dowolnego $a \in G$.*

Dowód. Prosta konsekwencja własności relacji kongruencji. □

Podgrupę N grupy G będziemy nazywać *dzielnikiem normalnym grupy* G wtedy i tylko wtedy, gdy $aNa^{-1} \subseteq N$ dla dowolnego $a \in G$. Zatem powyższe stwierdzenie moglibyśmy sformułować następująco: jeśli $\sim$ jest kongruencją, to $N_\sim$ jest dzielnikiem normalnym. Jak się przekonamy związek pomiędzy dzielnikami normalnymi oraz kongruencjami w grupie przypomina ten pomiędzy ideałami oraz kongruencjami w pierścieniu.

Zauważmy, że w grupie abelowej każda podgrupa jest dzielnikiem normalnym, na ogół nie jest to jednak prawdą w grupach, które nie są abelowe (patrz Ćwiczenie 2.2.8).

W przypadku dzielników normalnych nie musi być prawdą stwierdzenie, że jeśli N jest dzielnikiem normalnym grupy G oraz M jest dzielnikiem normalnym grupy N, to M jest dzielnikiem normalnym grupy G (patrz Ćwiczenie 2.4.3). Z drugiej strony, gdy N jest dzielnikiem normalnym grupy G oraz H jest podgrupą grupy G zawierającą N, to N jest dzielnikiem normalnym grupy H.

2.2.3. Poniższy lemat mówi między innymi, że podgrupa N grupy G jest dzielnikiem normalnym wtedy i tylko wtedy, gdy relacja $\sim_N$ zdefiniowana w poprzednim paragrafie pokrywa się z relacją $\sim^N$ zdefiniowaną w Ćwiczeniu 2.1.14.

LEMAT. *Niech N będzie podgrupą grupy G.*

(1) *N jest dzielnikiem normalnym grupy G wtedy i tylko wtedy, gdy dla dowolnego $a \in N$ zachodzi $aNa^{-1} = N$.*
(2) *N jest dzielnikiem normalnym grupy G wtedy i tylko wtedy, gdy dla dowolnego $a \in N$ zachodzi $aN = Na$.*

DOWÓD. (1) Oczywiście, jeśli $aNa^{-1} = N$ dla dowolnego $a \in N$, to N jest dzielnikiem normalnym. Przypuśćmy teraz, że N jest dzielnikiem normalnym. Aby udowodnić, że $aNa^{-1} = N$ dla dowolnego $a \in N$. musimy pokazać, że $N \subseteq aNa^{-1}$ dla dowolnego $a \in N$. Wiemy jednak, że $N = aa^{-1}Naa^{-1}$. Ponieważ $(a^{-1})^{-1} = a$, więc $a^{-1}Na \subseteq N$, skąd $N \subseteq aNa^{-1}$, co kończy dowód pierwszej części lematu.

(2) Jeśli N jest dzielnikiem normalnym, to korzystając z punktu (1) mamy ciąg równości $Na = aNa^{-1}a = aN$ dla dowolnego $a \in G$. Załóżmy zatem, że $aN = Na$ dla dowolnego $a \in N$. Wtedy $aNa^{-1} = Naa^{-1} = N$, co kończy dowód. □

Zauważmy, że punkt (2) powyższego lematu implikuje, że jeśli N jest dzielnikiem normalnym grupy G, to $XN = NX$ dla dowolnego zbioru X. Istotnie, $XN = \bigcup_{x\in X} xN = \bigcup_{x\in X} Nx = NX$.

2.2.4. Omówimy teraz zapowiadany związek pomiędzy dzielnikami normalnymi oraz kongruencjami w grupie.

STWIERDZENIE. *Jeśli N jest dzielnikiem normalnym grupy G, to relacja $\sim_N$ jest relacją kongruencji oraz $N_{\sim_N} = N$. Z drugiej strony, jeśli $\sim$ jest relacją kongruencji, to $\sim_{N_\sim}=\sim$.*

DOWÓD. Ze Stwierdzenia 2.1.3 wiemy, że $\sim_N$ jest relacją równoważności. Przypuśćmy zatem, że $a \sim_N b$ oraz $c \sim_N d$, tzn. $aN = bN$ oraz $cN = dN$. Wtedy $acN = adN = aNd = bNd = bdN$, skąd $ac \sim_N bd$, a więc $\sim_N$ jest istotnie kongruencją. Przypomnijmy, że $N_{\sim_N}$ jest warstwą 1 w relacji $\sim_N$, a ta na mocy Stwierdzenia 2.1.3 jest równa $1N = N$. Na koniec zauważmy, że $a \sim_{N_\sim} b$ wtedy i tylko wtedy, gdy $a^{-1}b \in N_\sim$, a więc $a^{-1}b \sim 1$, co oznacza, że $b \sim a$, gdyż zawsze $a \sim a$. □

2.2.5. Podobnie jak w przypadku pierścieniu kongruencje służą do zdefiniowania struktury ilorazowej.

STWIERDZENIE. *Jeśli $\sim$ jest relacją kongruencji, to w zbiorze klas abstrakcji $G/\sim$ następująca definicja działania $\cdot$*

$$[a]_\sim \cdot [b]_\sim = [ab]_\sim,\ a, b \in G,$$

jest poprawna oraz $G/\sim$ z działaniem $\cdot$ jest grupą.

Dowód. Poprawność definicji jest natychmiastową konsekwencją definicji relacji kongruencji. Łączność działania $\cdot$ jest oczywista. Elementem naturalnym jest $[1]_\sim$, zaś elementem odwrotnym do $[a]_\sim$, klasa $[a^{-1}]_\sim$. □

Przedstawiony w poprzednim stwierdzeniu związek pomiędzy kongruencjami oraz dzielnikami normalnymi pozwala nam sformułować następujący wniosek.

Wniosek. *Jeśli N jest dzielnikiem normalnym, to w zbiorze G/N następująca definicja działania $\cdot$*

$$aN \cdot bN = abN$$

jest poprawna oraz G/N z działaniem $\cdot$ jest grupą.

Dowód. Jest to przeformułowanie wcześniejszego stwierdzenia wykorzystujące Stwierdzenie 2.2.4 oraz Stwierdzenie 2.1.3. □

Zauważmy, że jeśli N jest dzielnikiem normalnym grupy G oraz H jest podgrupą grupy G zawierającą N, to H/N jest podgrupą grupy G. Ponadto każda podgrupa grupy G/N jest tej postaci. Analogiczna reguła obowiązuje w przypadku dzielników normalnych.

Ćwiczenia

2.2.1. Udowodnić, że relacja równoważności $\sim$ w grupie G jest kongruencją wtedy i tylko wtedy, gdy dla dowolnych $a, b, c \in G$, z faktu, że $a \sim b$ wynika, że $ac \sim bc$ oraz $ca \sim cb$.

2.2.2. Udowodnić, że jeśli grupa G jest abelowa oraz H jest podgrupą grupy G, to H jest dzielnikiem normalnym grupy G oraz G/H jest grupą abelową.

2.2.3. Udowodnić, że $\mathbb{Q}/\mathbb{Z}$ jest nieskończoną grupą abelową.

2.2.4. Niech p będzie liczbą pierwszą oraz

$$Z(p^\infty) = \left\{\frac{a}{b} + \mathbb{Z} \mid a \in \mathbb{Z},\, b = p^i \text{ dla } i \geq 0\right\} \subseteq \mathbb{Q}/\mathbb{Z}.$$

Udowodnić, że $Z(p^\infty)$ jest nieskończoną podgrupą grupy $\mathbb{Q}/\mathbb{Z}$.

2.2.5. Niech M i N będą dzielnikami normalnymi grupy G. Udowodnić, że jeśli $M \cap N = 1$, to $ab = ba$ dla dowolnych $a \in M$ i $b \in N$.

2.2.6. Niech N będzie podgrupą grupy G taką, że $[G : N] = 2$. Udowodnić, że N jest dzielnikiem normalnym grupy G.

2.2.7. Niech N_i, $i \in I$, będzie niepustą rodziną dzielników normalnych grupy G. Udowodnić, że $\bigcap_{i\in I} N_i$ jest dzielnikiem normalnym grupy G.

