

UNIwersytet w Białymstoku

Instytut Matematyki

Ryszard R. Andruszkiewicz

WYKŁADY Z ALGEBRY OGÓLNEJ

I

Białystok 2005

Copyright © Uniwersytet w Białymstoku, Białystok 2005

ISBN 83-7431-031-6

Korekta
Marcin Łuba

Redakcja techniczna i skład komputerowy
Ryszard R. Andruszkiewicz

Wydawnictwo Uniwersytetu w Białymstoku
15-097 Białystok, ul. M. Skłodowskiej-Curie 14,
tel. (085) 745 70 58, 745 70 59

Druk i oprawa:
Mazowieckie Zakłady Graficzne s.c.
tel. (086) 275 41 31

Spis treści

Wstęp	7
1 Pojęcie grupy	10
1.1 Określenie grupy	10
1.2 Całkowita potęga elementu grupy	13
1.3 Przykłady grup	14
2 Podgrupa grupy	18
3 Grupy cykliczne	24
3.1 Rząd elementu grupy	24
4 Warstwy, dzielniki normalne	31
4.1 Warstwy grupy względem podgrupy	31
4.2 Dzielnik normalny grupy	34
4.3 Komutant grupy	36
5 Grupa ilorazowa, iloczyn prosty, homomorfizm	38
5.1 Grupa ilorazowa	38
5.2 Iloczyn prosty grup	40
5.3 Homomorfizmy grup i ich własności	42
5.4 Twierdzenie o izomorfizmie	45
6 Przykłady homomorfizmów. Grupy permutacji I	47
6.1 Przykłady homomorfizmów grup	47
6.2 Grupy permutacji	51
7 Grupy permutacji II	56
7.1 Permutacje rozłączne	56

7.2	Rozkład permutacji na cykle	57
8	Zasadnicze twierdzenie algebry. Pojęcie pierścienia	63
8.1	Zasadnicze twierdzenie algebry i jego dowód	63
8.2	Pojęcie pierścienia	68
9	Podpierścienie, elementy odwracalne, dzielniki zera	71
9.1	Określenie podpierścienia	71
9.2	Przykłady pierścieni i podpierścieni	72
9.3	Elementy odwracalne	74
9.4	Dzielniki zera	75
10	Homomorfizmy i ideały	78
10.1	Pojęcie ideału pierścienia	78
10.2	Konstrukcja pierścienia ilorazowego	80
10.3	Ideały: pierwsze i maksymalne	81
10.4	Homomorfizmy pierścieni	83
11	Pierścienie wielomianów	87
11.1	Konstrukcja pierścienia wielomianów	87
11.2	Homomorfizmy na pierścieniach wielomianów	92
12	Ważne pierścienie	95
12.1	Dzielenie wielomianów	95
12.2	Dziedziny ideałów głównych	99
12.3	Arytmetyka dziedzin całkowitości	100
13	Rozkłady elementów pierścienia na czynniki	105
13.1	Wielomiany nierozkładalne w pierścieniach $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$.	105
13.2	Dziedziny z jednoznacznością rozkładu	109
14	Ciała i ich własności	111
14.1	Charakterystyka ciała	111
14.2	Podciała i ciała proste	112
14.3	Ciało ułamków	115
15	Rozszerzenia algebraiczne ciał	120
	Literatura	125

Wstęp

Niniejsza książka jest podręcznikiem do przedmiotu **Algebra ogólna I** wykładanego w Instytucie Matematyki Uniwersytetu w Białymstoku w oparciu o następujący program:

grupy : definicje i przykłady grup, podgrupy, twierdzenie Lagrange’a, grupy cykliczne, grupy przekształceń, grupy permutacji, twierdzenie Cayley’a, homomorfizmy, dzielniki normalne, grupy ilorazowe, twierdzenia o homomorfizmach.

pierścienie : definicje i przykłady, ideały, homomorfizmy, pierścienie ilorazowe, ideały maksymalne, pierścienie wielomianów, zasadnicze twierdzenie algebry, jednoznaczność rozkładu, twierdzenie Gaussa, pierścienie ideałów głównych.

ciała : definicje i przykłady, ciała proste, ciało ułamków dziedziny całkowitości, elementy algebraiczne, ciało liczb algebraicznych, stopień rozszerzenia ciał, rozszerzenia algebraiczne.

Wieloletnie doświadczenia autora związane z wykładaniem algebry ogólnej pokazały, że przedmiot ten sprawia spore trudności studentom. Okazało się, że powyższy program nie jest łatwo zrealizować w trakcie piętnastu wykładów w sposób przystępny dla słuchaczy bez dysponowania dobrymi materiałami dydaktycznymi. Okazało się też, że odsyłanie studentów do literatury nie jest (z wielu powodów) skutecznym rozwiązaniem problemu. Właśnie dlatego powstał ten skrypt. W oparciu o materiał tu umieszczony można sprawnie prowadzić wykłady ubogacając je dodatkowymi przykładami, uwagami dydaktycz-

nymi, informacjami historycznymi, ciekawostkami, zadaniami, problemami, itp.

Wskazane jest aby Czytelnik był obeznany z podstawowym kursem elementarnej teorii liczb oraz z podstawowym kursem algebry liniowej.

W podręczniku liczbami naturalnymi będziemy nazywali dodatnie liczby całkowite, zaś sam zbiór wszystkich liczb naturalnych będziemy oznaczali przez $\mathbb{N}$. Zatem $\mathbb{N} = \{1, 2, \dots\}$. Koniec dowodu oznaczamy symbolem $\square$.

Autor dziękuje mgr Marcinowi Łubie za pomoc w składzie komputerowym tego podręcznika.

Autor



Emil Artin
(1898 – 1962)



Augustin-Louis Cauchy
(1778 – 1857)



Evariste Galois
(1811 – 1832)



Carl Friedrich Gauss
(1777 – 1855)



David Hilbert
(1862 – 1943)



Joseph Louis Lagrange
(1736 – 1813)



Emma Amalie Noether
(1882 – 1935)



Henri Poincare
(1845 – 1912)



Ludwig Sylow
(1832 – 1918)



Joseph Wedderburn
(1882 – 1948)

Rozdział 1

Pojęcie grupy

1.1 Określenie grupy

Definicja 1. *Działaniem* w niepustym zbiorze A nazywamy każde odwzorowanie zbioru $A \times A$ w zbiór A . Jeżeli $\circ$ jest działaniem w zbiorze A i $a, b \in A$, to $\circ((a, b))$ oznaczamy przez $a \circ b$ i nazywamy *wynikiem działania* $\circ$ na parze (a, b) .

Działania będziemy oznaczali symbolami: $\circ$, $\cdot$, $+$, $\oplus$, itd.

Definicja 2. *Systemem algebraicznym* nazywamy układ postaci $(A, \circ_1, \dots, \circ_n, e_1, \dots, e_k)$, w którym A jest niepustym zbiorem, $\circ_1, \dots, \circ_n$ są działaniami w A oraz $e_1, \dots, e_k \in A$ są wyróżnionymi elementami zbioru A .

Działaniu w zbiorze skończonym A można przyporządkować tabelkę wpisując w lewym górnym rogu oznaczenie działania i wypisując dwukrotnie elementy zbioru A : raz w pierwszym rzędzie poziomym i raz w pierwszym rzędzie pionowym, a następnie wpisując na przecięciu rzędu poziomego odpowiadającego elementowi a i rzędu pionowego odpowiadającego elementowi b wynik omawianego działania na parze (a, b) . Odwrotnie, każda tabelka, która w pierwszym rzędzie poziomym i pierwszym rzędzie pionowym zawiera wszystkie elementy danego skończonego zbioru A napisane tylko jeden raz, a na pozostałych miejscach ma wpisane w dowolny sposób pewne elementy zbioru A ,

określa w A działanie. Wynikiem tego działania na parze (a, b) jest element stojący w rzędzie poziomym odpowiadającym a i rzędzie pionowym odpowiadającym b . Wynika stąd w szczególności, że w zbiorze n -elementowym można określić dokładnie n^2 różnych działań.

Niech $\circ$ będzie działaniem w zbiorze A . Powiemy, że

- (1) działanie $\circ$ jest *łączne*, jeżeli $\forall_{a,b,c \in A} (a \circ b) \circ c = a \circ (b \circ c)$,
- (2) działanie $\circ$ jest *przemienne*, jeżeli $\forall_{a,b \in A} a \circ b = b \circ a$,
- (3) $e \in A$ jest *elementem neutralnym* działania $\circ$, jeżeli $\forall_{a \in A} e \circ a = a \circ e = a$.

Można wykazać, że jeśli działanie $\circ$ w zbiorze A jest łączne, to wynik tego działania na układzie elementów $a_1, \dots, a_n \in A$ nie zależy od sposobu rozmieszczenia nawiasów. Na przykład

$$(a_1 \circ (a_2 \circ a_3)) \circ a_4 = (a_1 \circ a_2) \circ (a_3 \circ a_4) = a_1 \circ (a_2 \circ (a_3 \circ a_4)) = \\ = a_1 \circ ((a_2 \circ a_3) \circ a_4) = ((a_1 \circ a_2) \circ a_3) \circ a_4.$$

Pozwala to na pomijanie nawiasów i używanie zapisu $a_1 \circ a_2 \circ \dots \circ a_n$ dla dowolnej liczby naturalnej n .

Uwaga 1. Łatwo zauważyć, że działanie w zbiorze skończonym jest przemienne wtedy i tylko wtedy, gdy jego tabelka jest symetryczna względem głównej przekątnej. W szczególności w zbiorze n -elementowym istnieje dokładnie $n^{\frac{n(n-1)}{2}}$ różnych działań przemiennych.

Uwaga 2. Każde działanie w zbiorze A może posiadać co najwyżej jeden element neutralny. Rzeczywiście, niech e i f będą elementami neutralnymi działania $\circ$ w zbiorze A . Wtedy w szczególności $e \circ a = a$ oraz $b \circ f = b$ dla dowolnych $a, b \in A$. Podstawiając $a = f$ i $b = e$ uzyskamy stąd, że $e \circ f = f$ i $e \circ f = e$, skąd $e = f$.

Definicja 3. Grupą nazywamy system algebraiczny $(G, \circ, e)$ spełniający następujące warunki (aksjomaty):

- (G1.) $\forall_{a,b,c \in G} (a \circ b) \circ c = a \circ (b \circ c)$,
- (G2.) $\forall_{a \in G} e \circ a = a \circ e = a$,
- (G3.) $\forall_{a \in G} \exists_{x \in G} a \circ x = x \circ a = e$.

Definicja 4. Grupę $(G, \circ, e)$ nazywamy *abelową*, jeżeli działanie $\circ$ jest przemienne.

Nazwa *grupa abelowa* pochodzi od nazwiska norweskiego matematyka Nielsa Henrika Abela (1802-1829), który jako pierwszy prowadził systematyczne badania wykorzystujące własności grup przemennych.

Uwaga 3. W dowolnej grupie $(G, \circ, e)$ zachodzą następujące *prawa skracania równości*:

(I) $\forall_{a,b,c \in G} [a \circ b = a \circ c \Rightarrow b = c]$ oraz (II) $\forall_{a,b,c \in G} [b \circ a = c \circ a \Rightarrow b = c]$.

Rzeczywiście, na mocy **(G3)** istnieje $x \in G$ taki, że $x \circ a = a \circ x = e$, więc jeżeli $a \circ b = a \circ c$, to $x \circ (a \circ b) = x \circ (a \circ c)$, skąd z **(G1)** $(x \circ a) \circ b = (x \circ a) \circ c$, czyli $e \circ b = e \circ c$. Zatem z **(G2)** $b = c$, co dowodzi (I). Dowód (II) jest analogiczny.

Uwaga 4. Element x w aksjomacie **(G3)** jest wyznaczony jednoznacznie przez element a , gdyż jeżeli dodatkowo $y \in G$ spełnia warunek $a \circ y = y \circ a = e$, to $a \circ x = a \circ y$, więc z uwagi 3, $x = y$. Ten dokładnie jeden element x nazywamy *elementem odwrotnym (przeciwnym)* do a i oznaczamy przez a^{-1} (przez $-a$, gdy $\circ = +$). Z uwagi 3 wynika od razu, że x jest elementem odwrotnym do a wtedy i tylko wtedy, gdy $a \circ x = e$. Ponieważ $a^{-1} \circ a = e$, więc a jest elementem odwrotnym do a^{-1} , skąd mamy wzór

$$(a^{-1})^{-1} = a \text{ dla każdego } a \in G.$$

Ponadto dla dowolnych $a, b \in G$ zachodzi wzór:

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}.$$

Rzeczywiście, wystarczy zauważyć, że $(a \circ b) \circ (b^{-1} \circ a^{-1}) = e$. Z łączności działania $\circ$ mamy $(a \circ b) \circ (b^{-1} \circ a^{-1}) = ((a \circ b) \circ b^{-1}) \circ a^{-1} = (a \circ (b \circ b^{-1})) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$.

Przez prostą indukcję uzyskujemy stąd, że dla dowolnej liczby naturalnej n i dla dowolnych elementów $a_1, \dots, a_n$ grupy G zachodzi wzór:

$$(a_1 \circ a_2 \circ \dots \circ a_n)^{-1} = a_n^{-1} \circ \dots \circ a_2^{-1} \circ a_1^{-1}.$$

Uwaga 5. Niech $(G, \circ, e)$ będzie grupą i niech $a \in G$. Oznaczmy przez l_a odwzorowanie zbioru G w siebie dane wzorem $l_a(x) = a \circ x$

dla $x \in G$ oraz oznaczmy przez r_a odwzorowanie zbioru G w siebie dane wzorem $r_a(x) = x \circ a$ dla $x \in G$. Pokażemy, że wówczas l_a i r_a są bijekcjami G na G . Z uwagi 3 wynika od razu, że przekształcenia l_a i r_a są różnowartościowe. Ponadto dla każdego $b \in G$ jest $l_a(a^{-1} \circ b) = a \circ a^{-1} \circ b = e \circ b = b$ oraz $r_a(b \circ a^{-1}) = b \circ a^{-1} \circ a = b \circ e = b$, więc przekształcenia l_a i r_a są „na”.

Rzędem grupy $(G, \circ, e)$ nazywamy moc zbioru G . Rząd grupy $(G, \circ, e)$ będziemy oznaczali przez $|G|$. Jeśli $|G|$ jest liczbą naturalną, to mówimy, że grupa $(G, \circ, e)$ jest *skończona*. Z uwagi 5 wynika, że jeżeli $(G, \circ, e)$ jest grupą skończoną, to w każdym wierszu i w każdej kolumnie tabelki działania $\circ$ występują wszystkie elementy zbioru G .

1.2 Całkowita potęga elementu grupy

I. Niech $(G, \cdot, e)$ będzie grupą. Wówczas dla $a \in G$, a^{-1} jest elementem odwrotnym do a . Całkowitą potęgą elementu a określamy następująco:

1. $a^0 = e$,
2. $a^1 = a$,
3. $a^{n+1} = a^n \cdot a$ dla $n = 1, 2, \dots$
4. $a^{-n} = (a^{-1})^n$ dla $n = 1, 2, \dots$

Zatem dla $n = 1, 2, \dots$

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_n.$$

Można udowodnić, że dla dowolnych liczb całkowitych m , n i dla każdego $a \in G$ zachodzą wzory:

$$(1) a^n \cdot a^m = a^{n+m} \text{ oraz } (2) (a^n)^m = a^{nm}.$$

Ponadto jeżeli $a, b \in G$ są takie, że $a \cdot b = b \cdot a$, to dla dowolnego całkowitego n zachodzi wzór:

$$(a \cdot b)^n = a^n \cdot b^n.$$

Zapis użyty w I nazywamy *multiplikatywnym* (od łacińskiego *mutiplicare* — mnożyć). W tym zapisie często element neutralny e oznacza się przez 1, chociaż nie musi to być liczba naturalna 1.

II. Niech $(G, +, 0)$ będzie grupą. Wówczas dla $a \in G$, $-a$ jest elementem przeciwnym do a . Całkowitą wielokrotność elementu a określamy następująco:

$$1'. 0 \cdot a = 0,$$

$$2'. 1 \cdot a = a,$$

$$3'. (n + 1) \cdot a = n \cdot a + a \text{ dla } n = 1, 2, \dots$$

$$4'. (-n) \cdot a = n \cdot (-a) \text{ dla } n = 1, 2, \dots$$

Taki zapis nazywamy *addytywnym* (od łacińskiego *addere* — dodawać) i z reguły jest on stosowany jedynie w przypadku grup abelowych. W tym zapisie element neutralny grupy jest oznaczany przez 0, chociaż nie musi to być liczba całkowita 0.

Z I wynika, że dla dowolnych liczb całkowitych m, n i dla każdego $a \in G$ zachodzą wzory:

$$(1)' n \cdot a + m \cdot a = (n + m) \cdot a \text{ oraz } (2)' n \cdot (m \cdot a) = (nm) \cdot a.$$

Jeżeli napiszemy *niech G będzie grupą*, to będziemy mieli na myśli grupę multiplikatywną z działaniem oznaczonym kropką, którą — tak jak w przypadku wyrażeń algebraicznych — często będziemy pomijać.

1.3 Przykłady grup

Przykład 1. Niech $G = \{a\}$ będzie dowolnym zbiorem jednoelementowym. W zbiorze tym można określić tylko jedno działanie: $a \cdot a = a$. Wówczas $(G, \cdot, a)$ jest grupą. Nazywamy ją *grupą trywialną*.

Przykład 2. Addytywne grupy liczbowe. Tak będziemy nazywać grupy, których elementami są pewne liczby zespolone, a działaniami — zwykle dodawanie liczb. Najbardziej typowymi przykładami takich grup są: addytywna grupa liczb całkowitych $(\mathbb{Z}, +, 0)$ oznaczana przez $\mathbb{Z}^+$, wymiernych $(\mathbb{Q}, +, 0)$ oznaczana przez $\mathbb{Q}^+$, rzeczywi-

stych $(\mathbb{R}, +, 0)$ oznaczana przez $\mathbb{R}^+$ i zespolonych $(\mathbb{C}, +, 0)$ oznaczana przez $\mathbb{C}^+$.

Przykład 3. Multiplikatywne grupy liczbowe. Elementami takich grup są pewne niezerowe liczby zespolone, natomiast działaniem — zwykle mnożenie liczb. Wśród nich najbardziej typowymi są:

$$(\{-1, 1\}, \cdot, 1), (\mathbb{Q}^*, \cdot, 1), (\mathbb{R}^*, \cdot, 1), (\mathbb{C}^*, \cdot, 1), (\mathbb{C}_n, \cdot, 1), (\mathbb{C}_\infty, \cdot, 1),$$

gdzie $K^* = K \setminus \{0\}$ dla $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, natomiast $\mathbb{C}_n$ jest zbiorem wszystkich zespolonych pierwiastków stopnia n z 1, tzn.

$$\mathbb{C}_n = \left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} : k = 0, 1, \dots, n-1 \right\}$$

i wreszcie $\mathbb{C}_\infty = \bigcup_{n=1}^{\infty} \mathbb{C}_n$. Z algebry liniowej wiemy, że $|\mathbb{C}_n| = n$. Ważnym przykładem z punktu widzenia klasyfikacji grup abelowych są grupy $\mathbb{C}_{p^\infty} = \bigcup_{n=1}^{\infty} \mathbb{C}_{p^n}$, dla liczb pierwszych p .

Przykład 4. Jeżeli V jest przestrzenią liniową nad ciałem K , to V z dodawaniem wektorów $+$ i wyróżnionym elementem θ (wektor zerowy) tworzy grupę abelową $(V, +, \theta)$. Stąd mamy np. grupy $(K^n, +, \theta)$ dla $n = 1, 2, \dots$

Przykład 5. Jeżeli K jest ciałem, to $(K \setminus \{0\}, \cdot, 1)$ tworzy grupę abelową. Nazywamy ją grupą multiplikatywną ciała K i oznaczamy przez K^* .

Przykład 6. Addytywna grupa reszt modulo m . Niech m będzie dowolną liczbą naturalną i niech $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$. W zbiorze $\mathbb{Z}_m$ określamy *dodawanie modulo m* , $\oplus_m$ przyjmując, że dla dowolnych $a, b \in \mathbb{Z}_m$:

$$a \oplus_m b = \text{reszta z dzielenia } a + b \text{ przez } m.$$

W oparciu o własności kongruencji łatwo wykazać, że $(\mathbb{Z}_m, +, 0)$ jest grupą abelową i $|\mathbb{Z}_m| = m$. Grupę tę będziemy oznaczali przez $\mathbb{Z}_m^+$.

Przykład 7. Multiplikatywna grupa reszt modulo m . Przy oznaczeniach przykładu 6 niech

$$\mathbb{Z}_m^* = \{k \in \mathbb{Z}_m : \text{NWD}(k, m) = 1\}.$$

W zbiorze $\mathbb{Z}_m^*$ określamy *mnożenie modulo m* , $\odot_m$ przyjmując, że dla dowolnych $a, b \in \mathbb{Z}_m^*$:

$$a \odot_m b = \text{reszta z dzielenia } a \cdot b \text{ przez } m.$$

W oparciu o elementarną teorię liczb można łatwo wykazać, że dla $m > 1$, $(\mathbb{Z}_m^*, \odot_m, 1)$ tworzy grupę abelową. Grupę tę będziemy oznaczali przez $\mathbb{Z}_m^*$. Z elementarnej teorii liczb wiadomo, że $|\mathbb{Z}_m^*| = \varphi(m)$, gdzie φ jest funkcją Eulera.

Przykład 8. Niech K będzie ciałem i niech $n \in \mathbb{N}$ oraz niech $GL_n(K)$ oznacza zbiór wszystkich odwracalnych macierzy kwadratowych stopnia n nad K . Wówczas z algebry liniowej wiadomo, że macierz kwadratowa A stopnia n nad K należy do $GL_n(K)$ wtedy i tylko wtedy, gdy $\det(A) \neq 0$. Stąd łatwo wyprowadzić (przy pomocy twierdzenia Cauchy'ego), że $GL_n(K)$ ze zwykłym mnożeniem macierzy i macierzą jednostkową I_n tworzy grupę. Oznaczamy ją przez $GL_n(K)$. Dla $n \geq 2$ ta grupa nie jest abelowa. Rzeczywiście, niech A oznacza macierz, która ma jedynkę na głównej przekątnej oraz na drugim miejscu w pierwszym wierszu, a na pozostałych miejscach same zera i niech B oznacza macierz, która ma same jedynki na głównej przekątnej oraz na drugim miejscu w pierwszej kolumnie. Wtedy $\det(A) = \det(B) = 1$, więc $A, B \in GL_n(K)$. Ale $A \cdot B \neq B \cdot A$, gdyż macierze $A \cdot B$ i $B \cdot A$ mają inne elementy stojące w lewym górnym rogu.

Przykład 9. Niech X będzie dowolnym niepustym zbiorem. Oznaczmy przez $S(X)$ zbiór wszystkich bijekcji $f : X \rightarrow X$. Niech $\circ$ oznacza składanie przekształceń w $S(X)$, tzn. dla $f, g \in S(X)$ i $x \in X$: $(f \circ g)(x) = f(g(x))$. Niech ponadto id_X oznacza przekształcenie tożsamościowe zbioru X na siebie. Ze wstępu do matematyki wynika, że wówczas $(S(X), \circ, id_X)$ tworzy grupę. Nazywamy ją *grupą symetryczną* zbioru X i oznaczamy przez $S(X)$. Można wykazać, że jeśli zbiór X ma co najmniej 3 elementy, to grupa $S(X)$ nie jest abelowa. Jeżeli $X = \{1, 2, \dots, n\}$, to zamiast $S(\{1, 2, \dots, n\})$ piszemy S_n i S_n nazywamy *grupą permutacji* zbioru n -elementowego. Oczywiście $|S_n| = n!$.

Przykład 10. Izometrią płaszczyzny Π nazywamy każde odwzorowanie Π na Π zachowujące odległość punktów. Jeżeli $F \subseteq \Pi$, to izometrią własną figury F nazywamy taką izometrię f płaszczyzny Π , że $f(F) = F$. Niech $\circ$ oznacza składanie przekształceń i niech I będzie przekształceniem tożsamościowym Π na siebie. Wówczas dla każdej figury $F \subseteq \Pi$ zbiór $\mathbb{I}(F)$ wszystkich izometrii własnych figury F tworzy grupę ze względu na składanie przekształceń z wyróżnionym elementem id_{Π} . Dla $n = 3, 4, \dots$ przez D_n będziemy oznaczali grupę izometrii własnych n -kąta foremnego. Łatwo zauważyć, że $|D_n| = 2n$ oraz grupa D_n nie jest abelowa. Ponadto grupa $\mathbb{I}(\Pi)$ jest nieskończona i nie jest abelowa.

Rozdział 2

Podgrupa grupy

Definicja 1. Podgrupą grupy $(G, \cdot, e)$ nazywamy taki podzbiór $H \subseteq G$, że $e \in H$, $h^{-1} \in H$ dla każdego $h \in H$ oraz $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$.

Przykład 1. Centrum grupy. Zbiór

$$Z(G) = \{a \in G : a \cdot g = g \cdot a \text{ dla każdego } g \in G\}$$

nazywamy *centrum* grupy G . Pokażemy, że $Z(G)$ jest podgrupą grupy G . Ponieważ dla każdego $g \in G$ jest $g \cdot e = e \cdot g = g$, więc $e \in Z(G)$. Niech $h \in Z(G)$. Wtedy dla każdego $g \in G$ jest $h \cdot g = g \cdot h$, skąd $g = h^{-1}gh$ oraz $h^{-1} \cdot g = g \cdot h^{-1}$, a więc $h^{-1} \in Z(G)$. Weźmy dowolne $h_1, h_2 \in Z(G)$. Wtedy dla dowolnego $g \in G$, $(h_1 h_2)g = h_1(h_2 g) = h_1(gh_2) = (h_1 g)h_2 = (gh_1)h_2 = g(h_1 h_2)$, skąd $h_1 h_2 \in Z(G)$. Zatem $Z(G)$ jest podgrupą grupy G . Zauważmy jeszcze, że grupa G jest abelowa wtedy i tylko wtedy, gdy $G = Z(G)$.

Z definicji 1 mamy od razu, że każda podgrupa H grupy $(G, \cdot, e)$ tworzy grupę ze względu na ograniczenie do H działania $\cdot$. Na odwrót, niech $(G, \cdot, e)$ będzie grupą i niech H będzie takim podzbiorem G , że H tworzy grupę ze względu na ograniczenie do H działania $\cdot$. Wtedy istnieje $f \in H$ będące elementem neutralnym grupy H . Zatem $f \cdot f = f$, skąd $f = e$, czyli $e \in H$. Ponadto z założenia $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$. Niech $h \in H$. Wtedy istnieje $x \in H$ takie, że $h \cdot x =$

$= x \cdot h = e$. Ale $h, x \in G$, więc $x = h^{-1}$, skąd $h^{-1} \in H$. Wobec tego H jest podgrupą grupy G . W ten sposób udowodniliśmy następujące

Stwierdzenie 1. *Niech $(G, \cdot, e)$ będzie grupą. Podzbiór $H \subseteq G$ jest podgrupą grupy G wtedy i tylko wtedy, gdy H tworzy grupę ze względu na ograniczenie do H działania $\cdot$. $\square$*

Przykład 2. Ze stwierdzenia 1 wynika od razu, że G i $\{e\}$ są podgrupami grupy $(G, \cdot, e)$. Pierwszą z nich nazywamy *podgrupą niewłaściwą*, zaś drugą — *trywialną*. Z definicji podgrupy wynika też, że **podgrupa trywialna jest jedyną podgrupą jednoelementową grupy G .**

Stwierdzenie 2. *Niepusty podzbiór $H \subseteq G$ jest podgrupą grupy $(G, \cdot, e)$ wtedy i tylko wtedy, gdy $h_1 \cdot h_2^{-1} \in H$ dla dowolnych $h_1, h_2 \in H$.*

Dowód. Niech H będzie podgrupą grupy $(G, \cdot, e)$. Weźmy dowolne $h_1, h_2 \in H$. Wtedy $h_2^{-1} \in H$, skąd $h_1 \cdot h_2^{-1} \in H$.

Na odwrót, niech H będzie niepustym podzbiorem zbioru G takim, że $h_1 \cdot h_2^{-1} \in H$ dla dowolnych $h_1, h_2 \in H$. Wtedy istnieje $x \in H$, skąd $e = x \cdot x^{-1} \in H$, czyli $e \in H$. Weźmy dowolne $h \in H$. Wtedy $h^{-1} = e \cdot h^{-1} \in H$, więc $h^{-1} \in H$. W końcu dla dowolnych $h_1, h_2 \in H$ mamy, że $h_1 \cdot h_2 = h_1 \cdot (h_2^{-1})^{-1} \in H$, czyli $h_1 \cdot h_2 \in H$. Zatem H jest podgrupą grupy G . $\square$

Przykład 3. Podgrupa cykliczna. Niech $(G, \cdot, e)$ będzie grupą i niech $a \in G$. Udowodnimy, że podzbiór

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$$

jest najmniejszą (w sensie inkluzji) podgrupą grupy G zawierającą element a . Ponieważ $a = a^1$, więc $a \in \langle a \rangle$. W szczególności $\langle a \rangle \neq \emptyset$. Weźmy dowolne $h_1, h_2 \in \langle a \rangle$. Wtedy istnieją liczby całkowite k_1, k_2 takie, że $h_1 = a^{k_1}$ i $h_2 = a^{k_2}$. Zatem $h_1 \cdot h_2^{-1} = a^{k_1} \cdot (a^{k_2})^{-1} = a^{k_1} \cdot a^{-k_2} = a^{k_1 - k_2} \in \langle a \rangle$. Zatem ze stwierdzenia 2, $\langle a \rangle$ jest podgrupą grupy G oraz dodatkowo $a \in \langle a \rangle$. Niech H będzie dowolną podgrupą grupy G taką, że $a \in H$. Wtedy ze stwierdzenia 1 mamy, że $a^k \in H$ dla każdego $k \in \mathbb{Z}$, czyli $\langle a \rangle \subseteq H$. Zatem $\langle a \rangle$ jest najmniejszą podgrupą grupy G

zawierającą element a . Nazywamy ją *podgrupą cykliczną generowaną przez element a* . Natomiast a nazywamy *generatorem* podgrupy $\langle a \rangle$.

Definicja 2. Powiemy, że grupa G jest *cykliczna*, jeżeli istnieje element $a \in G$ (zwany *generatorem* tej grupy) taki, że $G = \langle a \rangle$.

Stwierdzenie 3. *Każda grupa cykliczna jest abelowa.*

Dowód. Niech G będzie grupą cykliczną o generatorze a . Wtedy $G = \{a^k : k \in \mathbb{Z}\}$. Weźmy dowolne $x, y \in G$. Wtedy istnieją $k, l \in \mathbb{Z}$ takie, że $x = a^k$ oraz $y = a^l$. Zatem $x \cdot y = a^k \cdot a^l = a^{k+l} = a^{l+k} = a^l \cdot a^k = y \cdot x$, czyli grupa G jest abelowa. $\square$

Twierdzenie 1. *Niech H będzie podgrupą grupy skończonej G . Wtedy $|H|$ jest dzielnikiem $|G|$.*

Dowód. Dla dowolnego $g \in G$ niech

$$gH = \{g \cdot h : h \in H\}.$$

Ponieważ $g = g \cdot e$ i $e \in H$, więc $g \in gH$, skąd

$$G = \bigcup_{g \in G} gH. \quad (2.1)$$

Z prawa skracania równości w grupie wynika, że odwzorowanie $h \mapsto g \cdot h$ dla $h \in H$ jest bijekcją H na gH , czyli

$$|H| = |gH| \text{ dla każdego } g \in G. \quad (2.2)$$

Niech $a, b \in G$ będą takie, że $aH \cap bH \neq \emptyset$. Wtedy istnieją $h_1, h_2 \in H$ takie, że $a \cdot h_1 = b \cdot h_2$. Zatem $b = ah_1h_2^{-1}$ oraz dla dowolnego $h \in H$, $b \cdot h = a \cdot (h_1h_2^{-1}h) \in aH$, gdyż $h_1h_2^{-1}h \in H$. Stąd $bH \subseteq aH$. Ale zbiory aH i bH są skończone, więc z (2.2), $bH = aH$. Stąd i z (2.1) oraz ze skończoności grupy G wynika, że istnieją $a_1, a_2, \dots, a_k \in G$ takie, że zbiory $a_1H, a_2H, \dots, a_kH$ są parami rozłączne oraz $G = \bigcup_{i=1}^k a_iH$.

Zatem $|G| = \sum_{i=1}^k |a_iH| = k \cdot |H|$, czyli $|H|$ dzieli $|G|$. $\square$

Stwierdzenie 4. Niech $H \subseteq G$ będzie skończonym niepustym podzbiorem grupy $(G, \cdot, e)$. Wówczas H jest podgrupą grupy G wtedy i tylko wtedy, gdy $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$.

Dowód. Jeśli H jest podgrupą grupy G , to $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$.

Na odwrót, założmy, że $h_1 \cdot h_2 \in H$ dla dowolnych $h_1, h_2 \in H$. Ponieważ $H \neq \emptyset$, więc istnieje $x \in H$. Wtedy $x^2 = x \cdot x \in H$ i jeśli dla pewnego naturalnego n , $x^n \in H$, to także $x^{n+1} = x^n \cdot x \in H$. Zatem $\{x, x^2, x^3, \dots\} \subseteq H$ i zbiór H jest skończony, więc istnieją liczby naturalne $m > n$ takie, że $x^m = x^n$. Stąd $x^{m-n} = e$ i $m - n \in \mathbb{N}$, więc $e \in H$. Ponadto z tego rozumowania wynika, że dla każdego $h \in H$ istnieje $n \in \mathbb{N}$ takie, że $h^n = e$ oraz $n > 1$. Zatem $h^{-1} = h^{n-1} \in H$. Stąd ostatecznie mamy, że H jest podgrupą grupy G . $\square$

Wniosek 1. Jeżeli rząd grupy G jest liczbą pierwszą, to grupa G jest cykliczna (a więc jest abelowa).

Dowód. Niech liczba pierwsza p będzie rzędem grupy G . Ponieważ $p > 1$, więc istnieje $a \in G$, $a \neq e$. Zatem podgrupa $\langle a \rangle$ ma co najmniej dwa różne elementy: e i a oraz z twierdzenia 1, $|\langle a \rangle|$ dzieli liczbę pierwszą p . Zatem $|\langle a \rangle| = p$, czyli $|\langle a \rangle| = |G|$, skąd $G = \langle a \rangle$ i grupa G jest cykliczna. Zatem ze stwierdzenia 3 grupa G jest abelowa. $\square$

Stwierdzenie 5. Część wspólna dowolnej niepustej rodziny podgrup grupy G jest podgrupą grupy G .

Dowód. Niech $\{H_t\}_{t \in T}$ będzie dowolną niepustą rodziną podgrup grupy $(G, \cdot, e)$. Wtedy $e \in H_t$ dla każdego $t \in T$, więc $e \in \bigcap_{t \in T} H_t$.

Niech $h_1, h_2 \in \bigcap_{t \in T} H_t$. Wtedy $h_1, h_2 \in H_t$ dla każdego $t \in T$. Zatem ze stwierdzenia 2, $h_1 \cdot h_2^{-1} \in H_t$ dla każdego $t \in T$. Stąd $h_1 \cdot h_2^{-1} \in \bigcap_{t \in T} H_t$.

Zatem ze stwierdzenia 2, $\bigcap_{t \in T} H_t$ jest podgrupą grupy G . $\square$

Przykład 4. Podgrupa generowana przez podzbiór grupy. Niech $X \subseteq G$ będzie dowolnym podzbiorem grupy $(G, \cdot, e)$. Oznaczmy przez $\mathcal{X}$ rodzinę wszystkich podgrup grupy G zawierających zbiór X .

Ponieważ $G \in \mathcal{X}$, więc rodzina $\mathcal{X}$ jest niepusta. Zatem ze stwierdzenia 5, $\langle X \rangle = \bigcap_{H \in \mathcal{X}} H$ jest podgrupą grupy G zawierającą zbiór X . Ponadto z określenia $\langle X \rangle$ wynika, że jeśli H jest podgrupą grupy G zawierającą zbiór X , to $H \in \mathcal{X}$ oraz $\langle X \rangle \subseteq H$. Zatem $\langle X \rangle$ jest najmniejszą (w sensie inkluzji) podgrupą grupy G zawierającą zbiór X . Nazywamy ją *podgrupą generowaną przez podzbiór X* i oznaczamy przez $\langle X \rangle$. Natomiast X nazywamy *zbiorem generatorów podgrupy $\langle X \rangle$* . Oczywiście $\langle \emptyset \rangle = \{e\}$, bo $\{e\}$ jest najmniejszą podgrupą grupy G . Jeśli zaś zbiór X jest niepusty, to łatwo zauważyć, że $\langle X \rangle$ jest zbiorem wszystkich elementów postaci $x_1^{k_1} \cdot x_2^{k_2} \cdot \dots \cdot x_n^{k_n}$, gdzie $x_1, \dots, x_n \in X$, $k_1, \dots, k_n \in \{1, -1\}$ oraz $n \in \mathbb{N}$. Jeśli zbiór X jest skończony i $X = \{x_1, \dots, x_n\}$, to zamiast $\langle \{x_1, \dots, x_n\} \rangle$ będziemy pisali $\langle x_1, \dots, x_n \rangle$.

