ALGEBRA 1
Skrypt do wykładu A

Roman Wencel

Wrocław, luty 2004

Spis treści

Wstęp

W niniejszym skrypcie przedstawione zostały podstawowe zagadnienia dotyczące działań w zbiorach, teorii grup oraz teorii pierścieni i ciał. Zakres materiału pokrywa się w dużym stopniu z wykładem ALGEBRA 1A, prowadzonym przez autora w Instytucie Matematycznym Uniwersytetu Wrocławskiego w latach akademickich 2002/2003 i 2003/2004. Przy pisaniu niektórych fragmentów skryptu zostały wykorzystane pozycje wymienione w bibliografii.

Zakładam u Czytelnika znajomość wstępu do matematyki (na przykład w zakresie skryptu prof. L. Newelskiego) oraz podstaw algebry liniowej.

Rozdział 0

Liczby naturalne, całkowite i wymierne

W skrypcie będziemy posługiwali się językiem teorii liczb naturalnych i korzystali z pewnych podstawowych ich własności.

Zbiór liczb naturalnych oznaczamy symbolem $\mathbb{N}$. W zbiorze tym wyróżniony jest element 0 (liczba naturalna zero) oraz określona jest opracja s, która każdej liczbie naturalnej n przyporządkowuje jej następnik $s(n)$. Wyróżniony element 0 oraz operacja następnika spełniają następujące aksjomaty – aksjomaty teorii liczb naturalnych (zwane też aksjomatami Peana[1]).

(a) Jeśli n jest liczbą naturalną różną od 0, to istnieje dokładnie jedna liczba naturalna m, dla której $n = s(m)$.

(b) Nie istnieje taka liczba naturalna n, że $s(n) = 0$.

(c) (Zasada indukcji) Niech $A \subseteq \mathbb{N}$. Jeśli $0 \in A$ oraz $(\forall n \in \mathbb{N})(n \in A \Longrightarrow s(n) \in A)$, to $A = \mathbb{N}$.

Zbiór liczb naturalnych różnych od 0 oznaczamy przez $\mathbb{N}_+$.

Przyjmując jako punkt wyjścia wprowadzone wyżej pojęcia: elementu 0 oraz operacji następnika i korzystając z aksjomatów teorii liczb naturalnych, można w zbiorze $\mathbb{N}$ określić operacje dodawania, mnożenia i porządku. Dla $m, n \in \mathbb{N}$ przyjmujemy:

(1) $n + 0 = n$,

(2) $n + s(m) = s(n + m)$,

(3) $n \cdot 0 = 0$,

(4) $n \cdot s(m) = n \cdot m + n$,

(5) jeśli istnieje $k \in \mathbb{N}$ ($k \in \mathbb{N}_+$) takie, że $n = m + k$, to przyjmujemy że $n \geq m$ (odpowiednio: $n > m$).

Można wykazać, że wprowadzone wyżej działania dodawania i mnożenia są łączne i przemienne. Mnożenie jest rozdzielne względem dodawania, $\leq$ jest dobrym porządkiem. Czytelnika zainteresowanego szczegółami odsyłamy do książki A. Grzegorczyka pt. *Zarys arytmetyki teoretycznej*. W książce tej znajdują się również formalne definicje zbiorów liczb całkowitych ($\mathbb{Z}$), wymiernych ($\mathbb{Q}$) i rzeczywistych ($\mathbb{R}$) wraz z dowodami podstawowych własności działań arytmetycznych w tych zbiorach.

Definicja 0.1 *Mówimy, że liczba całkowita n jest podzielna przez liczbę całkowitą m (oznaczenie: $m|n$), jeśli istnieje liczba całkowita k taka, że $n = km$.*

[1] G. Peano (1858 - 1932), matematyk i logik włoski

Jeśli $m|n$, mówimy też, że m jest dzielnikiem n, n dzieli się przez m, albo, że n jest wielokrotnością m. W poniższym twierdzeniu zostały zebrane najprostsze własności relacji podzielności liczb całkowitych.

Twierdzenie 0.2 *Niech $k, l, m, n \in \mathbb{Z}$. Wtedy*
(a) $1|k$,
(b) $k|0$,
(c) Jeśli $0|k$, to $k = 0$,
(d) Jeśli $k|l$ i $l|m$, to $k|m$,
(e) Jeśli $k|l$ i $l|k$, to $k = l$ lub $k = -l$,
(f) Jeśli $k|l$, to $k|lm$,
(g) Jeśli $k|l$ i $k|m$, to $k|l + m$ i $k|l - m$,
(h) Jeśli $k|l$ i $m|n$, to $km|ln$.

Niech $m \in \mathbb{N}_+$. Dowolną liczbę całkowitą n można jednoznacznie przedstawić w postaci: $n = qm + r$, gdzie $q \in \mathbb{Z}$, zaś $r \in \{0, \ldots, m-1\}$. Liczbę q nazywamy całością z dzielenia n przez m, zaś r resztą z tego dzielenia.

Liczbę całkowitą w, która jest podzielna przez każdą z danych liczb całkowitych $a_1, \ldots, a_m$ nazywamy wspólną wielokrotnością tych liczb. Dla każdego ciągu skończonego liczb całkowitych różnych od zera $a_1, \ldots, a_m$ istnieje nieskończenie wiele wspólnych wielokrotności tych liczb. Będą nimi na przykład liczby postaci $ka_1 \ldots a_m$. W przypadku, gdy któraś z liczb $a_1, \ldots, a_m$ jest równa 0, jedyną wspólną wielokrotnością liczb $a_1, \ldots, a_m$ jest 0.

Przypuśćmy, że $a_1, \ldots, a_m \in \mathbb{Z} \setminus \{0\}$. Najmniejszą liczbę naturalną dodatnią będącą wspólną wielokrotnością liczb $a_1, \ldots, a_m$ nazywamy najmniejszą wspólną wielokrotnością tych liczb i oznaczamy przez $NWW(a_1, \ldots, a_m)$. Jeśli któraś z liczb $a_1, \ldots, a_m$ jest równa 0, przyjmujemy, że największą wspólną wielokrotnością liczb $a_1, \ldots, a_n$ jest 0.

Twierdzenie 0.3 *Niech $a_1, \ldots, a_m$ oraz w będą liczbami całkowitymi. Wtedy następujące warunki są równoważne:*
(a) $|w| = NWW(a_1, \ldots, a_m)$,
(b) w jest wspólną wielokrotnością liczb $a_1, \ldots, a_m$ i jest dzielnikiem każdej wspólnej wielokrotności tych liczb.

Dowód. Teza twierdzenia jest oczywista gdy któraś z liczb $a_1, \ldots, a_m$ jest równa 0, ponieważ wtedy jedyną wspólną wielokrotnością liczb $a_1, \ldots, a_m$ jest 0. Wystarczy więc przeprowadzić dowód w pzypadku, gdy liczby $a_1, \ldots, a_m$ są wszystkie różne od 0.

(a)$\Longrightarrow$(b). Załóżmy, że $|w| = NWW(a_1, \ldots, a_m)$. Wtedy oczywiście w jest wspólną wielokrotnością liczb $a_1, \ldots, a_m$. Przypuśćmy nie wprost, że n jest wspólną wielokrotnością liczb $a_1, \ldots, a_m$, która nie dzieli się przez w. Wtedy n nie dzieli się przez $|w|$ i $n = q|w| + r$, gdzie $q \in \mathbb{Z}$, zaś r jest liczbą naturalną dodatnią, mniejszą od $|w|$. $a_1, \ldots, a_m$ są dzielnikami każdej z liczb n i $|w|$. Dlatego również $r = n - q|w|$ dzieli się przez każdą z liczb $a_1, \ldots, a_m$. Liczba naturalna dodatnia r jest więc wspólną wielokrotnością liczb $a_1, \ldots, a_m$, mniejszą od $NWW(a_1, \ldots, a_m)$. Sprzeczność.

(b)$\Longrightarrow$(a). Załóżmy, że zachodzi (b). Wtedy $|w| \in \mathbb{N}_+$ jest wspólną wielokrotnością liczb $a_1, \ldots, a_m$ oraz dzielnikiem każdej wspólnej wielokrotności tych liczb. Każda liczba naturalna dodatnia podzielna przez $|w|$ jest $\geq |w|$, dlatego $|w| = NWW(a_1, \ldots, a_m)$. ■

Niech $a_1, a_2, \ldots$ będzie skończonym lub nieskończonym ciągiem liczb całkowitych. Liczbę całkowitą d, która dzieli każdą z liczb $a_1, a_2, \ldots$ nazywamy wspólnym dzielnikiem tych liczb. Dla każdego ciągu (skończonego lub nieskończonego) liczb całkowitych istnieje ich wspólny dzielnik (na przykład liczba 1). Jeśli przynajmniej jedna spośród liczb $a_1, a_2, \ldots$ jest różna od 0, istnieje tylko skończenie wiele wspólnych dzielników tych liczb. W przypadku, gdy wszystkie spośród liczb $a_1, a_2, \ldots$ są zerami, zbiorem ich wspólnych dzielników jest $\mathbb{Z}$.

Przypuśćmy, że liczby $a_1, a_2, \ldots$ są całkowite i przynajmniej jedna z nich jest różna od 0. Największą liczbę naturalną dodatnią będącą wspólnym dzielnikeim liczb $a_1, a_2, \ldots$ nazywamy największym wspólnym dzielnikiem tych liczb i oznaczamy przez $NWD(a_1, a_2, \ldots)$. Dla ciągu złożonego z samych zer nie określamy największego wspólnego dzielnika.

Twierdzenie 0.4 *Niech $a_1, a_2, \ldots$ będzie skończonym lub nieskończonym ciągiem liczb całkowitych, z których przynajmniej jedna jest różna od 0 i niech $d \in \mathbb{Z}$. Wtedy następujące warunki są równoważne:*
(a) $|d| = NWD(a_1, a_2, \ldots)$.
(b) d jest wspólnym dzielnikiem liczb $a_1, a_2, \ldots$ i dzieli się przez każdy wspólny dzielnik tych liczb.

Dowód. (a)$\Longrightarrow$(b). Załóżmy, że $d \in \mathbb{Z}$ i $|d| = NWD(a_1, a_2, \ldots) \in \mathbb{N}$. Wtedy oczywiście d jest wspólnym dzielnikiem liczb $a_1, a_2, \ldots$.

Niech $d_1 < d_2 < \ldots < d_s$ będą wszystkimi wspólnymi dzielnikami liczb $a_1, a_2, \ldots$. Oczywiście $|d| = d_s$. Niech $w = NWW(d_1, \ldots, d_s)$. Ponieważ w dzieli się przez każdą z liczb $d_1, \ldots, d_s$, wystarczy wykazać, że $w = d_s$. Wprost z określenia w wynika, że $d_s \leq w$. Każda z liczb $a_1, a_2, \ldots$ jest wspólną wielokrotnością liczb $d_1, \ldots, d_s$. Dlatego, na mocy twierdzenia 0.3, w dzieli każdą z liczb $a_1, a_2, \ldots$, czyli jest ich wspólnym dzielnikiem. Stąd $w \leq d_s$.

(b)$\Longrightarrow$(a). Załóżmy, że zachodzi (b). Wtedy $|d|$ jest wspólnym dzielnikiem liczb $a_1, a_2, \ldots$ i $|d|$ dzieli się przez każdy wspólny dzielnik liczb $a_1, a_2, \ldots$. Stąd $|d| = NWD(a_1, a_2, \ldots)$. ■

Twierdzenie 0.5 *Jeśli $a, b \in \mathbb{N}_+$, to $NWD(a, b) \cdot NWW(a, b) = ab$.*

Dowód. Niech $a, b \in \mathbb{N}_+$, $d = NWD(a, b)$ i $w = NWW(a, b)$. Wtedy $a = kd$ i $b = ld$ dla pewnych $k, l \in \mathbb{N}_+$. Skąd $kld = la = kb$, co dowodzi, że kld jest wspólną wielokrotnością liczb a i b. Na mocy twierdzenia 0.3 oraz tego, że a i b dzielą w mamy:

$$kld = tw = tra = trkd \text{ oraz } kld = tw = tsb = tsld$$

dla pewnych $r, s, t \in \mathbb{N}_+$. Tak więc $l = tr$ i $k = ts$. Stąd dostajemy $a = kd = tsd$ i $b = ld = trd$. td jest więc wspólnym dzielnikiem liczb a i b, a ponieważ ich największym wspólnym dzielnikiem jest d, musi być $t = 1$. Uwzględniając dotychczasowe rozważania dostajemy: $ab = kdld = twd = wd$, co kończy dowód. ■

Zauważmy, że twierdzenie analogiczne do twierdzenia 0.5 nie jest prawdziwe dla trzech liczb naturalnych, gdyż na przykład

$$NWD(2, 4, 6) \cdot NWW(2, 4, 6) = 2 \cdot 12 \neq 2 \cdot 4 \cdot 6.$$

O liczbach całkowitych m i n, dla których $NWD(m, n) = 1$, mówimy, że są względnie pierwsze. Z twierdzenia 0.5 wynika, że jeśli liczby naturalne dodatnie m i n są względnie pierwsze to $NWW(mn) = mn$.

Twierdzenie 0.6 *(Zasadnicze twierdzenie arytmetyki) Jeśli $a, b, c \in \mathbb{Z} \setminus \{0\}$, $a|bc$ i $NWD(a, b) = 1$, to $a|c$.*

Dowód. Z założeń twierdzenia wynika, że bc jest wielokrotnością liczb a i b. Na mocy twierdzenia 0.3 oznacza to, że $NWW(a, b)|bc$. a i b są względnie pierwsze, więc $NWW(a, b) = |ab|$. Tak więc $ab|bc$, a stąd $a|c$. ■

Twierdzenie 0.7 *Jeśli $NWD(a, b) = 1$ i $c|b$, to $NWD(a, c) = 1$.*

Dowód. $NWD(a, c)|c$, zaś $c|b$. Stąd $NWD(a, c)|b$. Mamy również $NWD(a, c)|a$. Tak więc $NWD(a, c)$ jest wspólnym dzielnikiem liczb a i b, co wobec twiedzenia 0.4 i $NWD(a, b) = 1$ daje $NWD(a, c)|1$, czyli $NWD(a, c) = 1$. ■

Twierdzenie 0.8 *Jeśli $NWD(a,c) = NWD(b,c) = 1$, to $NWD(ab,c) = 1$.*

Dowód. Niech $d = NWD(ab,c)$. Ponieważ $d|c$ i $NWD(a,c) = 1$, na mocy twierdzenia 0.7 dostajemy $NWD(a,d) = 1$. $d|ab$, więc z twierdzenia 0.6 wynika, że $d|b$. Uwzględniając, że $d|c$ i $NWD(b,c) = 1$, wobec twierdzenia 0.4 mamy $d|1$, czyli $d = 1$. ■

Twierdzenie 0.9 *Jeśli liczby całkowite a i b, z których przynajniej jedna nie jest zerem podzielimy przez ich największy wspólny dzielnik, to otrzymamy liczby względnie pierwsze.*

Dowód. Niech a i b spełniają założenia twierdzenia i niech $d = NWD(a,b)$. Wtedy $a = da_1$ i $b = db_1$ dla pewnych $a_1, b_1 \in \mathbb{Z}$. Niech $\delta = NWD(a_1,b_1)$. Wówczas $a_1 = \delta a_2$ i $b_1 = \delta b_2$ dla pewnych $a_2, b_2 \in \mathbb{Z}$. Tak więc $a = d\delta a_2$ i $b = d\delta b_2$, co oznacza, że $d\delta$ jest wspólnym dzielnikiem liczb a i b. Wobec twierdzenia 0.4, $d\delta|d$. Oznacza to, że $\delta|1$, czyli $\delta = 1$. ■

Wniosek 0.10 *Każda liczba wymierna daje się przedstawić w postaci ilorazu dwóch liczb całkowitych względnie pierwszych.*

Dowód. Dowolną liczbę wymierną można przedstawić w postaci $\frac{a}{b}$, gdzie $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$. Niech $d = NWD(a,b)$. W myśl twierdzenia 0.9 będzie $a = da_1$ i $b = db_1$, gdzie a_1 i b_1 są liczbami całkowitymi względnie pierwszymi. Oczywiście $\frac{a}{b} = \frac{a_1}{b_1}$. ■

Przedstawimy teraz metodę znajdywania największego wspólnego dzielnika dwóch danych liczb naturalnych dodatnich a i b, zwaną algorytmem Euklidesa[2]. Gdyby bylo $b|a$, mielibyśmy $NWD(a,b) = b$. Przypuśćmy więc, że $b < a$ i b nie dzieli a. Wówczas, dzieląc a przez b otrzymamy iloraz całkowity q i resztę dodatnią $r < b$ i będzie $a = qb + r$.

Jeśli $d|a$ i $d|b$, to również d dzieli $r = a - qb$. Tak więc każdy wspólny dzielnik liczb a i b jest wspólnym dzielnikiem liczb b i r.

Jeśli zaś $\delta|b$ i $\delta|r$, to również δ dzieli $a = qb + r$. Tak więc każdy wspólny dzielnik liczb b i r jest wspólnym dzielnikiem liczb a i b.

Dowiedliśmy więc, że liczby a i b mają te same dzielniki wspólne, co b i r. Wynika stąd natychmiast, że

$$NWD(a,b) = NWD(b,r).$$

Wzór ten sprowadza obliczanie największego wsp'olnego dzielnika liczb a i b do obliczania największego wspólnego dzielnika liczb b i r odpowiednio mniejszych.

Jeżeli $r|b$, to oczywiście $NWD(b,r) = r$, w przeciwnym wypadku, oznaczając przez r_1 resztę z dzielenia b przez r, będziemy mieli $NWD(b,r) = NWD(r,r_1)$. Jeśli $r_1|r$, to $NWD(r,r_1) = r_1$, w przeciwnym wypadku znajdziemy $r_2 \in \mathbb{N}_+$, $r_2 < r_1$ takie, że $NWD(r,r_1) = NWD(r_1,r_2)$ itd. Tego rodzaju redukcje mogą być dokonywane co najwyżej $b-1$ razy, gdyż liczby $a, b, r, r_1, \ldots$ tworzą ciąg malejący. Musimy więc dojść do takiej pary liczb r_{k-1}, r_k, dla której $r_k|r_{k-1}$. Będzie wtedy $r_k = NWD(a,b)$.

Z powyższego rozumowania wynika następująca reguła wyznaczania największego wspólnego dzielnika dwóch liczb naturalnych dodatnich:

Chcąc znaleźć największy wspólny dzielnik liczb naturalnych dodatnich a i b, gdzie $a > b$, dzielimy a przez b i wyznaczamy resztę r_0 z tego dzielenia. Jeśli $r_0 \neq 0$, dzielimy b przez r_0 i wyznaczamy nową resztę r_1. Jeśli $r_1 \neq 0$, dzielimy r_0 przez r_1 i wyznaczamy nową resztę r_2 itd., aż dojdziemy do reszty 0. Ostatnia różna od zera reszta będzie równa $NWD(a,b)$.

Reguła ta znana jest pod nazwą metody kolejnych dzieleń albo **algorytmu Euklidesa.** Stosując ten algorytm do liczb a i b otrzymujemy więc ciąg wzorów:

[2]Euklides (365 p.n.e. - 300 p.n.e.), matematyk i fizyk grecki

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0q_1 + r_1 \\ r_0 &= r_1q_2 + r_2 \\ &\cdots\cdots\cdots \\ r_{k-2} &= r_{k-1}q_k + r_k \\ r_{k-1} &= r_kq_{k+1} + 0, \end{aligned}$$

i mamy $NWD(a,b) = r_k$.

Pierwszy z napisanych wzorów daje $r_0 = a - q_0b$. Indukcyjnie względem j można pokazać, że dla $j \leq k$ reszta r_j może być zapisana w postaci $ax_j + by_j$, gdzie $x_j, y_j \in \mathbb{Z}$. Stąd wynika następujące twierdzenie.