2.2.8. Niech

$$N = \{\sigma \in \mathscr{S}_4 \mid \sigma(4) = 4\}.$$

Czy N jest dzielnikiem normalnym grupy $\mathscr{S}_4$?

2.2.9. Niech M i N będą dzielnikami normalnymi grupy G. Udowodnić, że MN jest dzielnikiem normalnym grupy G.

2.3. Twierdzenia o izomorfizmie

Zgodnie z zapowiedzią poczynioną w paragrafie 1.6 udowodnimy teraz twierdzenia o izomorfizmie dla grup.

2.3.1. Jeśli G i H są grupami, to funkcję $\varphi : G \to H$ nazywamy *homomorfizmem grup* jeśli

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ dla dowolnych } a, b \in G.$$

Zauważmy, że powyższy warunek implikuje, iż $\varphi(1) = 1$ oraz $\varphi(a^{-1}) = (\varphi(a))^{-1}$ dla dowolnego $a \in G$. Podobnie jak w przypadku pierścieniu definiujemy pojęcia *monomorfizmu*, *epimorfizmu*, *izomorfizmu*, *endomorfizmu* oraz *automorfizmu*. Jeśli $\varphi : G \to H$ jest izomorfizmem, to funkcja odwrotna do φ też jest homomorfizmem, a więc także izomorfizmem. Jeśli istnieje izomorfizm $G \to H$ to mówimy, że *grupy G i H są izomorficzne* oraz piszemy $G \simeq H$. *Jądrem homomorfizmu* $\varphi : G \to H$ nazywamy zbiór wszystkich $a \in G$, dla których $\varphi(a) = 1$. *Obrazem homomorfizmu* φ nazywamy obraz zbioru G przy działaniu funkcji φ. Jądro homomorfizmu φ będziemy oznaczać $\operatorname{Ker}\varphi$, zaś jego obraz $\operatorname{Im}\varphi$.

Dla każdej grupy G funkcja identycznościowa $\mathbb{1}_G$ jest izomorfizmem. Ponadto, gdy $\varphi : G \to H$ i $\psi : H \to K$ są homomorfizmami grup, to $\psi \circ \varphi : G \to K$ też jest homomorfizmem grup. W szczególności zbiór wszystkich automorfizmów grupy G tworzy grupę, którą nazywamy *grupą automorfizmów grupy G* oraz oznaczamy $\operatorname{Aut}(G)$. Zauważmy, że $\operatorname{Aut}(G)$ jest podgrupą grupy $S(G)$.

Gdy H jest podgrupą grupy G, to funkcja $\varphi : H \to G$ dana wzorem $\varphi(a) = a$ jest monomorfizmem grup, który nazywamy *naturalnymi włożeniem*. Zauważmy, że $\operatorname{Ker}\varphi = 1$ oraz $\operatorname{Im}\varphi = H$. Dualnie, gdy N jest dzielnikiem normalnym grupy G, to funkcja $\varphi : G \to G/N$ dana wzorem $\varphi(a) = aN$ jest epimorfizmem grup zwanym *naturalnymi rzutowaniem*. Mamy $\operatorname{Ker}\varphi = N$ oraz $\operatorname{Im}\varphi = G/N$. Innym przekładem homomorfizmu jest funkcja $\varphi : \mathbb{R} \to \mathbb{C}^*$ dana wzorem $\varphi(x) = e^{2\pi ix}$ dla $x \in \mathbb{R}$. Zauważmy, że $\operatorname{Ker}\varphi = \mathbb{Z}$ oraz $\operatorname{Im}\varphi$ jest zbiorem liczb zespolonych o module 1.

Podobnie jak dla pierścieni można pokazać, że jeśli $\varphi : G \to H$ jest homomorfizmem grup, to $\operatorname{Ker}\varphi$ jest dzielnikiem normalnym grupy G, zaś $\operatorname{Im}\varphi$ jest podgrupą grupy H. Ogólniej, jeśli K jest podgrupą grupy G, to $\varphi(K)$ jest podgrupą grupy H, oraz gdy N jest dzielnikiem normalnym (podgrupą) grupy H, to $\varphi^{-1}(N)$ jest dzielnikiem normalnym (podgrupą) grupy G. Wiadomo, że φ jest monomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = 1$, oraz epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{Im}\varphi = H$. W szczególności φ jest izomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = 1$ oraz $\operatorname{Im}\varphi = H$. Na zakończenie zauważmy, że jeśli $\varphi : G \to H$ jest monomorfizmem grup, to funkcja $\phi : G \to \operatorname{Im}\varphi$ dana wzorem $\phi(a) = \varphi(a)$ jest izomorfizmem.

2.3.2. Udowodnimy teraz twierdzenia o izomorfizmie. Podobnie jak w przypadku pierścieni dowody będą się opierały na następującym fakcie.

TWIERDZENIE. *Niech $\varphi : G \to H$ będzie homomorfizmem grup oraz N dzielnikiem normalnym grupy G takim, że $N \subseteq \operatorname{Ker}\varphi$. Wtedy odwzorowanie $\phi : G/N \to H$ dane wzorem*

$$\phi(aN) = \varphi(a)$$

jest poprawnie określone oraz jest homomorfizmem, $\operatorname{Ker}\phi = \operatorname{Ker}\varphi/N$ *i* $\operatorname{Im}\phi = \operatorname{Im}\varphi$.

DOWÓD. Analogiczny jak w przypadku pierścieni. □

WNIOSEK 2.3.2.1 (Pierwsze Twierdzenie o Izomorfizmie). *Jeśli $\varphi : G \to H$ jest homomorfizmem grup, to funkcja*

$$G/\operatorname{Ker}\varphi \in a\operatorname{Ker}\varphi \mapsto \varphi(a) \in \operatorname{Im}\varphi$$

jest poprawnie określona oraz jest izomorfizmem grup.

DOWÓD. Zastosowanie poprzedniego twierdzenia dla $N = \operatorname{Ker}\varphi$. □

Jako pierwszy przykład zastosowania powyższego twierdzenia zauważmy, że funkcja $\mathbb{Z}/\mathbb{Z}m \ni k + \mathbb{Z}m \mapsto$ reszta z dzielenia k przez $m \in \mathbb{Z}_m$ jest poprawie określona oraz jest izomorfizmem. Podobnie, gdy V jest skończenie wymiarową przestrzenią liniową K nad ciałem K, to funkcja $\operatorname{GL}(V)/\operatorname{SL}(V) \ni A\operatorname{SL}(V) \mapsto \det A \in K^*$ jest izomorfizmem.

Przypomnijmy, że punkt (2) Lematu 2.2.3 implikuje, jeśli N jest dzielnikiem normalnym grupy G, to $XN = NX$ dla dowolnego podzbioru X grupy G. Wykorzystując tę obserwację można pokazać, że jeśli H jest podgrupą grupy G oraz N jest dzielnikiem normalnym grupy G, to HN jest podgrupą grupy G. Bezpośrednio z definicji można też sprawdzić, że w powyższej sytuacji $H \cap N$ jest dzielnikiem normalnym grupy H.

WNIOSEK 2.3.2.2 (Drugie Twierdzenie o Izomorfizmie). *Jeśli G jest grupą, H jest podgrupą grupy G oraz N jest dzielnikiem normalnym grupy G, to funkcja*

$$H/(H \cap N) \ni a(H \cap N) \mapsto aN \in HN/N$$

jest poprawnie określona oraz jest izomorfizmem grup.