Stwierdzenie 6. *Jeżeli a jest elementem grupy $(G, \cdot, e)$ i n jest najmniejszą liczbą naturalną taką, że $a^n = e$, to podgrupa $\langle a \rangle$ ma dokładnie n elementów oraz*

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}.$$

Dowód. Oczywiście $\{e, a, \dots, a^{n-1}\} \subseteq \langle a \rangle$. Niech $h \in \langle a \rangle$. Wtedy istnieje liczba całkowita k taka, że $h = a^k$. Dzieląc z resztą liczbę k przez liczbę n uzyskamy, że $k = qn + r$ dla pewnych $q, r \in \mathbb{Z}$ takich, że $r \in \{0, 1, \dots, n-1\}$. Zatem $h = a^{qn+r} = a^{qn} \cdot a^r = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r \in \{e, a, \dots, a^{n-1}\}$. Stąd $\langle a \rangle \subseteq \{e, a, \dots, a^{n-1}\}$ i ostatecznie $\langle a \rangle = \{e, a, \dots, a^{n-1}\}$. Gdyby podgrupa $\langle a \rangle$ nie miała dokładnie n elementów, to istniałyby liczby całkowite k, s takie, że $0 \leq k < s < n$ oraz $a^s = a^k$. Ale wtedy $a^{s-k} = e$ i $s - k \in \mathbb{N}$ oraz $s - k < n$, więc otrzymalibyśmy sprzeczność z minimalnością liczby n . Kończy to dowód naszego stwierdzenia. $\square$

Stwierdzenie 7. *Niech $n \in \mathbb{N}$ i niech a będzie elementem grupy $(G, \cdot, e)$ takim, że podgrupa $\langle a \rangle$ ma dokładnie n elementów. Wówczas $a^n = e$ oraz $a^k \neq e$ dla dowolnej liczby naturalnej $k < n$.*

Dowód. Z dowodu stwierdzenia 4 wynika, że istnieje najmniejsza liczba naturalna s taka, że $a^s = e$. Wtedy ze stwierdzenia 6 podgrupa $\langle a \rangle$ ma dokładnie s elementów, skąd $s = n$ i nasze stwierdzenie jest udowodnione. $\square$

Stwierdzenie 8. *Jeżeli $a^2 = e$ dla każdego elementu a grupy $(G, \cdot, e)$, to grupa G jest abelowa.*

Dowód. Weźmy dowolne $a, b \in G$. Wtedy $(ab)^2 = e$, $a^2 = e$ i $b^2 = e$. Zatem $abab = aabb$, skąd z praw skracania równości w grupie, $ba = ab$. Zatem grupa G jest abelowa. $\square$

Stwierdzenie 9. *Każda skończona grupa nieabelowa ma rząd większy niż 5.*

Dowód. Niech G będzie grupą rzędu co najwyżej 5. Wtedy $|G| \in \{1, 2, 3, 4, 5\}$. Jeśli $|G| = 1$, to $G = \{e\}$, więc G jest abelowa. Jeśli $|G| \in \{2, 3, 5\}$, to z wniosku 1 grupa G też jest abelowa. Niech dalej $|G| = 4$. Jeśli istnieje w G element a taki, że $\langle a \rangle = G$, to grupa G jest abelowa (bo jest grupą cykliczną). Załóżmy zatem, że $\langle a \rangle \neq G$ dla każdego $a \in G$. Weźmy dowolne $a \in G$, $a \neq e$. Wtedy podgrupa $\langle a \rangle$ ma co najmniej 2 różne elementy: e , a i jest różna od G , więc z twierdzenia 1, $|\langle a \rangle| = 2$. Zatem ze stwierdzenia 7, $a^2 = e$. Ponieważ dodatkowo $e^2 = e$, więc $a^2 = e$ dla każdego $a \in G$. Zatem ze stwierdzenia 8 grupa G jest abelowa i nasze stwierdzenie zostało udowodnione. $\square$

Rozdział 3

Grupy cykliczne

3.1 Rząd elementu grupy

Definicja 1. Niech a będzie elementem grupy $(G, \cdot, e)$. Jeżeli istnieje liczba naturalna k taka, że $a^k = e$, to najmniejszą taką liczbę naturalną k nazywamy *rzędem elementu a* . W przeciwnym przypadku (tzn. gdy $a^n \neq e$ dla każdego $n \in \mathbb{N}$) mówimy, że rząd elementu a jest równy ∞ (nieskończoność). Rząd elementu a oznaczamy przez $o(a)$.

Przykład 1. Zauważmy, że $o(-1) = 2$ w grupie $\mathbb{R}^*$, gdyż w tym przypadku $e = 1$ oraz $-1 \neq 1$ i $(-1)^2 = 1$. Natomiast w grupie $\mathbb{R}^+$ mamy, że $o(-1) = \infty$, bo wówczas $e = 0$ oraz dla każdego $n \in \mathbb{N}$ jest $n \cdot (-1) = -n \neq 0$.

Uwaga 1. Przykład 1 pokazuje, że należy być bardzo ostrożnym przy wyznaczaniu rzędu elementu grupy. Przede wszystkim musimy rozumieć naturę działania grupowego oraz wiedzieć jak wygląda element neutralny tej grupy.

Uwaga 2. Ze stwierdzeń 6 i 7 z poprzedniego rozdziału wynika od razu, że dla dowolnego elementu a skończonego rzędu grupy G zachodzi wzór:

$$o(a) = |\langle a \rangle|.$$

W szczególności z twierdzenia 1 z rozdziału 2 mamy, że **rzęd dowolnego elementu grupy skończonej G jest dzielnikiem rzędu grupy G .**

Stwierdzenie 1. *Niech a będzie elementem skończonego rzędu grupy $(G, \cdot, e)$. Wtedy dla dowolnego całkowitego k :*

$$a^k = e \iff o(a) \mid k.$$

Dowód. Jeśli $o(a) \mid k$, to istnieje $s \in \mathbb{Z}$ takie, że $k = s \cdot o(a)$. Zatem $a^k = a^{s \cdot o(a)} = (a^{o(a)})^s = e^s = e$. Na odwrót, założmy, że $a^k = e$. Wtedy istnieją $q, r \in \mathbb{Z}$ takie, że $k = q \cdot o(a) + r$ i $0 \leq r < o(a)$. Stąd $e = a^k = a^{q \cdot o(a) + r} = a^{q \cdot o(a)} \cdot a^r = e \cdot a^r = a^r$, czyli $a^r = e$. Ale $r < o(a)$, więc $r \notin \mathbb{N}$, czyli $r = 0$. Zatem $k = q \cdot o(a)$ i $o(a) \mid k$. $\square$

Stwierdzenie 2. *Jeżeli a i b są elementami skończonych względnie pierwszych rzędów grupy G oraz $a \cdot b = b \cdot a$, to $o(ab) = o(a) \cdot o(b)$.*

Dowód. Oznaczmy: $n = o(a)$, $m = o(b)$. Wtedy $m, n \in \mathbb{N}$, $(m, n) = 1$ oraz $a^n = e$ i $b^m = e$. Z rozdziału 1 mamy, że $(ab)^k = a^k b^k$ dla każdego $k \in \mathbb{Z}$. W szczególności $(ab)^{mn} = a^{mn} b^{mn} = e \cdot e = e$, skąd $l = o(ab) \leq mn$. Ale $e = (ab)^l = a^l b^l$, więc $e = (a^l b^l)^n = a^{ln} b^{ln} = e b^{ln} = b^{ln}$, czyli $b^{ln} = e$. Zatem ze stwierdzenia 1, $m \mid ln$. Ale $(m, n) = 1$, więc z zasadniczego twierdzenia arytmetyki, $m \mid l$. Analogicznie pokazujemy, że $n \mid l$. Ponieważ $m \mid l$ i $n \mid l$ oraz $(m, n) = 1$, więc $mn \mid l$, czyli $mn \leq l$. Ale wcześniej pokazaliśmy, że $l \leq mn$, więc ostatecznie $l = mn$, czyli $o(ab) = o(a) \cdot o(b)$. $\square$

Stwierdzenie 3. *Jeżeli a jest elementem nieskończonego rzędu grupy $(G, \cdot, e)$, to dla dowolnych liczb całkowitych k i l :*

$$a^k = a^l \iff k = l.$$

W szczególności grupa $\langle a \rangle$ jest nieskończona. Ponadto grupa $\langle a \rangle$ posiada dokładnie dwa generatory: a i a^{-1} .

Dowód. Załóżmy, że istnieją różne liczby całkowite k, l takie, że $a^k = a^l$. Bez zmniejszania ogólności możemy zakładać, że $k > l$. Wtedy $k - l \in \mathbb{N}$ i $a^{k-l} = e$, co przeczy temu, że $o(a) = \infty$. Implikacja odwrotna jest oczywista.

Ponieważ $a = (a^{-1})^{-1} \in \langle a^{-1} \rangle$, więc $\langle a \rangle \subseteq \langle a^{-1} \rangle$. Ale $\langle a^{-1} \rangle \subseteq \langle a \rangle$, więc $\langle a^{-1} \rangle = \langle a \rangle$, czyli a^{-1} jest generatorem grupy $\langle a \rangle$. Ponadto z pierwszej części dowodu $a^{-1} \neq a$. Niech teraz $b \in \langle a \rangle$ będzie generatorem grupy $\langle a \rangle$. Wtedy istnieje liczba całkowita k taka, że $b = a^k$ oraz $a \in \langle a^k \rangle$. Zatem istnieje $l \in \mathbb{Z}$ takie, że $a = (a^k)^l = a^{kl}$. Zatem z pierwszej części dowodu $kl = 1$, skąd $k = 1$ lub $k = -1$ oraz $b = a$ lub $b = a^{-1}$. $\square$

Lemat 1. Niech a będzie elementem skończonego rzędu grupy G . Wówczas dla dowolnej liczby całkowitej k :

$$\langle a^k \rangle = \langle a^{(o(a),k)} \rangle.$$

Dowód. Oznaczmy $d = (o(a), k)$. Wtedy $d \mid k$, więc istnieje całkowite l takie, że $k = dl$, skąd $a^k = (a^d)^l \in \langle a^d \rangle$. Zatem $\langle a^k \rangle \subseteq \langle a^d \rangle$. Ponadto z elementarnej teorii liczb wiemy, że istnieją liczby całkowite x, y takie, że $d = o(a)x + ky$. Stąd $a^d = a^{o(a)x+ky} = a^{o(a)x} \cdot a^{ky} = e \cdot a^{ky} = (a^k)^y \in \langle a^k \rangle$. Zatem $\langle a^d \rangle \subseteq \langle a^k \rangle$ i ostatecznie $\langle a^d \rangle = \langle a^k \rangle$. $\square$

Twierdzenie 1. Niech a będzie elementem skończonego rzędu grupy $(G, \cdot, e)$. Wówczas:

(i) dla dowolnego naturalnego dzielnika d liczby $o(a)$ zachodzi wzór:

$$o(a^d) = \frac{o(a)}{d},$$

(ii) dla dowolnej liczby całkowitej k zachodzi wzór:

$$o(a^k) = \frac{o(a)}{(o(a),k)}.$$

Dowód. (i) Zauważmy, że $\frac{o(a)}{d} \in \mathbb{N}$ i $(a^d)^{\frac{o(a)}{d}} = a^{d \cdot \frac{o(a)}{d}} = a^{o(a)} = e$. Zatem $k = o(a^d) \leq \frac{o(a)}{d}$. Ale $e = (a^d)^k = a^{dk}$, więc ze stwierdzenia 1 mamy, że $o(a) \mid dk$. Zatem $\frac{o(a)}{d} \mid k$, czyli $\frac{o(a)}{d} \leq k$ i ostatecznie $k = \frac{o(a)}{d}$.

(ii) Z lematu 1 mamy, że $\langle a^k \rangle = \langle a^{(o(a),k)} \rangle$. Ale $d = (o(a), k)$ jest naturalnym dzielnikiem $o(a)$, więc z (i) oraz z uwagi 2 uzyskujemy, że $\frac{o(a)}{(o(a),k)} = o(a^{(o(a),k)}) = |\langle a^{(o(a),k)} \rangle| = |\langle a^k \rangle| = o(a^k)$. $\square$

Twierdzenie 2. Załóżmy, że $\langle a \rangle$ jest skończoną grupą cykliczną rzędu n . Niech d będzie dzielnikiem naturalnym liczby n . Wtedy w grupie $\langle a \rangle$ istnieje dokładnie $\varphi(d)$ elementów rzędu d i są one postaci $a^{\frac{n}{d} \cdot k}$, gdzie $k \in \{1, \dots, d\}$ oraz $(k, d) = 1$.

Dowód. Niech $k \in \{1, \dots, d\}$ będzie takie, że $(k, d) = 1$. Wtedy $(\frac{n}{d} \cdot k, n) = (\frac{n}{d} \cdot k, \frac{n}{d} \cdot d) = \frac{n}{d} \cdot (k, d) = \frac{n}{d} \cdot 1 = \frac{n}{d}$. Zatem z twierdzenia 1, $o(a^{\frac{n}{d} \cdot k}) = \frac{n}{\frac{n}{d}} = d$.

Niech teraz $b \in \langle a \rangle$ będzie elementem rzędu d . Wtedy istnieje liczba naturalna $m \leq n$ taka, że $b = a^m$ oraz z twierdzenia 1, $d = o(a^m) = \frac{n}{(m, n)}$, skąd $(m, n) = \frac{n}{d}$. Ale $(m, n) \mid m$, więc istnieje $k \in \mathbb{N}$ takie, że $m = \frac{n}{d} \cdot k$. Ponadto $\frac{n}{d} = (m, n) = (\frac{n}{d} \cdot k, \frac{n}{d} \cdot d) = \frac{n}{d} \cdot (k, d)$, więc $(k, d) = 1$. Ale $m \leq n$, więc $\frac{n}{d} \cdot k \leq n$, skąd $k \leq d$.

Jeśli $k, l \in \{1, \dots, d\}$, $(k, d) = (l, d) = 1$ oraz $a^{\frac{n}{d} \cdot k} = a^{\frac{n}{d} \cdot l}$, to $a^{\frac{n}{d} \cdot (k-l)} = e$, więc ze stwierdzenia 1, $n \mid \frac{n}{d} \cdot (k-l)$, skąd $d \mid k-l$. Ale $k, l \in \{1, \dots, d\}$, więc $k = l$. $\square$

Wniosek 1. Skończona grupa cykliczna $\langle a \rangle$ rzędu n posiada dokładnie $\varphi(n)$ generatorów i są one postaci: a^k , gdzie $k \in \{1, \dots, n\}$ oraz $(k, n) = 1$.

Dowód. Element $b \in \langle a \rangle$ jest generatorem grupy $\langle a \rangle$ wtedy i tylko wtedy, gdy $o(b) = n$. Zatem z twierdzenia 2 grupa $\langle a \rangle$ posiada dokładnie $\varphi(n)$ generatorów i są one postaci: $a^{\frac{n}{n} \cdot k} = a^k$, gdzie $k \in \{1, \dots, n\}$ oraz $(k, n) = 1$. $\square$

Twierdzenie 3. Każda podgrupa grupy cyklicznej jest grupą cykliczną.

Dowód. Niech $(G, \cdot, e)$ będzie grupą cykliczną o generatorze a i niech H będzie dowolną podgrupą grupy G . Jeśli $H = \{e\}$, to $H = \langle e \rangle$, czyli grupa H jest cykliczna. Załóżmy więc dalej, że $H \neq \{e\}$. Wtedy istnieje $k \in \mathbb{Z}$ takie, że $e \neq a^k \in H$. Stąd $k \neq 0$ i $a^{-k} = (a^k)^{-1} \in H$. Zatem $k \in \mathbb{N}$ lub $-k \in \mathbb{N}$ i z zasady minimum istnieje najmniejsza liczba naturalna m taka, że $a^m \in H$. Wtedy $\langle a^m \rangle \subseteq H$. Weźmy dowolne $h \in H$. Istnieje $s \in \mathbb{Z}$ takie, że $h = a^s$. Ale $s = qm + r$ dla pewnych $q, r \in \mathbb{Z}$, $0 \leq r < m$, więc $a^s = a^{qm+r} = a^{qm} \cdot a^r = (a^m)^q \cdot a^r$, skąd $a^r = a^s \cdot (a^m)^{-q} \in H$, czyli $a^r \in H$. Ponadto $0 \leq r < m$, więc z minimalności m , $r \notin \mathbb{N}$, czyli $r = 0$. Zatem $h = (a^m)^q \in \langle a^m \rangle$, czyli

$H \subseteq \langle a^m \rangle$ i ostatecznie $H = \langle a^m \rangle$. $\square$

Twierdzenie 4. Grupa cykliczna nieskończona $\langle a \rangle$ posiada nieskończenie wiele podgrup i są one postaci: $\langle a^n \rangle$, gdzie $n = 0, 1, \dots$

Dowód. Z twierdzenia 3 wynika, że każda podgrupa H grupy $\langle a \rangle$ jest postaci $H = \langle a^k \rangle$ dla pewnego $k \in \mathbb{Z}$. Ale $a^k = (a^{-k})^{-1} \in \langle a^{-k} \rangle$, więc $\langle a^k \rangle \subseteq \langle a^{-k} \rangle$ oraz $\langle a^{-k} \rangle \subseteq \langle a^k \rangle$, bo $a^{-k} \in \langle a^k \rangle$, więc $\langle a^k \rangle = \langle a^{-k} \rangle$, czyli $H = \langle a^n \rangle$ dla pewnego $n = 0, 1, \dots$

Niech $m, n \in \{0, 1, \dots\}$ będą takie, że $\langle a^m \rangle = \langle a^n \rangle$. Wtedy $a^m \in \langle a^n \rangle$, więc istnieje $k \in \mathbb{Z}$ takie, że $a^m = (a^n)^k = a^{nk}$. Zatem ze stwierdzenia 3, $m = nk$, czyli $n \mid m$. Analogicznie pokazujemy, że $m \mid n$. Stąd $m \mid n$ i $n \mid m$ oraz $n, m \in \{0, 1, \dots\}$, więc $m = n$. $\square$

Przykład 2. Ponieważ $\mathbb{Z}^+ = \langle 1 \rangle$ i $o(1) = \infty$, więc z twierdzenia 4 wynika, że wszystkimi podgrupami grupy $\mathbb{Z}^+$ są: $\langle n \rangle = \{n \cdot k : k \in \mathbb{Z}\}$ dla $n = 0, 1, \dots$ Zauważmy, że podgrupa $\langle n \rangle$ jest nam dobrze znana już od szkoły podstawowej, gdyż jej elementami są wszystkie całkowite wielokrotności liczby n . Ponadto ze stwierdzenia 3 wynika, że grupa $\mathbb{Z}^+$ posiada dokładnie dwa generatory: 1 i -1 .

Twierdzenie 5. Wszystkimi podgrupami skończonej grupy cyklicznej $\langle a \rangle$ są podgrupy postaci $\langle a^d \rangle$, gdzie d przebiega wszystkie dzielniki naturalne liczby $o(a)$. W szczególności liczba wszystkich podgrup grupy $\langle a \rangle$ jest równa liczbie wszystkich dzielników naturalnych liczby $o(a)$.

Dowód. Jeśli $\langle a^{d_1} \rangle = \langle a^{d_2} \rangle$ dla pewnych dzielników naturalnych d_1, d_2 liczby $o(a)$, to z twierdzenia 1 i z uwagi 2: $\frac{n}{d_1} = o(a^{d_1}) = |\langle a^{d_1} \rangle| = |\langle a^{d_2} \rangle| = o(a^{d_2}) = \frac{n}{d_2}$, czyli $d_1 = d_2$.

Niech H będzie dowolną podgrupą grupy $\langle a \rangle$. Wtedy z twierdzenia 3 istnieje $k \in \mathbb{Z}$ takie, że $H = \langle a^k \rangle$. Ale z lematu 1, $\langle a^k \rangle = \langle a^{(o(a), k)} \rangle$ i $(o(a), k)$ jest dzielnikiem naturalnym liczby $o(a)$, więc twierdzenie zostało udowodnione. $\square$

Uwaga 3. Z twierdzenia 5 wynika, że istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy zbiorem wszystkich podgrup skończonej grupy cyklicznej $\langle a \rangle$ i zbiorem wszystkich dzielników naturalnych liczby $o(a)$. W szczególności wynika stąd, że dla każdej liczby

naturalnej d dzielącej rząd skończonej grupy cyklicznej $\langle a \rangle$ istnieje dokładnie jedna podgrupa rzędu d grupy $\langle a \rangle$.

Stwierdzenie 4. *Jeżeli liczba naturalna n posiada co najmniej dwa różne, nieparzyste dzielniki pierwsze, to grupa $\mathbb{Z}_n^*$ nie jest cykliczna.*

Dowód. Z założenia istnieją różne, nieparzyste liczby pierwsze p, q oraz liczby naturalne α, β, m takie, że $n = p^\alpha q^\beta m$ oraz m nie jest podzielne ani przez p ani przez q . Z chińskiego twierdzenia o resztach wynika zatem, że istnieją $a, b \in \mathbb{Z}_n^*$ takie, że $a \equiv -1 \pmod{p^\alpha}$, $a \equiv 1 \pmod{q^\beta m}$ oraz $b \equiv 1 \pmod{p^\alpha m}$ i $b \equiv -1 \pmod{q^\beta}$. Ponieważ liczby p i q są nieparzyste, więc $a \neq 1$ i $b \neq 1$. Gdyby $a = b$, to $1 \equiv -1 \pmod{p^\alpha}$, skąd $p^\alpha | 2$ i mamy sprzeczność. Zatem $a \neq b$ i wobec tego $\{1, a\} \neq \{1, b\}$. Ponadto $a^2 \equiv 1 \pmod{p^\alpha}$ i $a^2 \equiv 1 \pmod{q^\beta m}$, więc $a^2 \equiv 1 \pmod{n}$, skąd $a \odot_n a = 1$, czyli $o(a) = 2$ w grupie $\mathbb{Z}_n^*$, skąd $\langle a \rangle = \{1, a\}$. Podobnie pokazujemy, że $\langle b \rangle = \{1, b\}$. Zatem grupa $\mathbb{Z}_n^*$ posiada dwie różne podgrupy rzędu 2, więc z uwagi 3 ta grupa nie jest cykliczna. $\square$

Uwaga 4. Z elementarnej teorii liczb wiadomo, że jeśli $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, gdzie $p_1, \dots, p_s$ są różnymi liczbami pierwszymi oraz $\alpha_1, \dots, \alpha_s$ są nieujemnymi liczbami całkowitymi, to liczba wszystkich dzielników naturalnych liczby n jest równa $\Theta(n) = (\alpha_1 + 1) \cdots (\alpha_s + 1)$. Ponadto $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_s^{\alpha_s})$ i dla liczb pierwszych p oraz $\alpha \in \mathbb{N}$, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Przykład 3. Niech $n \in \mathbb{N}$, $n > 1$. Wtedy $\mathbb{Z}_n^+ = \langle 1 \rangle$ oraz $o(1) = n$. Zatem z wniosku 1 grupa $\mathbb{Z}_n^+$ posiada dokładnie $\varphi(n)$ generatorów i są nimi liczby naturalne $k \leq n$ względnie pierwsze z n . Ponadto podgrupy grupy $\mathbb{Z}_n^+$ są postaci: $\{0\}$ oraz $\langle d \rangle = \{0, d, 2d, \dots, (\frac{n}{d} - 1) \cdot d\}$, gdzie $d < n$ jest dzielnikiem naturalnym liczby n . Zatem grupa $\mathbb{Z}_n^+$ posiada dokładnie $\Theta(n)$ wszystkich podgrup.

Lemat 2. *Niech a będzie elementem maksymalnego rzędu w skończonej grupie abelowej A . Wówczas $o(b) \mid o(a)$ dla każdego $b \in A$.*

Dowód. Załóżmy, że istnieje $b \in A$ takie, że $o(b)$ nie dzieli $o(a)$. Wtedy istnieje liczba pierwsza p oraz liczby naturalne m, n niepodzielne przez p i nieujemne liczby całkowite α, β takie, że $\alpha < \beta$ oraz

$o(a) = p^\alpha m$ i $o(b) = p^\beta n$. Niech $x = a^{p^\alpha}$ i $y = b^n$. Wtedy z twierdzenia 1, $o(x) = m$ oraz $o(y) = p^\beta$. Ale $(m, p^\beta) = 1$, gdyż p nie dzieli m , więc ze stwierdzenia 2, $o(xy) = p^\beta m > p^\alpha m = o(a)$ i mamy sprzeczność. $\square$

Twierdzenie 6. *Jeżeli A jest skończoną grupą abelową i dla każdej liczby naturalnej d dzielącej $|A|$ istnieje dokładnie jedna podgrupa rzędu d grupy A , to grupa A jest cykliczna.*

Dowód. Załóżmy, że przy tych założeniach grupa A nie jest cykliczna. Niech a będzie elementem maksymalnego rzędu w grupie A . Wtedy $\langle a \rangle \neq A$, więc istnieje $b \in A$ takie, że $b \notin \langle a \rangle$. Z lematu 2, $o(b) \mid o(a)$. Zatem z twierdzenia 5 istnieje w grupie $\langle a \rangle$ podgrupa H rzędu $o(b)$. Ale $|\langle b \rangle| = o(b)$, więc na mocy założenia $\langle b \rangle = H$, skąd $b \in H \subseteq \langle a \rangle$, czyli $b \in \langle a \rangle$ i mamy sprzeczność. Zatem grupa A jest cykliczna. $\square$

Rozdział 4

Warstwy, dzielniki normalne

4.1 Warstwy grupy względem podgrupy

Niech H będzie podgrupą grupy $(G, \cdot, e)$. W zbiorze G wprowadzamy relacje $\sim_l$ oraz $\sim_r$ przyjmując, że dla dowolnych $a, b \in G$:

$$a \sim_l b \Leftrightarrow a^{-1} \cdot b \in H, \quad (4.1)$$

$$a \sim_r b \Leftrightarrow a \cdot b^{-1} \in H. \quad (4.2)$$

Ponieważ dla każdego $a \in G$ jest $a^{-1} \cdot a = e = a \cdot a^{-1}$ oraz $e \in H$, więc relacje $\sim_l$ i $\sim_r$ są zwrotne.

Ponadto dla dowolnych $a, b \in G$:

- jeżeli $a \sim_l b$, to $a^{-1} \cdot b \in H$, skąd $(a^{-1} \cdot b)^{-1} \in H$, czyli $b^{-1} \cdot a \in H$, więc $b \sim_l a$;

- jeżeli $a \sim_r b$, to $a \cdot b^{-1} \in H$, skąd $(a \cdot b^{-1})^{-1} \in H$, czyli $b \cdot a^{-1} \in H$, więc $b \sim_r a$.

Zatem relacje $\sim_l$ i $\sim_r$ są symetryczne.

W końcu, dla dowolnych $a, b, c \in G$:

- jeżeli $a \sim_l b$ i $b \sim_l c$, to $a^{-1} \cdot b \in H$ i $b^{-1} \cdot c \in H$, skąd $(a^{-1} \cdot b) \cdot (b^{-1} \cdot c) \in H$, czyli $a^{-1} \cdot c \in H$, więc $a \sim_l c$;

- jeżeli $a \sim_r b$ i $b \sim_r c$, to $a \cdot b^{-1} \in H$ i $b \cdot c^{-1} \in H$, skąd $(a \cdot b^{-1}) \cdot (b \cdot c^{-1}) \in H$, czyli $a \cdot c^{-1} \in H$, więc $a \sim_r c$.

Zatem relacje $\sim_l$ i $\sim_r$ są przechodnie.

Stąd wynika, że relacje $\sim_l$ i $\sim_r$ są relacjami równoważności w zbiorze G . Klasę abstrakcji relacji $\sim_l$ o reprezentancie $a \in G$ oznaczamy przez aH i nazywamy **warstwą lewostronną grupy G względem podgrupy H o reprezentancie a** .

1. Dla dowolnego $a \in G$ zachodzi wzór:

$$aH = \{a \cdot h : h \in H\}. \quad (4.3)$$

Dowód. Dla $h \in H$ mamy, że $a^{-1} \cdot (a \cdot h) = h \in H$, więc $a \sim_l a \cdot h$ oraz $a \cdot h \in aH$. Na odwrót, niech $g \in aH$. Wtedy $a \sim_l g$, skąd $a^{-1} \cdot g = h \in H$. Zatem $g = a \cdot h$. Zatem $aH = \{a \cdot h : h \in H\}$. $\square$

Z własności klas abstrakcji relacji równoważności mamy od razu następujący **warunek równości warstw lewostronnych względem podgrupy H** :

2. Dla dowolnych $a, b \in G$:

$$aH = bH \Leftrightarrow a^{-1} \cdot b \in H. \quad (4.4)$$

Zauważmy, że w szczególności dla $h \in H$ jest $hH = eH = H$.

Klasę abstrakcji relacji $\sim_r$ o reprezentancie $a \in G$ oznaczamy przez Ha i nazywamy **warstwą prawostronną grupy G względem podgrupy H o reprezentancie a** .

3. Dla dowolnego $a \in G$ zachodzi wzór:

$$Ha = \{h \cdot a : h \in H\}. \quad (4.5)$$

Dowód. Dla $h \in H$ mamy, że $a \cdot (h \cdot a)^{-1} = a \cdot a^{-1} \cdot h^{-1} = h^{-1} \in H$, więc $a \sim_r h \cdot a$ oraz $h \cdot a \in Ha$. Na odwrót, niech $g \in Ha$. Wtedy $a \sim_r g$, więc $g \sim_r a$, czyli $g \cdot a^{-1} = h \in H$, skąd $g = h \cdot a$. Zatem $Ha = \{h \cdot a : h \in H\}$. $\square$

Z własności klas abstrakcji relacji równoważności mamy od razu następujący **warunek równości warstw prawostronnych grupy G względem podgrupy H** :

4. Dla dowolnych $a, b \in G$:

$$Ha = Hb \Leftrightarrow a \cdot b^{-1} \in H. \quad (4.6)$$

Zauważmy, że w szczególności dla $h \in H$ jest $Hh = He = H$.

Z podstawowych własności klas abstrakcji relacji równoważności wynika

5. Dowolne dwie warstwy lewostronne (prawostronne) grupy G względem podgrupy H są albo równe albo rozłączne.

6. Dowolne dwie warstwy lewostronne (prawostronne) grupy G względem podgrupy H są równoliczne.

Dowód. Niech $a, b \in G$. Rozważmy przekształcenie $f : H \rightarrow aH$ dane wzorem $f(h) = a \cdot h$ dla $h \in H$. Z 1. wynika, że f jest „na”, zaś z prawa skracania równości w grupie mamy, że f jest różnowartościowe. Zatem zbiory aH i H są równoliczne. Analogicznie funkcja $g : H \rightarrow Hb$ dana wzorem $g(h) = h \cdot b$ dla $h \in H$ jest „na” oraz jest różnowartościowa, więc zbiory Hb i H też są równoliczne. Zatem zbiory aH i Hb dla dowolnych $a, b \in G$ też są równoliczne. $\square$

7. Zbiór $L_G(H)$ wszystkich warstw lewostronnych grupy G względem podgrupy H jest równoliczny ze zbiorem $P_G(H)$ wszystkich warstw prawostronnych grupy G względem podgrupy H .

Dowód. Z 1. i 3. mamy, że $L_G(H) = \{aH : a \in G\}$ oraz $P_G(H) = \{Hb : b \in G\}$. Niech $f : L_G(H) \rightarrow P_G(H)$ będzie dane wzorem: $f(aH) = Ha^{-1}$ dla $a \in G$. Wówczas dla dowolnych $a, b \in G$ mamy, że $f(aH) = f(bH) \Leftrightarrow Ha^{-1} = Hb^{-1} \Leftrightarrow a^{-1} \cdot (b^{-1})^{-1} \in H \Leftrightarrow a^{-1} \cdot b \in H \Leftrightarrow aH = bH$ na mocy podanych wcześniej własności warstw. Oznacza to, że f jest funkcją i f jest funkcją różnowartościową. Ponadto dla $b \in G$ mamy, że $b = (b^{-1})^{-1}$, więc $Hb = f(b^{-1}H)$, czyli f jest „na”. Zatem f jest bijekcją i zbiory $L_G(H)$ oraz $P_G(H)$ są równoliczne. $\square$

Moc zbioru wszystkich warstw lewostronnych (prawostronnych) grupy G względem podgrupy H nazywamy **indeksem podgrupy H w grupie G** i oznaczamy przez $(G : H)$.

Twierdzenie Lagrange’a. Jeżeli H jest podgrupą grupy skończonej G , to

$$|G| = |H| \cdot (G : H). \quad (4.7)$$

W szczególności rząd podgrupy H jest dzielnikiem rzędu grupy G .

Dowód. Ponieważ zbiór G jest skończony więc z zasady abstrakcji wynika, że istnieją $a_1, a_2, \dots, a_n \in G$ takie, że warstwy $a_1H, a_2H, \dots, a_nH$ są parami rozłączne i ich suma daje zbiór G , czyli $G = \bigcup_{i=1}^n a_iH$. Ale H jest zbiorem skończonym, więc na mocy **6.** mamy, że $|a_iH| = |H|$ dla $i = 1, 2, \dots, n$ oraz $n = (G : H)$, więc $|G| = |H| \cdot (G : H)$. $\square$

4.2 Dzielnik normalny grupy

Definicja 1. Niech H będzie podgrupą grupy $(G, \cdot, e)$. Powiemy, że H jest *dzielnikiem normalnym* (podgrupą normalną) grupy G , jeżeli

$$gH = Hg \text{ dla każdego } g \in G. \quad (4.8)$$

Piszemy wtedy: $H \triangleleft G$.

Przykład 1. $\{e\} \triangleleft G$ i $G \triangleleft G$.

Przykład 2. Każda podgrupa zawarta w centrum grupy G jest jej dzielnikiem normalnym. Rzeczywiście, niech H będzie podgrupą grupy G zawartą w $Z(G)$. Wtedy dla każdego $g \in G$ mamy, że $gH = \{g \cdot h : h \in H\} = \{h \cdot g : h \in H\} = Hg$. Zatem $H \triangleleft G$. W szczególności $Z(G) \triangleleft G$.

Przykład 3. W grupie abelowej G każda podgrupa jest dzielnikiem normalnym (bo wtedy $Z(G) = G$ i każda podgrupa grupy G jest zawarta w $Z(G)$).

Przykład 4. Każda podgrupa H indeksu 2 grupy G jest dzielnikiem normalnym grupy G . Rzeczywiście, z **7.** wynika, że grupa G ma dokładnie dwie warstwy lewostronne i dokładnie dwie warstwy prawostronne względem podgrupy H . Ponieważ $eH = H = He$, więc jedną z warstw lewostronnych (prawostronnych) jest H , zaś drugą warstwą lewostronną (prawostronną) jest $G \setminus H$. Weźmy dowolne $g \in G$. Jeżeli $g \in H$, to $gH = H = Hg$. Jeśli $g \notin H$, to $gH \neq H$ i $Hg \neq H$, więc $gH = G \setminus H = Hg$, czyli $gH = Hg$. Zatem dla każdego $g \in G$ jest

$gH = Hg$, a więc $H \triangleleft G$. Np. każda podgrupa rzędu 4 grupy izometrii własnych kwadratu jest jej dzielnikiem normalnym. Zaś w grupie izometrii własnych trójkąta równobocznego podgrupa obrotów jest dzielnikiem normalnym (natomiast żadna podgrupa rzędu 2 nie jest dzielnikiem normalnym tej grupy).

Stwierdzenie 1. *Niech H będzie podgrupą grupy G . Wówczas równoważne są warunki:*

- (i) $H \triangleleft G$;
- (ii) $g \cdot h \cdot g^{-1} \in H$ dla dowolnych $g \in G$ i $h \in H$.

Dowód. (i) $\Rightarrow$ (ii) Weźmy dowolne $g \in G$ oraz $h \in H$. Ponieważ $gH = Hg$ oraz $g \cdot h \in gH$, więc $g \cdot h \in Hg$. Zatem istnieje $k \in H$ takie, że $g \cdot h = k \cdot g$, skąd $g \cdot h \cdot g^{-1} = k \in H$.

(ii) $\Rightarrow$ (i) Weźmy dowolne $g \in G$. Wtedy dla $h \in H$ mamy, że $g \cdot h \cdot g^{-1} = k \in H$. Zatem $g \cdot h = k \cdot g \in Hg$. Stąd $gH \subseteq Hg$. Ponadto $g^{-1} \cdot h \cdot g = h_1 \in H$, więc $h \cdot g = g \cdot h_1 \in gH$. Stąd $Hg \subseteq gH$ i ostatecznie $gH = Hg$ dla każdego $g \in G$. Zatem $H \triangleleft G$. $\square$

Stwierdzenie 2. *Podgrupa H rzędu 2 grupy G jest jej dzielnikiem normalnym wtedy i tylko wtedy, gdy H jest zawarta w centrum grupy G .*

Dowód. Jeżeli $H \subseteq Z(G)$, to z przykładu 2 mamy, że $H \triangleleft G$. Na odwrót, założmy, że $H \triangleleft G$. Ponieważ $|H| = 2$, więc istnieje $a \in H$ takie, że $o(a) = 2$ i wtedy $a \neq e$ oraz $a^2 = e$ i $H = \{e, a\}$. Weźmy dowolne $g \in G$. Wtedy ze stwierdzenia 1 mamy, że $g \cdot a \cdot g^{-1} \in H$. Jeśli $g \cdot a \cdot g^{-1} = e$, to $g \cdot a = g$, skąd $a = e$ i mamy sprzeczność. Zatem $g \cdot a \cdot g^{-1} = a$, skąd $g \cdot a = a \cdot g$. Zatem $a \in Z(G)$. Ale $e \in Z(G)$, więc ostatecznie $H \subseteq Z(G)$. $\square$

Przykład 5. Część wspólna dowolnej niepustej rodziny dzielników normalnych grupy G jest dzielnikiem normalnym grupy G . Rzeczywiście, niech $\{H_i\}_{i \in I}$ będzie niepustą rodziną dzielników normalnych grupy G oraz niech $H = \bigcap_{i \in I} H_i$. Wtedy z rozdziału 2 mamy, że H jest podgrupą grupy G . Weźmy dowolne $g \in G$ i dowolne $h \in H$. Wtedy $h \in H_i$ dla każdego $i \in I$, więc ze stwierdzenia 1, $g \cdot h \cdot g^{-1} \in H_i$ dla $i \in I$, czyli $g \cdot h \cdot g^{-1} \in H$. Zatem ze stwierdzenia 1, $H \triangleleft G$.

Definicja 2. Iloczynem algebraicznym podgrup A, B grupy G nazywamy zbiór

$$AB = \{a \cdot b : a \in A, b \in B\}. \quad (4.9)$$

Stwierdzenie 3. Jeżeli H jest podgrupą grupy G , zaś A jest dzielnikiem normalnym grupy G , to $AH = HA$ oraz AH jest podgrupą grupy G .

Dowód. Weźmy dowolne $a \in A$ oraz $h \in H$. Wtedy ze stwierdzenia 1, $h \cdot a \cdot h^{-1} = b \in A$, skąd $h \cdot a = b \cdot h \in AH$. Zatem $HA \subseteq AH$. Ponadto ze stwierdzenia 1, $h^{-1} \cdot a \cdot h = c \in A$, więc $a \cdot h = h \cdot c \in HA$, więc $AH \subseteq HA$. Zatem $AH \subseteq HA$ i $HA \subseteq AH$, czyli $AH = HA$. Dalej, dla $a \in A$ mamy, że $a = e \cdot a \in HA$, bo $e \in H$, skąd $A \subseteq HA$. Analogicznie $H \subseteq HA$. Niech $a \in A$ oraz $h \in H$. Wtedy $(a \cdot h)^{-1} = h^{-1} \cdot a^{-1} \in HA$. Ponadto dla $a, b \in A$ oraz $h, k \in H$ mamy, że $h \cdot b = c \cdot l$ dla pewnych $c \in A$ oraz $l \in H$, więc $(a \cdot h) \cdot (b \cdot k) = a \cdot (h \cdot b) \cdot k = a \cdot (c \cdot l) \cdot k = (a \cdot c) \cdot (l \cdot k) \in AH$. Zatem AH jest podgrupą grupy G . $\square$

Przykład 6. Jeżeli A i B są dzielnikami normalnymi grupy G , to AB też jest dzielnikiem normalnym grupy G . Rzeczywiście, na mocy stwierdzenia 3 mamy, że AB jest podgrupą grupy G . Ponadto dla $g \in G$ oraz dla $a \in A$ i $b \in B$ mamy, że

$$g \cdot (a \cdot b) \cdot g^{-1} = (g \cdot a \cdot g^{-1}) \cdot (g \cdot b \cdot g^{-1}) \in AB,$$

bo $g \cdot a \cdot g^{-1} \in A$ oraz $g \cdot b \cdot g^{-1} \in B$. Zatem ze stwierdzenia 1 mamy, że $AB \triangleleft G$.