Twierdzenie 0.11 *Jeśli $a, b \in \mathbb{Z}\setminus\{0\}$, to istnieją liczby całkowite x, y takie, że $NWD(a,b) = ax+by$.*

Twierdzenie 0.12 *(Twierdzenie chińskie o resztach) Jeżeli m jest liczbą naturalną ≥ 2 oraz $a_1, \ldots, a_m$ są liczbami naturalnymi dodatnimi, z których każde dwie są względnie pierwsze, i jeżeli $r_1, \ldots, r_m$ są dowolnymi liczbami całkowitymi, to istnieją liczby całkowite $x_1, \ldots, x_m$, dla których*

$$(*)\ a_1x_1 + r_1 = a_2x_2 + r_2 = \ldots = a_mx_m + r_m.$$

Dowód. (Indukcja względem m) Niech $m = 2$. Wobec twierdzenia 0.11, istnieją liczby całkowite x, y takie, że $a_1x + a_2y = 1$. Mnożąc tę równość przez $r_2 - r_1$, a następnie podstawiając $x_1 = (r_2 - r_1)x$ i $-x_2 = (r_2 - r_1)y$, otrzymujemy $a_1x_1 - a_2x_2 = r_2 - r_1$, czyli $a_1x_1 + r_1 = a_2x_2 + r_2$.

Niech teraz m będzie liczbą naturalną ≥ 2 i przypuśćmy, że twierdzenie jest prawdziwe dla m liczb. Niech $a_1, \ldots, a_{m+1}$ będą liczbami naturalnymi dodatnimi, z których każde dwie są względnie pierwsze, zaś $r_1, \ldots, r_{m+1}$ dowolnymi liczbami całkowitymi. Z założenia, że twierdzenie jest prawdziwe dla m liczb wynika, że istnieją liczby całkowite $x_1, \ldots, x_m$, dla których słuszne są wzory $(*)$. Ponieważ każda z liczb $a_1, \ldots, a_m$ jest względnie pierwsza z liczbą a_{m+1}, na mocy twierdzenia 0.8 mamy $NWD(a_1 \cdot \ldots \cdot a_m, a_{m+1}) = 1$. To zaś oznacza, że istnieją liczby całkowite t i u takie, że

$$a_1 \ldots a_m t - a_{m+1}u = r_{m+1} - a_1x_1 - r_1.$$

Przyjmijmy oznaczenia:

$$x_i' = \frac{a_1 \ldots a_m}{a_i}t + x_i \text{ dla } i = 1, \ldots, m \text{ oraz } x_{m+1}' = u.$$

Liczby $x_1', \ldots, x_{m+1}'$ są całkowite i, jak łatwo sprawdzić, dla $i = 1, \ldots, m$ mamy:

$$a_ix_i' + r_i = a_1 \ldots a_m t + a_ix_i + r_i = a_{m+1}x_{m+1}' + r_{m+1} - a_1x_1 - r_1 + a_ix_i + r_i = a_{m+1}x_{m+1}' + r_{m+1},$$

co dowodzi prawdziwości twierdzenia dla $m+1$ liczb. Twierdzenie to zostało więc udowodnione przez indukcję. ■

Wniosek 0.13 *Jeśli każde dwie spośród $m \geq 2$ liczb naturalnych dodatnich $a_1, a_2, \ldots, a_m$ są względnie pierwsze, to istnieje liczba całkowita N, która przy dzieleniu przez te liczby daje odpowiednio dowolne dane reszty $r_1, \ldots, r_m$*

Liczba naturalna > 1 ma przynajmniej dwa różne dzielniki naturalne: 1 i n. Jeśli poza nimi nie ma ona żadnych innych dzielników pierwszych, to nazywamy ją liczbą pierwszą. Liczbę naturalną > 1, która nie jest pierwsza nazywamy złożoną.

Twierdzenie 0.14 *Każda liczba naturalna > 1 ma co najmniej jeden dzielnik pierwszy.*

Dowód. Niech n będzie liczbą naturalną większą od 1. Oznaczmy przez p najmniejszą liczbę naturalną > 1 będącą dzielnikiem n. Pokażemy, że p jest liczbą pierwszą.

Gdyby liczba p była złożona, mielibyśmy $p = ab$, gdzie a, b są liczbami naturalnymi > 1. Wtedy jednak $a < p$ i $a|n$. Sprzeczność z wyborem p. ■

Twierdzenie 0.15 *Jeśli p jest liczbą pierwszą, zaś a i b liczbami całkowitymi takimi, że $p|ab$, to $p|a$ lub $p|b$.*

Dowód. Niech p będzie liczbą pierwszą, $a, b \in \mathbb{Z}$ i $p|ab$. Przypuśćmy, że a nie dzieli się przez p. Wtedy $NWD(p, a) = 1$. Jeśli $b \neq 0$, to na mocy twierdzenia 0.6 dostajemy $p|b$. Jeśli $b = 0$, to oczywiście również $p|b$. ■

Wniosek 0.16 *Jeśli p jest liczbą pierwszą, $a_1, \ldots, a_n \in \mathbb{Z}$ i $p|a_1 \cdot \ldots \cdot a_n$, to p dzieli przynajmniej jedną z liczb $a_1, \ldots, a_k$.*

Twierdzenie 0.17 *Zbiór wszystkich liczb pierwszych jest nieskończony.*

Dowód. Załóżmy, że istnieje tylko skończenie wiele liczb pierwszych. Oznaczmy je przez $p_1, \ldots, p_k$. Wówczas liczba $n = p_1 \cdot \ldots \cdot p_k + 1$ nie dzieli się przez żadną z liczb $p_1, \ldots, p_k$. $n > 1$, więc zgodnie z twierdzeniem 0.14, n posiada pewien dzielnik pierwszy p. Oczywiście p nie jest żadną z liczb $p_1, \ldots, p_k$. Tak więc zbiór liczb pierwszych nie może być skończony. ■

W następującym twierdzeniu przez $p_1, p_2, p_3, \ldots$ oznaczamy kolejne liczby pierwsze.

Twierdzenie 0.18 *Dowolna liczba naturalna większa od 1 posiada jednoznaczne przedstawienie w postaci*

$$(*) \quad \prod_{j=1}^{m} p_{k_j}^{\alpha_j},$$

gdzie $\alpha_1, \ldots, \alpha_m \in \mathbb{N}_+$ i $k_1 < \ldots < k_m$.

Dowód. (Indukcja wzhlędem n) Jeśli $n = p_i$ jest liczbą pierwszą, to oczywiście n przedstawia się w postaci $(*)$. Co więcej, w dowolnym jej przedstawieniu w postaci $(*)$ występuje dokładnie jeden czynnik, którym jest p_i. Tak więc twierdzenie jest prawdziwe w przypadku, gdy n jest liczbą pierwszą. W szczególności jest ono słuszne dla $n = 2$.

Przypuśćmy więc, że $n > 1$ jest liczbą naturalną złożoną oraz, że dowolna liczba naturalna leżąca pomiędzy 1 a n posiada jednoznaczne przedstawienie w postaci $(*)$. Wobec złożoności liczby n i twierdzenia 0.14, $n = pr$, gdzie p jest liczbą pierwszą, zaś r liczbą naturalną leżą pomiędzy 1 a n. Na mocy założenia indukcyjnego r posiada przedstawienie postaci $(*)$, skąd natychmiast wynika, że również n posiada przedstawienie postaci $(*)$.

W celu wykazania jednoznaczności przedstawienia $(*)$, załóżmy, że dla liczby n mamy dwa przedstawienia:

$$(**) \quad n = \prod_{j=1}^{m} p_{k_j}^{\alpha_j} = \prod_{j=1}^{s} p_{l_j}^{\beta_j},$$

przy czym $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_s \in \mathbb{N}_+$, $k_1 < \ldots < k_m$ i $l_1 < \ldots < l_s$. Ponieważ n jest liczbą złożoną, w każdym z tych przedstawień występują przynajmniej dwa czynniki pierwsze (to znaczy $\alpha_1 + \ldots + \alpha_m \geq 2$ i $\beta_1 + \ldots + \beta_s \geq 2$). p_{k_1} dzieli prawą stronę równości $(**)$, więc na mocy wniosku 0.16 dostajemy $p_{k_1}|p_{l_j}$ dla pewnego $j \in \{1, \ldots, s\}$, co oznacza, że $p_{k_1} = p_{l_j}$. Dzieląc równość $(**)$ obustronie przez p_{k_1}, otrzymujemy dwa rozkłady liczby $\frac{n}{p_{k_1}}$ na czynniki pierwsze. $1 < \frac{n}{p_{k_1}} < n$, więc na mocy założenia indukcyjnego rozkłady te są identyczne. Stąd natychmiast wynika identyczność rozkładów $(**)$. ■

Twierdzenie 0.19 *Jeśli $k, n \in \mathbb{N}_+$ i n jest k-tą potęgą liczby wymiernej, to n jest k-tą potęgą liczby naturalnej.*

Dowód. Załóżmy, że $k, n \in \mathbb{N}_+$ i n jest k-tą potęgą liczby wymiernej. Wtedy istnieją względnie pierwsze liczby naturalne p i q takie, że $n = \left(\frac{p}{q}\right)^k$. Stąd dostajemy

$$(*)\ nq^k = p^k$$

i $q|p^k$. Z wniosku 0.16 wynika, że $q|p$. Ponieważ $NWD(p, q) = 1$, musi być $q = 1$, co po podstawieniu do $(*)$ daje $n = p^k$. ■

Rozdział 1

Działania i systemy algebraiczne. Pojęcie półgrupy

Podczas swojej edukacji matematycznej Czytelnik z pewnością niejednokrotnie zetknął się ze zbiorami, na których elementach dokonywano pewnych działań. Przykładami takich działań są: dodawanie i mnożenie liczb naturalnych, odejmowanie liczb całkowitych, dzielenie liczb wymiernych różnych od zera, dodawanie wektorów w przestrzeni liniowej i mnożenie macierzy kwadratowych wymiaru $n \times n$ dla ustalonego $n \in \mathbb{N}_+$. Wspólną cechą wszystkich wymienionych działań jest to, że każde z nich polega na przyporządkowaniu uporządkowanej parze elementów danego zbioru określonego elementu **tego samego zbioru**. Innego rodzaju działaniami, przyporządkowującymi elementowi danego zbioru element tego samego zbioru, są: pierwiaskowanie liczb rzeczywistych nieujemnych, sprzężenie liczby zespolonej czy przyporządkowanie macierzy nieosobliwej wymiaru $n \times n$ macierzy do niej odwrotnej.

Często w matematyce mamy do czynienia z ogólniejszą sytuacją, kiedy to skończonemu ciągowi elementów danego zbioru (ustalonej długości) przyporządkowujemy element tegoż zbioru. Jako przykład można wymienić przyporządkowanie ciągowi n liczb rzeczywistych $\langle a_1, \ldots, a_n \rangle$ jego średniej arytmetycznej $\frac{a_1+\ldots+a_n}{n}$.

Wymienione przykłady prowadzą do następującej definicji.

Definicja 1.1 *Niech A będzie zbiorem niepustym.*

(a) Działaniem jednoargumentowym określonym w zbiorze A nazywamy dowolną funkcję, której dziedziną jest zbiór A, i której wartości leżą w zbiorze A.

(b) Działaniem dwuargumentowym (lub po prostu działaniem) określonym w zbiorze A nazywamy dowolną funkcję odwzorowującą zbiór $A \times A$ w zbiór A.

(c) Niech $n \in \mathbb{N}_+$. Działaniem n-argumentowym określonym w zbiorze A nazywamy dowolną funkcję odwzorowującą zbiór A^n w zbiór A.

W dalszych rozważaniach będziemy zajmowali się najczęściej działaniami jedno- i dwuargumentowymi.

Jeśli $f : A \longrightarrow A$ jest działaniem jednoargumentuwym określonym w zbiorze A oraz $a \in A$, to $f(a)$ nazywamy wynikiem działania f na elemencie a. Podobnie, dla działania n-argumentowego g określonego w zbiorze A oraz elementów $a_1, \ldots, a_n \in A$, $g(a_1, \ldots, a_n)$ nazywamy wynikiem działania g na ciągu $\langle a_1, \ldots, a_n \rangle$.

W przypadku działań dwuargumentowych zwykle wygodniej jest zamiast oznaczeń literowych używać symboli takich jak $\circ$, $+$, $-$, $\cdot$, $\oplus$, $\odot$, itp. Wówczas wynik działania $\circ$ na parze uporządkowanej $\langle a, b \rangle$ zapisujemy jako $a \circ b$ zamiast formalnego $\circ(a, b)$. Podobnie, dla działań jednoargumentowych stosujemy tradycyjne oznaczenia, takie jak $-a$, $\sqrt{a}$, $\overline{z}$ czy M^{-1}.

Działania oznaczone przez $+$, $-$, $\cdot$, : będziemy najczęściej nazywać dodawaniem, odejmowaniem, mnożeniem i dzieleniem (odpowiednio). Wynik dodawania nazywamy sumą, odejmowania różnicą, mnożenia iloczynem, zaś dzielenia ilorazem. Zamiast $x \circ y$ czy $x \cdot y$ będziemy na ogół pisać xy.

Działaniu $\circ$ określonemu w skończonym zbiorze A można przyporządkować tabelkę wypisując dwukrotnie elementy zbioru A: raz w pierwszym rzędzie, raz w pierwszej kolumnie, a następnie umieszczając na przecięciu rzędu odpowiadającego elementowi a z kolumną odpowiaającą elementowi b wynik działania $\circ$ na parze $\langle a, b\rangle$.

$\circ$	$\ldots$	b	$\ldots$
		$\vdots$	
a	$\ldots$	$a \circ b$	$\ldots$
		$\vdots$	

Odwrotnie, każda tabelka, która w pierwszym rzędzie i w pierwszej kolumnie zawiera wszystkie elementy skończonego zbioru A, a na pozostałych miejscach ma wypisane pewne elementy ze zbioru A, określa w A działanie. Wynikiem tego działania na parze $\langle a, b\rangle$ jest element stojący w rzędzie odpowiadającym a i kolumnie odpowiadającej b.

Przykład 1. W każdym ze zbiorów $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ możemy określić działania przyporządkowując parze $\langle x, y\rangle$ elementów odpowiedniego zbioru ich sumę określoną w zwykły sposób. Otrzymane tak działanie nazywamy zwykłym dodawaniem liczb naturalnych, całkowitych, wymiernych, rzeczywistych i zespolonych (odpowiednio). Podobnie określamy pojęcie zwykłego mnożenia w każdym z wymienionych zbiorów. Zwykłe odejmowanie nie jest działaniem w $\mathbb{N}$, jest natomiast działaniem w $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Zwykłe dzielenie nie jest działaniem w żadnym ze zbiorów $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ale jest działaniem w $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$.

Przykład 2. Przyporządkowanie parze liczb naturalnych dodatnich największego wspólnego dzielnika tych liczb jest działaniem w $\mathbb{N}_+$ (wynik tego działania na parze $\langle m, n\rangle$ oznaczamy przez $NWD(m, n)$), ale nie jest działaniem w $\mathbb{N}$, gdyż nie istnieje największy wspólny dzielnik dla pary $\langle 0, 0\rangle$. Przyporządkowanie parze liczb naturalnych dodatnich największej wspólnej wielokrotności tych liczb jest działaniem w $\mathbb{N}_+$. Wynik tego działania na parze $\langle m, n\rangle$ oznaczamy przez $NWW(m, n)$.

Przykład 3. Niech $n \in \mathbb{N}_+$. Przyporządkowanie liczbie naturalnej jej reszty z dzielenia przez n jest działaniem jednoargumentowym w $\mathbb{N}$. Podobnie, przyporządkowanie liczbie całkowitej jej reszty z dzielenia przez n jest działaniem jednoargumentowym w $\mathbb{Z}$. Resztę z dzielenia liczby całkowitej (naturalnej) m przez n będziemy oznaczać przez $m \bmod n$. Oczywiście $m \bmod n \in \{0, \ldots, n-1\}$.

Przykład 4. Niech $n \in \mathbb{N}_+$. W zbiorze liczb naturalnych mniejszych od n (czyli w zbiorze reszt modulo n) definiujemy działania:

$$a +_n b = (a + b) \bmod n, \; a \cdot_n b = (a \cdot b) \bmod n.$$

Działania $+_n, \cdot_n$ nazywamy odpowiednio dodawaniem i mnożeniem modulo n. Tabelki działań dodawania i mnożenia modulo 4 w zbiorze $\{0, 1, 2, 3\}$ wyglądają następująco:

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Przykład 5. Niech X i Y będą zbiorami niepustymi. Przez Y^X oznaczamy zbiór funkcji, których dziedziną jest zbiór X, i których wartości leżą w zbiorze Y. W zbiorze $\mathbb{R}^X$ definiujemy działania dodawania i mnożenia funkcji:

$$(f+g)(x) = f(x) + g(x),\ (f \cdot g)(x) = f(x) \cdot g(x).$$

W zbiorze X^X definiujemy działanie składania funkcji: $(f \circ g)(x) = f(g(x))$.

Przykład 6. Dodawanie wektorów w przestrzeni liniowej V jest działaniem określonym w V. Mnożenie wektorów z V przez ustalony skalar jest działaniem jednoargumentowym w V.

Przykład 7. Składanie przekształceń jest działaniem w zbiorze przekształceń liniowych zachowujących orientację. Mnożenie macierzy jest działaniem w zbiorze macierzy kwadratowych wymiaru $n \times n$ o wyznaczniku dodatnim.

Przykład 8. W zbiorze wszystkich ciągów o wyrazach rzeczywistych definiujemy działania dodawania i mnożenia w sposób następujący:

$$\begin{aligned}\langle a_0, a_1, \ldots\rangle + \langle b_0, b_1, \ldots\rangle &= \langle a_0 + b_0, a_1 + b_1, \ldots\rangle,\\ \langle a_0, a_1, \ldots\rangle \cdot \langle b_0, b_1, \ldots\rangle &= \langle a_0 \cdot b_0, a_1 \cdot b_1, \ldots\rangle.\end{aligned}$$

Liczba działań możliwych do określenia w skończonym zbiorze A rośnie szybko wraz z liczbą jego elementów. Czytelnik zechce sprawdzić, że dla $m, n \in \mathbb{N}_+$, w zbiorze m-elementowym można określić dokładnie m^{m^n} działań n-argumentowych. Liczba działań n-argumentowych możliwych do określenia w zbiorze nieskończonym mocy κ wynosi 2^κ. W szczególności w nieskończonym zbiorze przeliczalnym jest ona równa $2^{\aleph_0}$ (tzn. continuum). Dowolne działania w zbiorach mogą być bardzo dziwaczne i mało interesuące. Dlatego też w typowych rozważaniach algebraicznych wyróżnia się kilka typów działań o specjalnych własnościach. Niektóre z nich zostały zdefiniowane niżej.

Definicja 1.2 *Załóżmy, że w zbiorze A określone jest działanie $\circ$. Działanie to nazywamy*

(a) łącznym, jeśli $x \circ (y \circ z) = (x \circ y) \circ z$ dla dowolnych $x, y, z \in A$,

(b) przemiennym, jeśli $x \circ y = y \circ x$ dla dowolnych $x, y \in A$.

Jeżeli w zbiorze A dodatkowo określone jest działanie $\oplus$, to działanie $\circ$ nazywamy

(c) lewostronnie rozdzielnym względem działania $\oplus$, jeśli $x \circ (y \oplus z) = (x \circ y) \oplus (x \circ z)$ dla dowolnych $x, y, z \in A$,

(d) prawostronnie rozdzielnym względem działania $\oplus$, jeśli $(y \oplus z) \circ x = (y \circ x) \oplus (z \circ x)$ dla dowolnych $x, y, z \in A$,

(e) (obustronnie) rozdzielnym względem działania $\oplus$, jeśli $\circ$ jest zarówno lewo- jak i prawostronnie rozdzielne względem $\oplus$.

Niemal wszystkie ważniejsze działania, z którymi będziemy mieli do czynienia, będą łączne, nie zawsze jednak będą one przemienne.

Przykład 9. Zwykłe dodawanie i mnożenie w $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ są łączne i przemienne. Ponadto mnożenie jest działaniem rozdzielnym względem dodawania. Również działania $+_n$, $\cdot_n$ określone w zbiorze reszt modulo n są łączne i przemienne. Działanie $\cdot_n$ jest rozdzielne względem $+_n$.

Przykład 10. Mnożenie macierzy kwadratowych wymiaru $n \times n$ jest łączne dla dowolnego $n \in \mathbb{N}_+$, ale przemienne tylko dla $n = 1$.