DOWÓD. Niech $\varphi : H \to HN/N$ będzie odwzorowaniem danym wzorem $\varphi(a) = aN$. Funkcja φ jest homomorfizmem grup, gdyż jest złożeniem naturalnego włożenia $H \to HN$ oraz naturalnego rzutowania $HN \to HN/N$. Łatwo sprawdzić, że $\operatorname{Im}\varphi = HN/N$, gdyż $abN = aN = \varphi(a)$ dla $a \in H$ oraz $b \in N$. Ponadto $\operatorname{Ker}\varphi = H \cap N$,

gdyż $aN = N$ wtedy i tylko wtedy, gdy $a \in N$. Teza wynika zatem z Pierwszego Twierdzenia o Izomorfizmie. □

Wniosek 2.3.2.3 (Trzecie Twierdzenie o Izomofizmie). *Jeśli M i N są dzielnikami normalnymi grupy G takimi, że $N \subseteq M$, to funkcja*

$$(G/N)/(M/N) \ni (aN)(M/N) \mapsto aM \in G/M$$

jest poprawnie określona oraz jest izomorfizmem.

Dowód. Niech $\varphi : G \to G/M$ będzie naturalnym rzutowaniem. Wiadomo, że $\operatorname{Ker}\varphi = M$ i $\operatorname{Im}\varphi = G/M$. Z powyższego twierdzenia zastosowanego dla N wynika, że funkcja $\psi : G/N \to G/M$ dana wzorem $\psi(aN) = aM$ jest poprawnie określona oraz jest homomorfizmem takim, że $\operatorname{Ker}\psi = M/N$ oraz $\operatorname{Im}\psi = G/M$. Stosując teraz Pierwsze Twierdzenie o Izomorfizmie dla ψ dostajemy tezę. □

Ćwiczenia

2.3.1. Udowodnić, że grupa G jest abelowa wtedy i tylko wtedy, gdy funkcja $G \ni a \mapsto a^{-1} \in G$ jest automorfizmem.

2.3.2. Niech $\mathbb{R}_+$ będzie grupą dodatnich liczb całkowitych z działaniem mnożenia (patrz Ćwiczenie 2.1.1). Udowodnić, że funkcja $\varphi : \mathbb{R}_+ \to \mathbb{R}$ dana wzorem $\varphi(x) = \ln x$ dla $x \in \mathbb{R}_+$ jest izomorfizmem grup. Znaleźć funkcję odwrotną.

2.3.3. Niech $n \geq 2$ będzie liczbą całkowitą oraz niech $H = \{\sigma \in \mathscr{S}_n \mid \sigma(n) = n\}$. Udowodnić, że grupy H i $\mathscr{S}_{n-1}$ są izomorficzne.

2.3.4. Niech $\varphi : G \to H$ będzie homomorfizmem grup. Jeśli grupa H jest abelowa oraz N jest podgrupą grupy G zawierającą $\operatorname{Ker}\varphi$, to N jest dzielnikiem normalnym grupy G.

2.3.5. Niech $\varphi : G \to H$ będzie homomorfizmem oraz niech K będzie podgrupą grupy G. Udowodnić, że $\varphi^{-1}(\varphi(K)) = K \operatorname{Ker}\varphi$. Wywnioskować stąd, że $\varphi^{-1}(\varphi(K)) = K$ wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi \subseteq K$.

2.3.6. Niech $\varphi : G \to H$ będzie homomorfizmem grup. Jeśli K jest podgrupą grupy G taką, że $|K| < \infty$, to $|\varphi(K)| < \infty$ oraz $|\varphi(K)|$ dzieli $|K|$.

2.3.7. Niech N będzie dzielnikiem normalnym grupy G oraz niech H będzie podgrupą grupy G. Udowodnić, że jeśli $N \cap H = 1$ oraz $NH = G$, to $G/N \simeq H$.

2.3.8. Niech N będzie dzielnikiem normalnym grupy G takim, że $[G : N] < \infty$. Jeśli H jest podgrupą grupy G taką, że $|H| < \infty$ oraz $([G : N], |H|) = 1$, to $H \subseteq N$.

2.3.9. Niech N będzie dzielnikiem normalnym grupy G takim, że $|N| < \infty$. Jeśli H jest podgrupą grupy G, to $[HN : H] < \infty$ oraz $[HN : H]$ dzieli $|N|$.

2.3.10. Niech N będzie dzielnikiem normalnym grupy G takim, że $|N| < \infty$. Jeśli H jest podgrupą grupy G taką, że $[G : H] < \infty$ oraz $(|N|, [G : H]) = 1$, to $N \subseteq H$.

2.3.11. Niech m i n będą dodatnimi liczbami całkowitymi. Udowodnić, że $\mathbb{Z}m/\mathbb{Z}mn \simeq \mathbb{Z}_n$.

2.4. Grupy cykliczne

W tym paragrafie sklasyfikujemy grupy cykliczne.

2.4.1. Analogicznie jak w dla ideałów pierścienia (patrz paragraf 1.2.4) pokazujemy, że dla każdego podzbioru X grupy G istnieje najmniejsza podgrupa grupy G zawierająca zbiór X. Podgrupę tę oznaczamy $\langle X\rangle$ i nazywamy *podgrupą generowaną przez zbiór* X. Jeśli $X = \{a_1, \ldots, a_n\}$, to piszemy $\langle a_1, \ldots, a_n\rangle$ zamiast $\langle\{a_1, \ldots, a_n\}\rangle$ i mówimy o *podgrupie generowanej przez elementy* $a_1, \ldots, a_n$. Grupy postaci $\langle a_1, \ldots, a_n\rangle$ dla $a_1, \ldots, a_n \in G$ nazywamy *skończenie generowanymi. Rzędem elementu* $a \in G$ nazwiemy rząd podgrupy $\langle a\rangle$ generowanej przez a. Rząd elementu a będziemy oznaczać przez $|a|$. Gdy istnieje element $a \in G$ taki, że $G = \langle a\rangle$, to grupę G nazywamy *cykliczną*. W tej sytuacji element a nazywamy *generatorem grupy* G i mówimy, że *grupa* G *jest generowana przez element* a.

2.4.2. Przypomnijmy, że jeśli $\varphi : G \to H$ jest homomorfizmem grup oraz K jest podgrupą grupy G, to $\varphi(K)$ jest podgrupą grupy H. Podobnie, gdy K jest podgrupą grupy H, to $\varphi^{-1}(H)$ jest podgrupą grupy G. Powyższe obserwacje będą przydatne w dowodzie poniższego lematu.

Lemat. *Niech $\varphi : G \to H$ będzie homomorfizmem grup. Jeśli X jest podzbiorem grupy G, to $\langle\varphi(X)\rangle = \varphi(\langle X\rangle)$.*

Dowód. Oczywiście $X \subseteq \langle X\rangle$, więc $\varphi(X) \subseteq \varphi(\langle X\rangle)$. Ponieważ $\varphi(\langle X\rangle)$ jest podgrupą grupy H, więc także $\langle\varphi(X)\rangle \subseteq \varphi(\langle X\rangle)$. Dla dowodu przeciwnego zawierania niech $K = \varphi^{-1}(\langle\varphi(X)\rangle)$. Oczywiście K jest podgrupą grupy G oraz $X \subseteq K$, zatem $\langle X\rangle \subseteq K$. Stąd $\varphi(\langle X\rangle) \subseteq \varphi(K) \subseteq \langle\varphi(X)\rangle$, co kończy dowód. □

2.4.3. Opiszemy teraz postać podgrupy generowanej przez zbiór. W tym celu wprowadzimy następujące oznaczenie. Niech Y będzie podzbiorem grupy G. Definiujemy $Y^0 = 1$ oraz $Y^n = \underbrace{Y \cdots Y}_{n \text{ razy}}$ dla $n > 0$.

Stwierdzenie. *Jeśli X jest podzbiorem grupy G, to*

$$\langle X\rangle = \bigcup_{n\geq 0}(X \cup X^{-1})^n,$$

tzn.

$$\langle X\rangle = \{x_1 \ldots x_n \mid x_i \in X \text{ lub } x_i^{-1} \in X,\ i = 1, \ldots, n,\ n \geq 0\}.$$

Dowód. Niech $H = \bigcup_{n\geq 0} Y^n$, gdzie $Y = X \cup X^{-1}$. Ponieważ $X \subseteq \langle X\rangle$ oraz $\langle X\rangle$ jest podgrupą grupy G, więc $Y \subseteq \langle X\rangle$, skąd $Y^n \subseteq \langle X\rangle$, zatem $H \subseteq \langle X\rangle$.