4.3 Komutant grupy

Niech G będzie grupą i niech $a, b \in G$. Komutatorem elementów a, b nazywamy element postaci

$$[a, b] = a^{-1} \cdot b^{-1} \cdot a \cdot b. \quad (4.10)$$

Zauważmy, że dla dowolnych $a, b, c \in G$ zachodzą wzory:

$$[a, b]^{-1} = [b, a] \quad (4.11)$$

Dowód. Mamy, że $[a, b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b, a]$. $\square$

$$c \cdot [a, b] \cdot c^{-1} = [cac^{-1}, cbc^{-1}] \quad (4.12)$$

Dowód. Mamy

$$\begin{aligned} c[a, b]c^{-1} &= c(a^{-1}b^{-1}ab)c^{-1} = ca^{-1}c^{-1}cb^{-1}c^{-1}cac^{-1}cbc^{-1} = \\ &= (cac^{-1})^{-1}(cbc^{-1})^{-1}(cac^{-1})(cbc^{-1}) = [cac^{-1}, cbc^{-1}]. \quad \square \end{aligned}$$

$$a \cdot b = b \cdot a \iff [a, b] = e. \quad (4.13)$$

Dowód. Jeśli $ab = ba$, to $b^{-1}ab = a$, skąd $a^{-1}b^{-1}ab = e$, czyli $[a, b] = e$. Na odwrót, niech $[a, b] = e$. Wtedy $a^{-1}b^{-1}ab = e$, skąd $b^{-1}ab = a$ oraz $ab = ba$. $\square$

Komutantem grupy G nazywamy zbiór G' wszystkich iloczynów wszystkich możliwych komutatorów utworzonych z elementów grupy G . Zatem G' składa się z elementów postaci: $[a, b]$, $[a, b] \cdot [c, d]$, $[a, b] \cdot [c, d] \cdot [g, h]$, itd. ($a, b, c, d, g, h, \dots \in G$). Zatem $e = [e, e] \in G'$ oraz dla $x, y \in G'$ istnieją komutatory $x_1, x_2, \dots, x_n, y_1, y_2, \dots, y_m$ takie, że $x = x_1x_2 \dots x_n$ oraz $y = y_1y_2 \dots y_m$. Stąd

$$xy^{-1} = x_1x_2 \dots x_ny_m^{-1}y_{m-1}^{-1} \dots y_1^{-1},$$

skąd na mocy (4.11) mamy, że $xy^{-1} \in G'$. Zatem G' jest podgrupą grupy G . Ponadto dla $g \in G$ mamy, że $gxg^{-1} = g(x_1x_2 \dots x_n)g^{-1} = (gx_1g^{-1})(gx_2g^{-1}) \dots (gx_ng^{-1}) \in G'$ na mocy (4.12). Wynika stąd, że $G' \triangleleft G$. Ponadto z określenia komutanta oraz z (4.13) wynika od razu, że grupa G jest abelowa wtedy i tylko wtedy, gdy $G' = \{e\}$.

Rozdział 5

Grupa ilorazowa, iloczyn prosty, homomorfizm

5.1 Grupa ilorazowa

Niech H będzie dzielnikiem normalnym grupy G . Oznaczmy przez G/H zbiór wszystkich warstw lewostronnych grupy G względem podgrupy H . Tak więc

$$G/H = \{gH : g \in G\} \quad (5.1)$$

oraz $|G/H| = (G : H)$. Ponadto, gdy grupa G jest skończona, to na mocy twierdzenia Lagrange'a $|G/H| = \frac{|G|}{|H|}$.

W zbiorze G/H wprowadzamy działanie $\circ$ przyjmując, że dla dowolnych $a, b \in G$:

$$(aH) \circ (bH) = (a \cdot b)H. \quad (5.2)$$

Uzasadnimy, że określenie działania $\circ$ jest poprawne, czyli, że nie zależy od wyboru reprezentantów warstw. Niech zatem $a, b, c, d \in G$ będą takie, że $aH = bH$ oraz $cH = dH$. Wtedy $a^{-1}b \in H$ oraz $c^{-1}d \in H$. Zatem $(ac)^{-1}(bd) = c^{-1}a^{-1}bd = (c^{-1}d)[d^{-1}(a^{-1}b)d] \in H$, gdyż $H \triangleleft G$. Zatem $(ac)H = (bd)H$.

Teraz uzasadnimy, że działanie $\circ$ jest łączne. W tym celu weźmy dowolne $a, b, c \in G$ i obliczmy:

$$(aH) \circ [(bH) \circ (cH)] = (aH) \circ ((b \cdot c)H) = (a \cdot (b \cdot c))H = ((ab)c)H = [(ab)H] \circ (cH) = [(aH) \circ (bH)] \circ (cH).$$

Sprawdźmy, że warstwa $eH = H$ jest elementem neutralnym działania $\circ$. Dla dowolnego $a \in G$ mamy, że $(aH) \circ H = (aH) \circ (eH) = (a \cdot e)H = aH = (e \cdot a)H = (eH) \circ (aH) = H \circ (aH)$. Ponadto $(aH) \circ (a^{-1}H) = (a \cdot a^{-1})H = eH = H$ oraz $(a^{-1}H) \circ (aH) = (a^{-1} \cdot a)H = eH = H$. Zatem warstwą odwrotną do warstwy (aH) jest warstwa $a^{-1}H$, czyli

$$(aH)^{-1} = a^{-1}H \text{ dla każdego } a \in G. \quad (5.3)$$

W ten sposób udowodniliśmy, że system algebraiczny $(G/H, \circ, H)$ jest grupą. Nazywamy ją *grupą ilorazową* względem dzielnika normalnego H . Jeżeli grupa G jest abelowa, to grupa ilorazowa G/H też jest abelowa, gdyż dla dowolnych $a, b \in G$ mamy, że $(aH) \circ (bH) = abH = baH = (bH) \circ (aH)$.

Twierdzenie 1. *Dla dowolnej grupy G grupa ilorazowa G/G' jest grupą abelową. Ponadto dla dzielnika normalnego H grupy G mamy, że G/H jest grupą abelową wtedy i tylko wtedy, gdy $G' \subseteq H$.*

Dowód. Niech H będzie dzielnikiem normalnym grupy G . Wtedy dla dowolnych $a, b \in G$ mamy, że $[aH, bH] = (aH)^{-1} \circ (bH)^{-1} \circ (aH) \circ (bH) = (a^{-1}H) \circ (b^{-1}H) \circ (abH) = (a^{-1}b^{-1}H) \circ (abH) = a^{-1}b^{-1}abH = [a, b]H$. Zatem grupa G/H jest abelowa wtedy i tylko wtedy, gdy $[a, b] \in H$ dla dowolnych $a, b \in G$, czyli wtedy i tylko wtedy, gdy $G' \subseteq H$ na mocy definicji komutanta grupy. W szczególności mamy stąd, że G/G' jest grupą abelową. $\square$

Przykład 1. Można wykazać, że istnieje grupa G rzędu 12 taka, że $|G'| = 4$. Pokażemy, że wówczas w grupie G nie istnieje podgrupa rzędu 6 (będzie to oznaczało, że nie można odwracać twierdzenia Lagrange'a!). W tym celu założmy, że grupa G posiada podgrupę H rzędu 6. Wtedy z twierdzenia Lagrange'a mamy, że $(G : H) = \frac{|G|}{|H|} = \frac{12}{6} = 2$, więc z poprzedniego rozdziału $H \triangleleft G$. Ponadto $|G/H| = 2$, więc grupa G/H jest abelowa (a nawet cykliczna). Zatem z twierdzenia 1 mamy, że $G' \subseteq H$. Ale $|G'| = 4$ i $|H| = 6$

oraz 4 nie dzieli 6, więc mamy sprzeczność z twierdzeniem Lagrange'a. Zatem taka grupa G nie posiada podgrupy rzędu 6. $\square$

5.2 Iloczyn prosty grup

Niech $(G_1, \cdot_1, e_1)$ i $(G_2, \cdot_2, e_2)$ będą dowolnymi grupami. W zbiorze $G = G_1 \times G_2$ wprowadzamy mnożenie „po współrzędnych” przyjmując, że dla dowolnych $a_1, b_1 \in G_1$, $a_2, b_2 \in G_2$:

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2). \quad (5.4)$$

Niech ponadto $e = (e_1, e_2)$. Sprawdzimy, że $(G, \cdot, e)$ tworzy grupę. W tym celu weźmy dowolne $a_1, b_1, c_1 \in G_1$ oraz dowolne $a_2, b_2, c_2 \in G_2$. Wówczas:

$$\begin{aligned} (a_1, a_2) \cdot [(b_1, b_2) \cdot (c_1, c_2)] &= (a_1, a_2) \cdot (b_1 \cdot_1 c_1, b_2 \cdot_2 c_2) = \\ &= (a_1 \cdot_1 (b_1 \cdot_1 c_1), a_2 \cdot_2 (b_2 \cdot_2 c_2)) = ((a_1 \cdot_1 b_1) \cdot_1 c_1, (a_2 \cdot_2 b_2) \cdot_2 c_2) = \\ &= (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2) \cdot (c_1, c_2) = [(a_1, a_2) \cdot (b_1, b_2)] \cdot (c_1, c_2), \end{aligned}$$

czyli działanie $\cdot$ jest łączne. Dalej,

$$(a_1, a_2) \cdot e = (a_1, a_2) \cdot (e_1, e_2) = (a_1 \cdot_1 e_1, a_2 \cdot_2 e_2) = (a_1, a_2)$$

oraz

$$e \cdot (a_1, a_2) = (e_1, e_2) \cdot (a_1, a_2) = (e_1 \cdot_1 a_1, e_2 \cdot_2 a_2) = (a_1, a_2),$$

skąd wynika, że e jest elementem neutralnym działania $\cdot$. W końcu

$$(a_1, a_2) \cdot (a_1^{-1}, a_2^{-1}) = (a_1 \cdot_1 a_1^{-1}, a_2 \cdot_2 a_2^{-1}) = (e_1, e_2) = e$$

oraz

$$(a_1^{-1} \cdot_1 a_1, a_2^{-1} \cdot_2 a_2) = (e_1, e_2) = e,$$

czyli $(G, \cdot, e)$ jest grupą oraz

$$(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1}) \text{ dla dowolnych } a_1 \in G_1, a_2 \in G_2. \quad (5.5)$$

Otrzymaną w ten sposób grupę oznaczamy przez $G_1 \times G_2$ i nazywamy *iloczynem prostym grup* G_1 i G_2 . Z określenia mnożenia w iloczynie prostym grup wynika od razu, że **iloczyn prosty grup abelowych jest grupą abelową**.

Zauważmy, że podzbiory

$$\bar{G}_1 = \{(a, e_2) : a \in G_1\} \text{ oraz } \bar{G}_2 = \{(e_1, b) : b \in G_2\} \quad (5.6)$$

są dzielnikami normalnymi grupy G . Rzeczywiście, $e = (e_1, e_2) \in \bar{G}_1 \cap \bar{G}_2$, dla $a, x \in G_1$ i $b, y \in G_2$ mamy

$$(a, e_2) \cdot (x, e_2)^{-1} = (a, e_2) \cdot (x^{-1}, e_2) = (a \cdot_1 x^{-1}, e_2 \cdot_2 e_2) = (a \cdot_1 x^{-1}, e_2) \in \bar{G}_1$$

oraz

$$(e_1, b) \cdot (e_1, y)^{-1} = (e_1 \cdot_1 e_1, b \cdot_2 y^{-1}) = (e_1, b \cdot_2 y^{-1}) \in \bar{G}_2,$$

skąd $\bar{G}_1$ i $\bar{G}_2$ są podgrupami grupy G . Ponadto dla $g \in G_1, h \in G_2$ mamy

$$\begin{aligned} (g, h) \cdot (a, e_2) \cdot (g, h)^{-1} &= (g \cdot_1 a, h \cdot_2 e_2) \cdot (g^{-1}, h^{-1}) = \\ &= (g \cdot_1 a \cdot_1 g^{-1}, h \cdot_2 e_2 \cdot_2 h^{-1}) = (g \cdot_1 a \cdot_1 g^{-1}, e_2) \in \bar{G}_1 \end{aligned}$$

oraz

$$\begin{aligned} (g, h) \cdot (e_1, b) \cdot (g, h)^{-1} &= (g \cdot_1 e_1, h \cdot_2 b) \cdot (g^{-1}, h^{-1}) = \\ &= (g \cdot_1 e_1 \cdot_1 g^{-1}, h \cdot_2 b \cdot_2 h^{-1}) = (e_1, h \cdot_2 b \cdot_2 h^{-1}) \in \bar{G}_2. \end{aligned}$$

Zatem rzeczywiście $\bar{G}_1 \triangleleft G$ oraz $\bar{G}_2 \triangleleft G$.

Z określenia podgrup $\bar{G}_1$ i $\bar{G}_2$ wynika od razu, że

$$\bar{G}_1 \cap \bar{G}_2 = \{e\} \text{ oraz } \bar{G}_1 \bar{G}_2 = G. \quad (5.7)$$

Niech teraz $a \in G_1$ i $b \in G_2$ będą elementami o skończonych rzędach równych odpowiednio n i m . Wykażemy, że wówczas element $g = (a, b) \in G$ ma rząd równy $[n, m]$. W tym celu zauważmy, że ponieważ $n \mid [n, m]$ i $m \mid [n, m]$, więc $a^{[n, m]} = e_1$ oraz $b^{[n, m]} = e_2$,

skąd $g^{[n,m]} = (a^{[n,m]}, b^{[n,m]}) = (e_1, e_2) = e$. Zatem $o(g) = k \in \mathbb{N}$ oraz $k \mid [n, m]$. Ponadto $e = g^k = (a^k, b^k)$, więc $a^k = e_1$ i $b^k = e_2$, skąd z własności rzędu elementu grupy wynika, że $n \mid k$ i $m \mid k$. Zatem z elementarnej teorii liczb $[n, m] \mid k$. W ten sposób wykazaliśmy, że $k \mid [n, m]$ oraz $[n, m] \mid k$, więc ponieważ k i $[n, m]$ są liczbami naturalnymi, to $k = [n, m]$. Z tych rozważań wynika od razu, że **iloczyn prosty skończonych grup cyklicznych o względnie pierwszych rządach jest grupą cykliczną**.

5.3 Homomorfizmy grup i ich własności

Definicja 1. Niech $(G_1, \cdot_1, e_1)$ i $(G_2, \cdot_2, e_2)$ będą grupami. Przekształcenie $f : G_1 \longrightarrow G_2$ takie, że

$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \text{ dla dowolnych } a, b \in G_1 \quad (5.8)$$

nazywamy *homomorfizmem grupy G_1 w grupę G_2* , zaś zbiór

$$\text{Ker}(f) = \{x \in G_1 : f(x) = e_2\} \quad (5.9)$$

nazywamy *jądrem homomorfizmu f* . Jeżeli dodatkowo f jest różnowartościowe, to mówimy, że f jest *zanurzeniem grupy G_1 w grupę G_2* . Jeżeli zaś homomorfizm f jest bijekcją, to mówimy, że f jest *izomorfizmem grup*.

Definicja 2. Powiemy, że grupa G_2 jest *obrazem homomorficznym grupy G_1* , jeżeli istnieje homomorfizm f grupy G_1 na grupę G_2 .

Definicja 3. Powiemy, że grupa G_1 *zanurza się w grupę G_2* , jeśli istnieje zanurzenie grup $f : G_1 \longrightarrow G_2$.

Definicja 4. Powiemy, że grupy G_1 i G_2 są *izomorficzne* i piszemy, $G_1 \cong G_2$, jeżeli istnieje izomorfizm grup $f : G_1 \longrightarrow G_2$.

Definicja 5. *Automorfizmem grupy G* nazywamy każdy izomorfizm grup $f : G \longrightarrow G$.

Własności homomorfizmów grup

1. *Złożenie homomorfizmów jest homomorfizmem, tzn. jeżeli $f : G_1 \rightarrow G_2$ i $g : G_2 \rightarrow G_3$ są homomorfizmami grup, to $g \circ f : G_1 \rightarrow G_3$ też jest homomorfizmem grup. W szczególności złożenie izomorfizmów jest izomorfizmem.*

Dowód. Rzeczywiście, dla dowolnych $a, b \in G_1$ mamy

$$(g \circ f)(ab) = g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = \\ = (g \circ f)(a)(g \circ f)(b). \quad \square$$

2. *Jeżeli $f : G_1 \rightarrow G_2$ jest izomorfizmem grup, to $f^{-1} : G_2 \rightarrow G_1$ też jest izomorfizmem grup.*

Dowód. Rzeczywiście, ponieważ f jest bijekcją, więc ze wstępu do matematyki f^{-1} istnieje, jest bijekcją oraz dla $x \in G_1$ i $y \in G_2$ mamy, że $y = f(x) \Leftrightarrow f^{-1}(y) = x$. Weźmy dowolne $y_1, y_2 \in G_2$. Wtedy istnieją $x_1, x_2 \in G_1$ takie, że $y_1 = f(x_1)$ i $y_2 = f(x_2)$, więc $y_1 y_2 = f(x_1)f(x_2) = f(x_1 x_2)$, skąd $f^{-1}(y_1 y_2) = x_1 x_2 = f^{-1}(y_1)f^{-1}(y_2)$. $\square$

Z **1.** i **2.** oraz z tego, że przekształcenie tożsamościowe grupy G w grupę G jest jej automorfizmem wynika od razu

3. *Dla dowolnych grup G_1, G_2, G_3 :*

a) $G_1 \cong G_1$,

b) *jeśli $G_1 \cong G_2$, to $G_2 \cong G_1$,*

c) *jeśli $G_1 \cong G_2$ i $G_2 \cong G_3$, to $G_1 \cong G_3$.* $\square$

Niech teraz $f : G_1 \rightarrow G_2$ będzie homomorfizmem grup. Dla uproszczenia zapisu działania w obu grupach będziemy oznaczać tak samo. Podobnie elementy neutralne tych grup też oznaczymy przez e . Wówczas

4. $f(e) = e$.

Dowód. Rzeczywiście, $f(e) = f(e \cdot e) = f(e) \cdot f(e)$, skąd po skróceniu $e = f(e)$. $\square$

5. $f(a^{-1}) = [f(a)]^{-1}$ dla każdego $a \in G_1$.

Dowód. Rzeczywiście, $f(a^{-1}) \cdot f(a) = f(a^{-1} \cdot a) = f(e) = e$ na mocy **4.**, więc $f(a^{-1}) = [f(a)]^{-1}$. $\square$

6. $f(a_1 \cdot a_2 \cdot \dots \cdot a_n) = f(a_1) \cdot f(a_2) \cdot \dots \cdot f(a_n)$ dla dowolnych $a_1, \dots, a_n \in G_1$ oraz dla dowolnego $n \geq 2$.

Dowód. Rzeczywiście, dla $n = 2$ teza wynika z definicji homomorfizmu, a jeżeli zachodzi ona dla pewnego naturalnego n oraz $a_1, \dots, a_n, a_{n+1} \in G_1$, to $f(a_1 \cdot \dots \cdot a_n \cdot a_{n+1}) = f((a_1 \cdot \dots \cdot a_n) \cdot a_{n+1}) = f(a_1 \cdot \dots \cdot a_n) \cdot f(a_{n+1}) = f(a_1) \cdot \dots \cdot f(a_n) \cdot f(a_{n+1})$. $\square$

Z 5. i 6. wynika od razu, że

7. $f(a^k) = [f(a)]^k$ dla dowolnych $a \in G_1, k \in \mathbb{Z}$. $\square$

8. Jeżeli $a \in G_1$ jest elementem skończonego rzędu, to $f(a)$ też jest elementem skończonego rzędu oraz $o(f(a)) \mid o(a)$.

Dowód. Rzeczywiście, niech $n = o(a)$. Wtedy $a^n = e$, skąd na mocy 4. i 7. $e = f(a^n) = [f(a)]^n$. Zatem istnieje liczba naturalna k taka, że $k = o(f(a))$ i z własności rzędu elementu grupy $k \mid n$, bo $[f(a)]^n = e$. $\square$

9. $\text{Ker}(f) \triangleleft G_1$.

Dowód. Z 4. mamy, że $e \in \text{Ker}(f)$. Jeśli $x, y \in \text{Ker}(f)$, to $f(x) = f(y) = e$, skąd $f(xy) = f(x)f(y) = e \cdot e = e$, czyli $xy \in \text{Ker}(f)$ oraz na mocy 5. $f(x^{-1}) = [f(x)]^{-1} = e^{-1} = e$, czyli $x^{-1} \in \text{Ker}(f)$. Zatem $\text{Ker}(f)$ jest podgrupą grupy G_1 . Ponadto dla $g \in G_1, h \in \text{Ker}(f)$ na mocy 6. i 5. mamy, że $f(ghg^{-1}) = f(g)f(h)[f(g)]^{-1} = f(g)e[f(g)]^{-1} = e$, skąd $ghg^{-1} \in \text{Ker}(f)$. Zatem $\text{Ker}(f) \triangleleft G_1$. $\square$

10. Homomorfizm f jest zanurzeniem wtedy i tylko wtedy, gdy $\text{Ker}(f) = \{e\}$.

Dowód. $\Rightarrow$ Niech $x \in \text{Ker}(f)$. Wtedy $f(x) = e = f(e)$, skąd $x = e$. Ale $e \in \text{Ker}(f)$, więc stąd $\text{Ker}(f) = \{e\}$.

$\Leftarrow$ Niech $a, b \in G_1$ będą takie, że $f(a) = f(b)$. Wtedy $e = f(a) \cdot [f(b)]^{-1} = f(a) \cdot f(b^{-1}) = f(ab^{-1})$, skąd $ab^{-1} \in \text{Ker}(f) = \{e\}$, czyli $ab^{-1} = e$. Zatem $a = b$ i f jest zanurzeniem. $\square$

11. Jeżeli H jest podgrupą grupy G_1 , to $f(H) = \{f(h) : h \in H\}$ jest podgrupą grupy G_2 .

Dowód. Z 4. mamy, że $e = f(e) \in f(H)$, gdyż $e \in H$. Niech $x, y \in f(H)$. Wtedy istnieją $a, b \in H$ takie, że $x = f(a)$ i $y = f(b)$. Zatem $a \cdot b^{-1} \in H$, skąd $f(a \cdot b^{-1}) \in f(H)$ oraz $x \cdot y^{-1} = f(a) \cdot [f(b)]^{-1} = f(a) \cdot f(b^{-1}) = f(a \cdot b^{-1})$, czyli $x \cdot y^{-1} \in f(H)$ i $f(H)$ jest podgrupą grupy G_2 . $\square$

12. Jeżeli K jest podgrupą grupy G_2 , to

$$f^{-1}(K) = \{x \in G_1 : f(x) \in K\}$$

jest podgrupą grupy G_1 .

Dowód. Ponieważ $e \in K$ i $e = f(e)$, więc $e \in f^{-1}(K)$. Niech $a, b \in f^{-1}(K)$. Wtedy $f(a), f(b) \in K$, skąd $f(ab^{-1}) = f(a) \cdot [f(b)]^{-1} \in K$, czyli $ab^{-1} \in f^{-1}(K)$. Zatem $f^{-1}(K)$ jest podgrupą grupy G_1 . $\square$

Jeżeli $f : G_1 \longrightarrow G_2$ jest izomorfizmem grup, to $|G_1| = |G_2|$ oraz każda własność grupy G_1 definiowana za pomocą działania w tej grupie jest zachowywana przez f . Z tego powodu w **algebrze utożsamia się grupy izomorficzne**.

5.4 Twierdzenie o izomorfizmie

Twierdzenie o izomorfizmie. Jeżeli $f : G_1 \longrightarrow G_2$ jest homomorfizmem grup, to

$$f(G_1) \cong G_1 / \text{Ker}(f).$$

W szczególności, jeżeli f jest „na”, to $G_2 \cong G_1 / \text{Ker}(f)$.

Dowód. Z własności 11. homomorfizmów mamy, że $f(G_1)$ jest podgrupą grupy G_2 . Ponadto f odwzorowuje grupę G_1 na $f(G_1)$. Oznaczmy $\text{Ker}(f) = H$. Wtedy z własności 9. homomorfizmów $H \triangleleft G_1$. Niech $F : G_1/H \longrightarrow f(G_1)$ będzie dane wzorem

$$F(xH) = f(x) \text{ dla } x \in G_1.$$

Wtedy dla $x, y \in G_1$ mamy

$$F(xH) = F(yH) \Leftrightarrow f(x) = f(y) \Leftrightarrow [f(x)]^{-1} \cdot f(y) = e \Leftrightarrow$$

$$\Leftrightarrow f(x^{-1}) \cdot f(y) = e \Leftrightarrow f(x^{-1} \cdot y) = e \Leftrightarrow x^{-1} \cdot y \in H \Leftrightarrow xH = yH.$$

Zatem F jest dobrze określoną funkcją różnowartościową. Stąd F jest bijekcją. Ponadto

$$F((xH) \circ (yH)) = F((xy)H) = f(xy) = f(x) \cdot f(y) = F(xH) \cdot F(yH).$$

Zatem F jest izomorfizmem grup, czyli $f(G_1) \cong G_1 / \text{Ker}(f)$. $\square$

Uwaga 1. Niech $(G, \cdot, e)$ będzie grupą i niech $f : A \longrightarrow G$ będzie bijekcją zbioru A na zbiór G . W zbiorze A wprowadzamy działanie o pomocy wzoru:

$$a \circ b = f^{-1}(f(a) \cdot f(b)) \text{ dla } a, b \in A.$$

Niech $\epsilon = f^{-1}(e)$. Wówczas $(A, \circ, \epsilon)$ jest grupą i f jest izomorfizmem grup, czyli $A \cong G$. Rzeczywiście, dla dowolnych $a, b, c \in A$ mamy

$$\begin{aligned} a \circ (b \circ c) &= a \circ f^{-1}(f(b) \cdot f(c)) = f^{-1}(f(a) \cdot f(f^{-1}(f(b) \cdot f(c)))) = \\ &= f^{-1}(f(a) \cdot (f(b) \cdot f(c))) = f^{-1}((f(a) \cdot f(b)) \cdot f(c)) \end{aligned}$$

oraz

$$\begin{aligned} (a \circ b) \circ c &= f^{-1}(f(a) \cdot f(b)) \circ c = f^{-1}(f(f^{-1}(f(a) \cdot f(b))) \cdot f(c)) = \\ &= f^{-1}((f(a) \cdot f(b)) \cdot f(c)). \end{aligned}$$

Zatem działanie $\circ$ jest łączne. Ponadto dla $a \in A$ mamy, że $a \circ \epsilon = f^{-1}(f(a) \cdot f(\epsilon)) = f^{-1}(f(a) \cdot e) = f^{-1}(f(a)) = a$ oraz $\epsilon \circ a = f^{-1}(f(\epsilon) \cdot f(a)) = f^{-1}(e \cdot f(a)) = f^{-1}(f(a)) = a$, więc ϵ jest elementem neutralnym działania $\circ$. W końcu dla $a \in A$ oraz dla $x = f^{-1}([f(a)]^{-1})$ mamy

$$a \circ x = f^{-1}(f(a) \cdot f(f^{-1}([f(a)]^{-1}))) = f^{-1}(f(a) \cdot [f(a)]^{-1}) = f^{-1}(e) = \epsilon$$

oraz

$$x \circ a = f^{-1}(f(f^{-1}([f(a)]^{-1})) \cdot f(a)) = f^{-1}([f(a)]^{-1} \cdot f(a)) = f^{-1}(e) = \epsilon,$$

więc każdy element $a \in A$ jest odwracalny i ostatecznie $(A, \circ, \epsilon)$ tworzy grupę. $\square$

Rozdział 6

Przykłady homomorfizmów. Grupy permutacji I

6.1 Przykłady homomorfizmów grup

Przykład 1. Niech $ABCD$ będzie prostokątem, który nie jest kwadratem. Oznaczmy przez a symetralną odcinka AB oraz przez b symetralną odcinka BC . Niech O będzie punktem przecięcia prostych a i b . Wówczas grupa K izometrii własnych tego prostokąta składa się z dokładnie czterech elementów: e (przekształcenie tożsamościowe), S_a , S_b , S_O . Tabelka działania $\circ$ wygląda następująco:

$\circ$	e	S_a	S_b	S_O
e	e	S_a	S_b	S_O
S_a	S_a	e	S_O	S_b
S_b	S_b	S_O	e	S_a
S_O	S_O	S_b	S_a	e

Zatem K jest grupą abelową, którą nazywa się *grupą czwórkową Kleina*. Niech teraz G będzie niecykliczną grupą rzędu 4. Wówczas z rozdziału 2 $x^2 = e$ dla każdego $x \in G$. Wówczas G jest grupą abelową oraz $G = \{e, x, y, z\}$, przy czym $x^2 = y^2 = z^2 = e$ oraz $yx = xy \neq e, x, y$, skąd $xy = z$. Podobnie $zx = xz = y$ oraz $zy = yz = x$. Na mocy uwagi 1 z rozdziału 5 mamy zatem, że $f : G \rightarrow K$ takie, że $f(e) = e$,

$f(x) = S_a, f(y) = S_b, f(z) = S_O$ jest izomorfizmem grup. W ten sposób wykazaliśmy, że istnieje tylko jedna z dokładnością do izomorfizmu niecykliczna grupa rzędu 4 (mianowicie jest nią grupa czwórkowa Kleina).

Przykład 2. Dla dowolnych grup G_1, G_2 przekształcenie $f : G_1 \rightarrow G_2$ dane wzorem

$$f(x) = e \text{ dla } x \in G_1$$

jest homomorfizmem grup. Nazywamy go *homomorfizmem trywialnym*.

Przykład 3. Niech G będzie grupą i $g \in G$. Wtedy przekształcenie $f : G \rightarrow G$ dane wzorem

$$f(x) = g \cdot x \cdot g^{-1} \text{ dla } x \in G$$

jest automorfizmem grupy G , gdyż dla $a, b \in G$ jest $f(a \cdot b) = g \cdot (a \cdot b) \cdot g^{-1} = (g \cdot a \cdot g^{-1}) \cdot (g \cdot b \cdot g^{-1}) = f(a) \cdot f(b)$ oraz przekształcenie $h : G \rightarrow G$ dane wzorem: $h(x) = g^{-1} \cdot x \cdot g$ dla $x \in G$ jest odwrotne do f . Taki automorfizm f nazywamy *automorfizmem wewnętrznym*.

Przykład 4. Niech H będzie dzielnikiem normalnym grupy G i niech $\pi : G \rightarrow G/H$ będzie odwzorowaniem danym wzorem

$$\pi(x) = xH \text{ dla } x \in G.$$

Wówczas dla dowolnych $a, b \in G$ mamy, że $\pi(ab) = (ab)H = (aH) \circ (bH) = \pi(a) \circ \pi(b)$, więc π jest homomorfizmem grup. Ponadto $G/H = \{aH = \pi(a) : a \in G\}$, więc π jest „na”. Dla $a \in G$ mamy, że $a \in \text{Ker}(\pi) \Leftrightarrow \pi(a) = H \Leftrightarrow aH = H \Leftrightarrow a \in H$, więc $\text{Ker}(\pi) = H$. Taki homomorfizm π nazywamy *epimorfizmem naturalnym*.

Przy okazji zauważmy, że każdy dzielnik normalny grupy G jest jądrem pewnego homomorfizmu określonego na tej grupie. Stąd wobec własności 9. homomorfizmów mamy, że **dzielniki normalne grupy G są to dokładnie jądra homomorfizmów określonych na grupie G** . Z twierdzenia o izomorfizmie wynika stąd zatem, że **każdy obraz homomorficzny grupy G jest izomorficzny z grupą ilorazową G/H dla pewnego $H \triangleleft G$** .

Przykład 5. Opiszemy wszystkie homomorfizmy określone na nieskończonej grupie cyklicznej G o generatorze a w dowolną grupę B . Z własności rzędu elementu grupy mamy, że $o(a) = \infty$. Zatem każdy element grupy G może być jednoznacznie zapisany w postaci a^k dla pewnego całkowitego k . Niech $f : G \rightarrow B$ będzie homomorfizmem grup. Oznaczmy $b = f(a)$. Wtedy z własności 7. homomorfizmów będziemy mieli, że $f(a^k) = b^k$ dla $k \in \mathbb{Z}$. Na odwrót, weźmy dowolny element $b \in B$ i niech

$$f(a^k) = b^k \text{ dla wszystkich } k \in \mathbb{Z}. \quad (6.1)$$

Wtedy z własności potęgowania w grupie mamy, że f jest homomorfizmem grupy G w grupę B , $f(a) = b$ oraz $f(G) = \langle b \rangle$. Wynika stąd, że istnieje dokładnie $|B|$ różnych homomorfizmów $f : G \rightarrow B$. Jeśli $o(b) = \infty$, to dla całkowitych k mamy, że $b^k = e \Leftrightarrow k = 0 \Leftrightarrow a^k = e$, więc f jest zanurzeniem. Jeśli zaś $o(b) = n \in \mathbb{N}$, to dla całkowitych k mamy, że $f(a^k) = e \Leftrightarrow b^k = e \Leftrightarrow n \mid k$, skąd $\text{Ker}(f) = \langle a^n \rangle$. Ponadto homomorfizm f dany wzorem (6.1) jest „na” wtedy i tylko wtedy, gdy b jest generatorem grupy B . Jeżeli $B = \langle b \rangle$ oraz $o(b) = \infty$, to homomorfizm f dany wzorem (6.1) jest izomorfizmem. W szczególności udowodniliśmy więc następujące

Twierdzenie 2. Każde dwie nieskończone grupy cykliczne $\langle a \rangle$ i $\langle b \rangle$ są izomorficzne. Ponadto przekształcenie $f : \langle a \rangle \rightarrow \langle b \rangle$ dane wzorem (6.1) jest izomorfizmem grup. $\square$

Przykład 6. Opiszemy wszystkie homomorfizmy określone na skończonej grupie cyklicznej $\langle a \rangle$ rzędu n w dowolną grupę B . Niech $f : \langle a \rangle \rightarrow B$ będzie homomorfizmem grup. Oznaczmy $b = f(a)$. Wtedy z własności 8. homomorfizmu mamy, że $o(b) \mid o(a)$ oraz z własności 7. homomorfizmu mamy, że $f(a^k) = b^k$ dla $k \in \mathbb{Z}$. Na odwrót, niech $b \in B$ będzie takie, że $o(b) \mid o(a)$. Wówczas przekształcenie f dane wzorem (6.1) jest dobrze określone, bo dla dowolnych $k, l \in \mathbb{Z}$ mamy, że jeśli $a^k = a^l$, to $a^{k-l} = e$, skąd $o(a) \mid k-l$. Ale $o(b) \mid o(a)$, więc stąd $o(b) \mid k-l$ i $b^{k-l} = e$, czyli $b^k = b^l$. Natomiast z własności potęgowania w grupie mamy, że takie f jest homomorfizmem grup. Ponadto taki homomorfizm f jest „na” wtedy i tylko wtedy, gdy $\langle b \rangle = B$ oraz

dla całkowitych k mamy, że $a^k \in \text{Ker}(f) \Leftrightarrow b^k = e \Leftrightarrow o(b) \mid k$, więc $\text{Ker}(f) = \langle a^{o(b)} \rangle$. Stąd dla b takiego, że $o(b) = o(a)$ jest $\text{Ker}(f) = \{e\}$, czyli f jest wtedy zanurzeniem grup. W ten sposób udowodniliśmy następujące

Twierdzenie 3. *Każde dwie grupy cykliczne skończone $\langle a \rangle$ i $\langle b \rangle$ tego samego rzędu są izomorficzne. Ponadto przekształcenie $f : \langle a \rangle \longrightarrow \langle b \rangle$ dane wzorem (6.1) jest izomorfizmem grup. $\square$*

Uwaga 2. Z twierdzenia 3 i z przykładu 1 wynika, że z dokładnością do izomorfizmu istnieją tylko dwie grupy rzędu 4. Mianowicie grupa czwórkowa Kleina i grupa cykliczna $\mathbb{Z}_4^+$. Ponadto z twierdzenia 3 mamy, że $\mathbb{C}_n^* \cong \mathbb{Z}_n^+$.

Uwaga 3. Z przykładu 4 mamy, że $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}_n^+$ dane wzorem $f(k) = k \cdot 1$ dla $k \in \mathbb{Z}$ jest homomorfizmem grupy $\mathbb{Z}^+$ na grupę $\mathbb{Z}_n^+$ oraz $\text{Ker}(f) = \langle n \rangle$. Zatem z twierdzenia o izomorfizmie mamy

$$\mathbb{Z}_n^+ \cong \mathbb{Z}^+ / \langle n \rangle.$$

Twierdzenie 4. *Niech $f : G \longrightarrow A$ będzie homomorfizmem grupy skończonej G w grupę A . Wówczas $|f(G)|$ dzieli $|G|$. Jeżeli dodatkowo A jest grupą skończoną, to $|f(G)|$ dzieli $(|G|, |A|)$.*

Dowód. Z twierdzenia o izomorfizmie mamy, że $f(G) \cong G / \text{Ker}(f)$, skąd na mocy twierdzenia Lagrange'a $|f(G)| = |G / \text{Ker}(f)| = \frac{|G|}{|\text{Ker}(f)|}$, a więc $|f(G)| \mid |G|$. Jeżeli dodatkowo grupa A jest skończona, to z twierdzenia Lagrange'a $|f(G)|$ dzieli $|A|$, więc z elementarnej teorii liczb $|f(G)|$ dzieli $(|G|, |A|)$. $\square$

Przykład 7. Pokażemy, że nie istnieje nietrywialny homomorfizm grupy D_3 izometrii własnych trójkąta równobocznego w grupę $\mathbb{Z}_{15}^+$. W tym celu założmy, że istnieje nietrywialny homomorfizm $f : D_3 \longrightarrow \mathbb{Z}_{15}^+$. Wtedy $|f(D_3)| > 1$ oraz z twierdzenia 4, $|f(D_3)| \mid (6, 15) = 3$, więc $|f(D_3)| = 3$ oraz z twierdzenia o izomorfizmie i z twierdzenia Lagrange'a $|\text{Ker}(f)| = 2$. Ale $\text{Ker}(f) \triangleleft D_3$ i grupa D_3 nie posiada dzielnika normalnego rzędu 2, więc mamy sprzeczność.