Przykład 11. W $\mathbb{N}$ określamy działanie: $m \circ n = m^n$. Przyjmujemy przy tym, że $m^0 = 1$ dla $m \in \mathbb{N}$. Działanie $\circ$ jest prawostronnie rozdzielne względem zwykłego mnożenia liczb naturalnych, mamy bowiem:

$$(m \cdot n) \circ k = (m \cdot n)^k = m^k \cdot n^k = (m \circ k) \cdot (n \circ k)$$

dla dowolnych $m, n, k \in \mathbb{N}$. $\circ$ nie jest jednak lewostronnie rozdzielne względem mnożenia, gdyż $2 \circ (1 \cdot 2) = 2^2 = 4$, ale $(2 \circ 1) \cdot (2 \circ 2) = 2^1 \cdot 2^2 = 8$.

Przykład 12. W zbiorze $\mathbb{Q}$ definiujemy działanie:

$$a \oplus b = \frac{a+b}{2}$$

(wzięcie średniej arytmetycznej liczb a i b). Działanie $\oplus$ jest przemienne, ale nie jest łączne, bo na przykład

$$1 \oplus (2 \oplus 2) = 1 \oplus \frac{2+2}{2} = 1 \oplus 2 = \frac{1+2}{2} = \frac{3}{2}, \text{ ale } (1 \oplus 2) \oplus 2 = \frac{1+2}{2} \oplus 2 = \frac{\frac{3}{2}+2}{2} = \frac{7}{4}.$$

Przykład 13. Niech X będzie dowolnym zbiorem. Suma, iloczyn i różnica symetryczna zbiorów są działaniami łącznymi i przemiennymi w $\mathcal{P}(X)$ (rodzina wszystkich podzbiorów zbioru X). Ponadto iloczyn zbiorów jest działaniem rozdzielnym względem sumy i różnicy symetrycznej zbiorów, zaś suma zbiorów działaniem rozdzielnym względem iloczynu zbiorów. Jeśli $X \neq \emptyset$, to różnica zbiorów nie jest działaniem łącznym w $\mathcal{P}(X)$. Mamy bowiem $X \setminus (X \setminus X) = X \setminus \emptyset = X$ oraz $(X \setminus X) \setminus X = \emptyset \setminus X = \emptyset$.

Jeśli działanie $\circ$ jest łączne, to wynik tego działania na układzie elementów a_1, a_2, a_3, a_4 nie zależy od rozmieszczenia nawiasów:

$$\begin{array}{lllll} ((a_1 \circ a_2) \circ a_3) \circ a_4 & = & (a_1 \circ (a_2 \circ a_3)) \circ a_4 & = & \\ a_1 \circ ((a_2 \circ a_3) \circ a_4) & = & a_1 \circ (a_2 \circ (a_3 \circ a_4)) & = & (a_1 \circ a_2) \circ (a_3 \circ a_4). \end{array}$$

Jeśli ponadto działanie $\circ$ jest przemienne, to wynik nie zależy od kolejności ustawienia czynników, na przykład:

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

Powyższe spostrzeżenia można łatwo uogólnić na dowolny układ elementów $a_1, \ldots, a_n$. Aby to uczynić, zdefiniujemy wpierw pojęcie iloczynu układu n elementów.

Rozważmy zbiór A z działaniem $\circ$ (niekoniecznie łącznym). Indukcyjnie określimy w A iloczyn dowolnej liczby czynników:

$$\prod_{i=1}^{1} a_i = a_1, \text{ i } \prod_{i=1}^{n+1} a_i = \prod_{i=1}^{n} a_i \circ a_{n+1} \text{ dla } n \in \mathbb{N}_+.$$

Twierdzenie 1.3 *Jeśli $\circ$ jest działaniem łącznym określonym w zbiorze A i $m, n \in \mathbb{N}_+$, to dla dowolnych $a_1, \ldots, a_{m+n} \in A$ zachodzi równość:*

$$\prod_{i=1}^{m} a_i \circ \prod_{j=1}^{n} a_{m+j} = \prod_{i=1}^{m+n} a_i.$$

Dowód. (Indukcja względem n). Dla $n = 1$ teza twierdzenia jest bezpośrednią konsekwencją definicji symbolu $\prod$. Załóżmy prawdziwość twierdzenia dla liczby $n \in \mathbb{N}_+$. Wówczas:

$$\begin{aligned}\prod_{i=1}^{m} a_i \circ \prod_{j=1}^{n+1} a_{m+j} &= \prod_{i=1}^{m} a_i \circ \left(\prod_{j=1}^{n} a_{m+j} \circ a_{m+n+1} \right) = \\ &= \left(\prod_{i=1}^{m} a_i \circ \prod_{j=1}^{n} a_{m+j} \right) \circ a_{m+n+1} = \prod_{i=1}^{m+n} a_i \circ a_{m+n+1} = \prod_{i=1}^{m+n+1} a_i.\end{aligned}$$

■

Z powyższego twierdzenia wynika, że jeśli działanie $\circ$ określone w zbiorze A jest łączne, to wynik tego działania na układzie elementów $a_1, \ldots, a_n$ nie zależy od rozmieszczenia nawiasów, można je więc opuszczać. Pozwala to na stosowanie oznaczenia $a_1 \circ \ldots \circ a_n$ zamiast $\prod_{i=1}^{n} a_i$. W przypadku, gdy $a_1 = \ldots = a_n = a$, piszemy

$$\prod_{i=1}^{n} a_i = a^n.$$

a^n nazywamy n-tą potęgą elementu a. Równoważnie można dla danego działania łącznego określić potęgę o wykładniku naturalnym dodatnim w sposób indukcyjny:

$$a^1 = a, \ a^{n+1} = a^n \circ a.$$

Pozostawiamy Czytelnikowi do sprawdzenia, że dla dowolnych $n, m \in \mathbb{N}_+$ oraz $a \in A$, prawdziwe są równości: $a^m \circ a^n = a^n \circ a^m = a^{m+n}$ oraz $(a^m)^n = (a^n)^m = a^{mn}$.

Łatwo również wykazać, że jeśli działanie $\circ$ określone w zbiorze A jest łączne i przemienne, to dla dowolnych $a, b \in A$ oraz $n \in \mathbb{N}_+$ mamy $(a \circ b)^n = a^n \circ b^n$.

Twierdzenie 1.4 *Jeśli działanie $\circ$ określone w zbiorze A jest łączne i przemienne, $a_1, \ldots, a_n \in A$ oraz σ jest bijekcją zbioru $\{1, \ldots, n\}$ na siebie, to*

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{\sigma(i)}.$$

Oznacza to, że wynik działania $\circ$ na układzie elementów $a_1, \ldots a_n$ nie zależy od kolejności ustawienia elementów.

Dowód. Dla $n = 1$ twierdzenie jest oczywiste. Pokażemy teraz, że prawdziwość twierdzenia dla n czynników implikuje jego prawdziwość dla $n+1$ czynników.

Niech $a_1, \ldots, a_{n+1} \in A$ i niech $\sigma : \{1, \ldots, n+1\} \longrightarrow \{1, \ldots, n+1\}$ będzie bijekcją. Oznaczmy przez k liczbę, dla której $\sigma(k) = n+1$. Rozważymy trzy przypadki. Jeśli $k = 1$, to

$$\prod_{i=1}^{n+1} a_{\sigma(i)} = a_{\sigma(1)} \circ \prod_{i=2}^{n+1} a_{\sigma(i)} = a_{n+1} \circ \prod_{i=2}^{n+1} a_{\sigma(i)} = \prod_{i=2}^{n+1} a_{\sigma(i)} \circ a_{n+1}.$$

Jeśli $1 < k \leq n$, to

$$\prod_{i=1}^{n+1} a_{\sigma(i)} = \prod_{i=1}^{k-1} a_{\sigma(i)} \circ a_{\sigma(k)} \circ \prod_{i=k+1}^{n+1} a_{\sigma(i)} = \prod_{i=1}^{k-1} a_{\sigma(i)} \circ a_{n+1} \circ \prod_{i=k+1}^{n+1} a_{\sigma(i)} = \prod_{i=1}^{k-1} a_{\sigma(i)} \circ \prod_{i=k+1}^{n+1} a_{\sigma(i)} \circ a_{n+1}.$$

Jeśli $k = n+1$, to

$$\prod_{i=1}^{k+1} a_{\sigma(i)} = \prod_{i=1}^{k} a_{\sigma(i)} \circ a_{\sigma(n+1)} = \prod_{i=1}^{k+1} a_{\sigma(i)} \circ a_{n+1}.$$

Definiujemy teraz bijekcję $\tau : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ wzorem

$$\tau(i) = \begin{cases} \sigma(i) & \text{jeśli } \ 1 \leq i < k \\ \sigma(i+1) & \text{jeśli } \ k \leq i \leq n. \end{cases}$$

We wszystkich trzech rozważanych wcześniej przypadkach, na mocy założenia indukcyjnego oraz definicji symbolu iloczynu, otrzymujemy:

$$\prod_{i=1}^{n+1} a_{\sigma(i)} = \prod_{i=1}^{n} a_{\tau(i)} \circ a_{n+1} = \prod_{i=1}^{n} a_i \circ a_{n+1} = \prod_{i=1}^{n+1} a_i.$$

■

Definicja 1.5 *Niech $\circ$ będzie działaniem określonym w zbiorze A. Mówimy, że $\circ$ spełnia:*

(a) lewostronne prawo skracań, jeśli dla dowolnych $a, b, c \in A$, warunek $a \circ b = a \circ c$ implikuje $b = c$,

(b) prawostronne prawo skracań, jeśli dla dowolnych $a, b, c \in A$, warunek $b \circ a = c \circ a$ implikuje $b = c$,

(c) (obustronne) prawo skracań, jeśli $\circ$ spełnia zarówno lewo- jak i prawostronne prawo skracań.

Przykładem działania spełniającego obustronne prawo skracań jest zwykłe dodawanie w każdym ze zbiorów $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Działanie $\circ$ określone w zbiorze liczb naturalnych dodatnich wzorem $m \circ n = m^n$ spełnia prawostronne prawo skracań, ale nie spełnia lewostronnego prawa skracań, gdyż $1 \circ n = 1^n = 1$ dla każdego $n \in \mathbb{N}_+$.

Definicja 1.6 *Niech $\circ$ będzie działaniem określonym w zbiorze A.*

(a) Mówimy, że element $e \in A$ jest elementem neutralnym lewostronnym działania $\circ$, jeśli $e \circ a = a$ dla wszystkich $a \in A$.

(b) Mówimy, że element $e \in A$ jest elementem neutralnym prawostronnym działania $\circ$, jeśli $a \circ e = a$ dla wszystkich $a \in A$.

(c) Mówimy, że element $e \in A$ jest elementem neutralnym (obustronnym) działania $\circ$, jeśli $a \circ e = e \circ a = a$ dla wszystkich $a \in A$.

Oczywiście, jeśli działanie $\circ$ jest przemienne, to pojęcia elementu neutralnego lewostronnego, prawostronnego i obustronnego są sobie równoważne.

Łatwo zauważyć że działanie może mieć tylko jeden element neutralny. Jeśli bowiem e_1, e_2 są elementami neutralnymi działania $\circ$, to wprost z definicji otrzymujemy: $e_1 = e_1 \circ e_2 = e_2$. To samo rozumowanie pokazuje, że jeśli e_1 jest lewostronnym elementem neutralnym działania $\circ$, zaś e_2 prawostronnym elementem neutralnym działania $\circ$, to $e_1 = e_2$.

Poniższa tabelka definiuje działanie w trzyelementowym zbiorze $\{a, b, c\}$ mające dwa elementy neutralne prawostronne.

$\circ$	a	b	c
a	a	a	c
b	b	b	a
c	c	c	b

Podobnie można określić działanie mające dwa elementy neuralne lewostronne.

Z uwagi po definicji 1.6 wynika, że jeśli działanie określone w A ma w zbiorze A co najmniej dwa elementy neutralne lewostronne (prawostronne), to nie posiada ono elementu neutralnego prawostronnego (odpowiednio: lewostronnego).

0 jest elementem neutralnym dla dodawania, zaś 1 elementem neutralnym dla mnożenia w każdym ze zbiorów: $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

Przykładem działania nie posiadającego elementu neutralnego jest dodawanie w zbiorze liczb naturalnych dodatnich. Inny przykład takiego działania rozpatrujemy poniżej.

Przykład 14. W zbiorze liczb rzeczywistych definiujemy działanie $\circ$ wzorem $x \circ y = x^2 + 2y$. $\circ$ nie ma elementu neutralnego. Przypuśćmy bowiem, że a jest elementem neutralnym dla $\circ$. Wtedy $x = x \circ a = x^2 + 2a$ dla każdego $x \in \mathbb{R}$. Stąd dla $x = 0$ dostajemy $a = 0$, zaś dla $x = -1$, $a = -1$. Sprzeczność.

Definicja 1.7 *Niech $\circ$ będzie działaniem określonym w zbiorze A i niech $a, b \in A$.*

(a) Jeśli e_L jest elementem neutralnym lewostronnym działania $\circ$ oraz $b \circ a = e_L$, to b nazywamy elementem odwrotnym lewostronnym do elementu a względem działania $\circ$.

(a) Jeśli e_P jest elementem neutralnym prawostronnym działania $\circ$ oraz $a \circ b = e_P$, to b nazywamy elementem odwrotnym prawostronnym do elementu a względem działania $\circ$.

(c) Jeśli e jest elementem neutralnym (obustronnym) działania $\circ$, to mówimy, że b jest elementem odwrotnym do elementu a (lub odwrotnością elementu a) względem działania $\circ$, jeśli $a \circ b = b \circ a = e$.

Z powyższej definicji natychmiast wynika, że jeśli b jest elementem odwrotnym do a, to a jest elementem odwrotnym do b.

Jeśli $\circ$ jest działaniem przemiennym określonym w zbiorze A i mającym element neutralny e, to b jest elementem odwrotnym do a wtedy i tylko wtedy, gdy $a \circ b = e$.

Jeśli $a \in \mathbb{R}$, to elementem odwrotnym do a względem dodawania jest $-a$, zaś względem mnożenia $\frac{1}{a}$ (pod warunkiem, że $a \neq 0$). Nie istnieje element odwrotny do 0 względem mnożenia.

Łatwo określić działanie z elementem neutralnym, względem którego pewien element posiada dwa elementy odwrotne. Przykład takiego działania w trzyelementowym zbiorze $\{a, b, c\}$ definiuje następująca tabelka.

$\circ$	a	b	c
a	a	b	c
b	b	a	a
c	c	a	a

a jest elementem neutralnym działania $\circ$. Elementami odwrotnymi do b są zarówno b jak i c. Działanie $\circ$ nie jest łączne, gdyż $(b \circ b) \circ c = a \circ c = c$, ale $b \circ (b \circ c) = b \circ a = b$.

Fakt 1.8 *Jeśli $\circ$ jest działaniem łącznym określonym w zbiorze A, mającym element neutralny e, to dowolny element zbioru A posiada co najwyżej jeden element odwrotny względem działania $\circ$.*

Dowód. Niech b_1, b_2 będą elementami odwrotnymi do elementu a względem działania $\circ$. Wtedy

$$b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2.$$

■

Przykład 15. Niech $n \in \mathbb{N}_+$. Pokażemy, że dla liczby $k \in \{0, \ldots, n-1\}$ istnieje w zbiorze $\{0, \ldots, n-1\}$ element odwrotny względem $\cdot_n$ wtedy i tylko wtedy, gdy $NWD(k, n) = 1$.

Jeśli $n = 1$, to 0 jest oczywiście elementem neutralnym względem mnożenia modulo n. Elementem odwrotnym do 0 względem $\cdot_n$ jest w tej sytuacj liczba 0. Dalej zakładamy, że $n > 1$. Wówczas elementem neutralnym w zbiorze $\{0, \ldots, n-1\}$ względem mnożenia modulo n jest 1.

Rozważmy przypadek $NWD(n, k) > 1$. Każda z liczb $0 \cdot_n k, \ldots, (n-1) \cdot_n k$ dzieli się przez $NWD(k, n)$, w szczególności $i \cdot_n k \neq 1$ dla $i \in \{0, \ldots, n-1\}$. Innymi słowy, k nie posiada w $\{0, \ldots, n-1\}$ elementu odwrotnego względem $\cdot_n$.

Przypuśćmy teraz, że $NWD(k, n) = 1$. Jeśli s i t są różnymi liczbami ze zbioru $\{0, \ldots, n-1\}$, to ich różnica nie dzieli się przez n. Z tego, że $NWD(k, n) = 1$ wynika, że $(s-t)k$ nie dzieli się przez n. Innymi słowy $s \cdot_n k \neq t \cdot_n k$. W ten sposób wykazaliśmy, że $0 \cdot_n k, \ldots, (n-1) \cdot_n k$ są różnymi elementami zbioru $\{0, \ldots, n-1\}$, czyli $\{0 \cdot_n k, \ldots, (n-1) \cdot_n k\} = \{0, \ldots, n-1\}$. Stąd wynika, że istnieje $i \in \{0, \ldots, n-1\}$ takie, że $i \cdot_n k = k \cdot_n i = 1$. i jest elementem odwrotnym do k względem mnożenia modulo n. Oczywiście, największym wspólnym dzielnikiem liczb i, n jest 1.

Definicja 1.9 *Załóżmy, że w zbiorze A określone jest działanie n-argumentowe f. Podzbiór $B \subseteq A$ nazywamy zamkniętym względem działania f, jeżeli $f(b_1, \ldots, b_n) \in B$ dla dowolnych $b_1, \ldots, b_n \in B$.*

Zbiór liczb naturalnych, rozpatrywany jako podzbiór $\mathbb{Z}$, jest zamknięty względem dodawania i mnożenia, ale nie jest zamknięty względem odejmowania. Jeśli $n \in \mathbb{N}_+$, to zbiór liczb całkowitych podzielnych przez n jest zamknięty względem dodawania i mnożenia.

Twierdzenie 1.10 *Niech f będzie działaniem n-argumentowym określonym w zbiorze A i niech $B \subseteq A$. Definiujemy indukcyjnie zbiory B_k dla $k \in \mathbb{N}$:*

$$B_0 = B, \; B_{k+1} = B_k \cup \{f(b_1, \ldots, b_n) : b_1, \ldots, b_n \in B_k\}.$$

Wtedy zbiór $B' = \bigcup_{k=0}^{\infty} B_k$ jest najmniejszym podzbiorem zbioru A zawierającym B i zamkniętym względem działania f.

Dowód. Pokażemy najpierw, że zbiór B' jest zamknięty względem działania f. Niech $a_1, \ldots, a_n \in B'$. Wtedy $a_1, \ldots, a_n \in B_k$ dla pewnego $k \in \mathbb{N}$. Stąd wynika, że $f(a_1, \ldots, a_k) \in B_{k+1} \subseteq B'$.

Niech teraz $C \subseteq A$ będzie zbiorem zawierającym B i zamkniętym względem działania f. Pokażemy, że $B' \subseteq C$. W tym celu indukcyjnie udowodnimy, że $B_k \subseteq C$ dla $k \in B_k$. Dla $k = 0$ stwierdzenie to jest oczywiste, ponieważ $B_0 = B$. Przypuśćmy, że $B_k \subseteq C$ i $a \in B_{k+1}$ dla pewnego $k \in \mathbb{N}$. Wtedy $a = f(a_1, \ldots, a_n)$, gdzie $a_1, \ldots, a_n \in B_k \subseteq C$. Ponieważ C jest zamknięty względem działania f, mamy $a = f(a_1, \ldots, a_n) \in C$. Tak więc $B_{k+1} \subseteq C$. ■

W algebrze często rozważa się zbiory z pewną liczbą wyróżnionych działań, czasami również pewną liczbą wyróżnionych relacji czy elementów o pewnych szczególnych własnościach. Na przykład:

(a) zbiór funkcji, odwzorowujących niepusty zbiór X w siebie z działaniem składania przekształceń,

(b) zbiór bijekcji niepustego zbioru X w siebie z działaniem składania przekształceń (oznaczenie: $(S_X, \circ)$),

(c) zbiór liczb całkowitych z działaniami dodawania i mnożenia (oznaczenie: $(\mathbb{Z}, +, \cdot)$),

(d) zbiór liczb zespolonych z działaniami dodawania i mnożenia (oznaczenie: $(\mathbb{C}, +, \cdot)$),

(e) zbiór liczb rzeczywistych z działaniami dodawania i mnożenia oraz z wyróżnionymi elementami 0 i 1 (oznaczenie: $(\mathbb{R}, +, \cdot, 0, 1)$),

(f) zbiór liczb rzeczywistych z działaniami dodawania i mnożenia, z wyróżnionymi elementami 0 i 1 oraz z relacją porządku.