Pokażemy teraz, że H jest podgrupą grupy G. Ponieważ $Y^0 = 1$, więc $1 \in H$. Ponadto $HH = (\bigcup_{n\geq 0} Y^n)(\bigcup_{n\geq 0} Y^n) = \bigcup_{m,n\geq 0} Y^n Y^m = \bigcup_{m,n\geq 0} Y^{n+m} = \bigcup_{k\geq 0} Y^k = H$.

Aby udowodnić, że $H^{-1} \subseteq H$ pokażemy najpierw, że $(Y^n)^{-1} = Y^n$. Dla $n = 0$ teza jest oczywista. Dla $n = 1$ mamy $(Y)^{-1} = (X\cup X^{-1})^{-1} = X^{-1} \cup X = Y$. Jeśli $n > 1$ oraz wiemy już, że $(Y^{n-1})^{-1} = Y^{n-1}$, to $(Y^n)^{-1} = (Y^{n-1}Y)^{-1} = Y^{-1}(Y^{n-1})^{-1} = YY^{n-1} = Y^n$. Stąd $H^{-1} = (\bigcup_{n\geq 0} Y^n)^{-1} = \bigcup_{n\geq 0}(Y^n)^{-1} = \bigcup_{n\geq 0} Y^n = H$, a więc H istotnie jest podgrupą. Ponieważ $X \subseteq H$, więc $\langle X\rangle \subseteq H$, a to oznacza, że $\langle X\rangle = H$. □

Szczególną postać powyższe twierdzenia przyjmuje, gdy zbiór X jest jednoelementową.

Wniosek. *Jeśli G jest grupą cykliczną generowaną przez element a, to*

$$G = \{a^k \mid k \in \mathbb{Z}\}.$$

Dowód. Przez prostą indukcję można pokazać, że jeśli $X = \{a\}$, to $\bigcup_{0\leq m\leq n}(X \cup X^{-1})^m = \{a^k \mid |k| \leq n\}$, co natychmiast implikuje tezę wniosku wobec powyższego stwierdzenia. □

2.4.4. Powyższy wniosek pozwala nam zidentyfikować obrać poniższego homomorfizmu.

Stwierdzenie. *Jeśli G jest grupą oraz $a \in G$, to funkcja $\varphi : \mathbb{Z} \to G$ dana wzorem $\varphi(k) = a^k$ dla $k \in \mathbb{Z}$ jest homomorfizmem grup takim, że* $\operatorname{Im}\varphi = \langle a\rangle$.

Dowód. Fakt, że φ jest homomorfizmem wynika z własności operacji podnoszenia do potęgi opisanej w paragrafie 1.1.4. Część tezy poświęcona obrazowi jest natomiast konsekwencją powyższego wniosku. □

2.4.5. Opiszemy teraz podgrupy grupy $\mathbb{Z}$.

Stwierdzenie. *Jeśli H jest podgrupą grupy $\mathbb{Z}$ oraz $H \neq 0$, to istnieje $m > 0$ takie, że $H = \mathbb{Z}m$.*

Dowód. Zauważmy, że podgrupy grupy $\mathbb{Z}$ pokrywają się z ideałami pierścienia $\mathbb{Z}$. W szczególności, elementy $a_1, \ldots, a_n$ generują H jako podgrupę wtedy i tylko wtedy, gdy generują H jako ideał. Ponieważ $\mathbb{Z}$ wraz z funkcją $n \mapsto |n|$ jest dziedziną Euklidesa, więc teza wynika z Twierdzenia 1.3.6. □

2.4.6. Powyższe obserwacje będą przydatne w dowodzie następującego twierdzenia klasyfikującego grupy cykliczne.

TWIERDZENIE. *Niech G będzie grupą cykliczną generowaną przez element a.*

(1) *Jeśli rząd grupy G jest nieskończony, to odwzorowanie $\mathbb{Z} \ni k \mapsto a^k \in G$ jest izomorfizmem.*
(2) *Jeśli $|G| = m$, to odwzorowanie $\mathbb{Z}_m \ni k \mapsto a^k \in G$ jest izomorfizmem.*

DOWÓD. Niech $\varphi : \mathbb{Z} \to G$ będzie funkcją daną wzorem $\varphi(k) = a^k$ dla $k \in \mathbb{Z}$. Ze Stwierdzenia 2.4.4 wynika, że φ jest homomorfizmem grup oraz $\operatorname{Im}\varphi = G$. Wiemy, że $\operatorname{Ker}\varphi$ jest podgrupą grupy $\mathbb{Z}$. Na mocy poprzedniego stwierdzenia wiemy zatem, że gdy $\operatorname{Ker}\varphi = 0$ lub istnieje $m > 0$ takie, że $\operatorname{Ker}\varphi = \mathbb{Z}m$. Gdy $\operatorname{Ker}\varphi = 0$, to φ jest izomorfizmem. Gdy $\operatorname{Ker}\varphi = \mathbb{Z}m$, to z Pierwszego Twierdzenia o Izomorfizmie wynika, że odwzorowanie $\phi : \mathbb{Z}/\mathbb{Z}m \to G$ dane wzorem $\phi(k+\mathbb{Z}m) = a^k$ dla $k \in \mathbb{Z}$ jest izomorfizmem. Przypomnijmy, że funkcja $\psi : \mathbb{Z}/\mathbb{Z}m \to \mathbb{Z}_m$ dana wzorem $\psi(k) =$ reszta z dzielenia k przez m jest izomorfizmem. Stąd $\phi\psi^{-1} : \mathbb{Z}_m \to G$ jest izomorfizmem. Zauważmy, że $\psi^{-1}(k) = k + \mathbb{Z}m$ dla $k \in \mathbb{Z}_m$, skąd $\phi\psi^{-1}(k) = a^k$. Powyższe rozważania kończą dowód. Istotnie, z porównania ilości elementów w dziedzinie i przeciwdziedzinie wynika, że jeśli rząd grupy G jest nieskończony, to mamy do czynienia z przypadkiem $\operatorname{Ker}\varphi = 0$, zaś gdy $|G| = m$, to $\operatorname{Ker}\varphi = \mathbb{Z}m$. □

2.4.7. Na zakończenie tego paragrafu scharakteryzujemy w inny sposób rząd elementu grupy.

STWIERDZENIE. *Niech G będzie grupą oraz $a \in G$.*

(1) *Jeśli rząd elementu a jest nieskończony, to $a^k = 1$ wtedy i tylko wtedy, gdy $k = 0$ oraz elementy a^k, $k \in \mathbb{Z}$, są parami różne.*
(2) *Niech $|a| = m$.*
   (a) *m jest najmniejszą liczbą naturalną $n > 0$ taką, że $a^n = 1$.*
   (b) *$a^k = 1$ wtedy i tylko wtedy, gdy m dzieli k.*
   (c) *$a^k = a^l$ wtedy i tylko wtedy, gdy $k \equiv l \pmod m$.*
   (d) *$\langle a\rangle = \{1 = a^0, a = a^1, a^2, \ldots, a^{m-1}\}$.*

DOWÓD. Przypuśćmy najpierw, że rząd elementu a jest nieskończony. Wtedy funkcja $\mathbb{Z} \ni k \mapsto a^k \in \langle a\rangle$ jest izomorfizmem. Stąd wynika teza. Podobnie postępujemy w przypadku, gdy rząd elementu $|a| = m$, z tą różnicą, że tym razem wykorzystujemy izomorfizm $\mathbb{Z}_m \ni k \mapsto a^k \in \langle a\rangle$. □

Ćwiczenia

2.4.1. Udowodnić, że podgrupy grupy $\mathbb{C}^*$ generowana przez $\imath$ jest izomorficzna z $\mathbb{Z}_4$.

2.4.2. Niech Q_8 będzie podgrupą grupy $\mathrm{GL}_2(\mathbb{C})$ generowaną przez macierze

$$A = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] \qquad \text{i} \qquad B = \left[\begin{smallmatrix} 0 & \imath \\ -\imath & 0 \end{smallmatrix}\right].$$

Udowodnić, że grupa Q nie jest przemienna i ma 8 elementów. Udowodnić, że wszystkie podgrupy grupy Q_8 są dzielnikami normalnymi.