Przykład 8. Pokażemy, że jeśli zbiory A i B są równoliczne, to grupy symetryczne $S(A)$ i $S(B)$ też są izomorficzne. Rzeczywiście, niech $f : A \rightarrow B$ będzie bijekcją. Określamy $F : S(A) \rightarrow S(B)$ wzorem $F(\phi) = f \circ \phi \circ f^{-1}$ dla $\phi \in S(A)$. Wtedy ze wstępu do matematyki mamy, że $F(\phi)$ jest bijekcją jako złożenie bijekcji, czyli $F(\phi) \in S(B)$ dla $\phi \in S(A)$. Ponadto dla dowolnych $\phi_1, \phi_2 \in S(A)$ mamy

$$\begin{aligned} F(\phi_1 \circ \phi_2) &= f \circ (\phi_1 \circ \phi_2) \circ f^{-1} = \\ &= (f \circ \phi_1 \circ f^{-1}) \circ (f \circ \phi_2 \circ f^{-1}) = F(\phi_1) \circ F(\phi_2), \end{aligned}$$

więc F jest homomorfizmem grup. Ponadto $G : S(B) \rightarrow S(A)$ dane wzorem $G(\psi) = f^{-1} \circ \psi \circ f$ dla $\psi \in S(B)$ jest przekształceniem odwrotnym do F . Zatem F jest izomorfizmem grup.

Twierdzenie 5 (Cayley’a). *Każda grupa G zanurza się w grupę symetryczną $S(G)$.*

Dowód. Niech dla $g \in G$: $l_g(x) = gx$ dla $x \in G$. Wtedy, jak wiemy l_g jest bijekcją zbioru G na siebie, więc $l_g \in S(G)$. Niech $F(g) = l_g$ dla $g \in G$. Wtedy dla $g, h, x \in G$ mamy, że $(F(gh))(x) = l_{gh}(x) = (gh)x = g(hx) = gl_h(x) = l_g(l_h(x)) = (l_g \circ l_h)(x) = (F(g) \circ F(h))(x)$, skąd $F(gh) = F(g) \circ F(h)$ i F jest homomorfizmem grup. Jeżeli $g \in \text{Ker}(F)$, to $l_g(x) = x$ dla $x \in G$, czyli $gx = x$ dla $x \in G$. Zatem $g = e$. Stąd z własności 10. homomorfizmów mamy, że F jest zanurzeniem grup. $\square$

Z twierdzenia Cayley’a i z przykładu 8 wynika od razu następujący

Wniosek 1. *Każda grupa skończona rzędu n zanurza się w grupę permutacji S_n zbioru n -elementowego $\{1, 2, \dots, n\}$. $\square$*

6.2 Grupy permutacji

Niech $n \geq 2$ będzie ustaloną liczbą naturalną. Niech $X_n = \{1, 2, \dots, n\}$. Każdą permutację $f \in S_n$ można zapisać w postaci dwuwierszowej

tablicy

$$f = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ f(1) & f(2) & \dots & f(i) & \dots & f(n) \end{pmatrix}, \quad (6.2)$$

w której w pierwszym wierszu umieszczone są wszystkie elementy zbioru X_n (najczęściej w porządku rosnącym), zaś w drugim wierszu umieszczone są kolejne obrazy tych elementów przy odwzorowaniu f . Niech $X_f = \{x \in X_n : f(x) \neq x\}$. Wtedy dla $x \in X_n$ jest $x \neq f(x)$, skąd $f(x) \neq f(f(x))$, więc $f(x) \in X_f$. Stąd $f(X_f) \subseteq X_f$, a ponieważ f jest różnowartościowe i zbiór X_f jest skończony, więc $f(X_f) = X_f$. Z tego powodu w zapisie permutacji f pomijamy zazwyczaj te i , dla których $f(i) = i$. Np. zamiast $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ można pisać $\begin{pmatrix} 2 & 3 \\ 3 & 2 \end{pmatrix}$. Przy tej notacji dla permutacji f mamy wzór:

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}. \quad (6.3)$$

Ponadto

$$e = \begin{pmatrix} 1 & 2 & \dots & i & \dots & n \\ 1 & 2 & \dots & i & \dots & n \end{pmatrix}. \quad (6.4)$$

Inwersje

*Inwersją permutacji $f \in S_n$ nazywamy taki podzbiór dwuelementowy $\{i, j\}$ zbioru X_n , że $i < j$ oraz $f(i) > f(j)$. Zbiór wszystkich inwersji permutacji $f \in S_n$ oznaczamy przez I_f . Np. $I_e = \emptyset$, więc $|I_e| = 0$, czyli **permutacja tożsamościowa nie posiada inwersji**.*

Przykład 9. Niech $i, j \in X_n$, $i < j$. Oznaczmy przez (i, j) permutację zbioru X_n , która zamienia miejscami elementy i, j oraz nie zmienia pozostałych elementów zbioru X_n (takie permutacje nazywamy *transpozycjami*). Zatem

$$(i, j) = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}. \quad (6.5)$$

Stąd $I_{(i,j)} = \underbrace{\{\{i, i+1\}, \{i, i+2\}, \{i, i+3\}, \dots, \{i, j-1\}, \{i, j\},$
 $\{i+1, j\}, \{i+2, j\}, \{i+3, j\}, \dots, \{j-1, j\}\}}_{j-i}$. Zatem $|I_{(i,j)}| = (j-i) +$
 $\underbrace{+ (j-1) - i}_{(j-1)-i} = 2(j-i) - 1$. Uzyskaliśmy zatem, że **każda transpozycja posiada nieparzystą liczbę wszystkich inwersji**.

Znak permutacji

Znakiem permutacji $f \in S_n$ nazywamy liczbę $\text{sgn}(f)$ określoną wzorem:

$$\text{sgn}(f) = (-1)^{|I_f|}. \quad (6.6)$$

Powiemy, że permutacja $f \in S_n$ jest *parzysta*, jeśli $\text{sgn}(f) = 1$ oraz, że f jest *nieparzysta*, jeśli $\text{sgn}(f) = -1$. Zatem z przykładu 9 mamy, że **dowolna transpozycja jest permutacją nieparzystą**. Ponieważ $\text{sgn}(e) = (-1)^0 = 1$, więc permutacja tożsamościowa jest parzysta. Zbiór wszystkich permutacji parzystych $f \in S_n$ będziemy oznaczali przez A_n .

Twierdzenie 6. *Dla dowolnych permutacji $f, g \in S_n$ zachodzi wzór:*

$$\text{sgn}(f \circ g) = \text{sgn}(f) \cdot \text{sgn}(g). \quad (6.7)$$

W szczególności $\text{sgn}(f^{-1}) = \text{sgn}(f)$.

Dowód. Oznaczmy przez P_n rodzinę wszystkich podzbiorów dwuelementowych zbioru X_n . Niech $h \in S_n$. Weźmy dowolne $A \in P_n$. Wtedy $A = \{i, j\}$ dla pewnych $i, j \in X_n$, $i \neq j$. Oznaczmy $\text{sgn}_h(A) = \text{sgn}\left(\frac{h(i)-h(j)}{i-j}\right)$. Określenie to jest poprawne, bo

$$\frac{h(j)-h(i)}{j-i} = \frac{-(h(i)-h(j))}{-(i-j)} = \frac{h(i)-h(j)}{i-j}.$$

Ponadto $A \in I_h \Leftrightarrow \text{sgn}_h(A) = -1$. Wynika stąd wzór:

$$\text{sgn}(h) = \prod_{A \in P_n} \text{sgn}_h(A). \quad (6.8)$$

Łatwo zauważyć, że dowolna permutacja $g \in S_n$ wyznacza bijekcję $G : P_n \rightarrow P_n$ przy pomocy wzoru $G(A) = \{g(i), g(j)\}$ dla $A = \{i, j\}$. Wynika stąd, że dla dowolnych $f, g \in S_n$ zachodzi wzór:

$$\operatorname{sgn}(f) = \prod_{A \in P_n} \operatorname{sgn}_f(G(A)). \quad (6.9)$$

Ponadto dla $A \in P_n$ mamy

$$\operatorname{sgn}_f(G(A)) \cdot \operatorname{sgn}_g(A) = \operatorname{sgn}_{f \circ g}(A). \quad (6.10)$$

Rzeczywiście, $A = \{i, j\}$ dla pewnych $i, j \in X_n$, $i \neq j$ oraz

$$\operatorname{sgn}_f(G(A)) = \operatorname{sgn}_f(\{g(i), g(j)\}) = \operatorname{sgn} \left(\frac{f(g(i)) - f(g(j))}{g(i) - g(j)} \right)$$

oraz

$$\operatorname{sgn}_g(A) = \operatorname{sgn} \left(\frac{g(i) - g(j)}{i - j} \right).$$

Ale $\operatorname{sgn}(x) \cdot \operatorname{sgn}(y) = \operatorname{sgn}(x \cdot y)$ dla dowolnych liczb rzeczywistych x, y , więc

$$\begin{aligned} \operatorname{sgn}_f(G(A)) \cdot \operatorname{sgn}_g(A) &= \operatorname{sgn} \left(\frac{f(g(i)) - f(g(j))}{g(i) - g(j)} \cdot \frac{g(i) - g(j)}{i - j} \right) = \\ &= \operatorname{sgn} \left(\frac{(f \circ g)(i) - (f \circ g)(j)}{i - j} \right) = \operatorname{sgn}_{f \circ g}(A). \end{aligned}$$

Zatem na mocy (6.8), (6.9) i (6.10) mamy

$$\begin{aligned} \operatorname{sgn}(f \circ g) &= \prod_{A \in P_n} \operatorname{sgn}_{f \circ g}(A) = \prod_{A \in P_n} [\operatorname{sgn}_f(G(A)) \cdot \operatorname{sgn}_g(A)] = \\ &= \prod_{A \in P_n} \operatorname{sgn}_f(G(A)) \cdot \prod_{A \in P_n} \operatorname{sgn}_g(A) = \prod_{A \in P_n} \operatorname{sgn}_f(A) \cdot \prod_{A \in P_n} \operatorname{sgn}_g(A) = \\ &= \operatorname{sgn}(f) \cdot \operatorname{sgn}(g). \end{aligned}$$

W szczególności mamy stąd, że $1 = \operatorname{sgn}(e) = \operatorname{sgn}(f \circ f^{-1}) = \operatorname{sgn}(f) \cdot \operatorname{sgn}(f^{-1})$, czyli $\operatorname{sgn}(f^{-1}) = \operatorname{sgn}(f)$. Kończy to dowód naszego twierdzenia. $\square$

Wniosek 2. Dla $n \geq 2$ A_n jest podgrupą normalną indeksu 2 grupy S_n .

Dowód. Ponieważ $\text{sgn}(e) = 1$, więc $e \in A_n$. Niech $f, g \in A_n$. Wtedy $\text{sgn}(f) = \text{sgn}(g) = 1$, skąd z twierdzenia 6 mamy, że $\text{sgn}(g^{-1}) = 1$ oraz $\text{sgn}(f \circ g^{-1}) = \text{sgn}(f) \cdot \text{sgn}(g^{-1}) = 1 \cdot 1 = 1$, czyli $f \circ g^{-1} \in A_n$. Zatem A_n jest podgrupą grupy S_n . Dalej, $n \geq 2$, więc $(1, 2) \in S_n$ oraz z przykładu 9 mamy, że $\text{sgn}((1, 2)) = -1$, więc $(1, 2) \notin A_n$. Weźmy dowolne $g \in S_n$. Jeśli $g \notin A_n$, to $\text{sgn}(g) = -1$, skąd na mocy twierdzenia 6 $\text{sgn}((1, 2) \circ g) = (-1) \cdot (-1) = 1$, czyli $f = (1, 2) \circ g \in A_n$. Ale $(1, 2) \circ (1, 2) = e$, więc $g = (1, 2) \circ f \in (1, 2)A_n$. Oznacza to, że $S_n = A_n \cup (1, 2)A_n$, więc ostatecznie $(S_n : A_n) = 2$. Zatem z rozdziału 4, $A_n \triangleleft S_n$. $\square$

Rozdział 7

Grupy permutacji II

7.1 Permutacje rozłączne

Definicja 1. Permutacje $f, g \in S_n$ nazywamy *rozłącznymi*, jeżeli $X_f \cap X_g = \emptyset$ (równoważnie: $f(x) = x$ lub $g(x) = x$ dla każdego $x \in X_n$).

Ponieważ dla $h \in S_n$ i dla $k \in \mathbb{N}$ mamy, że $X_{f^k} \subseteq X_f$ (bo jeśli $x \in X_{f^k}$, to $f^k(x) \neq x$, czyli $f(x) \neq x$ i $x \in X_f$), więc mamy stąd natychmiast następujące

Stwierdzenie 1. *Jeżeli permutacje $f, g \in S_n$ są rozłączne, to dla dowolnych liczb naturalnych k, l permutacje f^k i g^l też są rozłączne.* $\square$

Stwierdzenie 2. *Jeżeli permutacje $f, g \in S_n$ są rozłączne, to*

- (i) $f \circ g = g \circ f$,
- (ii) jeżeli $f \circ g = e$, to $f = g = e$,
- (iii) $o(f \circ g) = [o(f), o(g)]$.

Dowód. (i) Dla $x \in X_n \setminus (X_f \cup X_g)$ jest $f(x) = g(x) = x$, więc $(f \circ g)(x) = f(g(x)) = f(x) = x = g(x) = g(f(x)) = (g \circ f)(x)$. Ponadto dla $x \in X_f$ jest $f(x) \in X_f$, więc $f(x) \notin X_g$ oraz $g(f(x)) = f(x)$ i $f(g(x)) = f(x)$, bo $g(x) = x$, gdyż $x \notin X_g$. Zatem dla $x \in X_f$ mamy, że $(f \circ g)(x) = (g \circ f)(x)$. Podobnie pokazujemy, że $(f \circ g)(x) = (g \circ f)(x)$ dla $x \in X_g$. Stąd ostatecznie $f \circ g = g \circ f$.

(ii) Załóżmy, że $g \neq e$. Wtedy istnieje $x \in X_n$ takie, że $g(x) \neq x$, skąd $x \in X_g$, więc $g(x) \in X_g$, czyli $g(x) \notin X_f$ i $f(g(x)) = g(x)$. Ale $x = e(x) = (f \circ g)(x) = f(g(x)) = g(x)$ i mamy sprzeczność. Stąd $g = e$ i w konsekwencji $f = e$.

(iii) Oznaczmy $k = o(f)$, $l = o(g)$, $m = [k, l]$, $s = o(f \circ g)$. Wtedy $e = (f \circ g)^s = f^s \circ g^s$ na mocy (i), więc z (ii) i ze stwierdzenia 1 mamy, że $f^s = e$ i $g^s = e$. Zatem $k \mid s$ i $l \mid s$, skąd $m \mid s$. Ale na mocy (i) $(f \circ g)^m = f^m \circ g^m = e \circ e = e$, bo $k \mid m$ i $l \mid m$, więc $s \mid m$. Zatem $m \mid s$ i $s \mid m$, skąd $s = m$. $\square$

Uwaga 1. Wzór (iii) można uogólnić na większą liczbę parami rozłącznych permutacji.

7.2 Rozkład permutacji na cykle

Niech A będzie niepustym zbiorem oraz niech $b_0, b_1, \dots, b_{r-1}$ ($r \geq 2$) będą różnymi elementami zbioru A . Wówczas permutację postaci

$$\begin{pmatrix} b_0 & b_1 & \dots & b_{r-2} & b_{r-1} \\ b_1 & b_2 & \dots & b_{r-1} & b_0 \end{pmatrix} \quad (7.1)$$

nazywamy *cyklem*, a liczbę r — jego długością. Cykl (7.1) zapisujemy prościej jako $(b_0, b_1, \dots, b_{r-1})$. Zatem transpozycje są to dokładnie cykle długości 2. Z określenia cyklu mamy od razu wzór:

$$(b_0, b_1, \dots, b_{r-1})(b_i) = b_{i \oplus_r 1} \quad (7.2)$$

dla każdego $i = 0, 1, \dots, r-1$.

Ze wzoru (7.2) natomiast przez prostą indukcję uzyskujemy, że

$$(b_0, b_1, \dots, b_{r-1})^k(b_i) = b_{i \oplus_r k} \quad (7.3)$$

dla $k, i = 0, 1, \dots, r-1$.

Ze wzoru (7.3) mamy w szczególności, że $(b_0, b_1, \dots, b_{r-1})^k(b_0) = b_k \neq b_0$ dla naturalnych $k < r$, więc $(b_0, b_1, \dots, b_{r-1})^k \neq e$ dla naturalnych $k < r$. Ponadto ze wzoru (7.3) wynika, że $(b_0, b_1, \dots, b_{r-1})^r = e$. W ten sposób udowodniliśmy następujące

Stwierdzenie 3. *Rząd dowolnego cyklu długości r jest równy r . $\square$*

Teraz udowodnimy, że każdy cykl długości r jest złożeniem $r - 1$ transpozycji.

Stwierdzenie 4. *Dla dowolnych różnych elementów $a_1, a_2, \dots, a_r \in A$ ($r \geq 2$) zachodzi wzór:*

$$(a_1, a_2, \dots, a_r) = (a_1, a_r) \circ (a_1, a_{r-1}) \circ \dots \circ (a_1, a_2). \quad (7.4)$$

Dowód. Indukcja względem $r \geq 2$. Dla $r = 2$ teza jest oczywista. Jeżeli zaś teza zachodzi dla pewnego naturalnego $r \geq 2$ i $a_1, a_2, \dots, a_r, a_{r+1}$ są różnymi elementami zbioru A , to z założenia indukcyjnego

$$(a_1, a_3, \dots, a_r, a_{r+1}) = (a_1, a_{r+1}) \circ (a_1, a_r) \circ \dots \circ (a_1, a_3),$$

więc

$$\begin{aligned} (a_1, a_{r+1}) \circ (a_1, a_r) \circ \dots \circ (a_1, a_3) \circ (a_1, a_2) &= (a_1, a_3, \dots, a_r, a_{r+1}) \circ (a_1, a_2) = \\ &= \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_r & a_{r+1} \\ a_2 & a_3 & a_4 & \dots & a_{r+1} & a_1 \end{pmatrix} = (a_1, a_2, \dots, a_r, a_{r+1}). \quad \square \end{aligned}$$

Wniosek 1. *Cykl jest permutacją parzystą wtedy i tylko wtedy, gdy jego długość jest liczbą nieparzystą.*

Dowód. Niech $f = (a_1, a_2, \dots, a_r)$ będzie cyklem długości r . Wtedy ze stwierdzenia 4 mamy, że f jest złożeniem $r - 1$ transpozycji. Zatem z poprzedniego rozdziału mamy, że $\text{sgn}(f) = (-1)^{r-1}$, skąd mamy tezę. $\square$

Stwierdzenie 5. *Dla dowolnych różnych elementów $a_0, a_1, \dots, a_{r-1}$ zbioru A i dla dowolnej permutacji $f \in S(A)$ zachodzi wzór:*

$$f \circ (a_0, a_1, \dots, a_{r-1}) \circ f^{-1} = (f(a_0), f(a_1), \dots, f(a_{r-1})). \quad (7.5)$$

Dowód. Dla $a \in A \setminus \{a_0, a_1, \dots, a_{r-1}\}$ mamy

$$[f \circ (a_0, a_1, \dots, a_{r-1}) \circ f^{-1}](a) = [f \circ (a_0, a_1, \dots, a_{r-1})](a) = f(a)$$

oraz $f(a) \notin \{f(a_0), f(a_1), \dots, f(a_{r-1})\}$, więc

$$(f(a_0), f(a_1), \dots, f(a_{r-1}))(f(a)) = f(a).$$

Ponadto dla $i = 0, 1, \dots, r-1$ mamy

$$[f \circ (a_0, a_1, \dots, a_{r-1}) \circ f^{-1}](a_i) = [f \circ (a_0, a_1, \dots, a_{r-1})](a_i) = f(a_{i \oplus r, 1})$$

oraz

$$(f(a_0), f(a_1), \dots, f(a_{r-1}))(f(a_i)) = f(a_{i \oplus r, 1}).$$

Stąd mamy tezę. $\square$

Twierdzenie 1. *Każda permutacja $\neq e$ zbioru skończonego A jest złożeniem parami rozłącznych cykli. Przedstawienie permutacji w postaci złożenia parami rozłącznych cykli jest jednoznaczne z dokładnością do kolejności czynników.*

Dowód. Zastosujemy indukcję ze względu na liczbę n elementów zbioru A . Dla $n = 1$ i $n = 2$ teza jest oczywista. Załóżmy, że teza zachodzi dla permutacji zbiorów o liczbie elementów mniejszej niż n . Niech $f \neq e$ będzie permutacją zbioru n -elementowego A . Istnieje wtedy $a \in A$ takie, że $f(a) \neq a$. Rozpatrzmy ciąg $a_1 = a, a_2 = f(a_1), a_3 = f(a_2), \dots$. Ponieważ zbiór A jest skończony, więc wyrazy tego ciągu nie mogą być wszystkie różne. Niech a_{k+1} będzie najwcześniejszym jego wyrazem równym jednemu z wyrazów poprzednich, tzn. niech $a_{k+1} = a_s$ dla pewnego $s < k+1$. Jeżeli $s > 1$, to $f(a_k) = a_{k+1} = a_s = f(a_{s-1})$, skąd $a_k = a_{s-1}$, co przeczy minimalności $k+1$. Zatem $s = 1$ i wobec tego elementy $a_1, a_2 = f(a_1), \dots, a_k = f(a_{k-1})$ są różne oraz $f(a_k) = a_{k+1} = a_1$. W zapisie permutacji f przestawmy kolumny tak, aby w pierwszym wierszu na początku występowały elementy $a_1, a_2, \dots, a_k$. Wtedy

$$\begin{aligned} f &= \begin{pmatrix} a_1 & a_2 & \dots & a_{k-1} & a_k & a'_1 & \dots & a'_{n-k} \\ a_2 & a_3 & \dots & a_k & a_1 & f(a'_1) & \dots & f(a'_{n-k}) \end{pmatrix} = \\ &= (a_1, a_2, \dots, a_k) \circ \begin{pmatrix} a'_1 & \dots & a'_{n-k} \\ f(a'_1) & \dots & f(a'_{n-k}) \end{pmatrix}. \end{aligned}$$

Zatem f jest złożeniem cyklu $(a_1, \dots, a_k)$ oraz permutacji $g = \begin{pmatrix} a'_1 & \dots & a'_{n-k} \\ f(a'_1) & \dots & f(a'_{n-k}) \end{pmatrix}$ zbioru $A' = \{a'_1, \dots, a'_{n-k}\}$. Na mocy założenia indukcyjnego $g = e$ lub g jest złożeniem skończonej liczby cykli rozłącznych, z których każdy jest rozłączny z cyklem $(a_1, \dots, a_k)$, skąd f jest iloczynem parami rozłącznych cykli.

Dla dowodu drugiej części twierdzenia przypuśćmy, że permutacja $f \neq e$ ma dwa istotnie różne przedstawienia w postaci złożenia (iloczynu) cykli rozłącznych:

$$f = (a_1, \dots, a_k) \circ \dots = (b_1, b_2, \dots, b_s) \circ \dots$$

Niech np. cykl $(b_1, b_2, \dots, b_s)$ będzie różny od każdego z cykli występujących w pierwszym przedstawieniu permutacji f . Ponieważ $b_1 \in A$, więc element b_1 należy do pewnego cyklu występującego w pierwszym przedstawieniu permutacji f . Ale składanie cykli rozłącznych jest przemienne, więc można zakładać, że $b_1 = a_i$ dla pewnego $i = 1, 2, \dots, k$. Ponadto

$$(a_1, \dots, a_i, a_{i+1}, \dots, a_k) = (a_i, a_{i+1}, \dots, a_k, a_1, \dots, a_{i-1}),$$

więc można zakładać, że $b_1 = a_1$. Wtedy $b_2 = f(b_1) = f(a_1) = a_2$, $b_3 = f(b_2) = f(a_2) = a_3$, itd. Wynika stąd, że $s = k$ oraz $(b_1, b_2, \dots, b_s) = (a_1, a_2, \dots, a_k)$. Uzyskana sprzeczność kończy dowód naszego twierdzenia. $\square$

Ze stwierdzenia 2 oraz z dowodu wniosku 1 wynika od razu następujące

Twierdzenie 2. *Jeżeli permutacja f jest złożeniem s cykli parami rozłącznych o długościach $r_1, r_2, \dots, r_s$, to*

- (i) $o(f) = [r_1, r_2, \dots, r_s]$;
- (ii) $\text{sgn}(f) = (-1)^{r_1+r_2+\dots+r_s-s}$. $\square$

Z twierdzenia 1, ze stwierdzenia 4 oraz z tego, że $e = (1, 2) \circ (1, 2)$ wynika od razu następujące

Twierdzenie 3. *Każda permutacja $f \in S_n$ dla $n \geq 2$ jest złożeniem skończonej liczby transpozycji.* $\square$

Ponieważ znak złożenia permutacji jest równy iloczynowi znaków tych permutacji oraz transpozycje są permutacjami nieparzystymi, więc mamy też następujące

Twierdzenie 4. *Permutacja $f \in S_n$ dla $n \geq 2$ jest permutacją parzystą wtedy i tylko wtedy, gdy f jest złożeniem parzystej liczby transpozycji.* $\square$

Stwierdzenie 6. *Jeżeli x, y, z, t są różnymi elementami zbioru A , to w grupie permutacji $S(A)$ zachodzi wzór:*

$$[(x, y, z), (x, y, t)] = (x, y) \circ (z, t). \quad (7.6)$$

Dowód. Mamy

$$\begin{aligned} [(x, y, z), (x, y, t)] &= (x, y, z)^{-1} \circ (x, y, t)^{-1} \circ (x, y, z) \circ (x, y, t) = \\ &= (x, z, y) \circ (t, y, x) \circ (x, y, z) \circ (x, y, t) = \\ &= \begin{pmatrix} x & y & z & t \\ y & x & t & z \end{pmatrix} = (x, y) \circ (z, t). \quad \square \end{aligned}$$

Przykład 1. Niech w grupie S_4 :

$$V = \{e, (1, 2) \circ (3, 4), (1, 3) \circ (2, 4), (1, 4) \circ (2, 3)\}. \quad (7.7)$$

Oznaczmy: $a = (1, 2) \circ (3, 4)$, $b = (1, 3) \circ (2, 4)$, $c = (1, 4) \circ (2, 3)$. Wtedy $a^2 = b^2 = c^2 = e$. Ponadto $a \circ b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (1, 4) \circ (2, 3) = c$,

$b \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = c$, więc V jest podgrupą rzędu 4 grupy S_4

(izomorficzną z grupą czwórkową Kleina). Dla $f \in S_4$ na mocy stwierdzenia 5 mamy, że $f \circ a \circ f^{-1} = f \circ (1, 2) \circ (3, 4) \circ f^{-1} = [f \circ (1, 2) \circ f^{-1}] \circ [f \circ (3, 4) \circ f^{-1}] = (f(1), f(2)) \circ (f(3), f(4)) \in V$ i podobnie $f \circ b \circ f^{-1}, f \circ c \circ f^{-1} \in V$. Stąd $V \triangleleft S_4$. Ale $V \subseteq A_4$, więc $V \triangleleft A_4$. Dalej, $|A_4| = \frac{4!}{2} = 12$ i $|A_4/V| = \frac{|A_4|}{|V|} = \frac{12}{4} = 3$, więc grupa A_4/V jest abelowa, skąd z twierdzenia 1 z rozdziału 5, $A'_4 \subseteq V$. Ponadto $e = [e, e]$, więc ze stwierdzenia 6 każdy element grupy V

jest komutatorem dwóch cykli długości 3, które na mocy wniosku 1 są permutacjami parzystymi, więc $V \subseteq A'_4$ i ostatecznie $V = A'_4$. Z przykładu 1 z rozdziału 5 mamy zatem stąd, że w grupie A_4 nie istnieje podgrupa rzędu 6, chociaż 6 dzieli rząd grupy A_4 . $\square$

Twierdzenie 5. *Jeżeli A jest zbiorem o co najmniej trzech elementach, to $Z(S(A)) = \{e\}$.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje zbiór A o co najmniej trzech elementach i istnieje $f \in Z(S(A))$ takie, że $f \neq e$. Zatem istnieje $a \in A$ takie, że $f(a) \neq a$. Oznaczmy $b = f(a)$. Wtedy a i b są różnymi elementami zbioru A i zbiór A posiada co najmniej trzy elementy, więc istnieje $c \in A \setminus \{a, b\}$. Dalej, $f \in Z(S(A))$, więc na mocy stwierdzenia 5 $(b, f(c)) = f \circ (a, c) \circ f^{-1} = (a, c)$, skąd $\{b, f(c)\} = \{a, c\}$. Ale $c \neq b$, więc $c = f(c)$ oraz $a \neq b$, więc $a = f(c)$, czyli $a = c$ i mamy sprzeczność. Oznacza to, że $Z(S(A)) = \{e\}$. $\square$

Rozdział 8

Zasadnicze twierdzenie algebry. Pojęcie pierścienia

8.1 Zasadnicze twierdzenie algebry i jego dowód

Definicja 1. Wielomianem o współczynnikach zespolonych nazywamy funkcję $f : \mathbb{C} \rightarrow \mathbb{C}$ postaci

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0,$$

gdzie $a_0, a_1, \dots, a_n$ są ustalonymi liczbami zespolonymi oraz $n = 0, 1, \dots$. Ponadto dla $a_n \neq 0$ mówimy, że n jest stopniem wielomianu $f(x)$.

Lemat 1. *Niech $f(x)$ będzie wielomianem o współczynnikach zespolonych. Wówczas dla każdego $r > 0$ istnieje stała $K > 0$ taka, że*

$$|f(z_1) - f(z_2)| \leq K \cdot |z_1 - z_2|$$

dla wszystkich $z_1, z_2 \in \mathbb{C}$ takich, że $|z_1|, |z_2| < r$.

Dowód. Jeżeli $f(x) = a_0$ dla $x \in \mathbb{C}$, to wystarczy wziąć $K = 1$. Załóżmy więc, że $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, gdzie $n \geq 1$ i $a_n \neq 0$. Weźmy dowolne $z_1, z_2 \in \mathbb{C}$ takie, że $|z_1|, |z_2| < r$. Wtedy dla $k = 1, 2, \dots, n$ mamy, że

$$z_1^k - z_2^k = (z_1 - z_2) \cdot (z_1^{k-1} + z_1^{k-2}z_2 + \dots + z_1z_2^{k-2} + z_2^{k-1})$$

oraz z nierówności trójkąta:

$$\begin{aligned} & |z_1^{k-1} + z_1^{k-2}z_2 + \dots + z_1z_2^{k-2} + z_2^{k-1}| \leq \\ & \leq |z_1|^{k-1} + |z_1|^{k-2}|z_2| + \dots + |z_1||z_2|^{k-2} + |z_2|^{k-1} \leq kr^{k-1}. \end{aligned}$$

Stąd

$$\begin{aligned} |f(z_1) - f(z_2)| &= |a_n(z_1^n - z_2^n) + a_{n-1}(z_1^{n-1} - z_2^{n-1}) + \dots + a_1(z_1 - z_2)| \leq \\ &\leq |a_n||z_1^n - z_2^n| + |a_{n-1}||z_1^{n-1} - z_2^{n-1}| + \dots + |a_1||z_1 - z_2| \leq \\ &\leq |a_n||z_1 - z_2|nr^{n-1} + |a_{n-1}||z_1 - z_2|(n-1)r^{n-2} + \dots + |a_1||z_1 - z_2| = \\ &= |z_1 - z_2|(|a_n|nr^{n-1} + |a_{n-1}|(n-1)r^{n-2} + \dots + |a_2|2r + |a_1|), \end{aligned}$$

więc wystarczy wziąć $K = |a_n|nr^{n-1} + |a_{n-1}|(n-1)r^{n-2} + \dots + |a_2|2r + |a_1|$. $\square$

Definicja 2. Powiemy, że liczba zespolona z_0 jest granicą ciągu (z_n) liczb zespolonych, jeżeli

$$\forall \varepsilon > 0 \exists n_0 \in \mathbb{N} \forall n \geq n_0 |z_n - z_0| < \varepsilon.$$

Piszemy wtedy $\lim_{n \rightarrow \infty} z_n = z_0$.

Lemat 2. Niech $f(x)$ będzie wielomianem o współczynnikach zespolonych. Wówczas z $\lim_{n \rightarrow \infty} z_n = z_0$ wynika, że $\lim_{n \rightarrow \infty} |f(z_n)| = |f(z_0)|$.

Dowód. Weźmy dowolne $\varepsilon > 0$. Z lematu 1 dla $r = 1 + |z_0|$ istnieje stała $K > 0$ taka, że $|f(z) - f(z_0)| \leq K|z - z_0|$ dla wszystkich $z \in \mathbb{C}$ takich, że $|z| < 1 + |z_0|$, gdyż $|z_0| < 1 + |z_0|$. Ale $\lim_{n \rightarrow \infty} z_n = z_0$, więc dla $\delta = \min\{\frac{\varepsilon}{2K}, 1\}$ istnieje $n_0 \in \mathbb{N}$ takie, że dla wszystkich $n \geq n_0$ jest $|z_n - z_0| < \delta$, czyli $|z_n - z_0| < 1$, a więc $|z_n| = |(z_n - z_0) + z_0| \leq |z_n - z_0| + |z_0| < 1 + |z_0|$, skąd $|f(z_n) - f(z_0)| \leq K\frac{\varepsilon}{2K} = \frac{\varepsilon}{2} < \varepsilon$ dla $n \geq n_0$. Oznacza to, że $\lim_{n \rightarrow \infty} |f(z_n)| = |f(z_0)|$. $\square$

Definicja 3. Powiemy, że ciąg (z_n) liczb zespolonych jest *ograniczony*, jeżeli istnieje stała $A > 0$ taka, że $|z_n| \leq A$ dla wszystkich $n \in \mathbb{N}$.

Lemat 3. *Z każdego ciągu ograniczonego liczb zespolonych można wybrać podciąg zbieżny do pewnej liczby zespolonej.*

Dowód. Niech (z_n) będzie ograniczonym ciągiem liczb zespolonych. Wtedy istnieje stała $A > 0$ taka, że $|z_n| \leq A$ dla wszystkich $n \in \mathbb{N}$. Ponadto dla $n = 1, 2, \dots$ istnieją $a_n, b_n \in \mathbb{R}$ takie, że $z_n = a_n + b_n i$, więc $|a_n| \leq \sqrt{a_n^2 + b_n^2} = |z_n| \leq A$ i podobnie $|b_n| \leq A$ dla $n = 1, 2, \dots$. Zatem (a_n) i (b_n) są ograniczonymi ciągami liczb rzeczywistych. Stąd z twierdzenia Weierstrassa istnieje podciąg (a_{k_n}) ciągu (a_n) , który jest zbieżny do pewnej liczby rzeczywistej a_0 . Zatem z twierdzenia Weierstrassa istnieje podciąg $(b_{l_{k_n}})$ ciągu (b_{k_n}) zbieżny do pewnej liczby rzeczywistej b_0 . Stąd także podciąg $(a_{l_{k_n}})$ jest zbieżny do a_0 . Weźmy dowolne $\varepsilon > 0$. Wtedy istnieje $n_0 \in \mathbb{N}$ takie, że dla wszystkich $n \geq n_0$ jest $|a_{l_{k_n}} - a_0| < \frac{\varepsilon}{\sqrt{2}}$ i $|b_{l_{k_n}} - b_0| < \frac{\varepsilon}{\sqrt{2}}$. Zatem dla $z_0 = a_0 + b_0 i$ oraz dla $n \geq n_0$ mamy

$$|z_{l_{k_n}} - z_0| = \sqrt{|a_{l_{k_n}} - a_0|^2 + |b_{l_{k_n}} - b_0|^2} < \sqrt{\frac{\varepsilon^2}{2} + \frac{\varepsilon^2}{2}} = \varepsilon.$$

Oznacza to, że $\lim_{n \rightarrow \infty} z_{l_{k_n}} = z_0$. $\square$

ZASADNICZE TWIERDZENIE ALGEBRY. *Każdy wielomian dodatniego stopnia o współczynnikach zespolonych posiada pierwiastek zespolony.*

Dla wielomianów stopnia 1 nasze twierdzenie zachodzi, bo mają one postać $f(x) = ax + b$, gdzie $a, b \in \mathbb{C}$ i $a \neq 0$ oraz wtedy $f(-\frac{b}{a}) = 0$.

Wystarczy zatem udowodnić to twierdzenie dla wielomianów stopni ≥ 2 . Ale jeżeli $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, gdzie $a_0, a_1, \dots, a_n \in \mathbb{C}$, $a_n \neq 0$ i $n \geq 2$, to $f(x) = a_n \cdot g(x)$, gdzie $g(x) = x^n + \frac{a_{n-1}}{a_n} x^{n-1} + \dots + \frac{a_1}{a_n} x + \frac{a_0}{a_n}$ i wielomiany $f(x)$ i $g(x)$ mają takie same zbiory pierwiastków. Stąd wystarczy wykazać, że dla każdego $n \geq 2$ i dla dowolnych $a_0, a_1, \dots, a_{n-1} \in \mathbb{C}$ wielomian

$$f(x) = x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \quad (8.1)$$

posiada pierwiastek zespolony.

Lemat 4. *Dla wielomianu $f(x)$ postaci (8.1) i dla każdego $z \in \mathbb{C}$ takiego, że $|z| > 1 + |a_{n-1}| + \dots + |a_0|$ mamy, że $|f(z)| > 1 + |a_0|$.*

Dowód. Załóżmy, że $z \in \mathbb{C}$ i $|z| > 1 + |a_{n-1}| + \dots + |a_0|$. Wtedy $|z| > 1$, więc $|z|^k > 1$ dla $k = 1, 2, \dots$. Stąd dla takich z mamy

$$\begin{aligned} |f(z)| &= |z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0| \geq \\ &\geq |z^n| - |a_{n-1}z^{n-1} + \dots + a_1z + a_0| \geq |z|^n - |a_{n-1}||z|^{n-1} - \dots - |a_1||z| - |a_0|. \end{aligned}$$

Ale $|z|^k \leq |z|^{n-1}$ dla $k = 0, 1, \dots, n-1$, bo $|z| > 1$ i $n \geq 2$, więc

$$\begin{aligned} |f(z)| &\geq |z|^n - |z|^{n-1} \cdot (|a_{n-1}| + \dots + |a_1| + |a_0|) = \\ &= |z|^{n-1} \cdot (|z| - |a_{n-1}| - \dots - |a_1| - |a_0|) \geq |z|^{n-1} \geq |z|, \end{aligned}$$

bo $n \geq 2$ i $|z| \geq 1 + |a_{n-1}| + \dots + |a_0|$. Stąd

$$|f(z)| > 1 + |a_{n-1}| + \dots + |a_1| + |a_0| \geq 1 + |a_0|,$$

czyli $|f(z)| > 1 + |a_0|$ dla $|z| > 1 + |a_{n-1}| + \dots + |a_1| + |a_0|$. $\square$

Lemat 5. Dla wielomianu $f(x)$ postaci (8.1) istnieje $z_0 \in \mathbb{C}$ takie, że

$$|f(z)| \geq |f(z_0)|$$

dla każdego $z \in \mathbb{C}$.