System (a) nazywamy półgrupą odwzorowań zbioru X w siebie, system (b) grupą permutacji zbioru X, system (c) pierścieniem liczb całkowitych, system (d) ciałem liczb zespolonych, system (e) ciałem liczb rzeczywistych z wyróżnionymi elementami 0 i 1, zaś system (f) uporządkowanym ciałem liczb rzeczywistych z wyróżnionymi elementami 0 i 1.

Powyższe przykłady prowadzą do następujących definicji:

Definicja 1.11 *(a) Dowolny niepusty zbiór A z wyróżnionym układem działań n-argumentowych (liczby argumentów odpowiadające różnym działaniom mogą być różne) określonych w A oraz wyróżnionym układem elementów zbioru A nazywamy systemem algebraicznym.*

(b) Dowolny niepusty zbiór A z wyróżnionym układem działań n-argumentowych (liczby argumentów odpowiadające różnym działaniom mogą być różne) określonych w A, wyróżnionym układem elementów zbioru A oraz wyróżnionym układem relacji nazywamy systemem relacyjnym lub strukturą I rzędu.

W powyższej definicji (pkt. (a)) zarówno układ działań jak i układ wyróżnionych elementów mogą być puste. Wobec tego zarówno dowolny niepusty zbiór, w którym nie określiliśmy żadnych działań i nie wyróżniliśmy żadnego elementu, jak i niepusty zbiór z wyróżnionym jednym elementem (ale pustym układem działań) są systemami algebraicznymi. Z drugiej strony, dowolny niepusty zbiór z układem wszystkich działań możliwych do określenia w tym zbiorze i wyróżnionym układem wszystkich swoich elementów jest systemem algebraicznym. Wynika stąd, że pojęcie systemu algebraicznego jest bardzo szerokie i obejmuje wiele przykładów. To samo można powiedzieć o dowolnym systemie relacyjnym. Dalej w zasadzie ograniczymy się do systemów algebraicznych z jednym lub z dwoma działaniami dwuargumentowymi.

Poniżej definiujemy ważną klasę systemów algebraicznych z jednym działaniem dwuargumentowym.

Definicja 1.12 *Zbiór G z działaniem łącznym $\circ$ nazywamy półgrupą i oznaczamy przez $(G, \circ)$. Jeśli dodatkowo działanie $\circ$ posiada element neutralny, to $(G, \circ)$ nazywamy półgrupą z jednością.*

Jak łatwo zauważyć systemy algebraiczne $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ są półgrupami z jednością, zaś $(N_+, +)$ jest półgrupą bez jedności.

Przykład 16. Niech X będzie zbiorem niepustym, zaś G zbiorem funkcji z X w X. G z działaniem składania stanowi półgrupę z jednością. Jej elementem neutralnym jest przekształcenie identycznościowe.

Przykład 17. Niech Σ będzie zbiorem niepustym. Oznaczmy przesz Σ^* zbiór wszystkich ciągów

skończonych o wyrazach ze zbioru Σ, przyjmując przy tym, że Σ^* zawiera tak zwany ciąg pusty (oznaczenie: e). W zbiorze Σ^* definiujemy działanie $*$ (zwane konkatenacją) wzorami:

$$\sigma \circ e = e \circ \sigma = \sigma \text{ dla } \sigma \in \Sigma^*,$$
$$\langle a_1, \ldots, a_m \rangle \cdot \langle b_1, \ldots, b_n \rangle = \langle a_1, \ldots, a_m, b_1, \ldots, b_n \rangle \text{ dla } a_1, \ldots, a_m, b_1, \ldots, b_n \in \Sigma.$$

Oczywiście e jest elementem neutralnym działania $\circ$. Nietrudno przekonać się o tym, że $\circ$ jest działaniem łącznym. Tak więc $(\Sigma^*, \circ)$ jest półgrupą z jednością.

Rozdział 2

Grupy – zagadnienia wstępne

Dla ustalonego $n \in \mathbb{N}_+$, rozpatrzmy zbiór G, którego elementami są wszystkie nieosobliwe przekształcnia przestrzeni $\mathbb{R}^n$ na siebie (tzn. przekształcenia $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ określone wzorem $f(x) = Ax$, gdzie A jest pewną macierzą kwadratową wymiaru $n \times n$ o niezerowym wyznaczniku). Z kursu algebry liniowej wiadomo, że złożenie dwóch nieosobliwych przekształceń liniowych przestrzeni $\mathbb{R}^n$ jest przekształceniem nieosobliwym. Innymi słowy, $f, g \in G$ implikuje, że $f \circ g \in G$. Zatem składanie przekształceń jest działaniem określonym w zbiorze G. Działanie to jest łączne i posiada element neutralny (przekształcenie identycznościowe). Co więcej, dla każdego przekształcenia $f \in G$ istnieje przekształcenie odwrotne $f^{-1} \in G$. Zbiór G z działaniem składania przekształceń stanowi przykład tak zwanej grupy przekształceń.

W niniejszym rozdziale wprowadzimy i omówimy pojęcie grupy będące abstrakcyjnym uogólnieniem grupy przekształceń. Pojęcie to pojawiło się po raz pierwszy w rozważaniach E. Galois[1] dotyczących rozwiązywalności równań piątego stopnia. Grupy są obecnie jednymi z najważniejszych obiektów badań algebry i mają liczne zastosowania w różnych działach matematyki (geometria, analiza) oraz w innych dziedzinach wiedzy (m. in. w fizyce teoretycznej).

Definicja 2.1 *Zbiór G, w którym określone jest działanie $\circ$, nazywamy grupą, jeśli spełnione są następujące warunki:*
(1) działanie $\circ$ jest łączne,
(2) w G istnieje element neutralny względem działania $\circ$,
(3) dla każdego $g \in G$, istnieje w G element odwrotny do g względem działania $\circ$.

Warunki (1)-(3) w powyższej definicji nazywają się aksjomatami teorii grup (lub aksjomatami grupy). Zbiór G z działaniem $\circ$ oznaczamy zazwyczaj przez $(G, \circ)$. Czasami, gdy nie prowadzi to do nieporozumień, piszemy w skrócie G zamiast $(G, \circ)$. Mówimy też, że G jest grupą względem działania $\circ$. Oczywiście dowolna grupa jest półgrupą z jednością. Działanie w grupie na ogół nie jest przemienne.

Definicja 2.2 *Grupę $(G, \circ)$ nazywamy abelową[2] lub przemienną, jeśli działanie $\circ$ jest przemienne.*

Z rozważań rozdziału pierwszego wynika, że w dowolnej grupie $(G, \circ)$ istnieje dokładnie jeden element neutralny względem działania $\circ$ (patrz str. 16). Element taki będziemy nazywać krótko elementem neutralnym grupy $(G, \circ)$ lub jednością grupy $(G, \circ)$. Dla każdego elementu $g \in G$, istnieje w G dokładnie jeden element odwrotny do g względem działania $\circ$ (fakt 1.8).

Działanie w grupie oznacza się często symbolem $\cdot$ i nazywa mnożeniem. Wynik tego działania na parze $\langle a, b\rangle$ zapisujemy wtedy jako $a \cdot b$ lub ab. Powyższa nazwa działania i jego zapis, zwany multyplikatywnym, stosowane są w przypadku, gdy mówimy o grupach w ogóle oraz w przypadku grup nieabelowych Element neutralny w grupie G oznaczamy wówczas przez e_G lub po prostu przez

[1] Evariste Galois (1811-1832), matematyk francuski
[2] Niels Henrik Abel (1802-1829), matematyk norweski

e, zaś element odwrotny do g przez g^{-1}. Terminologia związana z tego rodzaju zapisem nazywa się multyplikatywną.

Działanie w grupie abelowej najczęściej oznacza się symbolem $+$ i nazywa dodawaniem. Element neutralny w tym przypadku oznaczamy symbolem 0_G (lub 0), zaś element odwrotny do a względem $+$ symbolem $-a$ (mówimy, że $-a$ jest elementem przeciwnym do a). Zamiast $a+(-b)$ piszemy $a-b$. Taka terminologia nazywa się addytywną. Rzecz jasna, wybór takiej, czy innej terminologii nie ma żadnego wpływu na treść teorii.

Jeśli $(G,\circ)$ jest grupą, to moc zbioru G (oznaczenie: $|G|$) nazywamy rzędem grupy G. Na przykład o grupie 8-elementowej mówimy, że jest to grupa rzędu 8. Grupy rzędu n dla $n\in\mathbb{N}_+$ nazywamy skończonymi. Grupy rzędu $\aleph_0$ nazywamy przeliczalnymi, zaś rzędu większego od $\aleph_0$ nieprzeliczalnymi.

Udowodnimy teraz kilka prostych własności działań w grupach.

Twierdzenie 2.3 *Niech $(G,\circ)$ będzie grupą i niech $a,b\in G$. Wtedy:*
(a) $e_G^{-1}=e_G$,
(b) $(a^{-1})^{-1}=a$,
(c) $(a\circ b)^{-1}=b^{-1}\circ a^{-1}$,

Dowód. Równość (a) wynika z równości $e_G\circ e_G=e_G$. W celu wykazania (b), zauważmy, że: $a\circ a^{-1}=a^{-1}\circ a=e_G$. Wynika stąd, że a jest elementem odwrotnym do a^{-1}, czyli $(a^{-1})^{-1}=a$.

Równości $b^{-1}\circ a^{-1}\circ a\circ b=b^{-1}\circ e_G\circ b=e_G$ oraz $a\circ b\circ b^{-1}\circ a^{-1}=a\circ e_G\circ a^{-1}=e_G$ pokazują, że $b^{-1}\circ a^{-1}$ jest elementem odwrotnym do elementu $a\circ b$, a więc prawdziwa jest równość (c). ■

Jeśli $(G,\circ)$ jest grupą abelową i $a,b\in G$, to $(a\circ b)^{-1}=a^{-1}\circ b^{-1}$. W terminologii addytywnej równości (a),(b) i (c) twierdzenia 2.3 zapisuje się następująco: $-0=0$, $-(-a)=a$ i $-(a+b)=(-b)+(-a)$.

Z powyższego twierdzenia łatwo można wywnioskować, że dla dowolnych elementów $a_1,\ldots,a_n$ grupy $(G,\circ)$ zachodzi równość $(a_1\circ\ldots\circ a_n)^{-1}=a_n^{-1}\circ\ldots\circ a_1^{-1}$. Indukcyjny dowód tego faktu pozostawiamy Czytelnikowi jako ćwiczenie. W zapisie addytywnym ostatnia równość przyjmuje postać $-(a_1+\ldots+a_n)=(-a_n)+\ldots+(-a_1)$.

Twierdzenie 2.4 *Niech $(G,\circ)$ będzie grupą.*
(a) Działanie $\circ$ spełnia obustronne prawo skracań.
(b) Jeśli $a,b\in G$, to każde z równań: $a\circ x=b$ i $y\circ a=b$ posiada jednoznaczne rozwiązanie w G.

Dowód. (a) Załóżmy, że $a\circ b=a\circ c$ dla pewnych $a,b,c\in G$. Mnożąc tę równość lewostronnie przez a^{-1} otrzymujemy $a^{-1}\circ(a\circ b)=a^{-1}\circ(a\circ c)$. Wobec łączności działania $\circ$ wynika stąd, że $e_G\circ b=e_G\circ c$, czyli $b=c$. Tym samym udowodniliśmy lewostronne prawo skracań dla działania $\circ$. Dowód prawostronnego prawa skracań jest podobny.

(b) Łatwo zauważyć, że elementy $x_0=a^{-1}\circ b$ oraz $y_0=b\circ a^{-1}$ są rozwiązaniami równań $a\circ x=b$ i $y\circ a=b$ (odpowiednio). Jeśli x_1 jest dowolnym rozwiązaniem pierwszego równania, to $a\circ x_1=a\circ x_0$, skąd na mocy (a) dostajemy $x_1=x_0$. Analogiczne dowodzimy jednoznaczności rozwiązania w przypadku drugiego równania. ■

Niech $(G,\circ)$ będzie grupą. Indukcyjnie definiujemy potęgę elementu $g\in G$ o wykładniku całkowitym. g^{-1} oznacza jak zwykle element odwrotny do g.

$$\begin{aligned} g^0 &= e_G,\\ g^{n+1} &= g^n\circ g \text{ dla } n\in\mathbb{N},\\ g^{-n} &= (g^{-1})^n \text{ dla } n\in\mathbb{N}_+. \end{aligned}$$

Pozostawiamy Czytelnikowi do wykazania (metodą indukcji matematycznej) następujące twierdzenie.

Twierdzenie 2.5 *Jeśli g i h są elementami grupy G, to dla dowolnych $m, n \in \mathbb{Z}$ prawdziwe są równości:*
(a) $g^m g^n = g^n g^m = g^{m+n}$,
(b) $(g^m)^n = (g^n)^m = g^{mn}$,
(c) Jeśli $gh = hg$, *to* $(gh)^n = g^n h^n$.

W terminologii addytywnej piszemy ng zamiast g^n. Wówczas trzy powyższe równości przyjmują postać: $mg + ng = ng + mg = (m+n)g$, $n(mg) = m(ng) = (mn)g$ i $n(g+h) = ng + nh$.

Poniżej omawiamy krótko kilkanaście przykładów grup.

Przykład 1. $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ są grupami abelowymi ($+$ oznacza tutaj zwykłe dodawanie liczb). W każdej z wymienionych grup elementem neutralnym jest liczba 0. $-a$ jest elementem odwrotnym do a względem dodawania.

Przykład 2. $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Q}_+, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{R}_+, \cdot)$, $(\mathbb{C} \setminus \{0\})$ są grupami abelowymi ($\cdot$ oznacza tutaj zwykłe mnożenie liczb). Liczba 1 jest elementem neutralnym w każdej z wymienionych grup. Elementem odwrotnym do a jest $\frac{1}{a}$. Żaden ze zbiorów $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ z mnożeniem nie stanowi grupy, gdyż nie istnieje element odwrotny do 0 względem mnożenia.

Przykład 3. Jeśli $(V, +)$ jest przestrzenią liniową nad $\mathbb{R}$, to $(V, +)$ jest grupą abelową. Elementem neutralnym tej grupy jest wektor zerowy, zaś elementem odwrotnym do danego wektora x, wektor przeciwny do x (oznaczenie: $-x$).

Przykład 4. Ustalmy $m, n \in \mathbb{N}_+$. Zbiór macierzy wymiaru $m \times n$ o wyrazach rzeczywistych (oznaczenie: $M_{m\times n}(\mathbb{R})$) stanowi grupę abelową względem dodawania macierzy. Jednością tej grupy jest macierz zerowa.

Przykład 5. Niech $n \in \mathbb{N}_+$. Zbiór macierzy kwadratowych wymiaru $n \times n$ o wyrazach rzeczywistych i wyznaczniku różnym od 0 (oznaczenie: $GL(n, \mathbb{R})$) z działaniem mnożenia macierzy stanowi grupę. Jednością grupy $GL(n, \mathbb{R})$ jest macierz identycznościowa. Elementem odwrotnym do macierzy M jest macierz odwrotna do M (dla macierzy o wyznaczniku różnym od 0 istnieje macierz odwrotna, również o wyznaczniku niezerowym). Zamkniętość zbioru $GL(n, \mathbb{R})$ względem mnożenia macierzy wynika ze wzoru na wyznacznik iloczynu macierzy kwadratowych wymiaru $n \times n$: $det(M_1 \cdot M_2) = det(M_1) \cdot det(M_2)$. Tak więc, jeśli $M_1, M_2 \in GL(n, \mathbb{R})$, to $det(M_1) \neq 0$ i $det(M_2) \neq 0$, a stąd $det(M_1 \cdot M_2) \neq 0$, co oznacza, że $M_1 \cdot M_2 \in GL(n, \mathbb{R})$.

Grupę $GL(n, \mathbb{R})$ nazywamy pełną grupą liniową (ang. general linear group). $GL(n, \mathbb{R})$ jest grupą abelową wtedy i tylko wtedy, gdy $n = 1$.

Przykład 6. Zbiór macierzy kwadratowych wymiaru $n \times n$ o wyrazach rzeczywistych i wyznaczniku równym 1 stanowi grupę względem mnożenia macierzy. Grupę tę oznaczamy przez $SL(n, \mathbb{R})$ i nazywamy specjalną grupą liniową (ang.: special linear group).

Przykład 7. Jeśli $n \in \mathbb{N}_+$, to zbiór $\mathbb{Z}_n = \{0, \ldots, n-1\}$ z działaniem dodawania modulo n (oznaczenie: $(\mathbb{Z}_n, +_n)$) jest grupą abelową zwaną grupą reszt modulo n. Elementem neutralnym tej grupy jest 0. Elementem odwrotnym do 0 jest oczywiście 0, zaś elementem odwrotnym do $k \in \mathbb{Z}_n \setminus \{0\}$ (dla $n > 1$) względem dodawania modulo n jest $n - k$.

Przykład 8. Niech $n \in \mathbb{N}_+$. Wtedy zbiór $\{x \in \mathbb{C} : x^n = 1\}$ jest grupą względem mnożenia liczb

zespolonych. Grupę tę nazywamy grupą zespolonych pierwiastków z jedności stopnia n.

Przykład 9. Niech p będzie liczbą pierwszą. Pokażemy, że wtedy zbiór $\mathbb{Z}_p \setminus \{0\} = \{1, \ldots, p-1\}$ jest grupą abelową względem mnożenia modulo p.

Jeśli $a, b \in \mathbb{Z}_p \setminus \{0\}$, to liczby a, b nie dzielą się przez p, a więc również ich iloczyn nie dzieli się przez p (p jest liczbą pierwszą). Stąd $a \cdot_p b = (a \cdot b) \bmod p \neq 0$, czyli $a \cdot_p b \in \mathbb{Z}_p \setminus \{0\}$. Tak więc $\cdot_p$ jest działaniem w $\mathbb{Z}_p \setminus \{0\}$.

Oczywiście 1 jest elementem neutralnym działania $\cdot_p$ w $\mathbb{Z}_p \setminus \{0\}$. Działanie $\cdot_p$ jest łączne i przemienne w $\mathbb{Z}_p \setminus \{0\}$. Ponieważ $NWD(k, p) = 1$ dla dowolnego $k \in \mathbb{Z}_p \setminus \{0\}$, z przykładu 15 ze strony 17 wynika, że każdy element zbioru $\mathbb{Z}_p \setminus \{0\}$ posiada w $\mathbb{Z}_p \setminus \{0\}$ element odwrotny względem mnożenia modulo p.

Przykład 10. (Uogólnienie poprzedniego przykładu) Niech $n \in \mathbb{N}_+$. Przyjmijmy oznaczenie:

$$G(n) = \{k \in \mathbb{Z}_n : NWD(k, n) = 1\}.$$

Używając przykładu 15 ze strony 17 nietrudno wykazać, że $(G(n), \cdot_n)$ jest grupą. Rząd tej grupy oznacza się zazwyczaj przez $\varphi(n)$. Na przykład $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$. Jeśli p jest liczbą pierwszą, to $\varphi(p) = p - 1$. Określona wyżej funkcję $\varphi : \mathbb{N}_+ \longrightarrow \mathbb{N}_+$ zwana jest funkcją Eulera.[3]

Przykład 11. Jeśli X jest dowolnym zbiorem, to $\mathcal{P}(X)$ (zbiór wszystkich podzbiorów zbioru X) stanowi grupę abelową względem różnicy symetrycznej zbiorów. Elementem neutralnym w grupie $(\mathcal{P}(X), \triangle)$ jest zbiór pusty. Dla każdego $A \subseteq X$, mamy: $A \triangle A = \emptyset$, co oznacza, że A jest elementem odwrotnym do samego siebie względem działania $\triangle$.

Przykład 12. Niech $K_4 = \{e, a, b, c\}$, gdzie elementy a, b, c, e są różne. Poniższa tabelka definiuje działanie $\circ$ w zbiorze K_4.

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$(K_4, \circ)$ jest grupą zwaną grupą czwórkową Kleina[4]. e jest elementem neutralnym w $(K_4, \circ)$. Ponadto każdy element z K_4 jest odwrotny do samego siebie.