2.4.3. Niech D_4 będzie podgrupą grupy $\mathrm{GL}_2(\mathbb{R})$ generowaną przez macierze

$$A = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right] \qquad \text{i} \qquad B = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right].$$

Udowodnić, że grupa D_4 nie jest przemienna i ma 8 elementów. Znaleźć dwie podgrupy H i K grupy D_4 takie, że H jest dzielnikiem normalnym grupy D_4 oraz K jest dzielnikiem normalnym grupy H, ale K nie jest dzielnikiem normalnym grupy D_4.

2.4.4. Niech p będzie liczbą pierwszą. Udowodnić, że $Z(p^\infty)$ jest podgrupą grupy $\mathbb{Q}/\mathbb{Z}$ generowaną przez elementy $\frac{1}{p^n} + \mathbb{Z}$, $n > 0$.

2.4.5. Niech p będzie liczbą pierwszą. Udowodnić, że każda grupa rzędu p jest cykliczna.

2.4.6. Niech G będzie grupą. Udowodnić następujące równości.

(a) $|a^{-1}| = |a|$ dla dowolnego $a \in G$.
(b) $|ab| = |ba|$ dla dowolnych $a, b \in G$.
(c) $|bab^{-1}| = |a|$ dla dowolnych $a, b \in G$.

2.4.7. Niech G będzie grupą oraz $a \in G$. Jeśli $|a| < \infty$, to $|a^k| = \frac{|a|}{(|a|,k)}$ dla $k \in \mathbb{Z}$.

2.4.8. Niech G będzie grupą abelową taka oraz niech $a, b \in G$ będą elementami skończonego rzędu. Udowodnić, że istnieje element $c \in G$ taki, że $|c| = \frac{|a||b|}{(|a|,|b|)}$.

2.4.9. Niech G będzie grupą abelową rzędu mn taką, że $(m, n) = 1$. Udowodnić, że jeśli w grupie G istnieją elementy rzędu m i n, to grupa G jest cykliczna.

2.4.10. Niech $A = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right], B = \left[\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Q})$. Udowodnić, że $|A| = 4$, $|B| = 3$ oraz $|AB| = \infty$.

2.4.11. Udowodnić, że jeśli G jest grupą cykliczną oraz $\varphi : G \to H$ jest epimorfizmem, to H jest grupą cykliczną.

2.4.12. Niech $f : G \to H$ będzie homomorfizmem grup oraz $a \in G$. Jeśli $|a| < \infty$, to $|\varphi(a)| < \infty$ oraz $|a|$ dzieli $|\varphi(a)|$.

2.4.13. Udowodnić, że jeśli H jest podgrupą grupy cyklicznej G, to H jest grupą cykliczną.

2.4.14. Udowodnić, że grupa, która ma tylko skończoną ilość podgrup, jest skończona.

2.4.15. Udowodnić, że jeśli G jest grupą cykliczną rzędu skończonego oraz $m \mid |G|$, to G ma dokładnie jedną podgrupę rzędu m.

2.4.16. Niech G będzie grupą abelową oraz H będzie zbiorem wszystkich element grupy G, których rząd jest skończony. Udowodnić, że H jest podgrupą grupy G.

2.4.17. Niech G będzie grupą cykliczną rzędu nieskończonego generowaną przez element a. Udowodnić, że a oraz a^{-1} są jedynymi generatorami grupy G.

2.4.18. Niech G będzie grupą cykliczną generowaną przez element a rzędu m. Udowodnić, że a^k jest generatorem grupy G wtedy i tylko wtedy, gdy $(k, m) = 1$. Znaleźć wszystkie generatory grup $\mathbb{Z}_m$, $m = 2, \ldots, 10$.

2.4.19. Niech G będzie grupą cykliczną generowaną przez zbiór X. Udowodnić, że jeśli $\varphi, \psi : G \to H$ są takimi homomorfizmami, że $\varphi(a) = \psi(a)$ dla wszystkich $a \in X$, to $\varphi = \psi$.

2.4.20. Niech G będzie grupą cykliczną generowaną przez element a. Udowodnić, że dla dowolnego $b \in G$ istnieje dokładnie jeden homomorfizm $\varphi : G \to G$ taki, że $\varphi(a) = b$. Pokazać, że φ jest automorfizmem wtedy i tylko wtedy, gdy b jest generatorem grupy G. Wyliczyć $\operatorname{Aut}\mathbb{Z}$ oraz $\operatorname{Aut}\mathbb{Z}_m$, $m = 2, \ldots, 10$.

2.4.21. Niech H będzie cykliczną podgrupą grupy G, która jest dzielnikiem normalnym grupy G. Udowodnić, że każda podgrupa grupy H jest dzielnikiem normalnym grupy G.

2.4.22. Niech p będzie liczbą pierwszą oraz niech $H \neq Z(p^\infty)$ będzie podgrupą grupy $Z(p^\infty)$,

(a) Udowodnić, że $|H| < \infty$ oraz, że istnieje $n \geq 0$ takie, że $H = \langle \frac{1}{p^n} + \mathbb{Z} \rangle$.
(b) Udowodnić, że $Z(p^\infty)/H \simeq Z(p^\infty)$.

2.4.23. Nich G będzie grupą nieskończoną. Udowodnić, że G jest grupą cykliczną wtedy i tylko wtedy, gdy $G \simeq H$ dla każdej podgrupy $H \neq 1$.

2.4.24. Niech K i L będą podgrupami grupy G oraz niech H będzie najmniejszą podgrupą grupy G zawierającą K i L. Udowodnić, że $[H : L] \geq [K : K \cap L]$.

2.4.25. Niech p i q będą liczbami pierwszymi takimi, że $p > q$. Udowodnić, że jeśli G jest grupą rzędu pq, to G ma co najwyżej jedną podgrupę rzędu p.

2.4.26. Udowodnić, że jeśli H jest dzielnikiem normalnym grupy G takim, że grupy H i G/H są skończenie generowane, to grupa G jest skończenie generowana.

2.5. Działania grup na zbiorach

W tym paragrafie omówimy pojęcie działania grupy na zbiorze, które odgrywa ważna rolę w wielu działach matematyki.

2.5.1. *Działaniem grupy G na zbiorze X* nazywamy każdą funkcję $G \times X \to X$, $(a, x) \mapsto ax$, taką, że

$$1x = x \text{ i } (ab)x = a(bx)$$

dla dowolnych $a, b \in G$ oraz $x \in X$. Mówimy też, że w powyższej sytuacji *grupa G działa na zbiorze X*.

Najbardziej podstawowym przykładem działania jest następująca sytuacja. Niech X będzie zbiorem oraz niech G będzie podgrupą grupy $\mathscr{S}(X)$. Wtedy wzór

$$G \times X \ni (f, x) \mapsto f(x) \in X$$

zadaje działanie grupy G na zbiorze X. Niech teraz G będzie dowolną grupą i H jej podgrupą. Innymi typowymi przykładami działań są: działanie podgrupy H na G przez *lewe przesunięcia* dane wzorem

$$H \times G \ni (a, b) \mapsto ab \in G,$$

przez *prawe przesunięcia* dane wzorem

$$H \times G \ni (a, b) \mapsto ba^{-1} \in G,$$

oraz przez *sprzężenia*

$$H \times G \ni (a, b) \mapsto aba^{-1} \in G.$$

Podobnie jak kongruencje można było opisać poprzez dzielniki normalne, tak zamiast mówić o działaniach grupy G na zbiorze X można mówić o homomorfizmach $G \to \mathscr{S}(X)$.