Dowód. Ponieważ dla każdego $z \in \mathbb{C}$ jest $|f(z)| \geq 0$, więc zbiór $\{|f(z)| : z \in \mathbb{C}\}$ jest ograniczony z dołu. Posiada on zatem kres dolny q . Wtedy $|f(z)| \geq q$ dla każdego $z \in \mathbb{C}$ oraz dla dowolnego $m \in \mathbb{N}$ istnieje $z_m \in \mathbb{C}$ takie, że $|f(z_m)| < q + \frac{1}{m}$. Gdyby dla pewnego m było $|z_m| > 1 + |a_{n-1}| + \dots + |a_1| + |a_0|$, to z lematu 4,

$$|f(z_m)| > 1 + |a_0| = |f(0)| + 1 \geq q + 1 \geq q + \frac{1}{m},$$

skąd $|f(z_m)| > q + \frac{1}{m}$ i mamy sprzeczność. Stąd $|z_m| \leq 1 + |a_{n-1}| + \dots + |a_0|$ dla $m \in \mathbb{N}$. Zatem z lematu 3 istnieje podciąg (z_{k_n}) ciągu (z_n) taki, że $\lim_{n \rightarrow \infty} z_{k_n} = z_0$ dla pewnego $z_0 \in \mathbb{C}$. Wówczas dla każdego $z \in \mathbb{C}$ i dla każdego m mamy, że $|f(z_m)| < |f(z)| + \frac{1}{m}$, skąd

$$|f(z)| > |f(z_{k_n})| - \frac{1}{k_n},$$

więc po przejściu do granicy z wykorzystaniem lematu 2 uzyskamy, że $|f(z)| \geq |f(z_0)|$. $\square$

Udowodnimy teraz lemat, który zakończy dowód zasadniczego twierdzenia algebry.

Lemat 6. *Dla wielomianu $f(x)$ postaci (8.1) i dla liczby z_0 z lematu 5 mamy, że $f(z_0) = 0$.*

Dowód. Niech $h(z) = f(z + z_0) = (z + z_0)^n + a_{n-1}(z + z_0)^{n-1} + \dots + a_1(z + z_0) + a_0 = z^n + b_{n-1}z^{n-1} + \dots + b_1z + b_0$ dla pewnych $b_0, b_1, \dots, b_{n-1} \in \mathbb{C}$, $b_n = 1$. Niech k będzie najmniejszą liczbą naturalną taką, że $b_k \neq 0$. Wówczas $h(z) = z^n + b_{n-1}z^{n-1} + \dots + b_kz^k + b_0$. Z lematu 5 mamy, że dla każdego $z \in \mathbb{C}$

$$|z^n + b_{n-1}z^{n-1} + \dots + b_kz^k + b_0| \geq |f(z_0)|$$

oraz $b_0 = h(0) = f(z_0)$, więc dla $z \in \mathbb{C}$ mamy

$$|z^n + b_{n-1}z^{n-1} + \dots + b_kz^k + b_0| \geq |b_0|. \quad (8.2)$$

Dla $c \in (0, 1)$ podstawmy w nierówności (8.2): $z = c \cdot \sqrt[k]{-\frac{b_0}{b_k}}$. Otrzymamy wówczas

$$|c^n \left(\sqrt[k]{-\frac{b_0}{b_k}} \right)^n + b_{n-1}c^{n-1} \left(\sqrt[k]{-\frac{b_0}{b_k}} \right)^{n-1} + \dots + b_kc^k \left(\sqrt[k]{-\frac{b_0}{b_k}} \right)^k + b_0| \geq |b_0|, \quad (8.3)$$

więc z (8.3) po uproszczeniach i podstawieniu

$$d_n = \left(\sqrt[k]{-\frac{b_0}{b_k}} \right)^n, d_{n-1} = b_{n-1} \left(\sqrt[k]{-\frac{b_0}{b_k}} \right)^{n-1}, \dots, d_{k+1} = b_{k+1} \left(\sqrt[k]{-\frac{b_0}{b_k}} \right)^{k+1}$$

uzyskamy

$$|d_nc^n + d_{n-1}c^{n-1} + \dots + d_{k+1}c^{k+1} - b_0c^k + b_0| \geq |b_0| \quad \text{dla } c \in (0, 1). \quad (8.4)$$

Oznaczmy $g(x) = d_nx^{n-k-1} + d_{n-1}x^{n-k-2} + \dots + d_{k+1}$. Wtedy z (8.4) mamy

$$|c^{k+1}g(c) + b_0(1 - c^k)| \geq |b_0| \quad \text{dla } c \in (0, 1). \quad (8.5)$$

Ponadto $|c^{k+1}g(c) + b_0(1 - c^k)| \leq |c^{k+1}g(c)| + |b_0||1 - c^k| = c^{k+1}|g(c)| + |b_0|(1 - c^k)$, bo $0 < c < 1$. Zatem z (8.5):

$$c^{k+1}|g(c)| + |b_0| - |b_0|c^k \geq |b_0| \text{ dla } c \in (0, 1),$$

a więc

$$c|g(c)| \geq |b_0| \text{ dla } c \in (0, 1).$$

Ponadto

$$\begin{aligned} |g(c)| &= |d_n c^{n-k-1} + d_{n-1} c^{n-k-2} + \dots + d_{k+1}| \leq \\ &\leq |d_n| c^{n-k-1} + |d_{n-1}| c^{n-k-2} + \dots + |d_{k+1}| \leq \\ &|d_n| + |d_{n-1}| + \dots + |d_{k+1}|, \end{aligned}$$

bo $0 < c < 1$. Zatem

$$c(|d_n| + |d_{n-1}| + \dots + |d_{k+1}|) \geq |b_0| \text{ dla } c \in (0, 1).$$

Stąd po przejściu do granicy względem $c \rightarrow 0$ otrzymamy, że $0 \geq |b_0|$, czyli $|b_0| = 0$. Ale $f(z_0) = b_0$, więc $f(z_0) = 0$. $\square$

8.2 Pojęcie pierścienia

Definicja 4. *Pierścieniem* nazywamy system algebraiczny $(P, +, \cdot, 0, 1)$ taki, że

- P1.** $(P, +, 0)$ jest grupą abelową;
- P2.** $\forall_{a,b,c \in P} a \cdot (b + c) = a \cdot b + a \cdot c$;
- P3.** $\forall_{a,b,c \in P} a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- P4.** $\forall_{a \in P} a \cdot 1 = a$;
- P5.** $\forall_{a,b \in P} a \cdot b = b \cdot a$.

Działanie oznaczane przez $+$ nazywamy *dodawaniem*, zaś działanie oznaczane przez $\cdot$ nazywamy *mnożeniem*, natomiast element oznaczony symbolem 1 nazywamy *jedynką pierścienia* P . Grupę abelową $(P, +, 0)$ nazywamy *grupą addytywną pierścienia* P i oznaczamy przez P^+ .

Własności działań w pierścieniu

Niech $(P, +, \cdot, 0, 1)$ będzie pierścieniem. Wówczas:

$$1. \forall_{a \in P} a \cdot 0 = 0 \cdot a = 0.$$

Dowód. Ponieważ $0 = 0 + 0$, więc na mocy **P2**: $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, czyli $a \cdot 0 + 0 = a \cdot 0 + a \cdot 0$, skąd z prawa skracania w grupach abelowych mamy, że $a \cdot 0 = 0$. Zatem na mocy **P5** także $0 \cdot a = 0$. $\square$

$$2. \forall_{a,b \in P} -(a \cdot b) = (-a) \cdot b = a \cdot (-b).$$

Dowód. Na mocy **P2** i **1** mamy, że $a \cdot b + a \cdot (-b) = a \cdot [b + (-b)] = a \cdot 0 = 0$, skąd $a \cdot (-b) = -(a \cdot b)$. Stąd na mocy **P5**: $-(a \cdot b) = -(b \cdot a) = b \cdot (-a) = (-a) \cdot b$. $\square$

$$3. \forall_{a,b,c \in P} (a + b) \cdot c = a \cdot c + b \cdot c.$$

Dowód. Na mocy **P5**, **P2** i znowu **P5** mamy, że $(a + b) \cdot c = c \cdot (a + b) = c \cdot a + c \cdot b = a \cdot c + b \cdot c$. $\square$

$$4. \forall_{a \in P} (-1) \cdot a = a \cdot (-1) = -a.$$

Dowód. Na mocy **P4** i **P5** mamy, że $a = a \cdot 1 = 1 \cdot a$, więc z **2** i **P5**, $-a = -(a \cdot 1) = a \cdot (-1) = (-1) \cdot a$. $\square$

$$5. \forall_{a,a_1,\dots,a_n \in P} a \cdot (a_1 + \dots + a_n) = a \cdot a_1 + \dots + a \cdot a_n.$$

Dowód. Indukcja względem n . Dla $n = 2$ teza wynika z **P2**. Załóżmy, że teza zachodzi dla pewnej liczby naturalnej $n \geq 2$ i niech $a_1, \dots, a_n, a_{n+1} \in P$. Wtedy na mocy **P2** i założenia indukcyjnego: $a \cdot (a_1 + \dots + a_n + a_{n+1}) = a \cdot [(a_1 + \dots + a_n) + a_{n+1}] = a \cdot (a_1 + \dots + a_n) + a \cdot a_{n+1} = a \cdot a_1 + \dots + a \cdot a_n + a \cdot a_{n+1}$, czyli teza zachodzi dla liczby $n + 1$. $\square$

$$6. \forall_{a,b,c \in P} a \cdot (b - c) = a \cdot b - a \cdot c.$$

Dowód. Z określenia odejmowania, z **P2**, z **2** i znowu z określenia odejmowania mamy, że $a \cdot (b - c) = a \cdot (b + (-c)) = a \cdot b + a \cdot (-c) = a \cdot b + (-(a \cdot c)) = a \cdot b - a \cdot c$. $\square$

Ponieważ $(P, +, 0)$ jest grupą abelową, więc ma sens całkowita wielokrotność $k \cdot a$ elementu $a \in P$ przez liczbę całkowitą k . Przypomnijmy jej określenie:

$$0 \cdot a = 0, 1 \cdot a = a \text{ oraz dla } n \in \mathbb{N}: n \cdot a = \underbrace{a + \dots + a}_n \text{ i } (-n) \cdot a = \underbrace{(-a) + \dots + (-a)}_n.$$

Z teorii grup mamy zatem następujące własności:

$$7. \forall a \in P \forall n, m \in \mathbb{Z} \quad n \cdot (m \cdot a) = (nm) \cdot a.$$

$$8. \forall a \in P \forall n, m \in \mathbb{Z} \quad (n + m) \cdot a = n \cdot a + m \cdot a.$$

$$9. \forall a, b \in P \forall n \in \mathbb{Z} \quad n \cdot (a + b) = n \cdot a + n \cdot b.$$

Można także udowodnić następującą własność:

$$10. \forall a, b \in P \forall n \in \mathbb{Z} \quad n \cdot (a \cdot b) = (n \cdot a) \cdot b = a \cdot (n \cdot b).$$

W pierścieniu P możemy też określić nieujemną całkowitą potęgę dowolnego elementu $a \in P$ przyjmując, że:

$$a^0 = 1, a^1 = a \text{ oraz dla } n \in \mathbb{N}: a^{n+1} = a^n \cdot a \text{ (czyli } a^n = \underbrace{a \cdot \dots \cdot a}_n).$$

Przez prostą indukcję możemy wówczas udowodnić następujące własności:

$$11. \forall a \in P \forall n, m \in \mathbb{Z} \quad a^n \cdot a^m = a^{n+m}.$$

$$12. \forall a \in P \forall n, m \in \mathbb{N} \quad (a^n)^m = a^{nm}.$$

$$13. \forall a, b \in P \forall n \in \mathbb{N} \quad (a + b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k.$$

Rozdział 9

Podpierścienie, elementy odwracalne, dzielniki zera

9.1 Określenie podpierścienia

Definicja 1. *Podpierścieniem pierścienia $(P, +, \cdot, 0, 1)$ nazywamy taki podzbiór $A \subseteq P$, który jest pierścieniem ze względu na wszystkie działania określone w pierścieniu P (zredukowane do A).*

Stwierdzenie 1. *Podzbiór A pierścienia P jest podpierścieniem pierścienia P wtedy i tylko wtedy, gdy spełnia następujące warunki:*

(I) $1 \in A$ oraz (II) $\forall a, b \in A \ a - b, a \cdot b \in A$.

Dowód. Załóżmy, że A jest podpierścieniem pierścienia P . Wtedy $0, 1 \in A$ (ze względu na wykonalność działań 0-argumentowych) oraz dla dowolnego $a \in A$, $-a \in A$ (ze względu na wykonalność działania 1-argumentowego) i ponadto dla $a, b \in A$, $a \cdot b \in A$ oraz $a - b = a + (-b) \in A$ (ze względu na wykonalność mnożenia i dodawania).

Na odwrót, załóżmy, że $1 \in A$ oraz $a - b, a \cdot b \in A$ dla dowolnych $a, b \in A$. Wtedy $0 = 1 - 1 \in A$, skąd dla $b \in A$, $-b = 0 - b \in A$, więc dla $a, b \in A$, $a + b = a - (-b) \in A$. Zatem w A jest wykonalne mnożenie i dodawanie. Ponieważ wszystkie aksjomaty pierścienia są spełnione nawet w P , więc $(A, +, \cdot, 0, 1)$ jest pierścieniem. $\square$

9.2 Przykłady pierścieni i podpierścieni

Przykład 1. Każde ciało jest pierścieniem. Podpierścienie ciał są pierścieniami.

Przykład 2. Podpierścienie ciała $\mathbb{C}$ nazywamy *pierścieniami liczbowymi*. Oczywiście są one pierścieniami. Przykłady pierścieni liczbowych:

- a) Pierścień liczb całkowitych $\mathbb{Z}$;
- b) Dla ustalonej liczby naturalnej $a > 1$ zbiór

$$\left[\frac{1}{a} \right] = \left\{ \frac{n}{a^k} : n, k \in \mathbb{Z}, k \geq 0 \right\}$$

jest pierścieniem liczbowym (sprawdzenie zostawiamy Czytelnikowi);

c) Niech d będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej. Wówczas z teorii liczb wiadomo, że d nie jest kwadratem liczby wymiernej. Określamy $\sqrt{d}$ jako zwykły pierwiastek arytmetyczny z liczby d dla $d > 0$, zaś dla $d < 0$ określamy $\sqrt{d} = \sqrt{|d|} \cdot i$. Zatem w obu przypadkach $(\sqrt{d})^2 = d$. Można sprawdzić, że wówczas zbiór $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ jest pierścieniem liczbowym;

d) Niech d będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej taką, że $d \equiv 1 \pmod{4}$. Można sprawdzić, że wtedy zbiór $\mathbb{Z} \left[\frac{1+\sqrt{d}}{2} \right] = \{x + y \cdot \frac{1+\sqrt{d}}{2} : x, y \in \mathbb{Z}\}$ jest pierścieniem liczbowym.

Przykład 3. Niech $m > 1$ będzie ustaloną liczbą naturalną i niech $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$. Dla $a, b \in \mathbb{Z}_m$ określamy:

$a \oplus_m b$ = reszta z dzielenia $a + b$ przez m ;

$a \odot_m b$ = reszta z dzielenia $a \cdot b$ przez m .

W oparciu o własności kongruencji można sprawdzić, że wówczas $(\mathbb{Z}_m, \oplus_m, \odot_m, 0, 1)$ jest pierścieniem.

Przykład 4. Zbiór wszystkich wielomianów o współczynnikach rzeczywistych z dodawaniem i mnożeniem funkcji tworzy pierścień. Oznaczamy go przez $\mathbb{R}[x]$.

Przykład 5. Zbiór wszystkich wielomianów o współczynnikach wymiernych z dodawaniem i mnożeniem funkcji tworzy pierścień.

Oznaczamy go przez $\mathbb{Q}[x]$.

Przykład 6. Zbiór wszystkich wielomianów o współczynnikach całkowitych z dodawaniem i mnożeniem funkcji tworzy pierścień. Oznaczamy go przez $\mathbb{Z}[x]$.

Przykład 7. Zbiór wszystkich wielomianów o współczynnikach zespolonych z dodawaniem i mnożeniem funkcji tworzy pierścień. Oznaczamy go przez $\mathbb{C}[x]$.

Przykład 8. Niech $P_1, \dots, P_n$ będą pierścieniami. W zbiorze $P_1 \times \dots \times P_n$ określamy dodawanie i mnożenie następująco:

$$\begin{aligned}(a_1, \dots, a_n) + (b_1, \dots, b_n) &= (a_1 + b_1, \dots, a_n + b_n), \\ (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) &= (a_1 \cdot b_1, \dots, a_n \cdot b_n),\end{aligned}$$

Ponadto określamy $0 = (0, \dots, 0)$ oraz $1 = (1, \dots, 1)$. Można sprawdzić, że wtedy $(P_1 \times \dots \times P_n, +, \cdot, 0, 1)$ tworzy pierścień. Nazywamy go *iloczynem kartezjańskim pierścieni* $P_1, \dots, P_n$.

Przykład 9. Dowolny zbiór jednoelementowy $P = \{a\}$ z działaniami $+$ i $\cdot$ takimi, że $a + a = a$ i $a \cdot a = a$ oraz z wyróżnionymi elementami $0 = 1 = a$ tworzy pierścień. Nazywamy go *pierścieniem zerowym*. Zauważmy, że jeśli pierścień P jest niezerowy, to $|P| > 1$, więc istnieje niezerowe $a \in P$. Wtedy $a = a \cdot 1$ oraz $a \cdot 0 = 0 \neq a$, skąd wynika, że $0 \neq 1$ w P . Na odwrót, jeśli $0 \neq 1$ w pierścieniu P , to $|P| > 1$, więc pierścień P nie jest zerowy.

Twierdzenie 1. Część wspólna dowolnej niepustej rodziny podpierścieni pierścienia P jest podpierścieniem tego pierścienia.

Dowód. Niech $\{A_t\}_{t \in T}$ będzie dowolną niepustą rodziną podpierścieni pierścienia P oraz niech $A = \bigcap_{t \in T} A_t$. Ponieważ $1 \in A_t$ dla każdego $t \in T$, więc $1 \in A$. Weźmy dowolne $a, b \in A$. Wtedy $a, b \in A_t$ dla każdego $t \in T$, więc ze stwierdzenia 1, $a - b, a \cdot b \in A_t$ dla każdego $t \in T$. Zatem $a - b, a \cdot b \in A$. Stąd na mocy stwierdzenia 1, A jest podpierścieniem pierścienia P . $\square$

Uwaga 1. Niech P będzie pierścieniem. Wówczas dla dowolnego podzbioru $X \subseteq P$ istnieje najmniejszy (w sensie inkluzji) podpierścień

pierścienia P zawierający zbiór X . Nazywamy go *podpierścieniem generowanym przez zbiór X* i oznaczamy przez $[X]$. Rzeczywiście, niech $\{A_t\}_{t \in T}$ będzie rodziną wszystkich podpierścieni pierścienia P zawierających zbiór X . Wtedy $P \in \{A_t\}_{t \in T}$, więc z twierdzenia 1 mamy, że $A = \bigcap_{t \in T} A_t$ jest podpierścieniem pierścienia P . Ale $X \subseteq A_t$ dla każdego $t \in T$, więc $X \subseteq A$, skąd A jest najmniejszym elementem w rodzinie $\{A_t\}_{t \in T}$, czyli A jest najmniejszym podpierścieniem pierścienia P zawierającym zbiór X .

Nietrudno jest zauważyć, że $[\emptyset] = \{k \cdot 1 : k \in \mathbb{Z}\}$, natomiast dla $X \neq \emptyset$ podpierścień $[X]$ składa się ze wszystkich skończonych sum elementów postaci $s \cdot 1$ oraz $k \cdot x_1 \cdot x_2 \cdot \dots \cdot x_n$, gdzie $s, k \in \mathbb{Z}$, $x_1, x_2, \dots, x_n \in X$ oraz $n = 1, 2, \dots$. Jeśli X jest zbiorem skończonym oraz $X = \{a_1, \dots, a_m\}$, to zamiast $[\{a_1, \dots, a_m\}]$ będziemy pisali $[a_1, \dots, a_m]$. Zatem w szczególności mamy stąd

$$[a] = \{k_0 \cdot 1 + k_1 \cdot a + \dots + k_n \cdot a^n : k_0, k_1, \dots, k_n \in \mathbb{Z}, n = 0, 1, 2, \dots\}.$$

Przykład 10. Niech A i B będą podpierścieniami pierścienia P . Oznaczmy przez AB zbiór wszystkich skończonych sum elementów postaci $a \cdot b$, gdzie $a \in A$, $b \in B$. Wtedy $1 = 1 \cdot 1 \in AB$. Ponadto z określenia AB oraz z tego, że $-(a \cdot b) = (-a) \cdot b$ wynika od razu, że jeśli $x, y \in AB$, to $x - y \in AB$. Ponadto z rozdzielności mnożenia względem dodawania i z tego, że dla $a_1, a_2 \in A$, $b_1, b_2 \in B$ jest $(a_1 \cdot b_1) \cdot (a_2 \cdot b_2) = (a_1 \cdot a_2) \cdot (b_1 \cdot b_2) \in AB$ wynika, że dla dowolnych $x, y \in AB$, $x \cdot y \in AB$. Zatem na mocy stwierdzenia 1 mamy, że AB jest podpierścieniem pierścienia P .

9.3 Elementy odwracalne

Definicja 2. Powiemy, że $a \in P$ jest *elementem odwracalnym pierścienia P* , jeżeli istnieje $x \in P$ takie, że $a \cdot x = 1$. Zbiór wszystkich elementów odwracalnych pierścienia P oznaczamy przez P^* .

Twierdzenie 2. Dla dowolnego pierścienia P system algebraiczny $(P^*, \cdot, 1)$ jest grupą abelową.

Dowód. Ponieważ $1 \cdot 1 = 1$, więc $1 \in P^*$. Niech $a \in P^*$. Wtedy istnieje $x \in P$ takie, że $a \cdot x = 1$, skąd $x \cdot a = 1$, czyli $x \in P^*$. Dalej, dla $a, b \in P^*$ istnieją $x, y \in P$ takie, że $a \cdot x = 1$ i $b \cdot y = 1$, więc $(a \cdot b) \cdot (x \cdot y) = (a \cdot x) \cdot (b \cdot y) = 1 \cdot 1 = 1$, czyli $a \cdot b \in P^*$. Ponieważ mnożenie jest łączne w P , więc mnożenie jest łączne w P^* . Zatem z tych rozważań mamy, że $(P^*, \cdot, 1)$ jest grupą. Natomiast z **P5** wynika od razu, że grupa ta jest abelowa. $\square$

Uwaga 2. Element odwrotny do elementu $a \in P^*$ oznaczamy przez a^{-1} . Z dowodu twierdzenia 2 wynika, że dla dowolnych $a, b \in P^*$ mamy wzór:

$$(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}.$$

Przykład 11. Z teorii liczb wynika, że dla dowolnej liczby naturalnej $m > 1$:

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m : (a, m) = 1\}.$$

W szczególności $|\mathbb{Z}_m^*| = \varphi(m)$. $\square$

Przykład 12. Można pokazać, że dla dowolnych pierścieni $P_1, \dots, P_n$ zachodzi wzór:

$$(P_1 \times \dots \times P_n)^* = P_1^* \times \dots \times P_n^*.$$

9.4 Dzielniki zera

Definicja 3. Mówimy, że element a pierścienia P jest *dzielnikiem zera*, jeżeli istnieje niezerowy element $b \in P$ taki, że $a \cdot b = 0$.

W każdym pierścieniu niezerowym P mamy, że $0 \neq 1$ oraz $0 \cdot 1 = 0$, więc 0 jest dzielnikiem zera w każdym pierścieniu niezerowym P . Dzielniki zera różne od 0 nazywamy *właściwymi dzielnikami zera*.

Przykład 13. Dla liczb złożonych m pierścień $\mathbb{Z}_m$ posiada właściwe dzielniki zera, gdyż istnieją liczby naturalne $a, b < m$ takie, że

$a \cdot b = m$ i wtedy a, b są niezerowymi elementami pierścienia $\mathbb{Z}_m$ oraz $a \odot_m b = 0$.

Twierdzenie 3. *W dowolnym pierścieniu P element odwracalny nie jest dzielnikiem zera.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje pierścień P oraz istnieje element odwracalny $a \in P$, który jest dzielnikiem zera. Zatem istnieje niezerowe $b \in P$ takie, że $a \cdot b = 0$ oraz istnieje $x \in P$ takie, że $a \cdot x = 1$. Zatem $b = b \cdot 1 = b \cdot (a \cdot x) = (b \cdot a) \cdot x = (a \cdot b) \cdot x = 0 \cdot x = 0$ i mamy sprzeczność. $\square$

Wniosek 1. *Dowolne ciało nie posiada właściwych dzielników zera.* $\square$

Elementy pierścienia P , które nie są dzielnikami zera nazywamy *elementami regularnymi*.

Twierdzenie 4. *W dowolnym pierścieniu P :*

- a) *iloczyn elementów regularnych jest elementem regularnym;*
- b) *jeśli $a \in P$ jest regularny i $a \cdot x = a \cdot y$, to $x = y$;*
- c) *1 jest elementem regularnym.*

Dowód. a) Niech $a, b \in P$ będą elementami regularnymi. Weźmy dowolny $x \in P$ taki, że $(ab)x = 0$. Wtedy $a(bx) = 0$, więc z regularności a , $bx = 0$, skąd $x = 0$, z regularności b . Zatem ab jest elementem regularnym.

b) Niech $a \in P$ będzie elementem regularnym i niech $x, y \in P$ będą takie, że $ax = ay$. Wtedy $a(x - y) = 0$, skąd z regularności a mamy, że $x - y = 0$, czyli $x = y$.

c) Niech $x \in P$ będzie takie, że $1 \cdot x = 0$. Ponieważ $1 \cdot x = x$, więc $x = 0$ i 1 jest elementem regularnym. $\square$

Definicja 4. Niezerowy pierścień P , który nie zawiera właściwych dzielników zera nazywamy *dziedzina całkowitości*.

Z tej definicji wynika od razu, że dziedziny całkowitości są to takie niezerowe pierścienie, w których każdy element niezerowy jest regularny. W szczególności na mocy wniosku 1, każde ciało jest dziedziną całkowitości, a nawet każdy podpierścień ciała jest dziedziną całkowitości.

tości. Z twierdzenia 4 mamy natychmiast następujący

Wniosek 2. *Jeżeli a jest niezerowym elementem dziedziny całkowitości P oraz $x, y \in P$ są takie, że $ax = ay$, to $x = y$. $\square$*

Rozdział 10

Homomorfizmy i ideały

10.1 Pojęcie ideału pierścienia

Definicja 1. Niepusty podzbiór I pierścienia P nazywamy *ideałem pierścienia P* (oznaczenie: $I \triangleleft P$), jeżeli

$$(I) \forall_{i,j \in I} i - j \in I \text{ oraz } (II) \forall_{i \in I} \forall_{a \in P} a \cdot i \in I.$$

Przykład 1. W dowolnym pierścieniu P zbiór $\{0\}$ jest ideałem (nazywamy go *ideałem zerowym*). Ponadto cały pierścień P jest ideałem P (nazywamy go *ideałem niewłaściwym*). Ideały I pierścienia P takie, że $I \neq P$ nazywamy *ideałami właściwymi*.

Uwaga 1. Niech I będzie ideałem pierścienia P . Wówczas I jest ideałem właściwym wtedy i tylko wtedy, gdy $1 \notin I$. Rzeczywiście, jeżeli $1 \notin I$, to $I \neq P$, a jeżeli $1 \in I$, to dla każdego $a \in P$, $a = a \cdot 1 \in I$ na mocy (II), skąd $I = P$.

Twierdzenie 1. Każde ciało K ma dokładnie dwa ideały: $\{0\}$ i K .

Dowód. Niech I będzie niezerowym ideałem ciała K . Wtedy istnieje niezerowe $i \in I$, skąd $1 = i^{-1} \cdot i \in I$. Zatem z uwagi 1, $I = K$. $\square$

Uwaga 2. Z określenia ideału wynika od razu, że każdy ideał I pierścienia P jest podgrupą grupy addytywnej P^+ tego pierścienia. W szczególności $0 \in I$ dla każdego $I \triangleleft P$. Ponadto jeśli $i_1, \dots, i_n \in I \triangleleft P$ oraz $a_1, \dots, a_n \in P$, to $a_1 \cdot i_1, \dots, a_n \cdot i_n \in I$, skąd $a_1 \cdot i_1 + \dots + a_n \cdot i_n \in I$.

Twierdzenie 2. Część wspólna dowolnej niepustej rodziny $\{I_t\}_{t \in T}$ ideałów pierścienia P jest ideałem pierścienia P .

Dowód. Niech $\{I_t\}_{t \in T}$ będzie niepustą rodziną ideałów pierścienia P i niech $I = \bigcap_{t \in T} I_t$. Wtedy $0 \in I_t$ dla $t \in T$, więc $0 \in I$. Dla $i, j \in I$ mamy, że $i, j \in I_t$ dla każdego $t \in T$, więc $i - j \in I_t$ dla $t \in T$, skąd $i - j \in I$. Ponadto dla $a \in P$, $i \in I$ mamy, że $i \in I_t$ dla $t \in T$, więc $ai \in I_t$ dla każdego $t \in T$, skąd $ai \in I$. Zatem $I \triangleleft P$. $\square$

Uwaga 3. Z twierdzenia 2 wynika, że dla dowolnego podzbioru X pierścienia P istnieje najmniejszy w sensie inkluzji ideał pierścienia P zawierający zbiór X . Nazywamy go *ideałem generowanym* przez zbiór X i oznaczamy przez (X) . Natomiast X nazywamy *zbiorem generatorów* ideału I . Np. $(\emptyset) = \{0\}$. Jeśli zbiór X jest skończony oraz $X = \{a_1, \dots, a_n\}$, to zamiast $(\{a_1, \dots, a_n\})$ piszemy $(a_1, \dots, a_n)$. Jeżeli istnieje $a \in P$ takie, że $I = (a)$, to mówimy, że *ideał I jest główny*. Jeżeli istnieją $a_1, \dots, a_n \in P$ takie, że $I = (a_1, \dots, a_n)$, to mówimy, że *ideał I jest skończenie generowany*.

Twierdzenie 3. Dla dowolnych elementów $a_1, \dots, a_n$ pierścienia P zachodzi wzór:

$$(a_1, \dots, a_n) = \{x_1 a_1 + \dots + x_n a_n : x_1, \dots, x_n \in P\}.$$

Dowód. Oznaczmy $J = \{x_1 a_1 + \dots + x_n a_n : x_1, \dots, x_n \in P\}$. Wtedy $x_i = 0 \cdot a_1 + \dots + 1 \cdot x_i + \dots + 0 \cdot a_n \in J$ dla $i = 1, \dots, n$. Zatem $\{a_1, \dots, a_n\} \subseteq J$. Niech $i, j \in J$, $a \in P$. Wtedy istnieją $x_1, \dots, x_n, y_1, \dots, y_n \in P$ takie, że $i = x_1 a_1 + \dots + x_n a_n$ oraz $j = y_1 a_1 + \dots + y_n a_n$, więc $i - j = (x_1 - y_1) a_1 + \dots + (x_n - y_n) a_n \in J$, $ai = (ax_1) a_1 + \dots + (ax_n) a_n \in J$. Zatem $J \triangleleft P$ oraz $\{a_1, \dots, a_n\} \subseteq J$. Niech A będzie dowolnym ideałem pierścienia P zawierającym zbiór $\{a_1, \dots, a_n\}$. Wtedy z uwagi 2 mamy, że $x_1 a_1 + \dots + x_n a_n \in A$ dla dowolnych $x_1, \dots, x_n \in P$. Zatem $J \subseteq A$, czyli J jest najmniejszym

ideałem pierścienia P zawierającym zbiór $\{a_1, \dots, a_n\}$. Zatem $J = (a_1, \dots, a_n)$. $\square$

Przykład 2. Z teorii grup wiemy, że wszystkimi podgrupami grupy $\mathbb{Z}^+$ są zbiory wielokrotności ustalonych nieujemnych liczb całkowitych. Na mocy twierdzenia 3 mamy więc stąd, że każdy ideał pierścienia $\mathbb{Z}$ jest główny i wszystkimi ideałami tego pierścienia są ideały postaci (k) dla $k = 0, 1, 2, \dots$

Podobnie jest w pierścieniu $\mathbb{Z}_m$, gdyż każda niezerowa podgrupa grupy addytywnej tego pierścienia składa się z całkowitych wielokrotności ustalonych dzielników naturalnych liczby m . Wynika stąd, że wszystkie ideały pierścienia $\mathbb{Z}_m$ są postaci: (d) , gdzie $d = 0$ lub $d < m$ jest naturalnym dzielnikiem liczby m . W szczególności każdy ideał pierścienia $\mathbb{Z}_m$ jest główny i ten pierścień posiada tyle ideałów, ile dzielników naturalnych ma liczba m .

Twierdzenie 4. *Jeżeli $I_1, \dots, I_n$ są ideałami pierścienia P , to $I_1 + \dots + I_n \triangleleft P$.*

Dowód. Z teorii grup mamy

$$I_1 + \dots + I_n = \{i_1 + \dots + i_n : i_k \in I_k \text{ dla } k = 1, \dots, n\}$$

jest podgrupą grupy P^+ zawierającą $I_1 \cup \dots \cup I_n$. Niech $a \in P$, $i \in I_1 + \dots + I_n$. Wtedy istnieją $i_k \in I_k$ dla $k = 1, \dots, n$ takie, że $i = i_1 + \dots + i_n$, skąd $ai = ai_1 + \dots + ai_n \in I_1 + \dots + I_n$, bo $ai_k \in I_k$ dla $k = 1, \dots, n$. $\square$

10.2 Konstrukcja pierścienia ilorazowego

Niech I będzie ideałem pierścienia P . Wówczas I jest podgrupą grupy P^+ , więc można zbudować grupę ilorazową $P/I = \{a + I : a \in P\}$. Wówczas:

$$a + I = \{a + i : i \in I\} \text{ dla } a \in P,$$

$$a + I = b + I \Leftrightarrow a - b \in I \text{ dla } a, b \in P,$$

$$(a + I) + (b + I) = (a + b) + I \text{ dla } a, b \in P,$$

$(P/I, +, I)$ tworzy grupę abelową.

W P/I można też określić naturalne mnożenie:

$$(a + I) \cdot (b + I) = ab + I \text{ dla } a, b \in P.$$

Sprawdźmy, czy mnożenie warstw nie zależy od wyboru reprezentantów. W tym celu weźmy dowolne $a_1, a_2, b_1, b_2 \in P$ takie, że $a_1 + I = a_2 + I$ oraz $b_1 + I = b_2 + I$. Wtedy $i = a_1 - a_2 \in I$ oraz $j = b_1 - b_2 \in I$, więc $a_1 = a_2 + i$, $b_1 = b_2 + j$, skąd $a_1 b_1 - a_2 b_2 = (a_2 + i)(b_2 + j) - a_2 b_2 = a_2 j + i b_2 + i j \in I$, gdyż $I \triangleleft P$. Zatem $a_1 b_1 + I = a_2 b_2 + I$ i mnożenie warstw jest dobrze określone.

Dla $a, b \in P$ mamy, że $(b + I) \cdot (a + I) = ba + I = ab + I = (a + I) \cdot (b + I)$, więc mnożenie warstw jest przemienne.

Dla $a, b, c \in P$ mamy, że $(a + I) \cdot [(b + I) \cdot (c + I)] = (a + I) \cdot (bc + I) = a(bc) + I = (ab)c + I = (ab + I) \cdot (c + I) = [(a + I) \cdot (b + I)] \cdot (c + I)$, więc mnożenie warstw jest łączne. Ponadto $(a + I) \cdot [(b + I) + (c + I)] = (a + I) \cdot (b + c + I) = a(b + c) + I = (ab + ac) + I = (ab + I) + (ac + I) = (a + I) \cdot (b + I) + (a + I) \cdot (c + I)$, więc mnożenie warstw jest rozdzielne względem dodawania warstw. Ponadto $(a + I) \cdot (1 + I) = a \cdot 1 + I = a + I$ dla $a \in P$, więc ostatecznie system algebraiczny $(P/I, +, \cdot, I, 1 + I)$ jest pierścieniem. Nazywamy go *pierścieniem ilorazowym względem ideału I* .

10.3 Ideały: pierwsze i maksymalne

Definicja 2. Właściwy ideał I pierścienia P nazywamy
(i) *ideałem pierwszym* pierścienia P , jeżeli

$$\forall_{a,b \in P} [ab \in I \Rightarrow (a \in I \text{ lub } b \in I)];$$

(ii) *ideałem maksymalnym* pierścienia P , jeżeli

$$\forall_{J \triangleleft P} [I \subseteq J \Rightarrow (I = J \text{ lub } J = P)].$$

Twierdzenie 5. *Niech I będzie ideałem pierścienia P . Wówczas równoważne są warunki:*

- (i) *I jest ideałem pierwszym pierścienia P ;*
- (ii) *pierścień ilorazowy P/I jest dziedziną całkowitości.*

Dowód. (i) $\Rightarrow$ (ii) Z założenia $I \neq P$, więc $1 \notin I$, czyli $1 + I \neq 0 + I$. Zatem pierścień P/I jest niezerowy. Niech $a, b \in P$ będą takie, że $(a + I) \cdot (b + I) = I$. Wtedy $ab + I = 0 + I$, więc $ab \in I$. Zatem z pierwszości I wynika, że $a \in I$ lub $b \in I$, czyli $a + I = 0 + I = I$ lub $b + I = 0 + I = I$. Zatem P/I jest dziedziną całkowitości.