Przykład 13. Niech I, A, B, C oznaczają macierze o wyrazach zespolonych zdefiniowane następująco:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, C = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

$Q_8 = \{I, -I, A, -A, B, -B, C, -C\}$ z działaniem mnożenia macierzy stanowi grupę. Grupę tę nazywamy grupą kwaternionów.

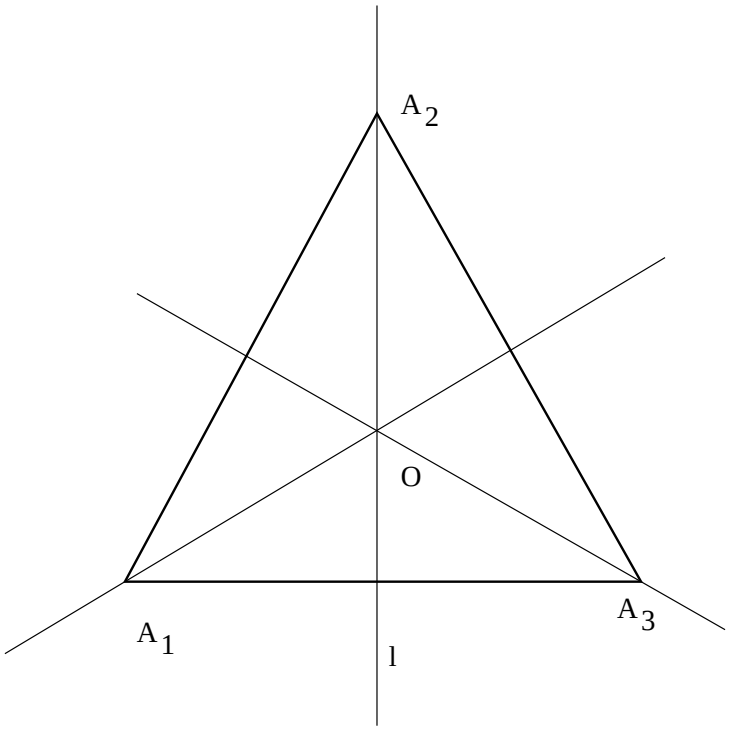
Przykład 14. Niech X będzie zbiorem niepustym. Przez S_X oznaczamy zbiór wszystkich wzajem-

[3] Leonhard Euler (1707-1783), matematyk niemiecki
[4] Felix Klein (1849-1925), matematyk niemiecki

nie jednoznacznych przekształceń zbioru X na siebie (tzn. zbiór bijekcji ze zbioru X na X). Ponieważ złożenie dwóch bijekcji stanowi bijekcję, składanie odwzorowań jest działaniem w S_X. Co więcej, S_X stanowi grupę względem składania odwzorowań. Grupę tę nazywamy grupą permutacji zbioru X lub grupą symetryczną zbioru X. Jeśli $X = \{1, \ldots, n\}$ $(n \in \mathbb{N}_+)$, to stosujemy oznaczenie: $S_X = S_n$. Elementem neutralnym w S_X jest przekształcenie identycznościowe zbioru X na siebie. Elementem edwrotnym do funkcji $f \in S_X$ jest funkcja odwrotna do f. Grupy permutacji omówimy dokładniej w rozdziale trzecim. Można wykazać, że S_X jest grupą abelową wtedy i tylko wtedy, gdy zbiór X ma co najwyżej 2 elementy.

Przykład 15. Niech A będzie pewnym podzbiorem $\mathbb{R}^n$. Oznaczmy przez G zbiór izometrii własnych zbioru A, to znaczy zbiór bijekcji zbioru A na siebie zachowujących odległość punktów. G z działaniem składania przekształceń stanowi grupę. Grupę tę nazywamy grupą izometrii własnych zbioru A.

Przykład 16. Opiszemy teraz szczegółowo grupę izometrii własnych trójkąta równobocznego. Rozważmy trójkąt równoboczny $A_1A_2A_3$ na płaszczyźnie. Przyjmijmy oznaczenia:
l : symetralna odcinka A_1A_3,
O : punkt przecięcia się wysokości trójkąta $A_1A_2A_3$,
S : symetria osiowa $\triangle A_1A_2A_3$ względem prostej l,
R : obrót $\triangle A_1A_2A_3$ wokół punktu O o kąt 120^o,
I : przekształcenie identycznościowe $\triangle A_1A_2A_3$.



Z elementarnej geometrii wiadomo, że:

(a) dowolna izometria własna trójkąta równobocznego przeprowadza zbiór jego wierzchołków na siebie, innymi słowy, dokonuje ona pewnej permutacji wierzchołków tegoż trójkąta,

(b) każda permutacja zbioru wierzchołków $\{A_1, A_2, A_3\}$, jednoznacznie określa pewną izometrię własną $\triangle A_1A_2A_3$.

Ponieważ istnieje dokładnie 6 permutacji zbioru trzyelementowego, grupa izometrii własnych $\triangle A_1A_2A_3$ ma rząd równy 6.

Następujące obliczenia wykonujemy w celu opisania poszczególnych izometrii $\triangle A_1A_2A_3$ w terminach przekształceń I, R, S.

$$
\begin{aligned}
&I(A_i) = A_i \text{ dla } i \in \{1,2,3\},\\
&R(A_1) = A_3, R(A_2) = A_1, R(A_3) = A_2,\\
&S(A_1) = A_3, S(A_2) = A_2, S(A_3) = A_1,\\
&R^2(A_1) = R(R(A_1)) = R(A_3) = A_2, R^2(A_2) = A_3, R^2(A_3) = A_1,\\
&S^2(A_i) = R^3(A_i) = A_i \text{ dla } i \in \{1,2,3\},\\
&(RS)(A_1) = (R \circ S)(A_1) = R(S(A_1)) = R(A_3) = A_2, (RS)(A_2) = A_1, (RS)(A_3) = A_3,\\
&(R^2S)(A_1) = R^2(S(A_1)) = R^2(A_3) = A_1, (R^2S)(A_2) = A_3, (R^2S)(A_1) = A_2.
\end{aligned}
$$

Zauważmy ponadto, że $(SR)(A_1) = A_1$, $(SR)(A_2) = A_3$, $(SR)(A_3) = A_2$. Oznacza to, że $SR = R^2S$. Stąd dostajemy

$$SR^2 = (S \circ R) \circ R = R^2 \circ S \circ R = R^2 \circ R^2 \circ S = R^3 \circ RS = RS.$$

W poniższej tabelce zostały zebrane wyniki przeprowadzonych wyżej obliczeń. P oznacza izometrię trójkąta $A_1A_2A_3$.

$P(A_1)$	$P(A_2)$	$P(A_3)$	Opis
A_1	A_2	A_3	$I = R^3 = S^2$
A_1	A_3	A_2	$R^2S = SR$
A_2	A_1	A_3	$RS = SR^2$
A_2	A_3	A_1	R
A_3	A_1	A_2	R^2
A_3	A_2	A_1	S

Wyprowadzone zależności pozwalają na sporządzenie tabelki działania w grupie izometrii własnych $\triangle A_1A_2A_3$.

$\circ$	I	R	R^2	S	RS	R^2S
I	I	R	R^2	S	RS	R^2
R	R	R^2	I	RS	R^2S	S
R^2	R^2	I	R	R^2S	S	RS
S	S	R^2S	RS	I	R^2	R
RS	RS	S	R^2S	R	I	R^2
R^2S	R^2S	RS	S	R^2	R	I

Dla przykładu wyliczymy złożenie:

$$R^2S \circ RS = R^2 \circ (S \circ R) \circ S = R^2 \circ R^2 \circ S \circ S = R^3 \circ R \circ S^2 = R.$$

Grupa izometrii własnych trójkąta równobocznego $A_1A_2A_3$ nie jest abelowa, gdyż $RS \neq SR$.

Przykład 17. Uogólniając rozważania zawarte w poprzednim przykładzie, opiszemy grupę izometrii własnych n-kąta foremnego. Niech $A_1, A_2, \ldots, A_n$ $(n \geq 3)$ będą kolejnymi wierzchołkami n-kąta foremnego zawartego w pewnej ustalonej płaszczyźnie. Przyjmijmy oznaczenia:
l : symetralna odcinka A_1A_n,
O : środek okręgu opisanego na wielokącie $A_1 \ldots A_n$,
S : symetria osiowa wielokąta $A_1 \ldots A_n$ względem prostej l,
R : obrót wielokąta $A_1 \ldots A_n$ wokół punktu O o kąt $\frac{360^o}{n}$,
I : przekształcenie identycznościowe wielokąta $A_1 \ldots A_n$.
Dla dowolnego $i \in \{1, \ldots n\}$ mamy:

$$S(A_i) = A_{n-i+1} \text{ oraz } R(A_i) = \begin{cases} A_{i-1} & \text{gdy } \ i \neq 1, \\ A_n & \text{gdy } \ i = 1. \end{cases}$$

Jest jasne, że $R^n = S^2 = I$.

Z elementarnej geometrii wiadomo, że:

(a) każda izometria własna n-kąta foremnego $A_1 \ldots A_n$ przeprowadza zbiór $\{A_1, \ldots, A_n\}$ na siebie,

(b) w dowolnej izometrii własnej wielokąta foremnego, obrazem wierzchołków sąsiednich są wierzchołki sąsiednie.

(c) przyporządkowanie ustalonej parze uporządkowanej wierzchołków sąsiednich wielokąta foremnego $A_1 \ldots A_n$ dowolnej pary uporządkowanej wierzchołków sąsiednich tegoż wielokąta jednoznacznie określa izometrię wielokąta $A_1, \ldots, A_n$.

Uporządkowaną parę wierzchołków sąsiednich n-kąta foremnego można wybrać na $2n$ sposobów. Oznacza to, że grupa izometrii własnych n-kąta foremnego (oznaczenie: D_n) ma rząd $2n$ (na przykład grupa izometrii własnych kwadratu składa się z 8 elementów). Elementami tymi są $I, R, \ldots, R^{n-1}$ oraz $S, RS, \ldots, R^{n-1}S$ (wypisane elementy są różne na mocy prawa skracań).

Pokażemy teraz indukcyjnie, że dla każdego $k \in \mathbb{N}$, w grupie D_n prawdziwa jest zależność:

$$(*)_k \ SR^k = R^{n-k}S.$$

Równość $(*)_0$ jest oczywista. Zauważmy, że jeśli $i \in \{2, \ldots, n\}$, to

$$\begin{aligned} (SR)(A_i) &= S(R(A_i)) = S(A_{i-1}) = A_{(n+1)-(i-1)} = A_{n-i+2} \text{ oraz} \\ (R^{n-1}S)(A_i) &= R^{-1}(S(A_i)) = R^{-1}(A_{n-i+1}) = A_{n-i+2}. \end{aligned}$$

Ponadto

$$(SR)(A_1) = S(R(A_1)) = S(A_n) = A_1 \text{ oraz } (R^{n-1}S)(A_1) = R^{-1}(S(A_1)) = R^{-1}(A_n) = A_1.$$

Zatem $SR = R^{n-1}S = R^{-1}S$. Przypuśćmy teraz, że prawdziwa jest równość $(*)_k$. Wtedy

$$SR^{k+1} = SR^k \circ R = R^{n-k} \circ S \circ R = R^{n-k} \circ R^{-1}S = R^{n-(k+1)}S,$$

co oznacza, że prawdą jest również $(*)_{k+1}$.

Przykład 18. Niech $(G, \circ)$ i $(H, *)$ będą grupami. W zbiorze $G \times H$ definiujemy działanie $\odot$

wzorem:

$$\langle a, b\rangle \odot \langle c, d\rangle = \langle a \circ c, b * d\rangle.$$

$G \times H$ z tak określonym działaniem jest grupą.

Istotnie, elementem neutralnym działania $\odot$ jest $\langle e_G, e_H\rangle$; elementem odwrotnym do $\langle a, b\rangle$ jest $\langle a^{-1}, b^{-1}\rangle$. Z łączności działań $\circ$ i $*$ wynika łączność działania $\odot$.

Łatwo też wykazać, że jeśli grupy $(G, \circ)$ i $(H, *)$ są abelowe, to grupa $(G \times H, \odot)$ jest abelowa.

Definicja 2.6 *Grupę zdefiniowaną w powyższym przykładzie oznaczamy przez $G \oplus H$ i nazywamy sumą prostą grup G i H. Analogicznie definiuje się sumę prostą dowolnej skończonej liczby grup.*

Definicja 2.7 *Niech G będzie grupą i niech $a \in G$. Jeśli $a^n \neq e$ dla wszystkich $n \in \mathbb{N}_+$, to mówimy, że a jest elementem rzędu niekończonego (piszemy wtedy: $rz(a) = \infty$). W przeciwnym wypadku rzędem elementu a nazywamy najmniejszą liczbę naturalną dodatnią taką, że $a^n = e$ (fakt ten zapisujemy w postaci: $rz(a) = n$).*

Element neutralny w dowolnej grupie ma rząd równy 1. Każdy niezerowy element w grupie $(\mathbb{Z}, +)$ ma rząd nieskończony. W grupie $(\mathbb{Z}_6, +_6)$ element 4 ma rząd 3. Mamy bowiem: $4 \neq 0$, $4 +_6 4 = 2 \neq 0$ i $4 +_6 4 +_6 4 = 0$.

Fakt 2.8 *Jeśli a jest elementem rzędu $n \in \mathbb{N}_+$ w grupie G, to dla dowolnego $k \in \mathbb{Z}$,*

$$a^k = e \iff n|k.$$

Dowód. Niech a będzie elementem rzędu n w grupie G. Wtedy $a^n = e$. Dla dowodu implikacji $\Longrightarrow$ załóżmy nie wprost, że k jest liczbą całkowitą, dla której $a^k = e$, ale k nie dzieli się przez n. Wtedy $sn < k < (s+1)n$ dla pewnego $s \in \mathbb{Z}$, skąd wynika, że $k - sn$ jest liczbą naturalną dodatnią mniejszą od n. Zauważmy, że: $a^{k-sn} = a^k(a^n)^{-s} = ee^{-s} = e$. Tak więc $\mathrm{rz}(a) \leq k - sn < n$. Sprzeczność.

Przypuśćmy teraz, że n dzieli k. Wtedy $k = nl$ dla pewnego $l \in \mathbb{Z}$. Stąd $a^k = a^{nl} = (a^n)^l = e^l = e$. ■

Twierdzenie 2.9 *Niech G będzie dowolną grupą i niech $a, b \in G$ będą elementami takimi, że $ab = ba$. Jeśli $rz(a) = m \in \mathbb{N}_+$, $rz(b) = n \in \mathbb{N}_+$ i $NWD(m, n) = 1$, to $rz(ab) = mn$.*

Dowód. Niech $a, b \in G$ spełniają założenia twierdzenia. Ponieważ $ab = ba$, dla dowolnego $k \in \mathbb{N}_+$ zachodzi równość: $(ab)^k = a^k b^k$. Z założenia $a^m = b^n = e$, więc $(ab)^{mn} = a^{mn}b^{mn} = (a^m)^n(b^n)^m = e$. To zaś oznacza, że rząd elementu ab jest skończony i nie większy od mn. Aby zakończyć dowód twierdzenia, pokażemy, że $\mathrm{rz}(ab) \geq mn$.

Niech $k = \mathrm{rz}(ab)$. Wtedy $(ab)^k = e$, czyli

$$(*)\ a^k b^k = e.$$

Podnosząc obie strony tej równości do potęgi n dostajemy $a^{nk}b^{nk} = e$, ale $b^{nk} = (b^n)^k = e$, więc $a^{nk} = e$. a jest elementem rzędu m, zatem na mocy faktu 2.8, $m|nk$. Wiemy, że $NWD(m, n) = 1$, więc $m|k$. Podobnie, podnosząc obie strony równości $(*)$ do potęgi m pokazujemy, że n dzieli k. Liczby m i n są względnie pierwsze, więc mn dzieli k. Stąd zaś wynika, że $k = \mathrm{rz}(ab) \geq mn$. ■

Rozdział 3

Grupy permutacji

Przypomnijmy, że permutacją niepustego zbioru X nazywamy dowolną bijekcję odwzorowującą zbiór X na siebie. Zbiór wszystkich permutacji zbioru X (oznaczenie: S_X) stanowi grupę względem składania przekształceń (przyklad 14, strona 23). Elementem neutralnym w grupie S_X jest przekształcenie identycznościowe. Będziemy je oznaczać przez e.

W niniejszym rozdziale zajmiemy się grupami permutacji zbiorów skończonych. Niech X będzie zbiorem n-elementowym ($n \in \mathbb{N}$). Ponieważ natura elementów tego zbioru nie będzie odgrywała w rozpatrywanych tu zagadnieniach żadnej roli, możemy uważać, że są to liczby $1, \ldots, n$. Grupę permutacji zbioru $\{1, \ldots, n\}$ (zwaną też n-tą grupą symetryczną) będziemy oznaczali przez S_n, zaś elementy tej grupy (najczęściej) małymi literami greckimi.

Jak wiadomo z elementarnej kombinatoryki, liczba permutacji zbioru n-elementowego wynosi $n!$. Oznacza to że S_n jest grupą rzędu $n!$.

Dowód poniższego faktu pozostawiamy jako proste ćwiczenie dla Czytelnika.

Fakt 3.1 *Niech X będzie niepustym zbiorem skończonym i niech $\sigma : X \longrightarrow X$. Wtedy następujące warunki są równoważne.*

(a) σ jest permutacją zbioru X.

(b) σ jest injekcją.

(c) σ jest surjekcją.

Tak więc S_n jest zbiorem wszystkich funkcji różnowartościowych ze zbioru $\{1, \ldots, n\}$ w siebie.

Permutację $\sigma \in S_n$ wygodnie jest zapisać w tak zwanej postaci tabelarycznej (dwuwierszowej):

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}.$$

W pierwszym wierszu występują tu wszystkie liczby od 1 do n, w drugim zaś pod liczbą $j \in \{1, \ldots, n\}$ występuje przyporządkowana jej liczba $\sigma(j)$. Ciąg $\langle a_1, \ldots, a_n \rangle$ różni się od ciągu $\langle 1, \ldots, n \rangle$ co najwyżej porządkiem. W tym zapisie permutacji nie gra roli porządek wyrazów w pierwszym rzędzie. Rozważmy na przykład permutację $\sigma \in S_4$ określoną wzorami: $\sigma(1) = 3$, $\sigma(2) = 4$, $\sigma(3) = 2$, $\sigma(4) = 1$. Wówczas można zapisać:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 & 3 & 2 \\ 3 & 1 & 2 & 4 \end{pmatrix}.$$

Oczywiście każdą permutację zbioru $\{1, \ldots, n\}$ można przedstawić w postaci dwuwierszowej na $n!$ sposobów.

Niech będą dane dwie permuacje $\sigma, \tau \in S_n$. Permutację $\varrho \in S_n$ określoną wzorem $\varrho(j) = \sigma(\tau(j))$ dla $j \in \{1, \ldots, n\}$ będziemy oznaczać przez $\sigma \circ \tau$ (lub po prostu przez $\sigma\tau$) i nazywać superpozycją (złożeniem) permutacji τ i σ.

W postaci dwuwierszowej złożenie permutacji σ, τ zapisujemy jako:

$$\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & \sigma(\tau(n)) \end{pmatrix}.$$

Na przykład dla $\sigma = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 3\ 2\ 1 \end{pmatrix}$ i $\tau = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 2\ 1\ 3 \end{pmatrix}$ mamy

$$\sigma\tau = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 3\ 2\ 1 \end{pmatrix} \circ \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 2\ 1\ 3 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 1\ 3\ 4\ 2 \end{pmatrix}.$$

Permutacja τ (po prawej stronie) przeprowadza 3 na 1, zaś σ przeprowadza 1 na 4. Tak więc $\sigma\tau$ przeprowadza 3 na 4. Składanie permutacji na ogół nie jest przemienne:

$$\tau\sigma = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 2\ 1\ 3 \end{pmatrix} \circ \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 3\ 2\ 1 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 1\ 2\ 4 \end{pmatrix} \neq \sigma\tau.$$

Permutację odwrotną do permutacji $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$ zapisujemy jako $\sigma^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ 1 & 2 & \dots & n \end{pmatrix}$, na przykład dla $\sigma = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 3\ 6\ 4\ 2\ 5\ 1 \end{pmatrix} \in S_6$ mamy

$$\sigma^{-1} = \begin{pmatrix} 3\ 6\ 4\ 2\ 5\ 1 \\ 1\ 2\ 3\ 4\ 5\ 6 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3\ 4\ 5\ 6 \\ 6\ 4\ 1\ 3\ 5\ 2 \end{pmatrix}.$$

Permutacja σ określona powyżej spełnia warunki: $\sigma(1) = 3$, $\sigma(3) = 4$, $\sigma(4) = 2$, $\sigma(2) = 6$, $\sigma(6) = 1$ i $\sigma(5) = 5$. Takie permutacje nazywać będziemy cyklami lub permutacjami cyklicznymi.