Stwierdzenie.

(1) *Jeśli $\delta : G \times X \to X$ jest działaniem grupy G zbiorze X, to funkcja $f_\delta : G \to \mathscr{S}(X)$ dana wzorem*

$$(f_\delta(a))(x) = \delta(a, x) \text{ dla } a \in G \text{ i } x \in X$$

jest homomorfizmem grup.

(2) *Jeśli X jest zbiorem oraz $f : G \to \mathscr{S}(X)$ jest homomorfizmem grup, to funkcja $\delta_f : G \times X \to X$ dana wzorem*

$$\delta_f(a, x) = (f(a))(x) \text{ dla } a \in G \text{ i } x \in X$$

jest działaniem grupy G na zbiorze G.

(3) *Jeśli δ jest działaniem grupy G zbiorze X, to $\delta_{f_\delta} = \delta$.*

(4) *Jeśli X jest zbiorem oraz $f : G \to \mathscr{S}(X)$ jest homomorfizmem grup, to $f_{\delta_f} = f$.*

Dowód. Ćwiczenie. □

Konsekwencją powyższej obserwacji jest możliwość traktowania każdej grupy jako podgrupy odpowiednio dużej grupy symetrycznej.

Wniosek (Cayley). *Jeśli G jest grupą, to istnieje monomorfizm grup $G \to \mathscr{S}(G)$.*

Dowód. Niech $\delta : G \times G \to G$ będzie działaniem grupy G na G przez lewe przesunięcia. Wtedy $f_\delta : G \to S(G)$ jest homomorfizmem grup. Musimy sprawdzić, że $\operatorname{Ker} f_\delta = 1$. Zauważmy, że $f_\delta(a) = \mathbb{1}_G$ wtedy i tylko wtedy, gdy $ab = b$ dla dowolnego $b \in G$. W szczególności $a = a1 = 1$, co kończy dowód. □

2.5.2. Zbadamy teraz bliżej działanie przez sprzężenia.

Stwierdzenie. *Jeśli δ jest działaniem grupy G na G przez sprzężenia, to* $\operatorname{Im} f_\delta \subseteq \operatorname{Aut}(G)$.

Dowód. Należy sprawdzić, że dla każdego $a \in G$ funkcja $\varphi_a = f_\delta(a)$ jest homomorfizmem grupy G, co wynika natychmiast z bezpośrednich rachunków. □

Automorfizmy grupy G postaci $f_\delta(a)$ dla $a \in G$, gdzie δ jest działaniem grupy G na G przez sprzężenia, nazywamy *automorfizmami wewnętrznymi*. Zbiór wszystkich automorfizmów wewnętrznych grupy G tworzy grupę (gdyż jest równy $\operatorname{Im} f_\delta$), którą nazywamy *grupą automorfizmów wewnętrznych grupy* G i oznaczamy $\operatorname{Inn}(G)$.

2.5.3. *Centrum grupy* G nazywamy zbiór wszystkich elementów $a \in G$ takich, że $ab = ba$ dla dowolnego $b \in G$. Centrum grupy G oznaczamy $C(G)$. Zauważmy, że $C(G) = G$ wtedy i tylko wtedy, gdy G jest grupą abelową. Dla przykładu zauważmy, że jeśli K jest ciałem, to $C(\mathrm{GL}_n(K))$ składa się z wszystkich macierzy diagonalnych.

Stwierdzenie. *Jeśli δ jest działaniem grupy G na G przez sprzężenia, to* $\operatorname{Ker} f_\delta = C(G)$. *W szczególności, $C(G)$ jest dzielnikiem normalnym grupy G oraz* $\operatorname{Inn}(G) \simeq G/C(G)$.

Dowód. Bezpośredni rachunek. □

Zauważmy, że $C(G)$ jest zawsze grupą abelową.

2.5.4. Wprowadzimy teraz pojęcie podgrup sprzężonych.

Lemat. *Jeśli H jest podgrupą grupy G oraz $a \in G$, to aHa^{-1} jest podgrupą grupy G izomorficzną z H.*

Dowód. Ze Stwierdzenia 2.5.2 wynika, że funkcja $\varphi : G \to G$ dana wzorem $\varphi(b) = aba^{-1}$, $b \in G$, jest automorfizmem grupy G. Stąd funkcja $\varphi i : H \to G$, gdzie $i : H \to G$ jest naturalnym włożeniem, jest monomorfizmem. Ponieważ $\operatorname{Im}(gi) = aHa^{-1}$, więc teza wynika z Pierwszego Twierdzenia o Izomorfizmie. □

Jeśli H i K są podgrupami grupy G oraz istnieje element $a \in G$ taki, że $K = aHa^{-1}$, to grupy H i K nazywamy *sprzężonymi* (zauważmy, że w tej sytuacji $H = a^{-1}Ka = a^{-1}K(a^{-1})^{-1}$). Możemy powiedzieć, że podgrupa G jest dzielnikiem normalnym wtedy i tylko wtedy, gdy $H = K$ dla dowolnej podgrupy K sprzężonej z H.

Ogólniej, niech H będzie podgrupą grupy G. Przez $N_G(H)$ oznaczać będziemy zbiór wszystkich $a \in G$ dla których $aHa^{-1} = H$. Zbiór $N_G(H)$ nazywamy *normalizatorem podgrupy H w grupie G*. Normalizator podgrupy H w grupie G jest podgrupą grupy G oraz H jest dzielnikiem normalnym grupy $N_G(H)$.

2.5.5. Jednym z działów matematyki, w którym wykorzystywane są działania grup jest kombinatoryka. Omówimy teraz ogólny schemat związany z rachunkowymi aspektami działań grup na zbiorach. Jeśli grupa G działa na zbiorze X to dla dowolnego $x \in X$ przez G_x będziemy oznaczać zbiór $a \in G$ takich, że $ax = x$. Zbiór G_x nazywamy *stabilizatorem elementu x*. Ponadto przez Gx oznaczać będziemy zbiór wszystkich elementów postaci $\{ax \mid a \in G\}$. Zbiór Gx będziemy nazywać *orbitą elementu x*.

STWIERDZENIE. *Załóżmy, że grupa G działa na zbiorze X.*

(1) *Relacja $\sim$ na zbiorze X dana wzorem*

$$x \sim y \text{ wtedy i tylko wtedy, gdy } y = ax \text{ dla } a \in G$$

jest relacją równoważności.

(2) *Klasą abstrakcji elementu $x \in X$ w powyższej relacji jest Gx.*

(3) *Dla każdego $x \in X$ zbiór G_x jest podgrupą grupy G.*

(4) *Jeśli $x \in X$ oraz $a \in G$, to $G_{ax} = aG_xa^{-1}$.*

DOWÓD. Bezpośrednie rachunki. □

Rachunkowy aspekt działania grup na zbiorach widoczny jest w poniższym twierdzeniu.

TWIERDZENIE. *Jeśli grupa G działa na zbiorze X oraz $x \in X$, to funkcja $G/G_x \in aG_x \mapsto ax \in Gx$ jest bijekcją.*

DOWÓD. Bezpośredni rachunek. □

Ćwiczenia

2.5.1. Niech n będzie dodatnią liczbą całkowitą oraz H będzie jedyną liczbą podgrupą grupy G rzędu n. Udowodnić, że H jest dzielnikiem normalnym grupy G.

2.5.2. Niech A będzie abelowym dzielnikiem normalnym grupy G. Udowodnić, że definicja

$$G/A \times A \ni (aA, b) \mapsto aba^{-1} \in A,\ a \in G,\ b \in A,$$

jest poprawna oraz definiuje działanie grupy G/A na A.

2.5.3. Udowodnić, że $C(\mathscr{S}_n) = 1$ dla $n \geq 3$.

2.5.4. Niech H i K będą podgrupami grupy G takimi, że H jest dzielnikiem normalnym grupy K. Udowodnić, że $K \subseteq N_G(H)$.