(ii) $\Rightarrow$ (i) Z założenia $1 + I \neq 0 + I$, skąd $1 \notin I$, więc $I \neq P$. Weźmy dowolne $a, b \in P$ takie, że $ab \in I$. Wtedy $ab + I = 0 + I$, skąd $(a + I) \cdot (b + I) = I$. Ale P/I jest dziedziną całkowitości, więc $a + I = I = 0 + I$ lub $b + I = I = 0 + I$, czyli $a \in I$ lub $b \in I$. Zatem I jest ideałem pierwszym pierścienia P . $\square$

Twierdzenie 6. *Niech I będzie ideałem pierścienia P . Wówczas równoważne są warunki:*

- (i) *I jest ideałem maksymalnym pierścienia P ,*
- (ii) *pierścień ilorazowy P/I jest ciałem.*

Dowód. (i) $\Rightarrow$ (ii) Z założenia $I \neq P$, więc $1 \notin I$, skąd $1 + I \neq 0 + I = I$. Weźmy dowolne $a \in P$ takie, że $a + I \neq 0 + I$. Wtedy $a \notin I$. Zatem $I \subset I + (a)$, więc z maksymalności I wynika, że $I + (a) = P$. Stąd $1 = i + xa$ dla pewnych $i \in I$ oraz $x \in P$. Zatem $1 - xa = i \in I$, więc $1 + I = xa + I = (x + I) \cdot (a + I)$, czyli $a + I$ jest elementem odwracalnym pierścienia P/I . Zatem P/I jest ciałem.

(ii) $\Rightarrow$ (i) Z założenia $1 + I \neq 0 + I$, skąd $1 \notin I$, więc $I \neq P$. Niech $J \triangleleft P$ oraz $I \subset J$. Wystarczy wykazać, że $J = P$. Ale istnieje $a \in J \setminus I$, więc $a + I \neq 0 + I$. Zatem istnieje $x \in P$ taki, że $(a + I) \cdot (x + I) = 1 + I$, czyli $ax + I = 1 + I$. Zatem $i = ax - 1 \in I$. Stąd $1 = ax - i \in J$, bo $ax \in J$, $i \in I \subset J$. Zatem $1 \in J$, skąd $J = P$. $\square$

Ponieważ każde ciało jest dziedziną całkowitości, więc z twierdzeń 5 i 6 mamy od razu następujący

Wniosek 1. *Każdy ideał maksymalny pierścienia P jest ideałem pierwszym pierścienia P . $\square$*

Uwaga 4. Implikacja odwrotna nie jest prawdziwa, bo np. $\{0\}$ jest ideałem pierwszym pierścienia $\mathbb{Z}$, ale $\{0\} \subset (2) \subset \mathbb{Z}$, więc $\{0\}$ nie jest ideałem maksymalnym pierścienia $\mathbb{Z}$.

Można wykazać, że w pierścieniu $P = \mathbb{Z}[x]$ ideał (x) jest pierwszy, ale $(x) \subset (x, 2) \subset P$, więc ideał (x) nie jest maksymalny w pierścieniu P .

10.4 Homomorfizmy pierścieni

Definicja 3. Niech A, B będą pierścieniami. Przekształcenie $f : A \longrightarrow B$ spełniające warunki:

- (I) $f(1) = 1$,
- (II) $\forall_{a,b \in A} f(a+b) = f(a) + f(b)$,
- (III) $\forall_{a,b \in A} f(ab) = f(a)f(b)$

nazywamy *homomorfizmem* pierścienia A w pierścień B . Natomiast zbiór $\text{Ker}(f) = \{x \in A : f(x) = 0\}$ nazywamy *jądrem homomorfizmu* f .

Przy powyższych oznaczeniach mamy następujące własności homomorfizmu f :

1. $\text{Ker}(f) \triangleleft A$.

Dowód. Ponieważ f jest homomorfizmem grupy A^+ w grupę B^+ , więc z teorii grup wynika, że $\text{Ker}(f)$ jest podgrupą grupy A^+ . Ponadto dla $i \in \text{Ker}(f)$, $a \in A$ jest $f(i) = 0$, więc $f(ai) = f(a)f(i) = f(a) \cdot 0 = 0$, skąd $ai \in \text{Ker}(f)$ i $\text{Ker}(f) \triangleleft A$. $\square$

2. Jeżeli P jest podpierścieniem pierścienia A , to $f(P)$ jest podpierścieniem pierścienia B .

Dowód. Ponieważ P jest podgrupą grupy A^+ i f jest homomorfizmem grup addytywnych, więc z teorii grup $f(P)$ jest podgrupą grupy B^+ . Ale $1 = f(1) \in f(P)$ oraz dla $x, y \in f(P)$ istnieją $a, b \in P$ takie, że $x = f(a)$, $y = f(b)$, więc $xy = f(a)f(b) = f(ab) \in f(P)$, bo $ab \in P$. Zatem $f(P)$ jest podpierścieniem pierścienia B . $\square$

3. Jeżeli S jest podpierścieniem pierścienia B , to $f^{-1}(S)$ jest podpierścieniem pierścienia A .

Dowód. Ponieważ S jest podgrupą grupy B^+ i f jest homomorfizmem grup addytywnych, więc z teorii grup mamy, że $f^{-1}(S)$ jest podgrupą grupy A^+ . Dalej, $f(1) = 1 \in S$, więc $1 \in f^{-1}(S)$. Ponadto dla $a, b \in f^{-1}(S)$ mamy, że $f(a), f(b) \in S$, skąd $f(ab) = f(a)f(b) \in S$, czyli $ab \in f^{-1}(S)$. Zatem $f^{-1}(S)$ jest podpierścieniem pierścienia A . $\square$

4. *Homomorfizm f jest różnowartościowy $\Leftrightarrow \text{Ker}(f) = \{0\}$.*

Dowód. Ponieważ f jest homomorfizmem grup addytywnych, więc teza wynika z teorii grup. $\square$

5. $f(a_1 a_2 \dots a_n) = f(a_1) f(a_2) \dots f(a_n)$ dla dowolnych $a_1, a_2, \dots, \dots, a_n \in A$.

Dowód. Prosta indukcja względem n . $\square$

Definicja 4. Powiemy, że homomorfizm f pierścienia A w pierścień B jest *izomorfizmem pierścieni*, jeżeli f jest bijekcją. Powiemy, że pierścień A jest izomorficzny z pierścieniem B i piszemy $A \cong B$, jeżeli istnieje izomorfizm pierścieni $f : A \rightarrow B$.

W algebrze utożsamia się pierścienie izomorficzne. Można łatwo pokazać, że jeżeli pierścienie A i B są izomorficzne, to np.

$$|A| = |B|;$$

A jest ciałem $\Leftrightarrow B$ jest ciałem;

A jest dziedziną całkowitości $\Leftrightarrow B$ jest dziedziną całkowitości.

Twierdzenie 7 (o izomorfizmie). *Jeżeli $f : A \rightarrow B$ jest homomorfizmem pierścienia A na pierścień B , to*

$$B \cong A/\text{Ker}(f).$$

Dowód. Niech $F : A/\text{Ker}(f) \rightarrow B$ będzie dane wzorem $F(a + \text{Ker}(f)) = f(a)$ dla $a \in A$. Wtedy z teorii grup wiadomo, że F jest bijekcją i dla $a, b \in A$: $F((a + \text{Ker}(f)) + (b + \text{Ker}(f))) = F(a + \text{Ker}(f)) + F(b + \text{Ker}(f))$. Ponadto $F(1 + \text{Ker}(f)) = f(1) = 1$ oraz dla $a, b \in A$: $F((a + \text{Ker}(f)) \cdot (b + \text{Ker}(f))) = F(ab + \text{Ker}(f)) = f(ab) = f(a)f(b) = F(a + \text{Ker}(f))F(b + \text{Ker}(f))$, więc ostatecznie F jest izomorfizmem pierścieni. $\square$

Wniosek 2. *Jeżeli $f : A \rightarrow B$ jest homomorfizmem pierścienia A w pierścień B , to*

$$f(A) \cong A/\text{Ker}(f).$$

Wniosek 3. Niech $f : A \longrightarrow B$ będzie homomorfizmem pierścienia A na pierścień B . Wówczas:

(i) $\text{Ker}(f)$ jest ideałem pierwszym pierścienia $A \Leftrightarrow B$ jest dziedziną całkowitości;

(ii) $\text{Ker}(f)$ jest ideałem maksymalnym pierścienia $A \Leftrightarrow B$ jest ciałem.

Dowód. Z twierdzenia o izomorfizmie mamy, że $B \cong A/\text{Ker}(f)$. Zatem z twierdzeń 5 i 6:

(i) B jest dziedziną całkowitości $\Leftrightarrow A/\text{Ker}(f)$ jest dziedziną całkowitości $\Leftrightarrow \text{Ker}(f)$ jest ideałem pierwszym pierścienia A ;

(ii) B jest ciałem $\Leftrightarrow A/\text{Ker}(f)$ jest ciałem $\Leftrightarrow \text{Ker}(f)$ jest ideałem maksymalnym pierścienia A . $\square$

Przykład 3. Niech $f : \mathbb{Z}[x] \longrightarrow \mathbb{Z}$ będzie takie, że $f(w) = w(0)$ dla $w \in \mathbb{Z}[x]$. Łatwo sprawdzić, że wówczas f jest homomorfizmem pierścienia $\mathbb{Z}[x]$ na pierścień $\mathbb{Z}$. Ponieważ $\mathbb{Z}$ jest dziedziną całkowitości, ale nie jest ciałem, więc z wniosku 3 mamy, że $\text{Ker}(f)$ jest ideałem pierwszym, ale nie jest ideałem maksymalnym pierścienia $\mathbb{Z}[x]$. Z twierdzenia Bezout wynika ponadto, że $\text{Ker}(f) = (x)$.

Przykład 4. Niech $m > 1$ będzie liczbą naturalną i niech $f : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ będzie funkcją daną wzorem:

$$f(k) = [k]_m \text{ dla } k \in \mathbb{Z}.$$

Wtedy dla $a \in \{0, 1, \dots, m-1\}$ mamy, że $f(a) = a$, więc f jest „na” oraz $f(1) = 1$. Ponadto dla $k, l \in \mathbb{Z}$ mamy

$$f(k+l) = [k+l]_m \equiv k+l \equiv [k]_m + [l]_m \equiv [k]_m \oplus_m [l]_m \pmod{m},$$

skąd $f(k+l) = f(k) \oplus_m f(l)$ i podobnie $f(kl) = f(k) \odot_m f(l)$. Zatem f jest homomorfizmem pierścienia $\mathbb{Z}$ na pierścień $\mathbb{Z}_m$. Ponadto

$$\text{Ker}(f) = \{k \in \mathbb{Z} : [k]_m = 0\} = \{k \in \mathbb{Z} : m \mid k\} = (m).$$

Zatem z twierdzenia o izomorfizmie mamy

$$\mathbb{Z}_m \cong \mathbb{Z}/(m).$$

Ponadto pierścień $\mathbb{Z}_m$ jest ciałem wtedy i tylko wtedy, gdy m jest liczbą pierwszą. Zatem z wniosku 3 wynika, że (m) jest ideałem maksymalnym pierścienia $\mathbb{Z}$ wtedy i tylko wtedy, gdy m jest liczbą pierwszą.

Rozdział 11

Pierścień wielomianów

11.1 Konstrukcja pierścienia wielomianów

Niech P będzie dowolnym niezerowym pierścieniem. Oznaczmy przez $P[x]$ zbiór wszystkich nieskończonych ciągów

$$f = (f_0, f_1, f_2, \dots) \quad (11.1)$$

takich, że $f_i \in P$ dla $i = 0, 1, \dots$ oraz istnieje k takie, że $0 = f_k = f_{k+1} = f_{k+2} = \dots$

Elementy zbioru $P[x]$ nazywamy *wielomianami* zmiennej x o współczynnikach z pierścienia P . Przyjmujemy umowę, że jeśli wielomian nazywa się g , to $g = (g_0, g_1, \dots)$, czyli $g_0, g_1, \dots$ są jego kolejnymi współczynnikami. Przy tych oznaczeniach dla wielomianów $f, g \in P[x]$ mamy

$$f = g \Leftrightarrow f_i = g_i \text{ dla każdego } i = 0, 1, 2, \dots \quad (11.2)$$

Wielomian $0 = (0, 0, \dots)$ nazywamy *zerowym*, zaś $1 = (1, 0, 0, \dots)$ nazywamy *jedynkowym*. Jeżeli $0 = f_1 = f_2 = \dots$ to wielomian f nazywamy *stałym*. *Wyrazem wolnym* wielomianu f postaci (11.1) jest współczynnik f_0 . Jeżeli $f \neq 0$, to istnieje największe n takie, że $f_n \neq 0$ i wówczas n nazywamy *stopniem wielomianu* f i piszemy $st(f) = n$, zaś f_n nazywamy *najstarszym współczynnikiem* tego wielomianu. Ponadto przyjmujemy, że $st(0) = -\infty$ oraz $-\infty < n$ dla $n = 0, 1, \dots$ i $(-\infty) + n = (-\infty) + (-\infty) = -\infty$ dla $n = 0, 1, \dots$

Jeżeli $f, g \in P[x]$, to istnieją $k, l \in \mathbb{N}_0$ takie, że $f_j = 0$ dla wszystkich $j > k$ oraz $g_j = 0$ dla wszystkich $j > l$. Zatem dla wszystkich $j > \max\{k, l\}$ jest $f_j + g_j = 0$, skąd wynika, że $(f_0 + g_0, f_1 + g_1, \dots) \in P[x]$. Możemy więc zdefiniować w naturalny sposób *sumę wielomianów* $f, g \in P[x]$ jako wielomian $f + g = (f_0 + g_0, f_1 + g_1, \dots)$. Wówczas z naszych rozważań mamy, że dla dowolnych wielomianów $f, g \in P[x]$:

$$st(f + g) \leq \max\{st(f), st(g)\}. \quad (11.3)$$

Jeżeli zaś $st(f) < st(g)$, to oczywiście $st(f + g) = st(g)$.

Z określenia dodawania wielomianów łatwo wynika, że system algebraiczny $(P[x], +, 0)$ jest grupą abelową, przy czym *wielomianem przeciwnym* do wielomianu f jest wielomian $-f = (-f_0, -f_1, \dots)$.

Iloczynem wielomianów $f, g \in P[x]$ nazywamy ciąg

$$f \cdot g = (f_0g_0, f_0g_1 + f_1g_0, f_0g_2 + f_1g_1 + f_2g_0, \dots). \quad (11.4)$$

Zatem dla każdego $n = 0, 1, \dots$

$$(f \cdot g)_n = \sum_{i=0}^n f_i g_{n-i} = \sum_{i+j=n} f_i g_j. \quad (11.5)$$

Zauważmy, że $f \cdot g \in P[x]$. Rzeczywiście, istnieją $k, l \in \mathbb{N}_0$ takie, że $f_i = 0$ dla wszystkich $i > k$ oraz $g_j = 0$ dla wszystkich $j > l$. Weźmy dowolne $n > k + l$ oraz $i, j \in \mathbb{N}_0$ takie, że $i + j = n$. Jeśli $i > k$, to $f_i = 0$, więc $f_i g_j = 0$; jeśli zaś $i \leq k$, to $j = n - i \geq n - k > k + l - k = l$, więc $g_j = 0$, czyli $f_i g_j = 0$. Stąd dla $n > k + l$ jest $(f \cdot g)_n = \sum_{i+j=n} f_i g_j = 0$

i $f \cdot g \in P[x]$.

Jeżeli $f_i = 0$ dla $i = 1, 2, \dots$ to ze wzoru (11.5) mamy

$$(f_0, 0, 0, \dots) \cdot (g_0, g_1, \dots) = (f_0g_0, f_0g_1, f_0g_2, \dots). \quad (11.6)$$

Jeżeli zaś $f_1 = 1$ oraz $f_i = 0$ dla $i = 0, 2, 3, \dots$ to ze wzoru (11.5) wynika, że

$$(0, 1, 0, 0, \dots) \cdot (g_0, g_1, \dots) = (0, g_0, g_1, \dots). \quad (11.7)$$

Niech teraz $f, g \in P[x] \setminus \{0\}$ i $n = st(f)$, $m = st(g)$. Wtedy z wcześniejszych wyliczeń mamy, że $(f \cdot g)_k = 0$ dla wszystkich $k > n + m$. Stąd i z (11.6) mamy

$$\forall_{f, g \in P[x]} st(f \cdot g) \leq st(f) + st(g). \quad (11.8)$$

Stwierdzenie 1. *Niech $f, g \in P[x] \setminus \{0\}$ będą takie, że najstarszy współczynnik wielomianu f lub najstarszy współczynnik wielomianu g jest elementem regularnym pierścienia P . Wtedy $st(f \cdot g) = st(f) + st(g)$ oraz najstarszy współczynnik wielomianu $f \cdot g$ jest iloczynem najstarszych współczynników wielomianów f i g .*

Dowód. Oznaczmy $n = st(f)$, $m = st(g)$. Weźmy dowolne $i, j \in \mathbb{N}_0$ takie, że $i + j = n + m$. Jeśli $i < n$, to $j = n + m - i > m$, skąd $g_j = 0$ oraz $f_i g_j = 0$. Jeśli $i > n$, to $f_i = 0$, więc $f_i g_j = 0$. Zatem ze wzoru (11.5) mamy, że $(f \cdot g)_{n+m} = f_n g_m \neq 0$, bo $f_n \neq 0$, $g_m \neq 0$ oraz f_n lub g_m jest elementem regularnym. Stąd ze wzoru (11.8) wynika teza naszego stwierdzenia. $\square$

Wniosek 1. *Jeżeli P jest dziedziną całkowitości, to dla dowolnych $f, g \in P[x]$*

$$st(f \cdot g) = st(f) + st(g). \quad \square$$

Ze wzorów (11.4) i (11.5) wynika od razu, że mnożenie wielomianów jest przemienne. Natomiast ze wzoru (11.6) wynika od razu, że $1 = (1, 0, 0, \dots)$ jest elementem neutralnym mnożenia wielomianów.

Teraz udowodnimy, że mnożenie wielomianów jest rozdzielne względem ich dodawania oraz mnożenie wielomianów jest łączne. W tym celu weźmy dowolne $f, g, h \in P[x]$. Wtedy dla $n \in \mathbb{N}_0$ mamy

$$\begin{aligned} (f \cdot (g + h))_n &= \sum_{i+j=n} f_i(g + h)_j = \sum_{i+j=n} f_i(g_j + h_j) = \\ &= \sum_{i+j=n} (f_i g_j + f_i h_j) = \sum_{i+j=n} f_i g_j + \sum_{i+j=n} f_i h_j = (f \cdot g)_n + (f \cdot h)_n, \end{aligned}$$

skąd $f \cdot (g + h) = f \cdot g + f \cdot h$.

$$\begin{aligned} \text{Ponadto } ((f \cdot g) \cdot h)_n &= \sum_{i+j=n} (f \cdot g)_i h_j = \sum_{i+j=n} \sum_{s+t=i} (f_s g_t) h_j = \\ &= \sum_{s+t+j=n} (f_s g_t) h_j = \sum_{s+t+j=n} f_s (g_t h_j) \text{ oraz } (f \cdot (g \cdot h))_n = \sum_{s+k=n} f_s (g \cdot h)_k = \\ &= \sum_{s+k=n} \sum_{t+j=k} f_s (g_t h_j) = \sum_{s+t+j=n} f_s (g_t h_j), \text{ więc } f \cdot (g \cdot h) = (f \cdot g) \cdot h. \end{aligned}$$

W ten sposób udowodniliśmy następujące

Twierdzenie 1. *System algebraiczny $(P[x], +, \cdot, 0, 1)$ tworzy pierścień.*

Ten pierścień nazywamy *pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia P* .

Ze wzorów (11.3) i (11.6) wynika od razu, że przekształcenie $\phi : P \rightarrow P[x]$ dane wzorem

$$\phi(a) = (a, 0, 0, \dots) \quad (11.9)$$

jest różnowartościowym homomorfizmem pierścieni. Z tego powodu można dokonać utożsamienia

$$(a, 0, 0, \dots) \equiv a \text{ dla } a \in P. \quad (11.10)$$

Przy takim utożsamieniu P jest podpierścieniem pierścienia $P[x]$.

Wprowadźmy teraz oznaczenie:

$$x = (0, 1, 0, 0, \dots). \quad (11.11)$$

Wówczas ze wzoru (11.7) przez prostą indukcję uzyskamy, że

$$x^n = (0, 0, \dots, 0, \overset{n}{1}, 0, \dots) \text{ dla } n = 0, 1, \dots \quad (11.12)$$

Niech $f \in P[x]$ będzie wielomianem stopnia $n \geq 1$. Wtedy $f_n \neq 0$ oraz $f_i = 0$ dla każdego $i \geq n + 1$. Ponadto ze wzorów (11.6) i (11.12) mamy, że $(f_k, 0, 0, \dots) \cdot x^k = (0, \dots, 0, \overset{k}{f_k}, 0, \dots)$ dla $k = 1, 2, \dots$ więc $f = (f_0, 0, 0, \dots) + (0, f_1, 0, \dots) + \dots + (0, 0, \dots, f_n, 0, \dots) \equiv f_0 + f_1 x +$

$+f_2x^2+\dots+f_nx^n$. Ponieważ dla wielomianu stałego f jest $f \equiv f_0$, więc dla dowolnego wielomianu $f \in P[x]$ stopnia $n \geq 0$ mamy utożsamienie:

$$f \equiv f_0 + f_1x + f_2x^2 + \dots + f_nx^n. \quad (11.13)$$

Otrzymujemy w ten sposób naturalną notację dla wielomianów z pierścienia $P[x]$. Przy tej notacji możemy powiedzieć, że wielomiany $f, g \in P[x]$ są równe wtedy i tylko wtedy, gdy $st(f) = st(g)$ oraz $f_i = g_i$ dla każdego i .

Z wniosku 1 i tego, że pierścień P jest podpierścieniem pierścienia $P[x]$ wynika od razu następujące

Twierdzenie 2. *Jeżeli pierścień P jest dziedziną całkowitości, to $P[x]$ też jest dziedziną całkowitości.*

Ponieważ podpierścień dziedziny całkowitości jest dziedziną całkowitości, więc zachodzi następujące

Twierdzenie 3. *Jeżeli pierścień $P[x]$ jest dziedziną całkowitości, to P też jest dziedziną całkowitości.*

Twierdzenie 4. *Jeżeli P jest dziedziną całkowitości, to $(P[x])^* = P^*$.*

Dowód. Niech $f \in (P[x])^*$. Wtedy istnieje $g \in P[x]$ takie, że $f \cdot g = 1$, skąd z wniosku 1 mamy, że $st(f) + st(g) = 0$, więc $st(f) = -st(g) = 0$. Zatem $f, g \in P$ i $f \cdot g = 1$, czyli $f \in P^*$. Jeżeli zaś $f \in P^*$, to istnieje $g \in P$ takie, że $f \cdot g = 1$, skąd $f \in (P[x])^*$. $\square$

Wniosek 2. *Pierścień $P[x]$ nigdy nie jest ciałem.*

Dowód. Załóżmy, że dla pewnego pierścienia P pierścień $P[x]$ jest ciałem. Wtedy P jako podpierścień $P[x]$ jest dziedziną całkowitości, więc na mocy twierdzenia 4, $(P[x])^* \subseteq P$. Ale $P[x]$ jest ciałem, więc stąd $x \in P$ i mamy sprzeczność. $\square$

Przykład 1. Załóżmy, że w pierścieniu P istnieje niezerowy element a taki, że $a^2 = 0$. Wtedy w pierścieniu $P[x]$ dla każdego $n = 1, 2, \dots$ mamy, że $(1 + ax^n) \cdot (1 - ax^n) = 1 - a^2x^{2n} = 1 - 0 \cdot x^{2n} = 1$. Zatem w pierścieniu $P[x]$ istnieją wielomiany odwracalne dowolnego

stopnia $n \geq 1$. Oznacza to, że dla takich pierścieni P twierdzenie 4 nie jest prawdziwe. Przykładem takiego pierścienia P jest $\mathbb{Z}_4$.

Definicja 1. *Wartością wielomianu $f = f_0 + f_1x + \dots + f_nx^n \in P[x]$ w punkcie $a \in P$ nazywamy $f(a) = f_0 + f_1a + \dots + f_na^n$.*

Definicja 2. *Pierwiastkiem wielomianu $f \in P[x]$ nazywamy takie $a \in P$, że $f(a) = 0$.*

Definicja 3. *Wielomiany $f, g \in P[x]$ nazywamy równymi funkcyjnie, jeżeli*

$$f(a) = g(a) \text{ dla każdego } a \in P.$$

Przykład 2. Niech P będzie niezerowym pierścieniem skończonym o n elementach oraz $P = \{a_1, \dots, a_n\}$. Ponieważ $0 \neq 1$ w P , więc 1 jest elementem regularnym w P i na mocy stwierdzenia 1 mamy, że wielomian $f = (x - a_1) \cdot (x - a_2) \cdot \dots \cdot (x - a_n) \in P[x]$ ma stopień n . Ponadto $f(a) = 0$ dla każdego $a \in P$, więc wielomiany f i 0 są równe funkcyjnie, chociaż $f \neq 0$. Z tego powodu wielomiany nad dowolnym pierścieniem P nie mogą być traktowane jako funkcje wielomianowe z pierścienia P w pierścień P .

11.2 Homomorfizmy na pierścieniach wielomianów

Twierdzenie 5. *Niech $f : P \rightarrow A$ będzie homomorfizmem pierścienia P w pierścień A i niech $a \in A$. Wtedy przekształcenie $F : P[x] \rightarrow A$ dane wzorem*

$$F((w_0, w_1, \dots)) = f(w_0) + f(w_1)a + f(w_2)a^2 + \dots \quad (11.14)$$

jest homomorfizmem pierścienia $P[x]$ w pierścień A oraz $(\text{Ker}(f)) \subseteq \subseteq \text{Ker}(F)$. Jeżeli dodatkowo f jest „na”, to F też jest „na”.

Dowód. Ponieważ istnieje n takie, że $w_i = 0$ dla wszystkich $i > n$, więc $f(w_i) = 0$ dla $i > n$ i wzór (11.14) ma sens. Ze wzoru (11.14)

mamy, że $F(1) = F((1, 0, 0, \dots)) = f(1) + f(0)a + f(0)a^2 + \dots = f(1) = 1$ oraz $F(w + u) = F(w) + F(u)$ dla dowolnych $w, u \in P[x]$. Ponadto dla $w, u \in P[x]$ mamy, że $(w \cdot u)_n = \sum_{i+j=n} w_i u_j$ dla $n = 0, 1, \dots$ oraz istnieje m takie, że dla wszystkich $k > m$ jest $(w \cdot u)_k = 0$, skąd $f((w \cdot u)_k) = 0$ dla $k > m$. Ponadto

$$\begin{aligned} F(w \cdot u) &= f(w_0 u_0) + f(w_0 u_1 + w_1 u_0)a + \dots + f\left(\sum_{i+j=n} w_i u_j\right)a^n + \dots = \\ &= f(w_0)f(u_0) + [f(w_0)f(u_1) + f(w_1)f(u_0)]a + \dots + \sum_{i+j=n} f(w_i)f(u_j)a^n + \dots \end{aligned}$$

oraz

$$\begin{aligned} F(w) \cdot F(u) &= [f(w_0) + f(w_1)a + \dots] \cdot [f(u_0) + f(u_1)a + \dots] = \\ &= f(w_0)f(u_0) + [f(w_0)f(u_1) + f(w_1)f(u_0)]a + \dots + \\ &+ [f(w_0)f(u_n) + f(w_1)f(u_{n-1}) + \dots + f(w_n)f(u_0)]a^n + \dots \end{aligned}$$

więc $F(w \cdot u) = F(w) \cdot F(u)$ dla dowolnych $w, u \in P[x]$. Zatem F jest homomorfizmem pierścienia. Jeżeli $b \in \text{Ker}(f)$, to $f(b) = 0$, więc dla $w \in P[x]$ jest $F(b \cdot w) = F(b) \cdot F(w) = f(b) \cdot F(w) = 0 \cdot F(w) = 0$, skąd $b \cdot w \in \text{Ker}(F)$. Zatem $(\text{Ker}(f)) \subseteq \text{Ker}(F)$. Jeżeli f jest „na” i $y \in A$, to istnieje $b \in P$ takie, że $f(b) = y$, skąd $F(b) = F((b, 0, 0, \dots)) = f(b) + 0 \cdot a + \dots = y$, więc F jest „na”. $\square$

Twierdzenie 6. Niech a będzie ustalonym elementem pierścienia P . Wtedy przekształcenie $F: P[x] \rightarrow P$ dane wzorem $F(w) = w(a)$ dla $w \in P[x]$ jest homomorfizmem pierścienia $P[x]$ na pierścień P o jądrze $(x - a)$. W szczególności

$$P[x]/(x - a) \cong P.$$

Dowód. Przekształcenie $f: P \rightarrow P$ dane wzorem $f(p) = p$ dla $p \in P$ jest homomorfizmem pierścienia P „na” pierścień P . Zatem na mocy twierdzenia 5 mamy, że F jest homomorfizmem pierścienia $P[x]$ „na” pierścień P . Zatem z twierdzenia o izomorfizmie $P[x]/\text{Ker}(F) \cong P$. Ponadto $F(x - a) = a - a = 0$, więc $x - a \in \text{Ker}(F)$, skąd $(x - a) \subseteq \text{Ker}(F)$. Niech teraz $w \in \text{Ker}(F)$. Wtedy $w = a_0 + a_1 x + \dots + a_n x^n$ dla pewnych $a_0, a_1, \dots, a_n \in P$ oraz $a_0 + a_1 a + \dots + a_n a^n = 0$. Stąd

$$\begin{aligned} w &= (a_0 + a_1x + \dots + a_nx^n) - (a_0 + a_1a + \dots + a_na^n) = \\ &= a_1(x - a) + a_2(x^2 - a^2) + \dots + a_n(x^n - a^n). \end{aligned}$$

Ale $x^k - a^k = (x - a)(x^{k-1} + x^{k-2}a + \dots + xa^{k-2} + a^{k-1})$ dla $k = 1, \dots, n$, skąd wynika, że $w \in (x - a)$. Zatem $\text{Ker}(F) = (x - a)$ oraz $P[x]/(x - a) \cong P$. $\square$

Twierdzenie 7. *Niech $f : A \longrightarrow B$ będzie homomorfizmem pierścienia A w pierścień B . Wówczas przekształcenie $F : A[x] \longrightarrow B[x]$ dane wzorem*

$$F(a_0 + a_1x + \dots + a_nx^n) = f(a_0) + f(a_1)x + \dots + f(a_n)x^n \quad (11.15)$$

dla $a_0, \dots, a_n \in A$, $n = 0, 1, \dots$ jest homomorfizmem pierścienia $A[x]$ w pierścień $B[x]$. Ponadto $\text{Ker}(F) = (\text{Ker}(f))$ oraz jeżeli f jest „na”, to F też jest „na”.

Dowód. Ponieważ B jest podpierścieniem pierścienia $B[x]$, więc f jest homomorfizmem pierścienia A w pierścień $B[x]$. Podstawiając $a = x$ w twierdzeniu 5 uzyskamy, że przekształcenie F dane wzorem (11.15) jest homomorfizmem pierścienia $A[x]$ w pierścień $B[x]$ oraz $(\text{Ker}(f)) \subseteq \text{Ker}(F)$. Niech $w \in \text{Ker}(F)$. Wtedy istnieją $a_0, \dots, a_n \in A$ takie, że $w = a_0 + a_1x + \dots + a_nx^n$ oraz $f(a_0) + f(a_1)x + \dots + f(a_n)x^n = 0$ oraz $f(a_i) \in B$ dla $i = 0, 1, \dots, n$, skąd $f(a_i) = 0$, czyli $a_i \in \text{Ker}(f)$ dla $i = 0, \dots, n$. Zatem $w \in (\text{Ker}(f))$. Stąd $\text{Ker}(F) = (\text{Ker}(f))$. Załóżmy, że f jest „na” i weźmy dowolne $b_0, \dots, b_n \in B$. Wtedy istnieją $a_0, \dots, a_n \in A$ takie, że $b_i = f(a_i)$ dla $i = 0, \dots, n$, skąd $b_0 + b_1x + \dots + b_nx^n = F(a_0 + a_1x + \dots + a_nx^n)$, czyli F jest „na”. $\square$

Rozdział 12

Ważne pierścienie

12.1 Dzielenie wielomianów

Definicja 1. Niech P będzie pierścieniem, który może nie być dziedziną całkowitości. Powiemy, że w pierścieniu $P[x]$ jest wykonalne dzielenie z resztą przez wielomian $f \in P[x]$, jeżeli dla każdego wielomianu $g \in P[x]$ istnieje dokładnie jedna para (q, r) wielomianów $q, r \in P[x]$ taka, że $g = q \cdot f + r$ oraz $st(r) < st(f)$.

Uwaga 1. Ponieważ $st(0) = -\infty$, więc dla powyższych f jest $f \neq 0$.

Uwaga 2. Wielomian r nazywamy *resztą*, zaś q nazywamy *niepełnym ilorazem* z dzielenia wielomianu g przez wielomian f .

Twierdzenie 1. Dla dowolnego pierścienia P i dla dowolnego wielomianu $f \in P[x]$ równoważne są warunki:

- (i) w pierścieniu $P[x]$ jest wykonalne dzielenie z resztą przez wielomian f ;
- (ii) najstarszy współczynnik wielomianu f jest elementem odwracalnym w P .

Dowód. Niech $st(f) = n$ i niech a będzie najstarszym współczynnikiem wielomianu f .

- (i) $\Rightarrow$ (ii) Załóżmy, że w pierścieniu $P[x]$ jest wykonalne dzielenie

z resztą przez wielomian f . Jeżeli a jest dzielnikiem zera w pierścieniu P , to istnieje $0 \neq b \in P$ takie, że $b \cdot a = 0$. Wtedy $st(bf) < n$ oraz $bf = b \cdot f + 0 = 0 \cdot f + bf$ i $(b, 0) \neq (0, bf)$ oraz $st(0) < n$, więc mamy sprzeczność. Zatem a jest elementem regularnym w pierścieniu P . Z założenia istnieją wielomiany $q, r \in P[x]$ takie, że $x^n = q \cdot f + r$ oraz $st(r) < n$. Stąd $q \neq 0$ i ze stwierdzenia 1 z rozdziału 11 mamy, że $st(q \cdot f) = st(q) + st(f) = st(q) + n > st(r)$, więc $n = st(q) + n$, czyli $st(q) = 0$. Zatem $q \in P$ i $q \neq 0$ oraz ze stwierdzenia 1 z rozdziału 11 najstarszym współczynnikiem wielomianu $q \cdot f + r$ jest qa , więc $qa = 1$, skąd $a \in P^*$.

(ii) $\Rightarrow$ (i) Załóżmy, że $a \in P^*$. Wtedy istnieje $b \in P$ takie, że $ab = 1$ i a jest elementem regularnym w pierścieniu P . Niech $q_1, q_2, r_1, r_2 \in P[x]$ będą takie, że $st(r_1), st(r_2) < n$ oraz $q_1 \cdot f + r_1 = q_2 \cdot f + r_2$. Wtedy $(q_1 - q_2) \cdot f = r_2 - r_1$. Ale ze stwierdzenia 1 z rozdziału 11 jest $st((q_1 - q_2) \cdot f) = st(q_1 - q_2) + st(f) = st(q_1 - q_2) + n$ oraz $st(r_2 - r_1) < n$, więc stąd $st(q_1 - q_2) = -\infty$, czyli $q_1 - q_2 = 0$. Zatem $r_2 - r_1 = 0$ oraz $r_2 = r_1$ i $q_2 = q_1$, a więc $(q_2, r_2) = (q_1, r_1)$. W ten sposób wykazaliśmy jednoznaczność reszty i niepełnego ilorazu.

Założmy teraz, że pewien wielomian z $P[x]$ nie jest podzielny z resztą przez wielomian f . Wtedy istnieje wielomian $g \in P[x]$ najniższego stopnia m niepodzielny z resztą przez wielomian f . Jeżeli $m < n$, to $g = 0 \cdot f + g$ i mamy sprzeczność. Zatem $m \geq n$. Niech c będzie najstarszym współczynnikiem wielomianu g i niech $h = g - cbx^{m-n}f$. Ponieważ ze stwierdzenia 1 z rozdziału 11 jest $st(cbx^{m-n}f) = m - n + n = m$ i najstarszy współczynnik wielomianu $cbx^{m-n}f$ jest równy $cba = c \cdot 1 = c$, więc $st(h) < m$. Z minimalności m wynika, że istnieją wielomiany $q_1, r \in P[x]$ takie, że $h = q_1 \cdot f + r$ i $st(r) < n$, skąd $g = (cbx^{m-n} + q_1) \cdot f + r$. Zatem mamy sprzeczność. $\square$

Uwaga 3. Algorytm dzielenia wielomianów z resztą znany ze szkoły średniej jest dobry dla dowolnego pierścienia wielomianów.

Uwaga 4. Wielomian $f \in P[x]$ o najstarszym współczynniku równym 1 nazywamy *wielomianem unormowanym*. Ponieważ $1 \in P^*$, więc z twierdzenia 1 w pierścieniu $P[x]$ jest wykonalne dzielenie z resztą przez wielomiany unormowane.

Twierdzenie 2. (Bezout). *Dla dowolnego wielomianu $g \in P[x]$ i dla dowolnego $a \in P$ reszta z dzielenia wielomianu g przez dwumian $x - a$ jest równa $g(a)$, tzn. istnieje wielomian $q \in P[x]$ taki, że $g = q \cdot (x - a) + g(a)$.*

Dowód. Z uwagi 4 istnieją $q, r \in P[x]$ takie, że $g = q \cdot (x - a) + r$ i $st(r) < 1 = st(x - a)$. Stąd $r \in P$ i $g(a) = q(a) \cdot (a - a) + r = r$, czyli $r = g(a)$ i $g = q \cdot (x - a) + g(a)$. $\square$

Definicja 2. Niech $f, g \in P[x]$. Powiemy, że wielomian f dzieli wielomian g w pierścieniu $P[x]$ i piszemy $f \mid g$, jeżeli istnieje wielomian $h \in P[x]$ taki, że $g = f \cdot h$.

Wniosek 1. *Dla dowolnego wielomianu $f \in P[x]$ i dla dowolnego $a \in P$ mamy*

$$x - a \mid g \text{ w pierścieniu } P[x] \Leftrightarrow g(a) = 0.$$

Dowód. Jeżeli $x - a \mid g$ w pierścieniu $P[x]$, to istnieje $q \in P[x]$ takie, że $g = q \cdot (x - a)$, skąd $g(a) = q(a) \cdot (a - a) = 0$. Na odwrót, niech $g(a) = 0$. Wtedy z twierdzenia Bezout istnieje $q \in P[x]$ takie, że $g = q \cdot (x - a)$, czyli $x - a \mid g$. $\square$

Stwierdzenie 1. *Niech $a_1, \dots, a_n$ będą parami różnymi elementami dziedziny całkowitości P . Wówczas dla dowolnego wielomianu $f \in P[x]$ równoważne są warunki:*

- (i) $(x - a_1) \cdot \dots \cdot (x - a_n) \mid f$ w pierścieniu $P[x]$;
- (ii) $f(a_1) = \dots = f(a_n) = 0$.