Definicja 3.2 *Niech $a_1, \dots, a_k$ będzie układem k różnych liczb ze zbioru $\{1, \dots, n\}$ $(2 \leq k \leq n)$. Permutację $\sigma \in S_n$ spełniającą warunki:*
$\sigma(a_j) = a_{j+1}$ dla $j \in \{1, \dots, k-1\}$,
$\sigma(a_k) = a_1$ oraz
$\sigma(i) = i$ dla $i \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$
nazywamy cyklem k-wyrazowym lub cyklem długości k i zapisujemy jako $\sigma = (a_1, \dots, a_k)$ pomijając w zapisie wyrazy, które przechodzą na siebie.

Używając wprowadzonej notacji, każdy cykl długości k można zapisać na k sposobów. Na przykład permutacja $\sigma = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 4\ 2\ 1\ 3 \end{pmatrix} \in S_4$ jest cyklem długości 3 i możemy zapisać ją jako:

$$\sigma = (1, 4, 3) = (4, 3, 1) = (3, 1, 4).$$

Oczywiście $(1, 3, 4) \neq (1, 4, 3)$, gdyż $(1, 3, 4) = \begin{pmatrix} 1\ 2\ 3\ 4 \\ 3\ 2\ 4\ 1 \end{pmatrix} \neq \sigma$.

Cykl długości 2 nazywamy transpozycją. Jeśli $\sigma = (a_1, a_2)$, to mówimy, że σ jest transpozycją elementów a_1 i a_2. Oczywiście $(a_1, a_2) = (a_2, a_1)$.

Czytelnik z łatwością sprawdzi, że

$$S_1 = \{e\}, S_2 = \{e, (1,2)\} \text{ i } S_3 = \{e, (1,2), (2,3), (1,3), (1,2,3), (1,3,2)\}.$$

Nietrudno przekonać się o tym, że grupy S_1 i S_2 są abelowe. Dla $n \geq 3$, grupa S_n nie jest abelowa, ponieważ:

$$(1,2) \circ (2,3) = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix} \circ \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}, \text{ zaś}$$

$$(2,3) \circ (1,2) = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix} \circ \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix} = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix}.$$

Dwa cykle $c_1 = (a_1, \ldots, a_k)$ i $c_2 = (b_1, \ldots, b_l)$ z S_n nazywamy rozłącznymi, jeśli $\{a_1, \ldots, a_k\}$ i $\{b_1, \ldots, b_l\}$ są rozłącznymi podzbiorami zbioru $\{1, \ldots, n\}$. Rozważany wcześniej przykład pokazuje, że składanie dowolnych cykli nie jest przemienne. Okazuje się jednak, że składanie cykli rozłącznych jest przemienne.

Lemat 3.3 *Jeśli $c_1, c_2 \in S_n$ są cyklami rozłącznymi, to $c_1 \circ c_2 = c_2 \circ c_1$.*

Dowód. Niech $c_1 = (a_1, \ldots, a_k)$ i $c_2 = (b_1, \ldots, b_l)$ będą cyklami rozłącznymi w grupie S_n i niech $j \in \{1, \ldots, n\}$. Pokażemy, że $c_1(c_2(j)) = c_2(c_1(j))$.

Jeśli $j \notin \{a_1, \ldots, a_k, b_1, \ldots, b_l\}$, to $c_1(j) = c_2(j) = j$, zatem $c_1(c_2(j)) = c_2(c_1(j)) = j$. Jeśli $j = a_s$ dla pewnego $s \in \{1, \ldots, k\}$, to

$$c_1(j) = c_1(a_s) = \begin{cases} a_{s+1} & \text{gdy} \quad s < k \\ a_1 & \text{gdy} \quad s = k. \end{cases}$$

Ponadto $c_2(a_r) = a_r$ dla $r \in \{1, \ldots, k\}$. Dlatego $c_2(c_1(j)) = c_1(j) = c_1(c_2(j))$. Analogicznie pokazujemy, że jeśli $j = b_s$ dla pewnego $s \in \{1, \ldots, l\}$, to $c_2(c_1(j)) = c_2(j) = c_1(c_2(j))$. ■

Twierdzenie 3.4 *Każda permutacja $\sigma \in S_n$ jest identycznością, albo cyklem, albo superpozycją cykli rozłącznych.*

Dowód. Dla permutacji $\tau \in S_n$ definiujemy zbiór $X_\tau = \{i \in \{1, \ldots, n\} : \tau(i) \neq i\}$. Przeprowadzimy dowód indukcyjny względem liczby elementów zbioru X_τ.

Ustalmy więc permutację $\sigma \in S_n$. Jeśli $X_\sigma = \emptyset$, to σ jest identycznością. Przyjmijmy teraz, że $X_\sigma \neq \emptyset$ i załóżmy, że teza twierdzenia jest prawdziwa dla dowolnej permutacji $\tau \in S_n$ takiej, że $|X_\tau| < |X_\sigma|$. Ponieważ zbiór X_σ jest niepusty, dla pewnego $i \in \{1, \ldots, n\}$ mamy $\sigma(i) \neq i$, a stąd $\sigma(\sigma(i)) \neq \sigma(i)$, czyli X_σ jest zbiorem przynajmniej dwuelementowym.

Niech $|X_\sigma| = m$. Ustalmy $i \in \{1, \ldots, n\}$ takie, że $\sigma(i) \neq i$. Ponieważ $\{1, \ldots, n\}$ jest zbiorem skończonym, ciąg $\langle i, \sigma(i), \sigma^2(i), \ldots \rangle$ nie jest różnowartościowy. To znaczy, istnieją $k \in \mathbb{N}$ oraz $l \in \mathbb{N}_+$ takie, że $\sigma^{k+l}(i) = \sigma^k(\sigma^l(i)) = \sigma^k(i)$. σ^k jest odwzorowaniem różnowartościowym, więc $\sigma^l(i) = i$.

Niech l_0 oznacza najmniejszą liczbę naturalną dodatnią taką, że $\sigma^{l_0}(i) = i$ (wtedy $l_0 \geq 2$) i niech $\tau = (i, \sigma(i), \ldots, \sigma^{l_0-1}(i))$. Wtedy $\tau^{-1} = (\sigma^{l_0-1}(i), \ldots, \sigma(i), i)$. Zauważmy, że

$$(\sigma \circ \tau^{-1})(i) = \sigma(\tau^{-1}(i)) = \sigma(\sigma^{l_0-1}(i)) = \sigma^{l_0}(i) = i.$$

Analogicznie

$$(\sigma \circ \tau^{-1})(\sigma^s(i)) = \sigma(\tau^{-1}(\sigma^s(i))) = \sigma(\sigma^{s-1}(i)) = \sigma^s(i)$$

dla $s \in \{1, \ldots, l_0 - 1\}$. Ponadto, dla dowolnego $j \in \{1, \ldots, n\}$, $\sigma(j) = j$ implikuje, że $(\sigma \circ \tau^{-1})(j) = j$. Oznacza to, że X_σ jest sumą rozłącznych zbiorów $X_{\sigma\circ\tau^{-1}}$ oraz $\{i, \ldots, \sigma^{l_0-1}(i)\}$, skąd wynika, że $|X_{\sigma\circ\tau^{-1}}| < |X_\sigma|$. Z założenia indukcyjnego $\sigma \circ \tau^{-1}$ jest identycznością, albo cyklem albo superpozycją cykli rozłącznych. Wtedy $\sigma = (\sigma \circ \tau^{-1}) \circ \tau$ jest cyklem albo superpozycją cykli rozłącznych. ■

Łatwo sprawdzić, że rozkład permutacji na cykle rozłączne jest jednoznaczny z dokładnością do porządku czynników.

Przykład 1. Rozważmy permutację

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 10 & 3 & 1 & 9 & 7 & 4 & 2 & 5 & 8 \end{pmatrix} \in S_{10}.$$

Z postaci dwuwierszowej permuacji σ odczytujemy, że $\sigma(1) = 6$, $\sigma(6) = 7$, $\sigma(7) = 4$, $\sigma(4) = 1$, $\sigma(2) = 10$, $\sigma(10) = 8$, $\sigma(8) = 2$, $\sigma(3) = 3$, $\sigma(5) = 9$, $\sigma(9) = 5$. Oznacza to, że

$$\sigma = (1, 6, 7, 4)(2, 10, 8)(5, 9).$$

Oczywiście kolejność cykli występujących w powyższym przedstawieniu jest nieistotna, albowiem składanie cykli rozłącznych jest przemienne.

Jeśli $\sigma \in S_n$ jest cyklem długości $k \geq 2$, to $\sigma^k = e$. Stąd łatwo wynika, że dla dowolnej liczby całkowitej m, $\sigma^m = \sigma^{m \bmod k}$. Używając tej własności oraz rozkładu permutacji na cykle możemy łatwo obliczać potęgi permutacji, jak również określić rząd permutacji jako elementu grupy S_n.

Twierdzenie 3.5 *Niech $\sigma = \sigma_1 \dots \sigma_k$, gdzie $\sigma_1, \dots, \sigma_k$ są rozłącznymi cyklami długości $l_1, \dots, l_k$ (odpowiednio). Wtedy*

(a) $\sigma^m = \sigma_1^{m \bmod l_1} \dots \sigma_k^{m \bmod l_k}$ dla dowolnego $m \in \mathbb{Z}$,

(b) rząd permutacji σ jest równy najmniejszej wspólnej wielokrotności liczb $l_1, \dots, l_k$.

Dowód. (a) Ponieważ cykle rozłączne są przemienne (lemat 3.3), $\sigma^m = \sigma_1^m \dots \sigma_k^m$, stąd zaś dostajemy tezę.

(b) Z punktu (a) wynika, że dla $m \in \mathbb{Z}$, $\sigma^m = e$ wtedy i tylko wtedy, gdy $m \bmod l_i = 0$ dla $i \in \{1, \dots k\}$, co jest równoważne podzielności liczby m przez $l_1, \dots, l_k$. Zatem $\sigma^m = e$ wtedy i tylko wtedy, gdy $NWW(l_1, \dots, l_k)$ dzieli m. To zaś oznacza, że rząd permutacji σ wynosi $NWW(l_1, \dots, l_k)$. ■

Dla zilustrowania twierdzenia 3.5 rozważmy permutację $\sigma \in S_{10}$:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 9 & 10 & 5 & 7 & 2 & 6 & 1 & 4 & 8 \end{pmatrix} = (1, 3, 10, 8)(2, 9, 4, 5, 7, 6).$$

σ jest superpozycją dwóch rozłącznych cykli długości 4 i 6. $NWW(4, 6) = 12$, więc rząd σ jako elementu grupy S_{10} wynosi 12.

Dla zdefiniowanej wyżej permutacji obliczymy potęgę σ^{2002}. Niech $\sigma_1 = (1, 3, 10, 8)$ i $\sigma_2 = (2, 9, 4, 5, 7, 6)$. σ_1 i σ_2 są rozłącznymi cyklami długości 4 i 6 (odpowiednio), więc zgodnie z twierdzeniem 3.5(b),

$$\sigma^{2002} = \sigma_1^{2002}\sigma_2^{2002} = \sigma_1^{2002 \bmod 4}\sigma^{2002 \bmod 6}.$$

$2002 = 500 \cdot 4 + 2 = 333 \cdot 6 + 4$, więc $2002 \bmod 4 = 2$ i $2002 \bmod 6 = 4$. Zatem $\sigma^{2002} = \sigma_1^2\sigma_2^4$. Jak łatwo obliczyć, $\sigma_1^2 = \sigma_1 \circ \sigma_1 = (1, 10)(3, 8)$ i $\sigma_2^4 = \sigma_2 \circ \sigma_2 \circ \sigma_2 \circ \sigma_2 = (2, 7, 4)(9, 6, 5)$. Po podstawieniu dostajemy

$$\sigma^{2002} = (1, 10)(3, 8)(2, 7, 4)(9, 6, 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 8 & 2 & 9 & 5 & 4 & 3 & 6 & 1 \end{pmatrix}.$$

Twierdzenie 3.6 *Każda permutacja $\sigma \in S_n$ jest identycznością, transpozycją, albo złożeniem co najwyżej $n - 1$ transpozycji.*

Dowód. Zauważmy, że każdy cykl k-wyrazowy ($k \geq 3$) jest złożeniem $k - 1$ transpozycji. Mamy bowiem

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

Z poprzedniego twierdzenia wiemy, że jeśli $\sigma \neq e$, to σ jest cyklem długości co najwyżej n, albo jest złożeniem pewnej liczby cykli rozłącznych. W pierwszym przypadku oczywiście σ jest transpozycją albo złożeniem co najwyżej $n - 1$ transpozycji.

Załóżmy teraz, że $\sigma = c_1 \circ \dots \circ c_k$, gdzie $c_1, \dots, c_k$ są cyklami rozłącznymi długości odpowiednio $l_1, \dots, l_k$. Oczywiście $l_1 + \dots + l_k \leq n$. c_i jest transpozycją dla $l_i = 2$, zaś złożeniem $l_i - 1$ transpozycji

dla $l_i \geq 3$. Zatem $\sigma = c_1 \circ \ldots \circ c_k$ jest złożeniem $l_1 + \ldots + l_k - k$ transpozycji. Ale $l_1 + \ldots + l_k - k \leq n - k \leq n - 1$, co kończy dowód. ■

Przedstawienie permutacji w postaci złożenia transpozycji nie jest jednoznaczne. Świadczy o tym następujący przykład permutacji z S_3:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1,2,3) = (1,2) \circ (2,3) = (2,3) \circ (3,1) = (3,1) \circ (1,2).$$

Twierdzenie 3.7 *Każda transpozycja jest transpozycją liczb sąsiednich lub superpozycją nieparzystej liczby transpozycji liczb sąsiednich.*

Dowód. Niech $\tau = (j,l) \in S_n$, gdzie $l - j \geq 2$. Wtedy

$$(j,l) = (j,j+1)(j+1,j+2)\ldots(l-1,l)(l-2,l-1)\ldots(j,j+1),$$

czyli (j,l) jest superpozycją $2(l-j)-1$ transpozycji liczb sąsiednich. ■

Z twierdzeń 3.6 i 3.7 natychmiast wynika następujący wniosek.

Wniosek 3.8 *Każda permutacja zbioru $\{1,\ldots n\}$ jest identycznością, albo transpozycją liczb sąsiednich, albo superpozycją transpozycji liczb sąsiednich.*

Przykład 2. Przedstawimy permutację

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix} \in S_6$$

w postaci złożenia transpozycji liczb sąsiednich. Dokonamy tego w trzech krokach stosując metody zawarte w dowodach twierdzeń 3.4, 3.6 i 3.7:

Krok 1: zapiszemy σ jako iloczyn cykli rozłącznych.

Krok 2: każdy cykl długości ≥ 3 otrzymany w kroku 1. przedstawimy w postaci złożenia transpozycji.

Krok 3: każdą transpozycję liczb nie sąsiadujących ze sobą otrzymaną w kroku 2 przedstawimy w postaci złożenia transpozycji liczb sąsiednich.

Ponieważ $\sigma(1) = 4$, $\sigma(4) = 1$, $\sigma(2) = 3$, $\sigma(3) = 6$, $\sigma(6) = 2$ i $\sigma(5) = 5$, mamy

$$\sigma = (1,4)(2,3,6) = (1,4)(2,3)(3,6).$$

Postępując jak w dowodzie twierdzenia 3.7 dostajemy

$$(1,4) = (1,2)(2,3)(3,4)(2,3)(1,2) \text{ i } (3,6) = (3,4)(4,5)(5,6)(4,5)(3,4).$$

Stąd

$$\sigma = (1,2)(2,3)(3,4)(2,3)(1,2)(2,3)(3,4)(4,5)(5,6)(4,5)(3,4).$$

Permutacja może mieć wiele przedstawień w postaci złożenia transpozycji. Jak widzieliśmy w rozpatrywanym wyżej przykładzie, liczby transpozycji występujące w dwóch różnych przedstawieniach nie muszą być takie same. Pomimo tego, istnieje pewien niezmiennik rozkładu permutacji na transpozycje. Okazuje się, mianowicie, że parzystość liczby transpozycji występujących w rozkładzie permutacji σ zależy od σ, zaś nie zależy od konkretnego rozkładu σ na transpozycje. Wprowadzimy teraz pojęcie inwersji w permutacji, które ułatwi zbadanie tego zagadnienia.

Definicja 3.9 *Niech będzie dana permutacja $\sigma \in S_n$, $n \geq 2$. Inwersją w permutacji σ będziemy nazywali dowolną parę uporządkowaną $\langle \sigma(i), \sigma(j) \rangle$ taką, że $i < j$ zaś $\sigma(i) > \sigma(j)$.*

Permutację σ nazywamy parzystą [nieparzystą], jeśli liczba inwersji w niej jest parzysta [odpowiednio: nieparzysta].

Na przykład w permutacji

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} \in S_5$$

występuje 7 inwersji, mianowicie: $\langle 4,1 \rangle$, $\langle 4,3 \rangle$, $\langle 4,2 \rangle$, $\langle 5,1 \rangle$, $\langle 5,2 \rangle$, $\langle 5,3 \rangle$ i $\langle 3,2 \rangle$. Oznacza to, że σ jest permutacją nieparzystą. Permutacja identycznościowa jest permutacją parzystą, gdyż liczba inwersji w niej wynosi 0.

Lemat 3.10 *Jeśli σ jest dowolną permutacją z S_n, $n \geq 2$, zaś $\tau \in S_n$ jest transpozycją to permutacje σ i $\sigma\tau$ różnią się parzystością.*

Dowód. Niech $\sigma \in S_n$, gdzie $n \geq 2$. Przeprowadzimy dowód najpierw w przypadku, gdy τ jest transpozycją liczb sąsiednich. Przyjmijmy $\tau = (i, i+1)$, gdzie $i \in \{1, \ldots, n-1\}$. Wtedy $(\sigma\tau)(i) = \sigma(i+1)$ i $(\sigma\tau)(i+1) = \sigma(i)$. Wynika stąd, że $\langle (\sigma\tau)(i), (\sigma\tau)(i+1) \rangle$ jest inwersją w permutacji $\sigma\tau$ wtedy i tylko wtedy, gdy $\langle \sigma(i), \sigma(i+1) \rangle$ nie jest inwersją w permutacji σ. Ponadto dla $j \in \{1, \ldots, n\} \setminus \{i, i+1\}$ mamy $(\sigma\tau)(j) = \sigma(j)$. Zatem zbiory inwersji dla permutacji σ i $\sigma\tau$ różnią się jednym elementem, co oznacza, że permutacje σ i $\sigma\tau$ różnią się parzystością.

Załóżmy teraz, że $\tau \in S_n$ jest dowolną transpozycją. Zgodnie z twierdzeniem 3.7, $\tau = \tau_1 \circ \ldots \circ \tau_{2k+1}$ dla pewnego $k \in \mathbb{N}$, gdzie $\tau_1, \ldots, \tau_{2k+1}$ są transpozycjami liczb sąsiednich. Pierwsza część dowodu implikuje, że kolejne permutacje ciągu $\sigma, \sigma\tau_1, \sigma\tau_1\tau_2, \ldots, \sigma\tau_1 \ldots \tau_{2k+1}$ różnią się parzystością. Stąd wynika teza. ■

Twierdzenie 3.11 *Iloczyn dowolnych k transpozycji z S_n ($n \geq 2$) jest permutacją, której parzystość jest zgodna z parzystością liczby k.*

Dowód. (Indukcja względem k) Niech $\tau \in S_n$, będzie transpozycją. $\tau = e\tau$. Ponieważ identyczność e jest permutacją parzystą, zgodnie z lematem 3.10 τ jest permutacją nieparzystą. Tak więc twierdzenie zachodzi dla $k = 1$ (iloczyn trzeba tu rozumieć jako daną transpozycję).