2.5.5. Niech a i b będą takimi dwoma elementami grupy G, że $a \neq b$, istnieje $c \in G$ takie, że $cac^{-1} = b$ oraz $dad^{-1} \in \{a, b\}$ dla każdego $d \in G$. Udowodnić, że $N = \langle a, b\rangle$ jest dzielnikiem normalnym grupy G takim, że $N \neq 1$ oraz $N \neq G$.

2.5.6. Niech H będzie podgrupą grupy G. *Centralizatorem podgrupy H w grupie G* nazywamy zbiór tych $g \in G$, dla których $gh = hg$ dla wszystkich $h \in H$. *Centralizator podgrupy H w grupie G* oznaczamy $C_G(H)$. Udowodnić, że $C_G(H)$ jest dzielnikiem normalnym grupy $N_G(H)$. Pokazać, że grupa $N_G(H)/C_G(H)$ jest izomorficzna z pewną podgrupą grupy $\operatorname{Aut} H$.

2.5.7. Niech G będzie grupą. Udowodnić, że $\operatorname{Inn} G$ jest dzielnikiem normalnym grupy $\operatorname{Aut} G$.

2.5.8. Podać przykład automorfizmu grupy $\mathbb{Z}_6$, który nie jest automorfizmem wewnętrznym.

2.5.9. Udowodnić, że jeśli grupa $G/C(G)$ jest cykliczna, to grupa G jest abelowa.

2.5.10. Niech G będzie grupą taką, że istnieje element $a \in G$ taki, że $a^2 \neq 1$. Udowodnić, że grupa G posiada automorfizm różny od identyczności. (*Wskazówka*: Rozpatrzyć osobno przypadki gdy G jest abelowa i gdy G nie jest abelowa).

2.5.11. Niech H będzie podgrupą grupy G i niech δ będzie działaniem grupy G na G/H przez lewe przesunięcia:

$$G \times G/H \ni (a, bH) \mapsto abH \in G/H.$$

Udowodnić, że $\operatorname{Ker} f_\delta \subseteq H$.

2.5.12. Udowodnić, że jeśli grupa G zawiera podgrupę H taką, że $H \neq G$ i $[G : H] < \infty$, to grupa G zawiera dzielnik normalny N taki, że $N \neq G$ oraz $[G : N] < \infty$.

2.5.13. Załóżmy, że grupa G posiada podgrupę indeksu n, która nie zawiera dzielnika normalnego grupy G różnego od 1. Udowodnić, że grupa G jest izomorficzna z podgrupą grupy $\mathscr{S}_n$.

2.5.14. Niech G będzie grupą skończoną oraz niech p będzie najmniejszą liczbą pierwszą dzielącą $|G|$. Udowodnić, że jeśli H jest podgrupą grupy G taką, że $[G : H] = p$, to p jest dzielnikiem normalnym grupy G.

2.5.15. Niech G będzie grupą rzędu pn, gdzie p jest liczbą pierwszą oraz $0 < n < p$. Udowodnić, że jeśli H jest podgrupą grupy G rzędu p, to H jest dzielnikiem normalnym grupy G.

2.6. Twierdzenia Sylowa

W tym paragrafie udowodnimy twierdzenia Sylowa stanowiące fundamentalny fakt dotyczący struktury grup skończonych.

2.6.1. Dla grupy G działającej na zbiorze X przez X^G będziemy oznaczać zbiór *punktów stałych tego działania*, tzn. zbiór wszystkich $x \in X$ dla których $Gx = \{x\}$ (równoważnie, $G_x = G$). Poniższy lemat będzie wielokrotnie wykorzystywany.

LEMAT. *Jeśli p jest liczbą pierwszą oraz G jest grupą rzędu p^n, $n \geq 0$, która działa na zbiorze X, to $|X^G| \equiv |X| \pmod{p}$.*

DOWÓD. Ze Stwierdzenia 2.5.5 wynika, że istnieją elementy $x_1, \ldots, x_k \in X$ takie, że $X = |X^G| \cup Gx_1 \cup \cdots \cup Gx_k$, $Gx_i \cap Gx_j = \varnothing$, $i \neq j$, oraz $|Gx_i| > 1$, $i = 1, \ldots, n$. Z Twierdzenia 2.5.5 oraz z Twierdzenia Lagrange'a wynika, że $|Gx_i|$ dzieli $|G| = p^n$. Ponieważ $|Gx_i| > 1$ oraz p jest liczbą pierwszą, więc wnioskujemy stąd, że p dzieli $|G_{x_i}|$, $i = 1, \ldots, n$, co kończy dowód. □

2.6.2. Jako pierwsze zastosowanie powyższego lematu udowodnimy następujące twierdzenie.

TWIERDZENIE (Cauchy). *Jeśli p jest liczbą pierwszą oraz G jest grupą skończoną, której rząd jest podzielny przez p, to w grupie G istnieje element, którego rząd jest równy p.*

DOWÓD. Niech X będzie zbiorem wszystkich ciągów $(a_1, \ldots, a_p)$ elementów grupy G takich, że $a_1 \cdots a_p = 1$. Zauważmy, że $|X| = |G|^{p-1}$, zatem p dzieli $|X|$. Rozważmy działanie grupy $\mathbb{Z}_p$ na zbiorze X dane wzorem

$$(k, (a_1, \ldots, a_p)) \mapsto (a_{k+1}, \ldots, a_p, a_1, \ldots, a_k).$$

Zauważmy, że $X^{\mathbb{Z}_p} = \{(a, \ldots, a) \mid a^p = 1\}$. Z poprzedniego lematu wynika, że p dzieli $|X^{\mathbb{Z}_p}|$. Ponieważ mamy $(1, \ldots, 1) \in X^{\mathbb{Z}_p}$, więc $|X^{\mathbb{Z}_p}| \geq p > 1$. W szczególności istnieje $a \neq 1$ takie, że $a^p = 1$. Ponieważ p jest liczbą pierwszą, więc ze Stwierdzenia 2.4.7 wynika, że $|a| = p$. □

Niech p będzie liczbą pierwszą. Grupę G nazwiemy *p-grupą*, jeśli rząd każdego elementu grupy G jest potęgą liczby p. Jeśli podgrupa H grupy G jest p-grupą, to H nazywamy *p-podgrupą*. Dzięki powyższemu twierdzeniu skończone p-grupy można scharakteryzować za pomocą ilości ich elementów.

WNIOSEK. *Jeśli p jest liczbą pierwszą oraz G jest grupą skończoną, to G jest p-grupą wtedy i tylko wtedy, gdy $|G|$ jest potęgą liczby p.*

DOWÓD. Oczywiście, jeśli $|G|$ jest potęgą liczby p, to z Twierdzenia Lagrange'a wynika, że rząd każdego elementu grupy G jest potęgą liczby p. Przypuśćmy teraz, że G jest p-grupą oraz niech liczba pierwsza q dzieli $|G|$. Wtedy z poprzedniego twierdzenia wynika, że istnieje element grupy G, którego rząd jest równy q. Stąd natychmiast otrzymujemy, że $q = p$, co kończy dowód. □

2.6.3. Udowodnimy teraz Pierwsze Twierdzenie Sylowa. Rozpoczniemy od następującego pomocniczego faktu.

LEMAT. *Jeśli p jest liczbą pierwszą oraz H jest p-podgrupą grupy skończonej G, to $[N_G(H) : H] \equiv [G : H] \pmod p$.*

DOWÓD. Grupa H działa na zbiorze G/H przez lewe przesunięcia zgodnie ze wzorem

$$H \times G/H \ni (a, bH) \mapsto abH \in G/H.$$

Zauważmy, że $bH \in (G/H)^H$ wtedy i tylko wtedy, gdy $b \in N_G(H)$. Stąd $|(G/H)^H| = [N_G(H) : H]$, co kończy dowód wobec Lematu 2.6.1. □

WNIOSEK. *Jeśli p jest liczbą pierwszą oraz H jest p-podgrupą grupy skończonej G taką, że p dzieli $[G : H]$, to $N_G(H) \neq H$. W szczególności istnieje p-podgrupa K grupy G taka, że H jest dzielnikiem normalnym grupy K oraz $[K : H] = p$.*

DOWÓD. Ponieważ $[N_G(H) : H] \equiv [G : H] \pmod p$, więc p dzieli $[N_G(H) : H]$. Stąd wynika teza pierwszej części, gdyż $[N_G(H) : H] \geq 1$.