Dowód. (i) $\Rightarrow$ (ii) Z założenia istnieje $h \in P[x]$ taki, że

$$f = h \cdot (x - a_1) \cdot \dots \cdot (x - a_n),$$

skąd $f(a_i) = h(a_i) \cdot (a_i - a_1) \cdot \dots \cdot (a_i - a_i) \cdot \dots \cdot (a_i - a_n) = 0$ dla $i = 1, \dots, n$.

(ii) $\Rightarrow$ (i) Stosujemy indukcję względem n . Dla $n = 1$ teza wynika od razu z wniosku 1. Załóżmy, że teza zachodzi dla pewnego naturalnego n i niech $a_1, \dots, a_{n+1}$ będą parami różnymi elementami pierścienia P takimi, że $f(a_1) = \dots = f(a_{n+1}) = 0$. Wtedy z założenia indukcyjnego istnieje $g \in P[x]$ takie, że $f = g \cdot (x - a_1) \cdot \dots \cdot (x - a_n)$. Ale

$0 = f(a_{n+1}) = g(a_{n+1}) \cdot (a_{n+1} - a_1) \cdot \dots \cdot (a_{n+1} - a_n)$, więc ponieważ P jest dziedziną całkowitości, to $g(a_{n+1}) = 0$ i z wniosku 1 istnieje $h \in P[x]$ taki, że $g = h \cdot (x - a_{n+1})$. Zatem $f = (x - a_1) \cdot \dots \cdot (x - a_n) \cdot (x - a_{n+1})$, czyli $(x - a_1) \cdot \dots \cdot (x - a_{n+1}) \mid f$. $\square$

Ze stwierdzenia 1 i ze stwierdzenia 1 z rozdziału 11 otrzymujemy natychmiast następujący

Wniosek 2. *Niech P będzie dziedziną całkowitości i niech $n \in \mathbb{N}$. Wówczas każdy wielomian $f \in P[x]$ stopnia n posiada co najwyżej n różnych pierwiastków w pierścieniu P .* $\square$

Wniosek 3. *Niech P będzie nieskończoną dziedziną całkowitości. Wówczas wielomiany $f, g \in P[x]$ równe funkcyjnie są równe.*

Dowód. Z założenia $f(a) = g(a)$ dla każdego $a \in P$, więc $(f - g)(a) = 0$ dla każdego $a \in P$. Stąd wielomian $f - g$ ma nieskończenie wiele pierwiastków w pierścieniu P . Zatem z wniosku 2, $f - g = 0$, czyli $f = g$. $\square$

Stwierdzenie 2. *Niech A będzie podciałem ciała K . Wówczas dla dowolnych wielomianów $f, g \in A[x]$ z tego, że $f \mid g$ w pierścieniu $K[x]$ wynika, że $f \mid g$ w pierścieniu $A[x]$.*

Dowód. Z założenia istnieje $h \in K[x]$ takie, że $g = h \cdot f$ i z twierdzenia 1 istnieją $q, r \in A[x]$ takie, że $g = q \cdot f + r$ i $st(r) < st(f)$. Zatem w pierścieniu $K[x]$ jest $h \cdot f + 0 = q \cdot f + r$, więc z twierdzenia 1, $r = 0$ i $h = q$. Stąd $g = q \cdot f$ i $f \mid g$ w pierścieniu $A[x]$. $\square$

Twierdzenie 3. *Niech $f \in P[x]$ będzie wielomianem stopnia $n \geq 1$ o najstarszym współczynniku odwracalnym w pierścieniu P . Wówczas dla ideału $I = (f) = \{f \cdot g : g \in P[x]\}$ pierścienia $P[x]$ mamy*

$$P[x]/I = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} + I : a_0, a_1, \dots, a_{n-1} \in P\} \quad (12.1)$$

oraz dla dowolnych $a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1} \in P$:

$$a_0 + \dots + a_{n-1}x^{n-1} + I = b_0 + \dots + b_{n-1}x^{n-1} + I \Leftrightarrow \forall_{i=0, \dots, n-1} a_i = b_i. \quad (12.2)$$

Dowód. Niech $g \in P[x]$. Wtedy z twierdzenia 1 istnieją $q, r \in P[x]$ takie, że $st(r) < n$ oraz $g = q \cdot f + r$, skąd $g - r = q \cdot f \in I$, więc $g + I = r + I$. Ponadto istnieją $a_0, a_1, \dots, a_{n-1} \in P$ takie, że $r = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$, co dowodzi wzoru (12.1).

We wzorze (12.2) implikacja $\Leftarrow$ jest oczywista. Załóżmy, że $a_0, \dots, a_{n-1}, b_0, \dots, b_{n-1} \in P$ są takie, że $a_0 + \dots + a_{n-1}x^{n-1} + I = b_0 + \dots + b_{n-1}x^{n-1} + I$. Wtedy $(a_0 + \dots + a_{n-1}x^{n-1}) - (b_0 + \dots + b_{n-1}x^{n-1}) \in I$, więc istnieje $g \in P[x]$ takie, że $r = (a_0 - b_0) + \dots + (a_{n-1} - b_{n-1})x^{n-1} = g \cdot f$, skąd $0 = g \cdot f + (-r) = 0 \cdot f + 0$, więc z twierdzenia 1, $-r = 0$, czyli $a_i = b_i$ dla $i = 0, \dots, n-1$. $\square$

Twierdzenie 4. *Jeżeli K jest ciałem, to każdy ideał pierścienia $K[x]$ jest główny.*

Dowód. Niech $I \triangleleft K[x]$. Jeśli $I = \{0\}$, to $I = (0)$. Niech dalej $I \neq \{0\}$. Wtedy w zbiorze $I \setminus \{0\}$ istnieje wielomian f minimalnego stopnia n . Stąd $(f) \subseteq I$, bo $f \in I$. Jeżeli $g \in I$, to z twierdzenia 1 istnieją $q, r \in K[x]$ takie, że $g = q \cdot f + r$ i $st(r) < n$. Ale $r = g - q \cdot f \in I$, więc z minimalności n jest $r = 0$, czyli $g = q \cdot f \in (f)$. Zatem $I \subseteq (f)$ i ostatecznie $I = (f)$. $\square$

12.2 Dziedziny ideałów głównych

Definicja 3. *Dziedziną ideałów głównych (w skrócie: d.i.g.) nazywamy dziedzinę całkowitości, w której każdy ideał jest ideałem głównym.*

Przykład 1. Pierścień liczb całkowitych $\mathbb{Z}$ jest dziedziną ideałów głównych.

Przykład 2. Z twierdzenia 4 wynika, że dla dowolnego ciała K pierścień $K[x]$ jest dziedziną ideałów głównych.

Twierdzenie 5. *W dziedzinie ideałów głównych każdy niezerowy ideał pierwszy jest ideałem maksymalnym.*

Dowód. Niech $I \neq \{0\}$ będzie ideałem pierwszym dziedziny ideałów głównych P . Wówczas $I \neq P$ i istnieje $a \in P$ takie, że $I = (a)$. Ale $I \neq \{0\}$, więc $a \neq 0$. Niech $J \triangleleft P$ i $I \subset J$. Wówczas istnieje $b \in P$

takie, że $J = (b)$. Gdyby $b \in I$, to $J = (b) \subseteq I$, skąd $I = J$ i mamy sprzeczność. Zatem $b \notin I$. Dalej, $a \in (a) = I \subseteq J = (b)$, więc istnieje $t \in P$ takie, że $a = b \cdot t$. Stąd $b \cdot t \in I$ i $b \notin I$, więc z pierwszości ideału I , $t \in I$ i istnieje $x \in P$ takie, że $t = a \cdot x$. Zatem $a = b \cdot a \cdot x$ i $a \neq 0$ oraz P jest dziedziną, więc $1 = b \cdot x \in J$, skąd $J = P$. Zatem I jest ideałem maksymalnym pierścienia P . $\square$

Z przykładu 2 i z twierdzenia 5 mamy natychmiast następujący

Wniosek 4. *Dla dowolnego ciała K każdy niezerowy ideał pierwszy pierścienia $K[x]$ jest ideałem maksymalnym pierścienia $K[x]$.* $\square$

Twierdzenie 6. *Jeżeli $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ są ideałami dziedziny ideałów głównych P , to istnieje n takie, że $I_n = I_{n+1} = I_{n+2} = \dots$*

Dowód. Niech $I = \bigcup_{k=1}^{\infty} I_k$. Wtedy $I_k \subseteq I$ dla $k = 1, 2, \dots$ skąd $I \neq \emptyset$. Weźmy dowolne $x, y \in I$. Wtedy istnieją $k, l \in \mathbb{N}$ takie, że $x \in I_k$, $y \in I_l$, więc dla $m = \max\{k, l\}$ mamy, że $x, y \in I_m$, skąd $x - y \in I_m$, czyli $x - y \in I$. Ponadto dla $a \in P$ jest $ax \in I_k$, więc $ax \in I$. Zatem $I \triangleleft P$ i P jest d.i.g., więc istnieje $c \in P$ takie, że $I = (c)$. Wtedy $c \in I$, więc istnieje naturalne n takie, że $c \in I_n$, skąd $I = (c) \subseteq I_n \subseteq I_k \subseteq I$ dla wszystkich $k \geq n$. Zatem $I_n = I_k$ dla wszystkich $k \geq n$. $\square$

12.3 Arytmetyka dziedzin całkowitości

Od tej pory o wszystkich omawianych pierścieniach będziemy zakładali, że są one dziedzinami całkowitości.

Definicja 4. Niech a, b będą elementami pierścienia P . Powiemy, że a dzieli b w pierścieniu P , jeżeli istnieje $t \in P$ takie, że $b = a \cdot t$. Piszemy wtedy $a \mid b$.

Przykład 3. Niech $k \in \mathbb{Z}$, $f \in \mathbb{Z}[x]$. Łatwo zauważyć, że $k \mid f$ w $\mathbb{Z}[x]$ wtedy i tylko wtedy, gdy k dzieli (w pierścieniu $\mathbb{Z}$) wszystkie współczynniki wielomianu f .

Uwaga 5. Dla dowolnych elementów a, b pierścienia P równoważne są warunki:

(i) $a \mid b$, (ii) $b \in (a)$, (iii) $(b) \subseteq (a)$.

Dowód. (i) $\Rightarrow$ (ii) Istnieje $t \in P$ takie, że $b = at$, skąd $b \in (a)$.

(ii) $\Rightarrow$ (iii) Istnieje $t \in P$ takie, że $b = at$, skąd dla $x \in P$, $bx = atx \in (a)$, czyli $(b) \subseteq (a)$.

(iii) $\Rightarrow$ (i) Ponieważ $b \in (b)$ i $(b) \subseteq (a)$, więc $b \in (a)$ i istnieje $t \in P$ takie, że $b = at$, skąd $a \mid b$. $\square$

Definicja 5. Powiemy, że elementy a, b pierścienia P są *stowarzyszone* w P i piszemy $a \sim b$, jeżeli $a \mid b$ i $b \mid a$ w P .

Uwaga 6. Dla dowolnych elementów a, b pierścienia P równoważne są warunki:

(i) $a \sim b$, (ii) $(a) = (b)$, (iii) $\exists_{u \in P^*} a = bu$, (iv) $\exists_{v \in P^*} b = av$.

Dowód. Z uwagi 5 mamy, że $(a) = (b) \Leftrightarrow [(a) \subseteq (b) \text{ i } (b) \subseteq (a)] \Leftrightarrow (b \mid a \text{ i } a \mid b) \Leftrightarrow a \sim b$. Dalej, dla $u \in P^*$ istnieje $v \in P^*$ takie, że $uv = 1$, skąd wynika natychmiast równoważność warunków (iii) i (iv).

(i) $\Rightarrow$ (iii) Niech $a \sim b$. Wtedy $a \mid b$ i $b \mid a$, więc istnieją $x, y \in P$ takie, że $b = ax$ i $a = by$. Jeśli $b = 0$, to $a = 0 \cdot y = 0$ i wystarczy wziąć $u = 1$. Jeśli zaś $b \neq 0$, to $b = byx$, skąd $1 = yx$, więc $y \in P^*$ i wystarczy wziąć $u = y$.

(iii) $\Rightarrow$ (i) Niech $a = bu$ dla pewnego $u \in P^*$. Wtedy $b \mid a$ i istnieje $v \in P^*$ takie, że $b = av$, skąd $a \mid b$. Zatem $a \sim b$. $\square$

Uwaga 7. Z uwagi 6 otrzymujemy od razu, że relacja $\sim$ jest relacją równoważności w pierścieniu P .

Definicja 6. Element a pierścienia P nazywamy *elementem rozkładalnym* w pierścieniu P , jeżeli istnieją niezerowe elementy nieodwracalne $x, y \in P$ takie, że $a = x \cdot y$.

Przykład 4. Wielomian $f \in K[x]$, gdzie K jest ciałem, jest elementem rozkładalnym w $K[x]$ wtedy i tylko wtedy, gdy f jest iloczynem dwóch wielomianów $g, h \in K[x]$ dodatnich stopni, gdyż $(K[x])^* = K \setminus \{0\}$. Jeżeli $st(f) > 1$ i istnieje $a \in K$ takie, że $f(a) = 0$, to z twierdzenia Bezout istnieje $g \in K[x]$ takie, że $f = g \cdot (x - a)$. Wtedy $st(f) = st(g) + 1$, więc $st(g) > 0$ i f jest elementem rozkładalnym

w $K[x]$. Stąd i z zasadniczego twierdzenia algebry wynika, że w pierścieniu $\mathbb{C}[x]$ każdy wielomian stopnia co najmniej 2 jest elementem rozkładalnym w tym pierścieniu. Wielomian $x^4 + 4 \in \mathbb{Q}[x]$ nie posiada nawet pierwiastka rzeczywistego, ale jest rozkładalny w $\mathbb{Q}[x]$, bo $x^4 + 4 = (x^2 + 2)^2 - (2x)^2 = (x^2 + 2 - 2x) \cdot (x^2 + 2 + 2x)$.

Definicja 7. Niezerowy element nieodwracalny a pierścienia P nazywamy *elementem nierozkładalnym* w P , jeżeli a nie jest elementem rozkładalnym w P , tzn. dla dowolnych $x, y \in P$ z tego, że $a = x \cdot y$ wynika, że $x \in P^*$ lub $y \in P^*$.

Przykład 5. Niech K będzie ciałem i $f \in K[x]$. Jeżeli $st(f) = 1$ oraz $g, h \in K[x]$ są takie, że $f = g \cdot h$, to $1 = st(g) + st(h)$, skąd $st(g) = 0$ lub $st(h) = 0$, czyli $g \in (K[x])^*$ lub $h \in (K[x])^*$. Zatem wielomian f stopnia 1 jest nierozkładalny w $K[x]$.

Przykład 6. Niech K będzie ciałem i $f \in K[x]$ oraz $st(f) = 2$ lub $st(f) = 3$. Pokażemy, że f jest nierozkładalny w $K[x]$ wtedy i tylko wtedy, gdy f nie ma pierwiastka w ciele K . Jeżeli f jest nierozkładalny w $K[x]$, to z przykładu 4, f nie ma pierwiastka w K . Na odwrót, założmy, że f nie ma pierwiastka w K . Weźmy dowolne $g, h \in K[x]$ takie, że $f = g \cdot h$ i $st(g) \leq st(h)$. Wtedy $st(f) = st(g) + st(h) \geq 2st(g)$. Ale $st(f) = 2$ lub $st(f) = 3$, więc stąd $st(g) \leq 1$. Jeśli $st(g) = 1$, to $g = ax + b$ dla pewnych $a, b \in P$, $a \neq 0$, czyli $g(-\frac{b}{a}) = 0$, więc też $f(-\frac{b}{a}) = 0$ i mamy sprzeczność. Zatem $st(g) = 0$, czyli $g \in (K[x])^*$ i f jest elementem nierozkładalnym w $K[x]$.

Lemat 1. Jeżeli a jest niezerowym elementem nieodwracalnym pierścienia P takim, że a nie jest iloczynem skończonej liczby elementów nierozkładalnych, to istnieje $b \in P$, które jest niezerowym elementem nieodwracalnym w P i nie jest iloczynem skończonej liczby elementów nierozkładalnych takie, że $(a) \subset (b)$.

Dowód. Z założenia wynika, że a jest elementem rozkładalnym w P , więc istnieją niezerowe elementy nieodwracalne $x, y \in P$ takie, że $a = xy$. Jeżeli $x = x_1 \cdots x_k$, $y = y_1 \cdots y_l$, gdzie $x_1, \dots, x_k, y_1, \dots, y_l$ są elementami nierozkładalnymi w P , to $a = x_1 \cdots x_k \cdot y_1 \cdots y_l$, wbrew założeniu. Zatem można zakładać, że x nie jest iloczynem skończonej

liczby elementów nierozkładalnych w P . Ponadto $x \mid a$, więc z uwagi 5, $(a) \subseteq (x)$. Jeśli $(a) = (x)$, to z uwagi 6 istnieje $u \in P^*$ takie, że $a = xu$, skąd $xu = xy$, czyli $y = u \in P^*$ i mamy sprzeczność. Zatem $(a) \subset (x)$ i wystarczy wziąć $b = x$. $\square$

Twierdzenie 7. *W dziedzinie ideałów głównych P każdy niezerowy element nieodwracalny jest iloczynem skończonej liczby elementów nierozkładalnych w P .*

Dowód. Gdyby tak nie było, to przez prostą indukcję z lematu 1 znaleźlibyśmy nieskończony ciąg elementów $a_1, a_2, \dots$ pierścienia P taki, że $(a_1) \subset (a_2) \subset (a_3) \subset \dots$ co przeczy twierdzeniu 6. $\square$

Wniosek 5. *Dla dowolnego ciała K każdy wielomian $f \in K[x]$ dodatniego stopnia jest iloczynem skończonej liczby wielomianów nierozkładalnych w $K[x]$.* $\square$

Twierdzenie 8. *Jeżeli $f \in \mathbb{R}[x]$ jest wielomianem nierozkładalnym w pierścieniu $\mathbb{R}[x]$, to $st(f) = 1$ lub $st(f) = 2$.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje $f \in \mathbb{R}[x]$ nierozkładalny w $\mathbb{R}[x]$ taki, że $st(f) \geq 3$. Z zasadniczego twierdzenia algebry wynika, że istnieje $z_0 \in \mathbb{C}$ takie, że $f(z_0) = 0$. Ponadto z przykładu 4 jest, że $z_0 \notin \mathbb{R}$, więc $z_0 \neq \overline{z_0}$. Ale $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ dla pewnych liczb rzeczywistych $a_0, \dots, a_n$, więc

$$\begin{aligned} f(\overline{z_0}) &= a_n (\overline{z_0})^n + a_{n-1} (\overline{z_0})^{n-1} + \dots + a_1 \overline{z_0} + a_0 = \\ &= \overline{a_n z_0^n} + \overline{a_{n-1} z_0^{n-1}} + \dots + \overline{a_1 z_0} + \overline{a_0} = \\ &= \overline{a_n z_0^n + a_{n-1} z_0^{n-1} + \dots + a_1 z_0 + a_0} = \overline{f(z_0)} = \overline{0} = 0. \end{aligned}$$

Niech $h = (x - z_0) \cdot (x - \overline{z_0}) = x^2 - (z_0 + \overline{z_0})x + z_0 \overline{z_0}$. Ponieważ $z_0 + \overline{z_0}, z_0 \overline{z_0} \in \mathbb{R}$, więc $h \in \mathbb{R}[x]$. Ponadto ze stwierdzenia 1 wynika, że $h \mid f$ w pierścieniu $\mathbb{C}[x]$. Ale $h, f \in \mathbb{R}[x]$, więc ze stwierdzenia 2, $h \mid f$ w pierścieniu $\mathbb{R}[x]$. Zatem istnieje $g \in \mathbb{R}[x]$ takie, że $f = h \cdot g$, skąd $st(f) = st(h) + st(g) = 2 + st(g)$. Ale $st(f) \geq 3$, więc $st(g) > 0$, co przeczy temu, że f jest nierozkładalny w $\mathbb{R}[x]$. Zatem $st(f) = 1$ lub $st(f) = 2$. $\square$

Z twierdzenia 8 i z wniosku 5 wynika od razu następujące

Twierdzenie 9. *Każdy wielomian dodatniego stopnia o współczynnikach rzeczywistych jest iloczynem skończonej liczby wielomianów o współczynnikach rzeczywistych stopni ≤ 2 . $\square$*

Z przykładów 4 i 5 oraz z twierdzenia 8 i wniosku 5 mamy od razu następujące

Twierdzenie 10. *Każdy wielomian dodatniego stopnia o współczynnikach zespolonych jest iloczynem skończonej liczby czynników liniowych. $\square$*

Uwaga 8. Na mocy przykładu 6 wielomian $f = ax^2 + bx + c \in \mathbb{R}[x]$ stopnia 2 jest nierozkładalny w pierścieniu $\mathbb{R}[x]$ wtedy i tylko wtedy, gdy f nie ma pierwiastka w $\mathbb{R}$, czyli gdy $\Delta = b^2 - 4ac < 0$.

Rozdział 13

Rozkłady elementów pierścienia na czynniki

13.1 Wielomiany nierozkładalne w pierścieniach $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$

Twierdzenie 1. *Niech p będzie liczbą pierwszą i niech $f, g \in \mathbb{Z}[x]$. Jeżeli w pierścieniu $\mathbb{Z}[x]$ $p \mid f \cdot g$, to $p \mid f$ lub $p \mid g$.*

Dowód. Z założenia istnieje $h \in \mathbb{Z}[x]$ takie, że $f \cdot g = p \cdot h$. Ponadto przekształcenie $T : \mathbb{Z}[x] \rightarrow \mathbb{Z}_p[x]$ dane wzorem

$$\begin{aligned} T(a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0) &= \\ &= [a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \dots + [a_1]_p x + [a_0]_p \end{aligned}$$

jest homomorfizmem pierścieni o jądrze (p) . Stąd $T(f) \cdot T(g) = 0$ w pierścieniu $\mathbb{Z}_p[x]$. Ale $\mathbb{Z}_p$ jest ciałem, gdyż p jest liczbą pierwszą, więc $\mathbb{Z}_p[x]$ jest dziedziną całkowitości, skąd $T(f) = 0$ lub $T(g) = 0$, czyli $f \in (p)$ lub $g \in (p)$. Zatem $p \mid f$ lub $p \mid g$ w pierścieniu $\mathbb{Z}[x]$. $\square$

Definicja 1. Powiemy, że wielomian

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$$

jest *wielomianem pierwotnym*, jeżeli $(a_0, a_1, \dots, a_n) = 1$, tzn. jeżeli nie istnieje liczba pierwsza p taka, że $p \mid f$ w pierścieniu $\mathbb{Z}[x]$.

Z twierdzenia 1 wynika od razu następujący

Lemat Gaussa. *Iloczyn wielomianów pierwotnych jest wielomianem pierwotnym.* $\square$

Twierdzenie 2. *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem pierwotnym. Wówczas równoważne są warunki:*

- (i) *f jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Z}[x]$,*
- (ii) *f jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Q}[x]$.*

Dowód. (ii) $\Rightarrow$ (i) Załóżmy, że f jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Q}[x]$. Wtedy $st(f) = n \geq 1$. Jeżeli $f = g \cdot h$ dla pewnych $g, h \in \mathbb{Z}[x]$, to $g \in \mathbb{Q}^*$ lub $h \in \mathbb{Q}^*$, skąd $g \in \mathbb{Z} \setminus \{0\}$ lub $h \in \mathbb{Z} \setminus \{0\}$. Można zakładać, że $g \in \mathbb{Z} \setminus \{0\}$. Jeśli $g \notin \mathbb{Z}^* = \{1, -1\}$, to $|g| > 1$, więc istnieje liczba pierwsza p taka, że $p|g$ w pierścieniu $\mathbb{Z}$, skąd $p|f$ w pierścieniu $\mathbb{Z}[x]$ i mamy sprzeczność. Zatem $g \in \mathbb{Z}^*$, skąd wynika, że f jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Z}[x]$.

(i) $\Rightarrow$ (ii) Załóżmy teraz, że f jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Q}[x]$. Ponieważ f jest wielomianem pierwotnym, więc stąd $st(f) \geq 1$. Załóżmy, że f nie jest wielomianem nierozkładalnym w pierścieniu $\mathbb{Q}[x]$. Istnieją wtedy wielomiany $g, h \in \mathbb{Q}[x]$ dodatnich stopni takie, że $f = g \cdot h$. Wtedy istnieją liczby naturalne k, l takie, że $kg, lh \in \mathbb{Z}[x]$ oraz $(kl)f = (kg) \cdot (lh)$. Istnieje zatem najmniejsza liczba naturalna s taka, że wielomian sf jest iloczynem dwóch wielomianów $\phi, \psi \in \mathbb{Z}[x]$ dodatnich stopni. Jeżeli $s > 1$, to istnieje liczba naturalna p taka, że $p \mid s$. Wtedy z twierdzenia 1, $p \mid \phi$ lub $p \mid \psi$ w pierścieniu $\mathbb{Z}[x]$. Bez zmniejszania ogólności możemy zakładać, że $p \mid \phi$. Wtedy $\frac{s}{p}f = (\frac{\phi}{p}) \cdot \psi$ i mamy sprzeczność z minimalnością s . Zatem $s = 1$ oraz $f = \phi \cdot \psi$. Ale $st(\phi), st(\psi) \geq 1$ oraz $(\mathbb{Z}[x])^* = \mathbb{Z}^* = \{1, -1\}$, więc mamy sprzeczność z nierozkładalnością wielomianu f w pierścieniu $\mathbb{Z}[x]$. $\square$

Twierdzenie 3. *Jeżeli wielomian unormowany $f \in P[x]$ jest elementem rozkładalnym w pierścieniu $P[x]$, to istnieją wielomiany unormowane $g, h \in P[x]$ dodatnich stopni takie, że $f = g \cdot h$.*

Dowód. Z założenia istnieją wielomiany niezerowe nieodwracalne $g_1, h_1 \in P[x]$ takie, że $f = g_1 \cdot h_1$. Niech a będzie najstarszym współczynnikiem wielomianu g_1 , zaś b niech będzie najstarszym współczyn-

nikiem wielomianu h_1 . Wtedy z założenia $1 = ab$, skąd $a, b \in P^* \subseteq (P[x])^*$. Zatem $st(g_1), st(h_1) \geq 1$ oraz bg_1, ah_1 są wielomianami unormowanymi dodatnich stopni i $(bg_1) \cdot (ah_1) = (ab)g_1 \cdot h_1 = g_1 \cdot h_1 = f$. $\square$

Uwaga 1. Twierdzenie odwrotne do twierdzenia 3 jest także prawdziwe, bo $(P[x])^* = P^*$.

Twierdzenie 4 (kryterium Eisensteina). *Niech $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ będzie wielomianem pierwotnym stopnia $n \geq 1$. Jeżeli istnieje liczba pierwsza p taka, że $p \nmid a_n$, $p \mid a_i$ dla $i = 0, 1, \dots, n-1$ oraz $p^2 \nmid a_0$, to f jest wielomianem nierozkładalnym w pierścieniach $\mathbb{Q}[x]$ i $\mathbb{Z}[x]$.*

Dowód. Dla $n = 1$ teza jest oczywista na mocy pierwotności wielomianu f . Niech dalej $n \geq 2$ i założmy, że f jest rozkładalny w $\mathbb{Q}[x]$. Wtedy z twierdzenia 2 mamy, że f jest rozkładalny w pierścieniu $\mathbb{Z}[x]$. Z pierwotności f wynika, że istnieją wielomiany $g, h \in \mathbb{Z}[x]$ dodatnich stopni takie, że $f = g \cdot h$. Niech $g = b_s x^s + b_{s-1} x^{s-1} + \dots + b_1 x + b_0$, $b_s \neq 0$ oraz $h = c_r x^r + c_{r-1} x^{r-1} + \dots + c_1 x + c_0$, $c_r \neq 0$. Wtedy $s + r = n$ i $c_r b_s = a_n$ oraz $b_0 c_0 = a_0$. Stąd z pierwszości p mamy, że $p \mid b_0$ lub $p \mid c_0$. Bez zmniejszania ogólności rozważań możemy zakładać, że $p \mid b_0$. Ponieważ $p^2 \nmid a_0$, więc stąd $p \nmid c_0$. Ponadto $p \nmid a_n$, więc $p \nmid b_s$ i $p \nmid c_r$. Istnieje zatem największa nieujemna liczba całkowita $k \leq s-1$ taka, że $p \mid b_k$. Ponadto $k+1 \leq s < n$, więc $p \mid a_{k+1} = \sum_{i=0}^{k+1} b_i c_{k+1-i} = \sum_{i=0}^k b_i c_{k+1-i} + b_{k+1} c_0$. Ale $p \mid b_i$ dla $i = 0, 1, \dots, k$, więc $p \mid b_{k+1} c_0$ i $p \nmid c_0$, więc $p \mid b_{k+1}$ i mamy sprzeczność z maksymalnością k . Oznacza to, że wielomian f jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$ i na mocy twierdzenia 2 f jest nierozkładalny w pierścieniu $\mathbb{Z}[x]$. $\square$

Wniosek 1. *W pierścieniu $\mathbb{Q}[x]$ istnieją wielomiany nierozkładalne dowolnego dodatniego stopnia.*

Dowód. Dla naturalnych n wielomian $f_n = x^n + 2$ jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$ na mocy kryterium Eisensteina przy $p = 2$. $\square$

Elementy pierwsze

Definicja 2. Powiemy, że niezerowy element nieodwracalny a pierścienia P jest *elementem pierwszym* w P , jeżeli dla dowolnych $x, y \in P$ z tego, że $a \mid xy$ wynika, że $a \mid x$ lub $a \mid y$.

Twierdzenie 5. *Każdy element pierwszy pierścienia P jest elementem nierozkładalnym w P .*

Dowód. Niech p będzie elementem pierwszym pierścienia P . Wtedy $p \neq 0$ i $p \notin P^*$. Weźmy dowolne $x, y \in P$ takie, że $p = xy$. Wtedy $p \mid xy$, więc $p \mid x$ lub $p \mid y$. Zatem $x = pt$ lub $y = pt$ dla pewnego $t \in P$. Stąd $p = pty$ lub $p = xpt$, więc $1 = ty$ lub $1 = xt$, czyli $y \in P^*$ lub $x \in P^*$. Zatem p jest elementem nierozkładalnym w pierścieniu P . $\square$

Uwaga 2. Nie zawsze element nierozkładalny jest elementem pierwszym. Mianowicie $P = \mathbb{Z} + (x^2)$ jest podpierścieniem dziedziny całkowitości $\mathbb{Z}[x]$ i można wykazać, że $a = x^2$ jest elementem nierozkładalnym w pierścieniu P , ale nie jest elementem pierwszym w P .

Twierdzenie 6. *Dla dowolnego niezerowego elementu p pierścienia P równoważne są warunki:*

- (i) p jest elementem pierwszym w P ,
- (ii) ideał (p) jest pierwszy w P .

Dowód. (i) $\Rightarrow$ (ii) Z założenia $p \notin P^*$, więc $1 \notin (p)$, czyli $(p) \neq P$. Niech $a, b \in P$ będą takie, że $ab \in (p)$. Wtedy $p \mid ab$, więc z pierwszości p , $p \mid a$ lub $p \mid b$, czyli $a \in (p)$ lub $b \in (p)$. Zatem (p) jest ideałem pierwszym w P .

(ii) $\Rightarrow$ (i) Z założenia $(p) \neq P$, więc $1 \notin (p)$, czyli $p \notin P^*$. Ponadto z założenia $p \neq 0$. Weźmy dowolne $x, y \in P$ takie, że $p \mid xy$. Wtedy $xy \in (p)$, więc z pierwszości ideału (p) , $x \in (p)$ lub $y \in (p)$, czyli $p \mid x$ lub $p \mid y$. Zatem p jest elementem pierwszym w pierścieniu P . $\square$

Twierdzenie 7. *W dziedzinie ideałów głównych każdy element nierozkładalny jest elementem pierwszym.*

Dowód. Niech $a \in P$ będzie elementem nierozkładalnym w dziedzinie ideałów głównych P . Wtedy $a \neq 0$ i $a \notin P^*$, skąd $1 \notin (a)$, więc

$(a) \neq P$. Niech $I \triangleleft P$ oraz $(a) \subset I$. Wtedy istnieje $b \in I$ takie, że $I = (b)$, więc $(a) \subset (b)$. Zatem $b \mid a$ i istnieje $t \in P$ takie, że $a = bt$. Stąd z nierozkładalności a mamy, że $b \in P^*$ lub $t \in P^*$. Jeśli $t \in P^*$, to $a \sim b$, skąd $(a) = (b)$ i mamy sprzeczność. Zatem $b \in P^*$, skąd $1 \in (b)$, czyli $(b) = P$. Zatem (a) jest ideałem maksymalnym w P . Stąd (a) jest ideałem pierwszym w P i na mocy twierdzenia 6, a jest elementem pierwszym w P . $\square$

13.2 Dziedziny z jednoznacznością rozkładu

Definicja 3. Niech a będzie niezerowym elementem nieodwracalnym dziedziny całkowitości P . Powiemy, że a ma *rozkład jednoznaczny* w P , jeżeli $a = p_1 \cdot \dots \cdot p_n$ dla pewnych nierozkładalnych elementów $p_1, \dots, p_n$ pierścienia P oraz jeśli $q_1, \dots, q_s$ są elementami nierozkładalnymi w P takimi, że $a = q_1 \cdot \dots \cdot q_s$, to $s = n$ oraz po ewentualnej permutacji indeksów uzyskamy, że $p_i \sim q_i$ dla $i = 1, \dots, n$.

Definicja 4. Powiemy, że dziedzina całkowitości P jest *dziedziną z jednoznacznością rozkładu*, jeżeli każdy niezerowy element nieodwracalny pierścienia P ma rozkład jednoznaczny.

Twierdzenie 8. W dziedzinie z jednoznacznością rozkładu każdy element nierozkładalny jest elementem pierwszym.

Dowód. Niech p będzie elementem nierozkładalnym dziedziny z jednoznacznością rozkładu P . Weźmy dowolne $x, y \in P$ takie, że $p \mid xy$. Jeśli $x = 0$, to $p \mid x$, jeśli $y = 0$, to $p \mid y$. Możemy zatem dalej zakładać, że $x \neq 0$ i $y \neq 0$. Istnieje $t \in P$ takie, że $xy = tp$. Jeśli $x \in P^*$, to $y = x^{-1}tp$, skąd $p \mid y$. Jeśli $y \in P^*$, to analogicznie $p \mid x$. Niech dalej $x \notin P^*$ i $y \notin P^*$. Wtedy $x = q_1 \cdot \dots \cdot q_r$, $y = t_1 \cdot \dots \cdot t_s$ dla pewnych elementów nierozkładalnych $q_1, \dots, q_r, t_1, \dots, t_s$ pierścienia P . Zatem $tp = q_1 \cdot \dots \cdot q_r \cdot t_1 \cdot \dots \cdot t_s$. Ale w rozkładzie tp na czynniki nierozkładalne występuje p , więc z jednoznaczności rozkładu elementu tp mamy, że $p \sim q_i$ dla pewnego $i \leq r$, skąd $p \mid x$ lub $p \sim t_j$ dla pewnego $j \leq s$, skąd $p \mid y$. Zatem p jest elementem pierwszym

w pierścieniu P . $\square$

Twierdzenie 9. *Niech P będzie dziedziną całkowitości, w której każdy element nierozkładalny jest elementem pierwszym. Wówczas równoważne są warunki:*

(i) *P jest dziedziną z jednoznacznością rozkładu,*

(ii) *każdy niezerowy element nieodwracalny pierścienia P jest iloczynem skończonej liczby elementów nierozkładalnych w pierścieniu P .*

Dowód. (i) $\Rightarrow$ (ii) Oczywiście. (ii) $\Rightarrow$ (i) Niech zachodzi (ii), ale nie zachodzi (i). Wtedy istnieje niezerowy element nieodwracalny $a \in P$ rozkładający się na iloczyn najmniejszej liczby elementów nierozkładalnych $p_1, \dots, p_n$ i nie posiadający jednoznacznego rozkładu w P . Zatem istnieją elementy nierozkładalne $q_1, \dots, q_s$ pierścienia P takie, że $a = q_1 \cdot \dots \cdot q_s = p_1 \cdot \dots \cdot p_n$ oraz nie można spermutować elementów $p_1, \dots, p_n$ tak aby $p_i \sim q_i$ dla $i = 1, \dots, n$ lub $n \neq s$. Z założenia $n \geq s$. Jeżeli $n = 1$, to $s = 1$, skąd $q_1 = p_1$ i mamy sprzeczność. Zatem $n > 1$. Ponadto p_n jest elementem pierwszym w P oraz $p_n \mid q_1 \cdot \dots \cdot q_s$, więc dla pewnego $i \leq s$, $p_n \mid q_i$. Bez zmniejszania ogólności można zakładać, że $i = s$, tzn. $p_n \mid q_s$. Stąd z nierozkładalności p_n i q_s mamy, że $p_n \sim q_s$, czyli $q_s = p_n u$ dla pewnego $u \in P^*$ oraz $q_1 \cdot \dots \cdot q_{s-2} \cdot (q_{s-1} u) = p_1 \cdot \dots \cdot p_{n-1}$. Ale $q_{s-1} u$ jest elementem nierozkładalnym w P , więc z minimalności n mamy, że $n - 1 = s - 1$, skąd $n = s$. Ponadto po ewentualnej permutacji indeksów $p_i \sim q_i$ dla $i = 1, \dots, n - 2$ i $p_{n-1} \sim q_{s-1} u \sim q_{s-1}$. Stąd $p_i \sim q_i$ dla $i = 1, \dots, n$ i mamy sprzeczność. $\square$

Z twierdzeń 7 i 9 oraz z twierdzenia 7 z rozdziału 12 wynika od razu następujący

Wniosek 2. *Każda dziedzina ideałów głównych jest dziedziną z jednoznacznością rozkładu.* $\square$

Rozdział 14

Ciała i ich własności

14.1 Charakterystyka ciała

Określenie ciała i własności działań w ciele były omówione na algebrze liniowej. Niech $(K, +, \cdot, 0, 1)$ będzie ciałem. Przypomnijmy, że iloczyn elementu $a \in K$ przez liczbę naturalną określamy następująco:

$$1 \cdot a = a \text{ oraz } (n+1) \cdot a = n \cdot a + a \text{ dla } n = 1, 2, \dots$$

Zatem $n \cdot a = \underbrace{a + \dots + a}_n$.

Jeżeli istnieje liczba naturalna n taka, że $n \cdot 1 = 0$ w ciele K , to najmniejszą taką liczbę naturalną n nazywamy *charakterystyką ciała K* . Jeżeli takiej liczby naturalnej nie ma, to mówimy, że ciało K ma charakterystykę 0. Charakterystykę ciała K oznaczamy przez $ch(K)$.