Niech teza twierdzenia będzie prawdziwa dla pewnego $k \in \mathbb{N}_+$. Wówczas jej prawdziwość dla $k+1$ wynika z tego, że liczby k i $k+1$ mają różną parzystość, zaś iloczyn $k+1$ transpozycji powstaje z iloczynu k transpozycji przez pomnożenie go przez transpozycję. ■

Wniosek 3.12 *Przy dowolnym rozkładzie permutacji na iloczyn transpozycji parzystość liczby czynników jest ta sama i równa parzystości permutacji.*

Wniosek 3.13 *Złożenie dwóch permutacji tej samej parzystości jest permutacją parzystą, zaś złożenie dwóch permutacji różnej parzystości jest permutacją nieparzystą.*

Z wniosku 3.13 wynika, że w celu znalezienia parzystości permutacji wystarczy znaleźć jej dowolny rozkład na transpozycje i stwierdzić, czy liczba czynników występujących w tym rozkładzie jest parzysta czy też nieparzysta.

Definiujemy znak permutacji $\sigma \in S_n$ ($n \geq 2$) w sposób następujący:

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{gdy } \sigma \text{ jest parzysta} \\ -1 & \text{gdy } \sigma \text{ jest nieparzysta.} \end{cases}$$

Z wniosku 3.13 wynika, że dla dowolnych $\sigma, \tau \in S_n$ zachodzi równość: $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$. Nietrudno też dowieść, że $\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\sigma)$

Wniosek 3.14 *Zbiór permutacji parzystych zbioru $\{1, \ldots, n\}$ ($n \geq 2$) z działaniem składania permutacji jest grupą. Grupę tę oznaczamy przez A_n i nazywamy n-tą grupą alternującą.*

Twierdzenie 3.15 *Dla $n \geq 2$ w S_n istnieje dokładnie $\frac{n!}{2}$ permutacji parzystych i dokładnie $\frac{n!}{2}$ permutacji nieparzystych.*

Dowód. Niech $\sigma_1, \ldots, \sigma_k$ będą wszystkimi (różnymi) permutacjami parzystymi w S_n, zaś $\tau_1, \ldots, \tau_m$ wszystkimi (różnymi) permutacjami nieparzystymi z S_n. Tak więc $k + m = n!$. Oznaczmy przez τ pewną transpozycję z S_n. Wtedy $\sigma_1\tau, \ldots, \sigma_k\tau$ są różnymi permutacjami nieparzystymi, zatem $k \leq m$. $\tau_1\tau, \ldots, \tau_m\tau$ są różnymi permutacjami parzystymi, co oznacza, że $m \leq k$. Stąd $k = m = \frac{n!}{2}$. ■

Rozdział 4

Podgrupy, dzielniki normalne i homomorfizmy grup

Rozpatrzmy grupę nieosobliwych macierzy kwadratowych wymiaru 2×2 o wyrazach rzeczywistych i jej podzbiór H złożony z macierzy o wyznaczniku 1. Jak łatwo spostrzec (przykład 6, ze strony 22), H jest grupą względem mnożenia macierzy. Przykład ten jest ilustracją pojęcia podgrupy, które zdefiniujemy obecnie.

Definicja 4.1 *Podzbiór H grupy $(G, \circ)$ będący grupą względem działania $\circ$ nazywamy podgrupą grupy G.*

Zamiast pisać, że H jest podgrupą grupy $(G, \circ)$, będziemy czasami używać oznaczenia $H < G$.

Niech H będzie podgrupą grupy $(G, \circ)$. Bezpośrednio z definicji podgrupy wynika, że element neutralny w grupie $(H, \circ)$ pokrywa się z elementem neutralnym w grupie $(G, \circ)$. Jeśli $a \in H$, to element odwrotny do a w grupie H pokrywa się z elementem odwrotnym do a w grupie G.

Twierdzenie 4.2 *Niech $(G, \circ)$ będzie grupą i niech $H \subseteq G$. Wtedy następujące warunki są równoważne.*
(a) H jest podgrupą grupy $(G, \circ)$.
(b) $e \in H$, $(\forall a \in H)(a^{-1} \in H)$ i $(\forall a, b \in H)(a \circ b \in H)$.
(c) $H \neq \emptyset$, $(\forall a \in H)(a^{-1} \in H)$ i $(\forall a, b \in H)(a \circ b \in H)$.
(d) $H \neq \emptyset$ i $(\forall a, b \in H)(a \circ b^{-1} \in H)$.
(e) $e \in H$ i $(\forall a, b \in H)(a \circ b^{-1} \in H)$.

Dowód. (a)$\Longrightarrow$(b). Jeśli H jest podgrupą grupy $(G, \circ)$, to $(H, \circ)$ jest grupą, skąd wynika (b).

Implikacja (b)$\Longrightarrow$(c) jest oczywista.

(c)$\Longrightarrow$(d): Załóżmy, że $a, b \in H$. Z (c) wynika, że $b^{-1} \in H$ i $a \circ b^{-1} \in H$.

W celu wykazania implikacji (d)$\Longrightarrow$(e), wystarczy dowieść, że (d)$\Longrightarrow e \in H$. Na mocy (d) istnieje element $a \in H$ i $a \circ a^{-1} \in H$. Oznacza to, że $e \in H$.

(e)$\Longrightarrow$(a). Załóżmy, że zachodzi warunek (e). Pokażemy, że H z działaniem $\circ$ ograniczonym do zbioru H stanowi grupę. Z założenia $e \in H$. Niech $a, b \in H$. Wtedy $b^{-1} = e \circ b^{-1} \in H$ oraz $a \circ b = a \circ (b^{-1})^{-1} \in H$. Tak więc $\circ$ jest działaniem w H i $(H, \circ)$ jest grupą. ■

Pozostawiamy Czytelnikowi do sprawdzenia, że w powyższym twierdzeniu możemy warunki (d) i (e) zastąpić następującymi:

(d') $H \neq \emptyset$ i $(\forall a, b \in H)(a^{-1} \circ b \in H)$,

(e') $e \in H$ i $(\forall a, b \in H)(a^{-1} \circ b \in H)$.

Każda grupa zawiera jako podgrupy samą siebie i podgrupę złożoną z samego elementu neutralnego. Są to tak zwane *podgrupy niewłaściwe*. Każda inna podgrupa nazywa się *podgrupą właściwą*. Podamy teraz przykłady podgrup w kilku różnych grupach.

Przykład 1. Niech $n \in \mathbb{N}_+$. Wtedy $n\mathbb{Z} = \{ni : i \in \mathbb{Z}\}$ jest podgrupą grupy $(\mathbb{Z}, +)$.

Przykład 2. $(\mathbb{Q} \setminus \{0\}, \cdot) < (\mathbb{R} \setminus \{0\}, \cdot) < (\mathbb{C} \setminus \{0\}, \cdot)$, $(\mathbb{Q}_+, \cdot) < (\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}_+, \cdot) < (\mathbb{R} \setminus \{0\}, \cdot)$.

Przykład 3. Grupa translacji płaszczyzny jest podgrupą grupy izometrii płaszczyzny, a ta z kolei jest podgrupą grupy przekształceń wzajemnie jednoznacznych płaszczyzny na siebie. Działaniem we wszystkich wymienionych grupach jest składanie przekształceń.

Przykład 4. Zbiór obrotów trójkąta równobocznego o kąty 0^0, 120^0 i 240^0 (przy oznaczeniach z przykładu 16 ze strony 24 jest to zbiór $\{I, R, R^2\}$) jest podgrupą grupy izometrii własnych tegoż trójkąta.

Przykład 5. Jak wiemy z wniosku 3.14, zbiór permutacji parzystych zbioru $\{1, \ldots, n\}$ $(n \geq 2)$ jest grupą względem działania składania permutacji. Zatem A_n jest podgrupą grupy S_n. Zbiór permutacji nieparzystych zbioru $\{1, \ldots n\}$ nie jest podgrupą grupy S_n, gdyż złożenie dwóch permutacji nieparzystych jest permutacją parzystą.

Przykład 6. Zbiór macierzy wymiaru $n \times n$ $(n \in \mathbb{N}_+)$ o wyznaczniku równym 1 jest podgrupą grupy macierzy nieosobliwych wymiaru $n \times n$.

Przykład 7. Niech G będzie grupą i niech $g \in G$. Zbiór elementów grupy G, które są przemienne z elementem g nazywamy centralizatorem elementu g i oznaczamy przez $C(g)$. Tak więc

$$C(g) = \{h \in G : hg = gh\}.$$

Pokażemy, że $C(g)$ jest podgrupą grupy G dla dowolnego $g \in G$. W tym celu udowodnimy warunek (b) twierdzenia 4.2 . Ustalmy $g \in G$. Z definicji elementu neutralnego wynika, że $eg = ge$, zatem $e \in C(g)$. Niech $a, b \in C(g)$. Wtedy

$$abg = agb = gab,$$

więc $ab \in C(g)$.

Zauważmy, że jeśli $b \in C(g)$, to

$$bg = gb \Longrightarrow (bg)^{-1} = (gb)^{-1} \Longrightarrow g^{-1}b^{-1} = b^{-1}g^{-1}.$$

Mnożąc ostatnią równość przez g z lewej i z prawej strony, otrzymujemy: $gg^{-1}b^{-1}g = gb^{-1}g^{-1}g$, czyli $b^{-1}g = gb^{-1}$. To zaś oznacza, że $b^{-1} \in C(g)$.

Przykład 8. Niech G będzie grupą. Zbiór

$$Z(G) = \{a \in G : \forall g \in G(ag = ga)\}$$

nazywamy centrum grupy G. $Z(G)$ jest podgrupą grupy G. Dowód tego faktu wymaga nieznacznej modyfikacji rozumowania z poprzedniego przykładu.

Dowód poniższego twierdzenia pozostawiamy jako ćwiczenie dla Czytelnika.

Twierdzenie 4.3 *Jeśli H jest podgrupą grupy G i $c \in G$, to zbiór:*

$$c^{-1}Hc = \{c^{-1}hc : h \in H\}$$

również jest podgrupą grupy G.

Podgrupa postaci $c^{-1}Hc$, występująca w twierdzeniu 4.3, zwana jest podgrupą sprzężoną do H względem elementu c.

Definicja 4.4 *Niech a i b będą elementami grupy G. Mówimy, że elementy te są sprzężone w grupie G (oznaczenie: $a \sim b$), jeśli istnieje element $c \in G$ taki, że $b = c^{-1}ab$.*

Nietrudno wykazać, że relacja sprzężenia w dowolnej grupie jest relacją równoważności. Dla grup abelowych jej klasy abstrakcji są oczywiście jednoelementowe.

Twierdzenie 4.5 *Przekrój dowolnej niepustej rodziny podgrup grupy G jest podgrupą grupy G.*

Dowód. Niech $\mathcal{H}$ będzie niepustą rodziną podgrup grupy G i niech

$$K = \bigcap_{H \in \mathcal{H}} H.$$

W celu wykazania, że $K < G$, udowodnimy warunek (e) twierdzenia 4.2 .

Z definicji podgrupy, $e_G \in H$ dla każdej podgrupy H z rodziny $\mathcal{H}$. Zatem $e_G \in K$. Niech teraz $a, b \in K$. Wtedy $a, b \in H$ dla wszystkich $H \in \mathcal{H}$. Wynika stąd, że $ab^{-1} \in H$ dla $H \in \mathcal{H}$, czyli $ab^{-1} \in K$. ■

Załóżmy, że A jest podzbiorem grupy G. Definiujemy zbiór:

$$\langle A \rangle_G = \{a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} : a_1, \ldots, a_n \in A, \varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}, n \in \mathbb{N}_+\} \cup \{e_G\}.$$

Nietrudno sprawdzić, że $\langle A \rangle_G$ jest podgrupą grupy G. Jeśli $\langle A \rangle_G = G$, to mówimy, że G jest grupą generowaną przez A lub A jest zbiorem generatorów grupy G.

Twierdzenie 4.6 *Jeśli G jest grupą i $A \subseteq G$, to $\langle A \rangle_G$ jest przekrojem rodziny wszystkich podgrup grupy G zawierających zbiór A.*

Dowód. Niech $\mathcal{H}$ będzie rodziną wszystkich podgrup grupy G zawierających A. Oczywiście $\langle A \rangle_G \in \mathcal{H}$, więc

$$\bigcap_{H \in \mathcal{H}} H \subseteq \langle A \rangle_G.$$

Z drugiej strony, jeśli H jest podgrupą grupy G zawierającą A, to $e_G \in H$ i $a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \in H$ dla dowolnych $a_1, \ldots, a_n \in A$ i $\varepsilon_1, \ldots, \varepsilon_n \in \{-1, 1\}$. To zaś oznacza, że

$$\langle A \rangle_G \subseteq \bigcap_{H \in \mathcal{H}} H,$$

co kończy dowód. ■

Definicja 4.7 *Niech H będzie podgrupą grupy G. Każdy zbiór postaci*

$$aH = \{ah : h \in H\},$$

gdzie $a \in G$, nazywamy warstwą lewostronną podgrupy H w grupie G. Podobnie, każdy zbiór postaci

$$Ha = \{ha : h \in H\},$$

gdzie $a \in G$, nazywamy warstwą prawostronną podgrupy H w grupie G.

Jeśli H jest podgrupą grupy G, zaś a dowolnym elementem G, to a należy do każdej z warstw aH i Ha. Dlatego warstwę aH nazywa się też warstwą lewostronną elementu a względem podgrupy H. Podobnie dla warstwy Ha.

Twierdzenie 4.8 *Niech H będzie podgrupą grupy G. Dowolne dwie warstwy lewostronne podgrupy H są sobie równe bądź rozłączne. To samo dla warstw prawostronnych.*

Dowód. Przeprowdzimy dowód tylko dla warstw lewostronnych. Niech $a, b \in G$ i załóżmy, że warstwy aH, bH mają wspólny element c. Pokażemy, że wtedy $aH = bH$.

Niech $g \in aH$, to znaczy $g = ah$ dla pewnego $h \in H$. Ponieważ $c \in aH \cap bH$, istnieją $h_1, h_2 \in H$ takie, że $c = ah_1 = bh_2$. Przy tych oznaczeniech mamy:

$$g = ah = ah_1h_1^{-1}h = bh_2h_1^{-1}h.$$

$h_2h_1^{-1}h \in H$, więc $g \in bH$. W ten sposób pokazaliśmy, że $aH \subseteq bH$. Zamieniając rolami a i b w powyższym rozumowaniu, dostajemy inkluzję przeciwną, co kończy dowód. ■

Z powyższego twierdzenia wynika, że każdy element grupy G należy do jednej i tylko jednej warstwy lewostronnej (prawostronnej) względem podgrupy H.

Lemat 4.9 *Załóżmy, że H jest podgrupą grupy G. Jeśli $a, b \in G$, to*
(a) $aH = bH \iff Ha^{-1} = Hb^{-1} \iff a^{-1}b \in H$,
(b) $Ha = Hb \iff a^{-1}H = b^{-1}H \iff ab^{-1} \in H$.

Dowód. (a) Z twierdzenia 4.8 wynika, że warstwy aH i bH są równe wtedy i tylko wtedy, gdy $aH \cap bH \neq \emptyset$. Podobnie dla warstw Ha^{-1} i Hb^{-1}. Stąd:

$$\begin{aligned} aH = bH &\iff aH \cap bH \neq \emptyset \iff (\exists h_1, h_2 \in H)(ah_1 = bh_2) \iff \\ &\iff (\exists h_1, h_2 \in H)((ah_1)^{-1} = (bh_2)^{-1}) \iff (\exists h_1, h_2 \in H)(h_1^{-1}a^{-1} = h_2^{-1}b^{-1}) \iff \\ &\iff Ha^{-1} \cap Hb^{-1} \neq \emptyset \iff Ha^{-1} = Hb^{-1}. \end{aligned}$$

Aby zakończyć dowód (a), musimy jeszcze wykazać, że równość $aH = bH$ jest równoważna warunkowi $a^{-1}b \in H$. Jeśli $aH = bH$, to $ah_1 = bh_2$ dla pewnych $h_1, h_2 \in H$. Mnożąc tę równość przez a^{-1} z lewej strony i przez h_2^{-1} z prawej strony dostajemy $a^{-1}b = h_1h_2^{-1} \in H$.

Załóżmy teraz, że $a^{-1}b = h \in H$. Wtedy $b = ah \in aH \cap bH$, co oznacza, że $aH \cap bH \neq \emptyset$. Na mocy twierdzenia 4.8 otrzymujemy $aH = bH$.

Dowód części (b) twierdzenia przebiega podobnie. ■

Twierdzenie 4.10 *Niech G będzie grupą, zaś H jej podgrupą. Zbiór warstw lewostronnych podgrupy H jest równoliczny ze zbiorem jej warstw prawostronnych.*

Dowód. Niech F będzie odwzorowaniem ze zbioru warstw lewostronnych w zbiór warstw prawostronnych podgrupy H określonym następująco: $F(aH) = Ha^{-1}$. Z lematu 4.9 wynika, że odwzorowanie F jest dobrze określone i różnowartościowe. F jest również surjekcją, gdyż dla dowolnego $a \in G$ zachodzi: $Ha = H(a^{-1})^{-1} = F(a^{-1}H)$. ■

Twierdzenie 4.11 *Dowolne dwie warstwy lewostronne (prawostronne) względem tej samej podgrupy są równoliczne. Dowolna warstwa lewostronna jest równoliczna z dowolną warstwą prawostronną.*

Dowód. Niech G będzie grupą, zaś H jej podgrupą. Wybierzmy dowolne elementy $a, b \in G$. Pokażemy, że warstwy aH i bH są równoliczne. W tym celu określamy odwzorowanie $f : aH \longrightarrow bH$ wzorem $f(ah) = bh$ dla $h \in H$. f jest oczywiście surjekcją. f jest też odwzorowaniem różnowartościowym, gdyż dla $h_1, h_2 \in H$ zachodzi:

$$f(ah_1) = f(ah_2) \Longrightarrow bh_1 = bh_2 \Longrightarrow h_1 = h_2 \Longrightarrow ah_1 = ah_2.$$

Podobnie dowodzimy, że równoliczne są dowolne dwie warstwy prawostronne.

Druga część tezy wynika z pierwszej części i z tego, że $H = eH = He$, czyli jest warstwą zarówno lewo- jak i prawostronną względem H. ■

W związku z powyższym twierdzeniem przyjmujemy następującą definicję.

Definicja 4.12 *Niech H będzie podgrupą grupy G. Moc zbioru warstw lewostronnych (równoważnie: prawostronnych) podgrupy H w grupie G nazywamy indeksem grupy H w G i oznaczamy przez $[G : H]$.*

Twierdzenie 4.13 *(Twierdzenie Lagrange'a[1]) Niech G będzie grupą skończoną, zaś H jej podgrupą. Wtedy*

$$|G| = [G : H] \cdot |H|.$$

Tak więc rząd oraz indeks podgrupy H w skończonej grupie G są dzielnikami $|G|$.

Dowód. Dwie różne warstwy lewostronne podgrupy H w grupie G są rozłączne (twierdzenie 4.11) i równoliczne. Ponadto każdy element grupy G leży w pewnej warstwie lewostronnej podgrupy H. Dlatego liczba elementów grupy G jest równa iloczynowi liczby warstw lewostronnych podgrupy H przez liczbę elementów w jednej warstwie (czyli $|H|$). Stąd wynika teza. ■

Wzór występujący w powyższym twierdzeniu jest słuszny również dla grup nieskończonych. Po prawej stronie mamy wówczas iloczyn liczb kardynalnych oznaczających odpowiednio moc zbioru warstw podgrupy H w grupie G oraz moc grupy H. Tak też należy rozumieć prawą stronę równości pojawiającej się w punkcie (c) twierdzenia 4.14.

Z twierdzenia Lagrange'a wynika, że jeśli G jest grupą skończoną, to rząd jej dowolnej podgrupy jest dzielnikiem $|G|$. Innymi słowy, zbiór rzędów wszystkich podgrup grupy G zawiera się w zbiorze dzielników dodatnich rzędu grupy G. Inkluzja odwrotna nie jest prawdziwa. Na przykład 12-elementowa grupa A_4 nie posiada podgrupy rzędu 6.

Twierdzenie 4.14 *Jeśli H i K są podgrupami grupy G oraz $K \subseteq H$, to*

(a) K jest podgrupą grupy H,

(b) Indeks $[G : K]$ jest skończony wtedy i tylko wtedy, gdy indeksy $[G : H]$ oraz $[H : K]$ są skończone.