Dla dowodu drugiej części wniosku zauważmy, że z Twierdzenia Cauchy'ego istnieje podgrupa L rzędu p w grupie $N_G(H)/H$. Niech $K = \varphi^{-1}(L)$, gdzie $\varphi : N_G(H) \to H$ jest naturalnym rzutowaniem. Wtedy K jest podgrupą grupy $N_G(H)$, a więc także grupy G. Ponadto $[K : H] = |L| = p$, zatem K jest p-grupą. Ponadto H jest dzielnikiem normalnym grupy K, gdyż $K \subseteq N_G(H)$. □

Przez prostą indukcję otrzymujemy, jako natychmiastowa konsekwencja powyższego wniosku, następujące twierdzenie.

TWIERDZENIE (Pierwsze Twierdzenie Sylowa). *Niech p będzie liczbą pierwszą oraz G będzie grupą rzędu $p^n m$, gdzie $n \geq 0$ oraz $(p, m) = 1$. Wtedy dla każdego $i = 0, \ldots, n$ istnieje podgrupa grupy G rzędu p^i oraz dla każdego $i = 0, \ldots, n-1$ każda podgrupa grupy G rzędu p^i jest dzielnikiem normalnym pewnej podgrupy grupy G rzędu p^{i+1}.* □

2.6.4. Jeśli p jest liczbą pierwszą, to podgrupę P grupy G nazywamy *p-podgrupą Sylowa*, jeśli P jest maksymalną (w sensie zawierania) p-podgrupą. Łatwo zauważyć, że każda p-podgrupa H grupy skończonej G jest zawarta w pewnej p-podgrupie Sylowa. Dowód tego samego faktu dla grup nieskończonych wymaga wykorzystania lematu Kuratowskiego–Zorna. W szczególności w każdej grupie G istnieje p-podgrupa Sylowa. Mamy też następujące konsekwencje Pierwszego Twierdzenia Sylowa.

WNIOSEK. *Niech p będzie liczbą pierwszą oraz G będzie grupą rzędu $p^n m$, gdzie $n \geq 0$ oraz $(p, m) = 1$.*

(1) *Podgrupa H grupy G jest p-podgrupą Sylowa wtedy i tylko wtedy, gdy $|H| = p^n$.*

(2) *Jeśli grupa H jest sprzężona z p-podgrupą Sylowa, to H jest p-podgrupą Sylowa.*

Dowód. Oczywiste. □

Z drugiego punktu powyższego wniosku wynika między innymi, że jeśli p jest liczbą pierwszą i w skończonej grupie G istnieje dokładnie jedna p-podgrupa Sylowa P, to P jest dzielnikiem normalnym grupy G. Okazuje się też, że implikację w drugim punkcie powyższego wniosku można odwrócić.

Twierdzenie (Drugie Twierdzenie Sylowa). *Niech p będzie liczbą pierwszą. Dowolne dwie p-podgrupy Sylowa grupy skończonej G są ze sobą sprzężone.*

Dowód. Niech P i Q będą dwoma p-podgrupami Sylowa grupy G. Grupa Q działa na zbiorze G/P przez lewe przesunięcia zgodnie ze wzorem

$$Q \times G/P \ni (a, bP) \mapsto abP \in G/P.$$

Wiemy, że $|(G/P)^Q| \equiv [G : Q] \pmod{p}$ na mocy Lematu 2.6.1. Ponieważ P jest p-podgrupą Sylowa, więc p nie dzieli $[G : Q]$, stąd $(G/P)^Q \neq \varnothing$. Zauważmy, że $aP \in (G/P)^Q$ wtedy i tylko wtedy, gdy $Q \subseteq aPa^{-1}$. Ponieważ $|Q| = |P| = |aPa^{-1}|$, więc $Q = aPa^{-1}$. □

2.6.5. Trzecie Twierdzenie Sylowa udziela nam informacji o ilości p-podgrup Sylowa grupy skończonej.

Twierdzenie (Trzecie Twierdzenie Sylowa). *Niech p będzie liczbą pierwszą oraz N będzie ilością p-podgrup Sylowa grupy skończonej G. Wtedy N dzieli $|G|$ oraz $N \equiv 1 \pmod{p}$.*

Dowód. Niech P będzie p-podgrupą Sylowa grupy G. Z Drugiego Twierdzenia Sylowa wynika, że N jest równe ilości podgrup sprzężonych z P. Zauważmy, że $aPa^{-1} = bPb^{-1}$ wtedy i tylko wtedy, gdy $aN_G(P) = bN_G(P)$, zatem $N = [G : N_G(P)]$ skąd wynika, że N dzieli $|G|$.

Niech X będzie zbiorem wszystkich p-podgrup Sylowa grupy G. Grupa P działa na X przez sprzężenia, tzn.

$$P \times X \ni (a, Q) \mapsto aQa^{-1} \in X.$$

Zauważmy, że jeśli $Q \in X^P$, to $P \subseteq N_G(Q)$. Zatem P jest p-podgrupą Sylowa grupy $N_G(Q)$, więc istnieje $a \in N_G(Q)$ taki, że $aQa^{-1} = P$. Ale $aQa^{-1} = Q$, zatem $Q = P$, więc $X^P = \{P\}$, co kończy dowód twierdzenia wobec Lematu 2.6.1. □

Ćwiczenia

2.6.1. Niech G będzie grupą rzędu p^n, gdzie p jest liczbą pierwszą oraz $n \geq 1$. Udowodnić, że $C(G) \neq 1$.

2.6.2. Niech G będzie grupą rzędu p^n, gdzie p jest liczbą pierwszą oraz $n \geq 1$. Udowodnić, że jeśli N jest dzielnikiem normalnym grupy G rzędu p, wtedy $N \subseteq C(G)$.

2.6.3. Niech p będzie liczbą pierwszą oraz niech P będzie p-podgrupą Sylowa grupy G. Udowodnić, że $N_G(N_G(P)) = P$.

2.6.4. Niech p będzie liczbą pierwszą oraz N będzie takim dzielnikiem normalnym grupy G, że N oraz G/N są p-grupami. Udowodnić, że G jest p-grupą.

2.6.5. Niech p będzie liczbą pierwszą oraz G skończoną p-grupą. Udowodnić, że jeśli H jest dzielnikiem normalnym grupy G takim, że $H \neq 1$, to $H \cap C(G) \neq 1$.

2.6.6. Niech G będzie grupą rzędu p^n, gdzie p będzie liczbą pierwszą oraz $n \geq 1$. Udowodnić, że dla każdego $k = 0, \ldots, n$ istnieje podgrupa normalna grupy G rzędu p^k.

2.6.7. Niech p będzie liczbą pierwszą oraz niech P będzie p-pogrupą Sylowa grupy skończonej G taką, że P jest dzielnikiem normalnym grupy G. Udowodnić, że $\varphi(P) \subseteq P$ dla dowolnego endomorfizmu $\varphi : G \to G$ grupy G.

2.6.8. Niech H będzie dzielnikiem normalnym grupy skończonej G. Udowodnić, że jeśli rząd grupy H jest potęgą liczby pierwszej p, to H jest zawarta w każdej p-podgrupie Sylowa grupy G.

2.6.9. Niech p i q będą liczbami pierwszymi takimi, że $p > q$. Jeśli G jest grupą rzędu $p^n q$, $n \geq 1$, to G zawiera jedyny dzielnik normalny rzędu p^n.

2.6.10. Udowodnić, że każda grupa G rzędu 12 (28, 56, 200) posiada dzielnik normalny różny od 1 oraz G.

2.6.11. Niech p będzie liczbą pierwszą. Udowodnić, że każda grupa rzędu p^2 jest abelowa.