Twierdzenie 1. *Jeżeli n jest charakterystyką ciała K i $n \in \mathbb{N}$, to n jest liczbą pierwszą.*

Dowód. Załóżmy, że n nie jest liczbą pierwszą. Ponieważ $0 \neq 1$ w K oraz $1 \cdot 1 = 1$, więc $n > 1$ i istnieją $k, l \in \mathbb{N}$ takie, że $1 < k, l < n$ oraz $n = k \cdot l$. Wtedy $0 = n \cdot 1 = (k \cdot l) \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{kl} =$
 $= \underbrace{(1 + \dots + 1)}_k \cdot \underbrace{(1 + \dots + 1)}_l = (k \cdot 1) \cdot (l \cdot 1)$ i K jest ciałem, więc

$k \cdot 1 = 0$ lub $l \cdot 1 = 0$. Ale $k, l < n$, więc mamy sprzeczność z określeniem charakterystyki n ciała K . $\square$

Przykład 1. Dla dowolnej liczby pierwszej p ciało $\mathbb{Z}_p$ ma charakterystykę p , bo dla $k \in \mathbb{N}, k < p$ jest $k \cdot 1 = \underbrace{1 \oplus_p \dots \oplus_p 1}_k = k \neq 0$ oraz

$$p \cdot 1 = \underbrace{1 \oplus_p \dots \oplus_p 1}_p = \underbrace{[1 + \dots + 1]_p}_p = [p]_p = 0.$$

Przykład 2. Ciało $\mathbb{Q}$ ma charakterystykę 0, bo dla $n \in \mathbb{N}$ jest $n \cdot 1 = n \neq 0$.

Twierdzenie 2. Każde ciało skończone ma dodatnią charakterystykę.

Dowód. Niech K będzie ciałem skończonym o m elementach. Wówczas elementy $1 \cdot 1, 2 \cdot 1, 3 \cdot 1, \dots, m \cdot 1, (m+1) \cdot 1$ nie mogą być parami różne. Zatem istnieją liczby naturalne $i > j$ takie, że $i \cdot 1 = j \cdot 1$. Stąd $(i-j) \cdot 1 = 0$. Ale $i-j \in \mathbb{N}$, więc $ch(K) \in \mathbb{N}$, czyli $ch(K) > 0$. $\square$

14.2 Podciała i ciała proste

Definicja 1. Niech $(K, +, \cdot, 0, 1)$ będzie ciałem i niech $L \subseteq K$. Powiemy, że L jest podciałem ciała K , jeżeli L tworzy ciało ze względu na wszystkie działania określone w K , tzn. gdy $0, 1 \in L$ oraz dla dowolnych $a, b \in L$ mamy, że $-a \in L$, $a + b \in L$, $a \cdot b \in L$ i dla $a \neq 0$ jest, że $\frac{1}{a} \in L$.

Twierdzenie 3. Zbiór $L \subseteq K$ jest podciałem ciała K wtedy i tylko wtedy, gdy $1 \in L$ oraz dla dowolnych $a, b \in L$ jest $a - b \in L$ i dla dowolnych $a, b \in L$ takich, że $b \neq 0$ jest $\frac{a}{b} \in L$.

Dowód. $\Rightarrow$ Załóżmy, że L jest podciałem ciała K . Wtedy $1 \in L$. Niech $a, b \in L$. Wtedy $-b \in L$, stąd $a - b = a + (-b) \in L$. Niech $a, b \in L$, $b \neq 0$. Wtedy $\frac{1}{b} \in L$, więc $\frac{a}{b} = a \cdot \frac{1}{b} \in L$.

$\Leftarrow$ Na odwrót, $1 \in L$, więc $0 = 1 - 1 \in L$. Niech $a, b \in L$. Wtedy $-b = 0 - b \in L$ oraz $a + b = a - (-b) \in L$. Ponadto dla $b \neq 0$ jest

$a \cdot b = 0 \in L$, a dla $b \neq 0$, $\frac{1}{b} \in L$, bo $1 \in L$, więc $\frac{a}{b} = a \cdot b \in L$. Zatem L jest podciałem ciała K . $\square$

Uwaga 1. Z określenia charakterystyki ciała wynika od razu, że jeżeli L jest podciałem ciała K , to $ch(L) = ch(K)$.

Definicja 2. Jeżeli ciało K nie posiada podciała różnych od K , to mówimy, że K jest *ciałem prostym*.

Przykład 3. Zauważmy, że $\mathbb{Q}$ jest ciałem prostym. Rzeczywiście, niech $K \subseteq \mathbb{Q}$ będzie podciałem ciała $\mathbb{Q}$. Wówczas $1 \in K$. Jeżeli dla pewnego $n \in \mathbb{N}$ jest $n \in K$, to $n+1 \in K$, stąd przez indukcję mamy, że $\mathbb{N} \subseteq K$. Ale $0 \in K$ i dla $n \in \mathbb{N}$ jest, że $-n \in K$, bo $n \in K$, więc $\mathbb{Z} \subseteq K$. Weźmy dowolne $q \in \mathbb{Q}$. Wówczas istnieją $n \in \mathbb{Z}$ i $k \in \mathbb{N}$ takie, że $q = \frac{n}{k}$. Ale $n, k \in K$ i $k \neq 0$, więc $q \in K$. Stąd $\mathbb{Q} \subseteq K$, czyli $K = \mathbb{Q}$.

Przykład 4. Dla dowolnej liczby pierwszej p , $\mathbb{Z}_p$ jest ciałem prostym. Rzeczywiście, niech $K \subseteq \mathbb{Z}_p$ będzie podciałem ciała $\mathbb{Z}_p$. Wówczas $1 \in K$, stąd $1 \oplus_p 1 = 2 \in K$, więc też $3 \cdot 1 \in K$ itd. W końcu $1, 2, \dots, p-1, 0 \in K$, czyli $K = \mathbb{Z}_p$.

Twierdzenie 4. Jedynymi ciałami prostymi z dokładnością do izomorfizmu są $\mathbb{Q}$ i $\mathbb{Z}_p$ dla p będących liczbami pierwszymi.

Dowód. Niech K będzie ciałem prostym. Jeżeli $ch(K) = 0$, to dla $n \in \mathbb{N}$ mamy, że $n \cdot 1 \neq 0$, więc dla $m \in \mathbb{Z}$, $n \in \mathbb{N}$ mamy, że $\frac{m \cdot 1}{n \cdot 1} \in K$. Łatwo sprawdzić, że wówczas zbiór $L = \{\frac{m \cdot 1}{n \cdot 1} : m \in \mathbb{Z}, n \in \mathbb{N}\}$ jest podciałem ciała K , skąd $L = K$. Ponadto przekształcenie $f : \mathbb{Q} \rightarrow L$ dane wzorem $f(\frac{m}{n}) = \frac{m \cdot 1}{n \cdot 1}$ dla $m \in \mathbb{Z}, n \in \mathbb{N}$ jest izomorfizmem ciał. Stąd $K \cong \mathbb{Q}$.

Niech teraz $ch(K) = p > 0$. Z twierdzenia 1 p jest liczbą pierwszą. Łatwo zauważyć, że wtedy $M = \{0 \cdot 1, 1 \cdot 1, \dots, (p-1) \cdot 1\}$ jest podciałem ciała K , skąd $K = M$. Ponadto przekształcenie $g : \mathbb{Z}_p \rightarrow M$ dane wzorem $g(k) = k \cdot 1$ dla $k \in \mathbb{Z}_p$ jest izomorfizmem ciał, więc $K \cong \mathbb{Z}_p$. $\square$

Uwaga 2. Z dowodu twierdzenia 4 wynika, że jeśli ciało K ma charakterystykę 0, to istnieje w nim podciało izomorficzne z ciałem $\mathbb{Q}$,

a jeżeli ciało K ma charakterystykę $p > 0$, to istnieje w nim podciało izomorficzne z $\mathbb{Z}_p$ i jest to najmniejsze (w sensie inkluzji) podciało ciała K .

Definicja 3. Jeżeli L jest podciałem ciała K , to mówimy, że K jest rozszerzeniem ciała L .

Uwaga 3. Jeżeli ciało K jest rozszerzeniem ciała L , to K jest przestrzenią liniową nad ciałem L , jeżeli dla $\alpha \in K$, $a \in L$ określimy

$$a \circ \alpha = a \cdot \alpha,$$

gdzie $\cdot$ oznacza mnożenie w ciele K . Moc dowolnej bazy K nad L oznaczamy przez $(K : L)$ i nazywamy *stopniem rozszerzenia* $L \subseteq K$. Jeżeli $(K : L)$ jest liczbą naturalną, to mówimy, że K jest *skończonym rozszerzeniem* ciała L .

Twierdzenie 5. Jeżeli K jest ciałem skończonym, to istnieją liczba pierwsza p oraz liczba naturalna n takie, że $ch(K) = p$ i $|K| = p^n$. Jeżeli L jest podciałem ciała K , to istnieje $m \in \mathbb{N}$ takie, że $m \mid n$ oraz $|L| = p^m$.

Dowód. Z twierdzeń 1 i 2 wynika, że istnieje liczba pierwsza p taka, że $ch(K) = p$. Niech L będzie podciałem ciała K . Wtedy K jest przestrzenią liniową nad ciałem L . Ale K jest skończone, więc istnieje baza $\{\alpha_1, \dots, \alpha_s\}$ K nad L . Każdy element należący do K może być zapisany jednoznacznie w postaci kombinacji liniowej elementów tej bazy. Zatem $|K| = |L^s| = |L|^s$.

Z uwagi 2 istnieje podciało F takie, że $|F| = p$. Stąd $|K| = p^n$ dla pewnego $n \in \mathbb{N}$. Jeżeli L jest dowolnym podciałem ciała K , to z uwagi 2 $F \subseteq L$, więc $|L| = p^m$ dla pewnego $m \in \mathbb{N}$. Ale $p^n = |K| = |L|^s = p^{ms}$ dla pewnego $s \in \mathbb{N}$, więc $n = ms$ i $m \mid n$. $\square$

Twierdzenie 6. Niech K będzie ciałem dodatniej charakterystyki p . Wówczas dla dowolnych $a, b \in K$:

$$a^p + b^p = (a + b)^p.$$

Dowód. Ze wzoru Newtona mamy

$$(a + b)^p = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k \cdot b^{p-k}.$$

Ale z elementarnej teorii liczb dla $k = 1, \dots, p-1$ mamy, że $p \mid \binom{p}{k}$, więc $\binom{p}{k} = p \cdot l_k$, $l_k \in \mathbb{N}$. Zatem $\binom{p}{k} \cdot 1 = (p \cdot l_k) \cdot 1 = l_k \cdot (p \cdot 1) = l_k \cdot 0 = 0$, stąd wynika teza. $\square$

Uwaga 4. Z twierdzenia 6 przez prostą indukcję uzyskujemy, że jeżeli K jest ciałem dodatniej charakterystyki p , to dla $n \in \mathbb{N}$ i $a, b \in K$ zachodzi wzór:

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Przykład 5. $(\mathbb{C} : \mathbb{R}) = 2$, to $\{1, i\}$ jest bazą $\mathbb{C}$ nad $\mathbb{R}$. Natomiast $(\mathbb{R} : \mathbb{Q}) = \infty$, bo $\mathbb{R}$ jest nieprzeliczalne, a $\mathbb{Q}$ jest przeliczalne.

14.3 Ciało ułamków

Każdy podpierścień ciała jest dziedziną całkowitości. Okazuje się, że także każda dziedzina całkowitości jest podpierścieniem pewnego ciała.

Definicja 4. Powiemy, że ciało K jest *ciałem ułamków* dziedziny całkowitości P , jeżeli

- (i) P jest podpierścieniem K oraz
- (ii) każdy element ciała K można zapisać w postaci $\frac{a}{b}$ dla pewnych $a, b \in P$, $b \neq 0$.

Przedstawimy teraz konstrukcję ciała ułamków dowolnej dziedziny całkowitości P . Niech $S = P \times (P \setminus \{0\})$. W zbiorze S określamy relację $\sim$ przyjmując, że dla dowolnych $(a_1, b_1), (a_2, b_2) \in S$:

$$(a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1.$$

Sprawdźmy, że $\sim$ jest relacją równoważności w S :

1° Jeżeli $(a, b) \in S$, to $a \cdot b = a \cdot b$ więc $(a, b) \sim (a, b)$.

2° Jeżeli $(a, b), (c, d) \in S$ oraz $(a, b) \sim (c, d)$ to $a \cdot d = c \cdot b$. Stąd $c \cdot b = a \cdot d$, czyli $(c, d) \sim (a, b)$.

3° Jeżeli $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in S$ są takie, że $(a_1, b_1) \sim (a_2, b_2)$ oraz $(a_2, b_2) \sim (a_3, b_3)$, to $a_1 \cdot b_2 = a_2 \cdot b_1$ i $a_2 \cdot b_3 = a_3 \cdot b_2$, stąd $a_1 \cdot b_2 \cdot b_3 = a_2 \cdot b_1 \cdot b_3$ i $a_2 \cdot b_3 \cdot b_1 = a_3 \cdot b_2 \cdot b_1$, więc $a_1 \cdot b_2 \cdot b_3 = a_3 \cdot b_2 \cdot b_1$. Ale $b_2 \neq 0$ i P jest dziedziną całkowitości, więc $a_1 \cdot b_3 = a_3 \cdot b_1$, stąd $(a_1, b_1) \sim (a_3, b_3)$.

Klasę abstrakcji o reprezentancie $(a, b) \in S$ będziemy oznaczali przez $\frac{a}{b}$. Zbiór wszystkich klas abstrakcji relacji $\sim$ będziemy oznaczali przez P_0 .

Zauważmy najpierw, że dla $(a, b) \in S$ i $0 \neq d \in P$ jest $\frac{a}{b} = \frac{a \cdot d}{b \cdot d}$. Rzeczywiście, $a \cdot (b \cdot d) = (a \cdot d) \cdot b$ stąd $(a, b) \sim (a \cdot d, b \cdot d)$, więc $\frac{a}{b} = \frac{a \cdot d}{b \cdot d}$.

Dla $(a, b) \in S$ mamy też, że $\frac{a}{b} = \frac{0}{1} \Leftrightarrow a = 0$. Rzeczywiście, dla $a = 0$ jest $a \cdot 1 = 0 = 0 \cdot b$, więc $(a, b) \sim (0, 1)$, stąd $\frac{a}{b} = \frac{0}{1}$. Jeżeli zaś $\frac{a}{b} = \frac{0}{1}$, to $(a, b) \sim (0, 1)$, skąd $a \cdot 1 = 0 \cdot b$, czyli $a = 0$.

Niech $1 = \frac{1}{1}$ i $0 = \frac{0}{1}$. Ponieważ $0 \neq 1$ w P , więc z naszych rozważań wynika, że $0 \neq 1$ w K .

Określamy teraz w P_0 dodawanie i mnożenie przy pomocy wzorów:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2}, \quad (14.1)$$

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2}. \quad (14.2)$$

Sprawdźmy, że te określenia nie zależą od wyboru reprezentantów klas. Niech $(a_1, b_1), (x_1, y_1), (a_2, b_2), (x_2, y_2) \in S$ oraz $(a_1, b_1) \sim (x_1, y_1)$, $(a_2, b_2) \sim (x_2, y_2)$. Wtedy $a_1 \cdot y_1 = x_1 \cdot b_1$ i $a_2 \cdot y_2 = x_2 \cdot b_2$. Musimy udowodnić, że wówczas $(a_1 \cdot b_2 + a_2 \cdot b_1, b_1 \cdot b_2) \sim (x_1 \cdot y_2 + x_2 \cdot y_1, y_1 \cdot y_2)$ i $(a_1 \cdot a_2, b_1 \cdot b_2) \sim (x_1 \cdot x_2, y_1 \cdot y_2)$, czyli że $(a_1 \cdot b_2 + a_2 \cdot b_1) \cdot y_1 y_2 = (x_1 y_2 + x_2 y_1) \cdot b_1 \cdot b_2$ i $a_1 \cdot a_2 \cdot y_1 \cdot y_2 = x_1 \cdot x_2 \cdot b_1 \cdot b_2$. Ale $a_1 \cdot a_2 \cdot y_1 \cdot y_2 = (a_1 \cdot y_1) \cdot (a_2 \cdot y_2) = x_1 \cdot b_1 \cdot x_2 \cdot b_2 = x_1 \cdot x_2 \cdot b_1 \cdot b_2$ oraz $(a_1 \cdot b_2 + a_2 \cdot b_1) \cdot y_1 y_2 = (a_1 y_1) \cdot b_2 y_2 + (a_2 y_2) \cdot b_1 y_1 = x_1 \cdot b_1 \cdot b_2 \cdot y_2 + x_2 \cdot b_2 \cdot b_1 \cdot y_1 = (x_1 \cdot y_2 + x_2 \cdot y_1) \cdot b_1 \cdot b_2$, więc wzory (14.1) i (14.2) są dobrze określone.

Teraz udowodnimy, że $(K, +, \cdot, 0, 1)$ jest ciałem. W tym celu sprawdzamy spełnienie aksjomatów ciała:

1. Niech $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in S$. Wtedy

$$\begin{aligned} \left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) + \frac{a_3}{b_3} &= \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2} + \frac{a_3}{b_3} = \frac{a_1 \cdot b_2 \cdot b_3 + a_2 \cdot b_1 \cdot b_3}{b_1 \cdot b_2 \cdot b_3} + \frac{a_3 \cdot b_1 \cdot b_2}{b_1 \cdot b_2 \cdot b_3} = \\ &= \frac{a_1 \cdot b_2 \cdot b_3 + a_2 \cdot b_1 \cdot b_3 + a_3 \cdot b_1 \cdot b_2}{b_1 \cdot b_2 \cdot b_3}, \end{aligned}$$

bo $\frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 + a_2}{b}$, gdyż $\frac{a_1}{b} + \frac{a_2}{b} = \frac{a_1 \cdot b + a_2 \cdot b}{b^2} = \frac{(a_1 + a_2) \cdot b}{b \cdot b} = \frac{a_1 + a_2}{b}$.

Ponadto

$$\begin{aligned} \frac{a_1}{b_1} + \left(\frac{a_2}{b_2} + \frac{a_3}{b_3}\right) &= \frac{a_1}{b_1} + \frac{a_2 \cdot b_3 + a_3 \cdot b_2}{b_2 \cdot b_3} = \frac{a_1 \cdot b_2 \cdot b_3}{b_1 \cdot b_2 \cdot b_3} + \frac{a_2 \cdot b_3 \cdot b_1 + a_3 \cdot b_2 \cdot b_1}{b_1 \cdot b_2 \cdot b_3} = \\ &= \frac{a_1 \cdot b_2 \cdot b_3 + a_2 \cdot b_3 \cdot b_1 + a_3 \cdot b_2 \cdot b_1}{b_1 \cdot b_2 \cdot b_3}, \end{aligned}$$

wiec dodawanie jest łączne.

2. Niech $(a_1, b_1), (a_2, b_2) \in S$. Wtedy

$$\frac{a_2}{b_2} + \frac{a_1}{b_1} = \frac{a_2 \cdot b_1 + a_1 \cdot b_2}{b_2 \cdot b_1} = \frac{a_1 \cdot b_2 + a_2 \cdot b_1}{b_1 \cdot b_2} = \frac{a_1}{b_1} + \frac{a_2}{b_2},$$

wiec dodawanie jest przemienne.

3. Niech $(a, b) \in S$. Wtedy $0 = \frac{0}{b}$ oraz $\frac{a}{b} + 0 = \frac{a}{b} + \frac{0}{b} = \frac{a+0}{b} = \frac{a}{b}$, więc 0 jest elementem neutralnym dodawania.

4. Niech $(a, b) \in S$. Wtedy $(-a, b) \in S$ oraz $\frac{a}{b} + \frac{-a}{b} = \frac{a+(-a)}{b} = \frac{0}{b} = 0$.
Zatem $-(\frac{a}{b}) = \frac{(-a)}{b}$.

5. Niech $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in S$. Wtedy

$$\left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) \cdot \frac{a_3}{b_3} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2} \cdot \frac{a_3}{b_3} = \frac{a_1 \cdot a_2 \cdot a_3}{b_1 \cdot b_2 \cdot b_3}$$

i

$$\frac{a_1}{b_1} \cdot \left(\frac{a_2}{b_2} \cdot \frac{a_3}{b_3}\right) = \frac{a_1}{b_1} \cdot \frac{a_2 \cdot a_3}{b_2 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot a_3}{b_1 \cdot b_2 \cdot b_3},$$

więc mnożenie jest łączne.

6. Niech $(a_1, b_1), (a_2, b_2) \in S$. Wtedy $\frac{a_2}{b_2} \cdot \frac{a_1}{b_1} = \frac{a_2 \cdot a_1}{b_2 \cdot b_1} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2} = \frac{a_1}{b_1} \cdot \frac{a_2}{b_2}$, więc mnożenie jest przemienne.
7. Niech $(a, b) \in S$. Wtedy $\frac{a}{b} \cdot 1 = \frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$, czyli 1 jest elementem neutralnym mnożenia.
8. Niech $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in S$. Wtedy

$$\frac{a_1}{b_1} \cdot \left(\frac{a_2}{b_2} + \frac{a_3}{b_3} \right) = \frac{a_1}{b_1} \cdot \frac{a_2 \cdot b_3 + a_3 \cdot b_2}{b_2 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot b_3 + a_1 \cdot a_3 \cdot b_2}{b_1 \cdot b_2 \cdot b_3}$$

oraz

$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} + \frac{a_1}{b_1} \cdot \frac{a_3}{b_3} = \frac{a_1 \cdot a_2}{b_1 \cdot b_2} + \frac{a_1 \cdot a_3}{b_1 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot b_3}{b_1 \cdot b_2 \cdot b_3} + \frac{a_1 \cdot a_3 \cdot b_2}{b_1 \cdot b_2 \cdot b_3} = \frac{a_1 \cdot a_2 \cdot b_3 + a_1 \cdot a_3 \cdot b_2}{b_1 \cdot b_2 \cdot b_3},$$

więc mnożenie jest rozdzielne względem dodawania.

9. Niech $(a, b) \in S$ będzie takie, że $\frac{a}{b} \neq 0$. Wtedy, jak wiemy $a \neq 0$, więc $(b, a) \in S$ oraz $\frac{a}{b} \cdot \frac{b}{a} = \frac{a \cdot b}{b \cdot a} = \frac{1}{1} = 1$, bo $a, b \neq 0$. Stąd $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$

Z 1–9 wynika zatem, że $(P_0, +, \cdot, 0, 1)$ jest ciałem.

Niech $f: P \rightarrow P_0$ będzie funkcją daną wzorem $f(a) = \frac{a}{1}$ dla $a \in P$. Dla $a, b \in P: f(a) = f(b) \Leftrightarrow \frac{a}{1} = \frac{b}{1} \Leftrightarrow (a, 1) \sim (b, 1) \Leftrightarrow a \cdot 1 = b \cdot 1 \Leftrightarrow a = b$. Zatem f jest różnowartościowe. Ponadto $f(1) = \frac{1}{1} = 1$ oraz dla $a, b \in P$:

$$f(a + b) = \frac{a + b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$$

i

$$f(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1 \cdot 1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b).$$

Zatem f jest zanurzeniem pierścieni. Stąd dla $a \in P$ można dokonać utożsamienia:

$$a \equiv \frac{a}{1}.$$

Przy tym utożsamieniu P jest podpierścieniem ciała P_0 . Dla $0 \neq b \in P$ mamy, że $\frac{1}{b} = (\frac{b}{1})^{-1} = b^{-1}$, więc dla $a \in P$ jest $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = a \cdot b^{-1}$, stąd $P_0 = \{a \cdot b^{-1} : a, b \in P, b \neq 0\}$, czyli P_0 jest ciałem ułamków dla P . Ponadto dla $(a_1, b_1), (a_2, b_2) \in S$ mamy, że $\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1$, bo $\frac{a_1}{b_1} = \frac{a_2}{b_2} \Leftrightarrow (a_1, b_1) \sim (a_2, b_2) \Leftrightarrow a_1 \cdot b_2 = a_2 \cdot b_1$.

Jeżeli L jest ciałem, to ciało ułamków pierścienia $L[x]$ oznaczamy przez $L(x)$ i nazywamy *ciałem funkcji wymiernych zmiennej x nad ciałem L* . Wówczas L jest podciałem $L(x)$, skąd $ch(L(x)) = ch(L)$. Ponieważ $1, x, x^2, \dots$ są liniowo niezależne nad L i należą do $L(x)$, więc $(L(x) : L) = \infty$. Podstawiając $L = \mathbb{Z}_p$ uzyskamy stąd, że **istnieją ciała nieskończone dowolnej dodatniej charakterystyki**.

Rozdział 15

Rozszerzenia algebraiczne ciał

Twierdzenie 1. *Gdy $K \subseteq L \subseteq M$ są ciałami oraz $(L:K) = r \in \mathbb{N}$ i $(M:L) = s \in \mathbb{N}$, to $(M:K) = r \cdot s$.*

Dowód. Niech $a_1, \dots, a_r \in L$ będzie bazą L nad K oraz niech $b_1, \dots, b_s \in M$ będzie bazą M nad L . Udowodnimy, że

$$\{a_i \cdot b_j : 1 \leq i \leq r, 1 \leq j \leq s\}$$

jest bazą M nad K . W tym celu weźmy dowolne $c_{ij} \in K, i = 1, \dots, r, j = 1, \dots, s$ takie, że $\sum_{i,j} c_{ij} a_i b_j = 0$. Wówczas $\sum_{j=1}^s \left(\sum_{i=1}^r c_{ij} a_i \right) b_j = 0$.

Elementy stojące w nawiasach należą do ciała L , więc dla $j = 1, \dots, s$ mamy, że $\sum_{i=1}^r c_{ij} a_i = 0$. Stąd z liniowej niezależności elementów $a_1, \dots, a_r$

wynika, że $c_{ij} = 0$ dla $i = 1, \dots, r$. Zatem $c_{ij} = 0$ dla wszystkich i, j , czyli elementy $a_i \cdot b_j$ dla $i = 1, \dots, r, j = 1, \dots, s$ są liniowo niezależne nad K . Weźmy teraz dowolne $a \in M$. Wówczas istnieją $t_1, \dots, t_s \in L$

takie, że $a = \sum_{j=1}^s t_j \cdot b_j$ oraz dla $j = 1, \dots, s$ istnieją $c_{1j}, c_{2j}, \dots, c_{rj} \in K$

takie, że $t_j = \sum_{i=1}^r c_{ij} \cdot a_i$. Stąd $a = \sum_{i,j} c_{ij} (a_i \cdot b_j)$. Zatem elementy $a_i \cdot b_j$

dla $i = 1, \dots, r$, $j = 1, \dots, s$ generują M nad K . Stąd mamy tezę. $\square$

Definicja 1. Niech K będzie podciałem ciała L . Powiemy, że element $a \in L$ jest *algebraiczny* względem ciała K , jeżeli istnieje niezerowy wielomian $f \in K[x]$ taki, że $f(a) = 0$. W przeciwnym przypadku element $a \in L$ nazywamy *przestępnym* względem ciała K . Ciało L nazywamy *rozszerzeniem algebraicznym* ciała K , gdy każdy element $a \in L$ jest algebraiczny względem K .

Uwaga 1. Zauważmy, że $x \in K(x)$ jest elementem przestępnym nad K .

Uwaga 2. Liczby zespolone a , które są elementami algebraicznymi względem ciała $\mathbb{Q}$ nazywamy krótko *liczbami algebraicznymi*. Liczbę $a \in \mathbb{C}$ nazywamy *przestępną*, jeżeli a nie jest liczbą algebraiczną. Np. $a = e$ i $a = \pi$ są przestępne.

Twierdzenie 2. Niech K będzie podciałem ciała L i $a \in L$. Wówczas a jest algebraiczny względem ciała K wtedy i tylko wtedy, gdy istnieje wielomian nierozkładalny $f \in K[x]$ taki, że $f(a) = 0$. Ponadto, gdy $g \in K[x]$ i $g(a) = 0$, to $f \mid g$ w $K[x]$.

Dowód. $\Rightarrow$ Oczywiście. $\Leftarrow$ Załóżmy, że $a \in L$ jest algebraiczny względem K . Wtedy istnieje niezerowy wielomian $f \in K[x]$ najniższego stopnia taki, że $f(a) = 0$. Stąd $f \notin K$ i jeżeli $w, u \in K[x]$ są takie, że $f = w \cdot u$, to $0 = w(a) \cdot u(a)$, skąd $w(a) = 0$ lub $u(a) = 0$. Bez zmniejszania ogólności można zakładać, że $w(a) = 0$. Wówczas $st(f) = st(w) + st(u)$, więc z minimalności $st(f)$ mamy, że $st(w) = st(f)$. Stąd $st(u) = 0$ i $u \in K^*$. Zatem wielomian f jest nierozkładalny w $K[x]$. Niech teraz $g \in K[x]$ będzie takie, że $g(a) = 0$. Wówczas istnieją $q, r \in K[x]$ takie, że $g = f \cdot q + r$ i $st(r) < st(f)$. Stąd $0 = g(a) = f(a) \cdot q(a) + r(a) = r(a)$, bo $f(a) = 0$, więc z minimalności $st(f)$ wynika, że $r = 0$ i $g = f \cdot q$, czyli $f \mid g$. $\square$

Wniosek 1. Gdy element $a \in L \supseteq K$ jest algebraiczny względem ciała K , to wielomian nierozkładalny $f \in K[x]$, którego a jest pierwiastkiem, jest wyznaczony jednoznacznie z dokładnością do stałego czynnika.

Dowód. Jeżeli $f_1, f_2 \in K[x]$ są wielomianami nierozkładalnymi w $K[x]$ takimi, że $f_1(a) = f_2(a) = 0$, to z twierdzenia 2 mamy, że $f_1 \mid f_2$ i $f_2 \mid f_1$, więc $f_1 \sim f_2$. Stąd istnieje $0 \neq c \in K$ takie, że $f_2 = c \cdot f_1$. $\square$

Gdy element $a \in L$ jest algebraiczny względem podciała $K \subseteq L$, to stopień wielomianu nierozkładalnego $f \in K[x]$ takiego, że $f(a) = 0$ nazywamy *stopniem elementu a względem ciała K* , zaś f nazywamy *wielomianem minimalnym dla a względem ciała K* .

Niech K będzie podciałem ciała L i $a \in L$. Wówczas istnieje najmniejsze w sensie inkluzji podciało ciała L zawierające a oraz K . Oznaczmy je przez $K(a)$. Oczywiście $K(a)$ jest częścią wspólną wszystkich podciał ciała L zawierających $K \cup \{a\}$.

Twierdzenie 3. *Gdy $a \in L$ jest elementem algebraicznym stopnia n względem podciała $K \subseteq L$, to:*

- (i) $K(a) = \{b_0 + b_1 \cdot a + \dots + b_{n-1} \cdot a^{n-1} : b_0, b_1, \dots, b_{n-1} \in K\}$;
- (ii) Bazą $K(a)$ nad K jest układ: $1, a, a^2, \dots, a^{n-1}$;
- (iii) $(K(a) : K) = n$.

Dowód. Jeżeli $n = 1$, to $a \in K$ i $K(a) = K$, więc teza jest oczywista. Niech dalej $n > 1$ i niech $f \in K[x]$ będzie wielomianem minimalnym a względem K . Wtedy $st(f) = n$. Niech

$$M = \{b_0 + b_1 \cdot a + \dots + b_{n-1} \cdot a^{n-1} : b_0, b_1, \dots, b_{n-1} \in K\}.$$

Wówczas $K \subseteq M$ i $a \in M$. Jeżeli $b_0, b_1, \dots, b_{n-1} \in K$ są takie, że $b_0 + b_1 \cdot a + \dots + b_{n-1} \cdot a^{n-1} = 0$, to $g(a) = 0$ dla $g = b_0 + b_1 \cdot x + \dots + b_{n-1} \cdot x^{n-1} \in K[x]$, więc z minimalności $st(f)$ mamy, że $b_0 = b_1 = \dots = b_{n-1} = 0$. Zatem elementy $1, a, a^2, \dots, a^{n-1}$ są liniowo niezależne nad K . Jeśli $h \in K[x]$, to istnieją $q, r \in K[x]$ takie, że $h = q \cdot f + r$ i $st(r) < n$, więc $h(a) = q(a)f(a) + r(a) = r(a) \in M$. Zatem $M = \{h(a) : h \in K[x]\}$. Stąd od razu mamy, że M jest podpierścieniem ciała L . Weźmy dowolne $b_0, b_1, \dots, b_{n-1} \in K$ takie, że $b_0 + b_1 \cdot a + \dots + b_{n-1} \cdot a^{n-1} \neq 0$. Wtedy, jak wiemy $g = b_0 + b_1 \cdot x + \dots + b_{n-1} \cdot x^{n-1} \neq 0$ i f jest nierozkładalny w $K[x]$. Zatem istnieją wielomiany $u, v \in K[x]$ takie, że $g \cdot u + f \cdot v = 1$, stąd $g(a) \cdot u(a) + f(a) \cdot v(a) = 1$, czyli $\frac{1}{g(a)} = u(a) \in M$. Zatem M jest

podciałem ciała L zawierającym $K \cup \{a\}$. Niech N będzie dowolnym podciałem ciała L zawierającym $K \cup \{a\}$. Wtedy $1, a, a^2, \dots, a^{n-1} \in N$ oraz dla dowolnych $b_0, b_1, \dots, b_{n-1} \in K$, $b_0 + b_1 \cdot a + \dots + b_{n-1} \cdot a^{n-1} \in N$. Stąd $M \subseteq N$. Zatem $M = K(a)$ i wobec powyższego $1, a, a^2, \dots, a^{n-1}$ jest bazą $K(a)$ nad K , czyli $(K(a) : K) = n$. $\square$

Twierdzenie 4. *Element $a \in L$ jest algebraiczny względem podciała K wtedy i tylko wtedy, gdy $(K(a) : K) < \infty$.*

Dowód. $\Rightarrow$ Wynika z twierdzenia 2. $\Leftarrow$ Załóżmy, że $(K(a) : K) = n < \infty$, wówczas elementy $1, a, a^2, \dots, a^n$ są liniowo zależne nad K oraz należą do $K(a)$, więc istnieją $b_0, b_1, \dots, b_n \in K$ nie wszystkie równe 0 i takie, że $b_0 + b_1 \cdot a + \dots + b_n \cdot a^n = 0$, stąd $g(a) = 0$ dla $0 \neq b_0 + b_1 \cdot x + \dots + b_n \cdot x^n \in K[x]$. Zatem a jest elementem algebraicznym względem ciała K . $\square$

Wniosek 2. *Każde rozszerzenie skończone jest algebraiczne.*

Dowód. Niech $(L : K) = n < \infty$ i $a \in L$. Wtedy $K(a) \subseteq L$, więc $(K(a) : K) \leq n$, stąd wobec twierdzenia 4 a jest elementem algebraicznym względem ciała K . $\square$

Jeżeli $a_1, \dots, a_n \in L \supseteq K$, gdzie K jest podciałem ciała L , to istnieje najmniejsze podciało ciała L zawierające $K \cup \{a_1, \dots, a_n\}$. Oznaczmy je przez $K(a_1, \dots, a_n)$. Łatwo zauważyć, że dla dowolnych $a_1, \dots, a_n, a_{n+1} \in L$ i dla dowolnego $n \in \mathbb{N}$, $K(a_1, \dots, a_n, a_{n+1}) = (K(a_1, \dots, a_n))(a_{n+1})$.

Wniosek 3. *Gdy $a_1, \dots, a_n \in L$ są elementami algebraicznymi względem $K \subseteq L$, to $K(a_1, \dots, a_n)$ jest rozszerzeniem algebraicznym i skończonym ciała K .*

Dowód. Indukcja względem n . Dla $n = 1$ teza wynika z twierdzenia 4. Załóżmy, że teza zachodzi dla pewnego naturalnego n i niech $a_1, \dots, a_n, a_{n+1} \in L$ będą elementami algebraicznymi względem K . Jeśli $f \in K[x]$ jest wielomianem minimalnym dla a_{n+1} względem K , to $f \in K(a_1, \dots, a_n)[x]$, więc $(K(a_1, \dots, a_n)(a_{n+1}) : K(a_1, \dots, a_n)) \leq (K(a_{n+1}) : K) < \infty$, czyli $(K(a_1, \dots, a_n, a_{n+1}) : K(a_1, \dots, a_n)) < \infty$. Ponadto z założenia indukcyjnego $(K(a_1, \dots, a_n) : K) < \infty$, więc z twierdzenia 1, $(K(a_1, \dots, a_n, a_{n+1}) : K) < \infty$. Stąd z wniosku 2

rozszerzenie $K \subseteq K(a_1, \dots, a_{n+1})$ jest algebraiczne. $\square$

Wniosek 4. *Niech K będzie podciałem ciała L . Wówczas zbiór $M \subseteq L$ wszystkich elementów algebraicznych względem K jest podciałem ciała L zawierającym K .*

Dowód. Ponieważ każde $a \in K$ jest pierwiastkiem wielomianu $x - a \in K[x]$, więc $K \subseteq M$. Niech $a, b \in M$. Wtedy z wniosku 3 $K(a, b)$ jest rozszerzeniem algebraicznym ciała K , czyli $K(a, b) \subseteq M$. Zatem $a - b \in M$ i $\frac{a}{b} \in M$ dla $b \neq 0$. Stąd z twierdzenia 3 z rozdziału 14, M jest podciałem ciała L . $\square$

Twierdzenie 5. *Jeżeli ciało L jest algebraicznym rozszerzeniem ciała K i ciało M jest algebraicznym rozszerzeniem ciała L , to ciało M jest algebraicznym rozszerzeniem ciała K .*

Dowód. Weźmy dowolne $a \in M$. Wówczas istnieje $0 \neq f \in L[x]$ takie, że $f(a) = 0$. Ale $f = l_1 + l_1x + \dots + l_nx^n$ dla pewnych $l_0, \dots, l_n \in L$ oraz z wniosku 3 mamy, że $(K(l_0, \dots, l_n) : K) < \infty$. Ponadto a jest algebraiczny nad $K(l_0, \dots, l_n)$, więc z twierdzenia 4 mamy, że $((K(l_0, \dots, l_n))(a) : K(l_0, \dots, l_n)) < \infty$. Zatem z twierdzenia 1 i z wniosku 2, a jest algebraiczny nad ciałem K . $\square$

Literatura

- [1] Cz. Bagiński, *Wstęp do teorii grup*, SCRIPT, Warszawa 2002.
- [2] A. Białynicki-Birula, *Algebra*, PWN, Warszawa 1971.
- [3] J. Browkin, *Teoria ciał*, PWN, Warszawa 1977.
- [4] M. Bryński i J. Jurkiewicz, *Zbiór zadań z algebry*, PWN, Warszawa 1978.
- [5] A. I. Kostykin, *Wstęp do algebry*, PWN, Warszawa 1984.
- [6] A. I. Kostykin, *Zbiór zadań z algebry*, PWN, Warszawa 1995.