(c) $[G : K] = [G : H] \cdot [H : K]$.

Dowód. Niech G będzie grupą, zaś H i K jej podgrupami takimi, że $K \subseteq H$. Wprost z definicji podgrupy wynika, że wówczas $K < H$.

Przypuśćmy, że indeks $[G : K]$ jest skończony, to znaczy, w grupie G istnieje jedynie skończenie wiele warstw lewostronnych względem podgrupy K. Ponieważ każda warstwa lewostronna podgrupy K w grupie H jest również jej warstwą lewostronną w grupie G, otrzymujemy $[H : K] \leq [G : K]$, w szczególności, indeks $[H : K]$ jest skończony. Zauważmy ponadto, że przyporządkowanie warstwie aK warstwy aH stanowi surjekcję ze zbioru warstw lewostronnych podgrupy K w grupie G w zbiór warstw lewostronnych podgrupy H w grupie G. Oznacza to, że $[G : H] \leq [G : K]$, a więc również indeks $[G : H]$ jest skończony.

[1] Joseph Louis Lagrange (1736-1813) urodzony we Włoszech, studiował w Paryżu. Zajmował się algebrą, teorią liczb, równaniami różniczkowymi, jak również zastosowaniami matematyki w fizyce i astronomii.

Załóżmy teraz, że indeksy $[G : H]$ oraz $[H : K]$ są oba skończone. Niech $a_1H, \ldots, a_mH$ będą wszystkimi (różnymi) warstwami lewostronnymi grupy H w grupie G, zaś $b_1K, \ldots, b_nK$ wszystkimi (różnymi) warstwami lewostronnymi grupy K w grupie H. Twierdzimy, że wówczas a_ib_jK, gdzie $1 \leq i \leq m$ i $1 \leq j \leq n$ są wszystkimi (różnymi) warstwami grupy K w grupie G. Mamy bowiem:

- Jeśli $g \in G$, to $g = a_ih = a_ib_jk$, gdzie $h \in H$, $1 \leq i \leq m$, $k \in K$ oraz $1 \leq j \leq n$. Oznacza to, że $g \in a_ib_jK$.
- Jeśli $a_ib_jK = a_{i'}b_{j'}K$, to

  $$(*)\ a_ib_j = a_{i'}b_{j'}k \text{ dla pewnego } k \in K.$$

  Stąd, ponieważ $b_j, b_{j'}k \in H$, mamy $a_iH = a_{i'}H$, czyli $i = i'$. Uwzględniając ten fakt w $(*)$ dostajemy $b_j = b_{j'}k$, skąd wynika, że $b_jK = b_{j'}K$ i $j = j'$.

W ten sposób wykazaliśmy równoważność (b) oraz równość (c) w przypadku, gdy indeks $[G : K]$ jest skończony. Ogólny dowód równości z punktu (c) wymaga niewielkiej modyfikacji powyższego rozumowania. ■

Równość z punktu (c) twierdzenia 4.14 dla skończonej grupy G jest bezpośrednią konsekwencją twierdzenia Lagrange'a. Mamy bowiem:

$$[G : K] = \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = [G : H] \cdot [H : K].$$

Twierdzenie 4.15 *Jeśli G jest grupą skończoną, to rząd dowolnego jej elementu jest dzielnikiem $|G|$.*

Dowód. Niech a będzie elementem rzędu n w skończonej grupie G. Wtedy $H = \{a^i : 0 \leq i \leq n-1\}$ jest n-elementową podgrupą grupy G. Zgodnie z twierdzeniem Lagrange'a, n dzieli $|G|$. ■

Twierdzenie 4.16 *Jeśli G jest grupą skończoną rzędu n i $a \in G$, to $a^n = e_G$.*

Dowód. Niech a będzie elementem rzędu k w skończonej grupie G i niech $n = |G|$. Z twierdzenia 4.15 wynika, że $k|n$, czyli $n = kl$ dla pewnego $l \in \mathbb{N}_+$. Stąd $a^n = a^{kl} = (a^k)^l = e^l = e$. ■

Twierdzenie 4.17 *Niech H będzie podgrupą grupy G. Wtedy relacja $\sim$ określona wzorem*

$$a \sim b \iff ab^{-1} \in H \text{ dla } a, b \in G$$

jest relacją równoważności w zbiorze G. Jej klasami abstrakcji są warstwy prawostronne podgrupy H.

Dowód. Zauważmy, że dla dowolnych $a, b \in G$,

$$a \sim b \iff ab^{-1} \in H \iff H(ab^{-1}) = H \iff Ha = Hb.$$

Stąd już łatwo wynika, że $\sim$ jest relacją zwrotną, symetryczną i przechodnią, a więc jest relacją równoważności.

Warunek $Ha = Hb$ oznacza, że a i b leżą w tych samych warstwach prawostronnych podgrupy H. Zatem klasami abstrakcji relacji $\sim$ są warstwy prawostronne podgrupy H. ■

Niewielka modyfikacja powyższego rozumowania pozwala udowodnić następujące twierdzenie.

Twierdzenie 4.18 *Niech H będzie podgrupą grupy G. Wtedy relacja $\sim$ określona wzorem*

$$a \sim b \iff a^{-1}b \in H \text{ dla } a, b \in G$$

jest relacją równoważności w zbiorze G. Jej klasami abstrakcji są warstwy lewostronne podgrupy H.

Jako zastosowanie teorii grup udowodnimy fakt z teorii liczb – tak zwane małe twierdzenie Fermata.[2]

Twierdzenie 4.19 *(Małe twierdzenie Fermata) Jeśli p jest liczbą pierwszą, zaś a liczbą całkowitą niepodzielną przez p, to $p|a^{p-1}-1$.*

Dowód.[3] Niech p będzie liczbą pierwszą, zaś $a \in \mathbb{Z}$ liczbą niepodzielną przez p. Oznaczmy przez k resztę z dzielenia a przez p. Wtedy $k \in \mathbb{Z}_p \setminus \{0\}$. $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ jest grupą rzędu $p-1$ (przykład 9, strona 23), zatem na mocy twierdzenia 4.16, $\underbrace{k \cdot_p \ldots \cdot_p k}_{p-1\text{razy}} = 1$. To zaś oznacza, że reszta z dzielenia liczby k^{p-1} przez p wynosi 1. Ponieważ reszty z dzielenia liczb a i k przez p są takie same, również reszta z dzielenia liczby a^{p-1} wynosi 1. Tak więc $p|a^{p-1}-1$. ■

Wniosek 4.20 *Jeśli p jest liczbą pierwszą i $a \in \mathbb{Z}$, to $p|a^p - a$.*

Dowód. Wniosek jest oczywisty, jeśli liczba a jest podzielna przez p. Jeśli p nie dzieli a, to na mocy małego twierdzenia Fermata, liczba $a^{p-1}-1$ jest podzielna przez p, a więc również liczba $a(a^{p-1}-1) = a^p - a$ jest podzielna przez p. ■

Przykład 9. Używając małego twierdzenia Fermata znajdziemy resztę z dzielenia liczby 137^{621} przez 13. UWAGA: pisząc $a \equiv b(\text{mod } n)$ mamy na myśli, że $n|a-b$.

Zauważmy, że $137 = 13 \cdot 10 + 7$ i $621 = 12 \cdot 51 + 9$. Dlatego

$$137^{621} \equiv 7^{12 \cdot 51 + 9}(\text{mod } 13) \equiv (7^{12})^{51} \cdot 7^9(\text{mod } 13).$$

Z małego twierdzenia Fermata wynika, że $7^{12} \equiv 1(\text{mod } 13)$. Stąd $137^{621} \equiv 7^9(\text{mod } 13)$. Dalej zauważmy, że

$$7^9 = 49^4 \cdot 7 \equiv 10^4 \cdot 7(\text{mod } 13) \equiv (-3)^4 \cdot 7(\text{mod } 13) \equiv 81 \cdot 7(\text{mod } 13) \equiv 3 \cdot 7(\text{mod } 13) \equiv 8(\text{mod } 13).$$

Zatem reszta z dzielenia liczby 137^{621} przez 13 wynosi 8.

Dowód kolejnego twierdzenia jest uogólnieniem dowodu małego twierdzenia Fermata ($\varphi(n)$ oznacza funkcję Eulera zdefiniowaną w przykładzie 10 ze strony 23).

Twierdzenie 4.21 *Jeśli $n \in \mathbb{N}_+$, $a \in \mathbb{Z}$ i $NWD(a,n) = 1$, to $n|a^{\varphi(n)} - 1$, czyli $a^{\varphi(n)} \equiv 1(mod\ n)$.*

Dowód. Załóżmy, że $n \in \mathbb{N}$, $a \in \mathbb{Z}$ oraz $NWD(a,n) = 1$. Oznaczmy przez k resztę z dzielenia liczby a przez n. Wtedy $k \in \mathbb{Z}_n$ oraz $NWD(k,n) = 1$, czyli k jest elementem grupy $G(n)$ (przykład 10, strona 23). Rząd grupy $G(n)$ wynosi $\varphi(n)$, zatem na mocy twierdzenia 4.16, $\underbrace{k \cdot_n \ldots \cdot_n k}_{\varphi(n)\text{razy}} = 1$. To zaś oznacza, że reszta z dzielenia liczby $k^{\varphi(n)}$ przez n wynosi 1. Ponieważ reszty z dzielenia liczb a i k przez n są takie same, również reszta z dzielenia liczby $a^{\varphi(n)}$ wynosi 1. Tak więc $n|a^{\varphi(n)} - 1$. ■

Definicja 4.22 *Podgrupę H grupy G nazywamy jej dzielnikiem normalnym, jeśli $aH = Ha$ dla dowolnego $a \in G$. Jeżeli H jest dzielnikiem normalnym grupy G, to piszemy $H \lhd G$.*

Jeśli G jest dowolną grupą, to $\{e\}$ oraz G są jej dzielnikami normalnymi. Dowolna podgrupa grupy abelowej jest jej dzielnikiem normalnym.

Przykład 10. Niech $n \geq 2$. Jak już wiemy, $A_n < S_n$ (przykład 5 ze strony 36). $|S_n| = n! = 2|A_n|$, więc na mocy twierdzenia Lagrange'a w grupie S_n istnieją dokładnie dwie warstwy grupy A_n. Jedna z nich jest równa A_n, zaś druga $S_n \setminus A_n$ (zbiór permutacji nieparzystych w S_n). Jeśli $\sigma \in S_n$ jest permutacją parzystą, to $\sigma A_n = A_n = A_n\sigma$. W przeciwnym wypadku $\sigma A_n = S_n \setminus A_n = A_n\sigma$. Tak więc A_n jest dzielnikiem normalnym grupy S_n.

Przykład 11. Łatwo sprawdzić, że $H = \{e, (1,2)\}$ jest podgrupą grupy S_3. H nie jest jednak dzielnikiem normalnym grupy S_3, ponieważ

$$(2,3)H = \{(2,3),(2,3)(1,2)\} = \{(2,3),(3,2)(2,1)\} = \{(2,3),(3,2,1)\} = \{(2,3),(1,3,2)\},$$
$$H(2,3) = \{(2,3),(1,2)(2,3)\} = \{(2,3),(1,2,3)\} \neq (2,3)H.$$

Twierdzenie 4.23 *Niech H będzie podgrupą grupy G. Wtedy następujące warunki są równoważne.*
(a) H jest dzielnikiem normalnym grupy G,
(b) $(\forall a \in G)(\forall h \in H)(a^{-1}ha \in H)$.

Dowód. Załóżmy, że $H \triangleleft G$, $a \in G$ i $h \in H$. $Ha = aH$, więc $ha = ah_1$ dla pewnego $h_1 \in H$. Stąd $a^{-1}ha = h_1 \in H$.

Aby dowieść, że (b) implikuje (a), załóżmy, że spełniony jest warunek (b). Niech $a \in G$. Pokażemy, że $aH \subseteq Ha$. W tym celu ustalmy $x = ah \in aH$. Z (b) wynika, że $aha^{-1} = h_1$ dla pewnego $h_1 \in H$. Tak więc $ah = h_1a \in Ha$. Podobnie pokazuje się, że $Ha \subseteq aH$. Stąd $aH = Ha$ dla każdego $a \in G$, czyli $H \triangleleft G$.

Definicja 4.24 *Niech $(G, \circ)$ i $(H, *)$ będą grupami. Odwzorowanie $f : G \longrightarrow H$ nazywamy*

(a) homomorfizmem, jeśli f zachowuje działanie grupowe, to znaczy $f(a \circ b) = f(a) * f(b)$ dla dowolnych $a, b \in G$,

(b) monomorfizmem lub zanurzeniem, jeśli f jest homomorfizmem różnowartościowym,

(c) epimorfizmem, jeśli f jest homomorfizmem i jest surjekcją,

(d) izomorfizmem, jeśli f jest homomorfizmem oraz bijekcją.

Definicja 4.25 *Niech $(G, \circ)$ będzie grupą. Dowolny homomorfizm grupy G w siebie nazywamy jej endomorfizmem. Izomorfizm $f : G \longrightarrow G$ nazywamy automorfizmem grupy G. Zbiór automorfizmów grupy G oznaczamy przez $Aut(G)$.*

Z definicji 4.24 natychmiast wynika, że każdy izomorfizm grup jest monomorfizmem oraz epimorfizmem. To samo można powiedzieć o automorfizmie dowolnej grupy. W poniższym twierdzeniu zostały zebrane najprostsze własności homomorfizmów grup.

Twierdzenie 4.26 *Niech f będzie homomorfizmem z grupy $(G, \circ)$ w grupę $(H, *)$. Wtedy:*
(a) $f(e_G) = e_H$,
(b) $f(a^{-1}) = f(a)^{-1}$ dla dowolnego $a \in G$,
(c) $f(a^n) = f(a)^n$ dla dowolnych $a \in G$ i $n \in \mathbb{Z}$,
(d) $rz(f(a)) \leq rz(a)$ dla dowolnego $a \in G$.

[2]Pierre de Fermat (1601-1665), matematyk francuski (z zawodu prawnik), zajmował się teorią liczb, geometrią analityczną i rachunkiem prawdopodobieństwa. Pozostawił hipotezę (zwaną Wielkim Twierdzeniem Fermata), zgodnie z którą dla żadnej liczby naturalnej $n > 2$ równanie $x^n + y^n = z^n$ nie ma rozwiązań w $\mathbb{N}_+$. WTF zostało udowodnione przez Andrew Wilesa w 1994 roku.

[3]Istnieje oczywiście elementarny (tzn. nie wykorzystujący teorii grup) dowód małego twierdzenia Fermata. Jeśli liczba całkowita a dzieli się przez p, to oczywiście $p|a^p - a$. Nietrudno pokazać, że dla dowolnej liczby całkowitej a, warunek $p|a^p - a$ pociąga za sobą $p|(a+1)^p - (a+1)$. Z obu tych faktów wynika łatwo, że dla dowolnej liczby całkowitej a, $p|a^p - a$, co w przypadku gdy p nie dzieli a daje $p|a^{p-1} - 1$.

Dowód. (a) Zauważmy, że

$$f(e_G) * f(e_G) = f(e_G \circ e_G) = f(e_G) = f(e_G) * e_H.$$

Stąd na mocy prawa skracań otrzymujemy $f(e_G) = e_H$.

(b) Niech $a \in G$. Wtedy

$$f(a) * f(a^{-1}) = f(a \circ a^{-1}) = f(e_G) = e_H.$$

Podobnie $f(a^{-1}) * f(a) = e_H$. Zatem $f(a^{-1}) = f(a)^{-1}$.

(c) Niech $a \in G$. Udowodnimy najpierw matodą indukcji matematycznej, że równość $f(a^n) = f(a)^n$ jest prawdziwa dla $n \in \mathbb{N}$. Z (a) wynika, że $f(a^0) = f(e_G) = e_H = f(a)^0$. Załóżmy teraz, że $f(a^n) = f(a)^n$, gdzie $n \in \mathbb{N}$. Wtedy:

$$f(a^{n+1}) = f(a^n \circ a) = f(a^n) * f(a) = f(a)^n * f(a) = f(a)^{n+1}.$$

W ten sposób wykazaliśmy, że $f(a^n) = f(a)^n$ dla $n \in \mathbb{N}$.

Jeśli $n \in \mathbb{N}_+$, to na mocy powyższego rozumowania i punktu (b) otrzymujemy:

$$f(a^{-n}) = f((a^{-1})^n) = f(a^{-1})^n = (f(a)^{-1})^n = f(a)^{-n}.$$

Tak więc równość z punktu (c) jest słuszna dla wszystkich wykładników całkowitych.

Nierówność $rz(f(a)) \leq rz(a)$ jest oczywista w przypadku, gdy $rz(a) = \infty$. Załóżmy, że $rz(a) = n \in \mathbb{N}_+$.

$$f(a)^n = f(a^n) = f(e_G) = e_H,$$

co oznacza, że $rz(f(a)) \leq n$. ■

Twierdzenie 4.27 *Złożenie dwóch homomorfizmów grup jest homomorfizmem grup. To samo dla monomorfizmów, epimorfizmów i izomorfizmów.*

Dowód. Niech $(G, \odot)$, $(H, *)$ i $(K, \cdot)$ będą grupami, zaś odwzorowania $f : G \longrightarrow H$ i $g : H \longrightarrow K$ homomorfizmami. Jeśli $a, b \in G$, to

$$(g \circ f)(a \odot b) = g(f(a \odot b)) = g(f(a) * f(b)) = g(f(a)) \cdot g(f(b)) = (g \circ f)(a) \cdot (g \circ f)(b).$$

Pozostała część twierdzenia wynika z tego, że złożenie dwóch injekcji jest injekcją, zaś złożenie dwóch surjekcji jest surjekcją. ■

Definicja 4.28 *Mówimy, że grupy G i H są izomorficzne, jeśli istnieje izomorfizm $f : G \longrightarrow H$. Piszemy wtedy: $G \cong H$.*

Twierdzenie 4.29 *Niech G, H i K będą grupami. Wtedy:*
(a) $G \cong G$,
(b) jeśli $G \cong H$, to $H \cong G$,
(c) jeśli $G \cong H$ i $H \cong K$, to $G \cong K$.

Dowód. Zależność (a) wynika z tego, że odwzorowanie identycznościowe jest izomorfizmem, zaś (c) jest konsekwencją twierdzenia 4.27.

W celu wykazania (b) załóżmy, że $f : G \longrightarrow H$ jest izomorfizmem grup $(G, \circ)$ i $(H, *)$. Wtedy f jest bijekcją, a więc istnieje funkcja odwrotna do f (oznaczenie: f^{-1}), która również jest bijekcją. Pokażemy, że f^{-1} jest homomorfizmem. Niech $a, b \in H$. Wtedy:

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

■

Przykład 12. Grupy $(\mathbb{R}, +)$ i $(\mathbb{R}_+, \cdot)$ są izomorficzne. Łatwo sprawdzić, że odwzorowanie $f : \mathbb{R} \longrightarrow \mathbb{R}_+$ określone wzorem $f(x) = 2^x$ jest izomorfizmem.

Przykład 13. Grupy $(\mathbb{R} \setminus \{0\}, \cdot)$ i $(\mathbb{R}_+, \cdot)$ nie są izomorficzne. Dle dowodu pokażemy, że dowolny homomorfizm z grupy $(\mathbb{R} \setminus \{0\}, \cdot)$ w grupę $(\mathbb{R}_+, \cdot)$ nie jest różnowartościowy.

Niech $f : \mathbb{R} \longrightarrow \mathbb{R}_+$ będzie homomorfizmem rozważanych grup. Wtedy

$$1 = f(1) = f((-1) \cdot (-1)) = f(-1)^2.$$

Stąd zaś wynika, że $f(-1) = 1 = f(1)$. Tak więc $(\mathbb{R} \setminus \{0\}, \cdot) \ncong (\mathbb{R}_+, \cdot)$. W ten sam sposób można pokazać, że $(\mathbb{Q} \setminus \{0\}, \cdot) \ncong (\mathbb{Q}_+, \cdot)$.

Przykład 14. Grupy $(\mathbb{Q}, +)$ i $(\mathbb{Q}_+, \cdot)$ nie są izomorficzne. Przypuśćmy bowiem, że istnieje izomorfizm f z grupy $(\mathbb{Q}, +)$ w grupę $(\mathbb{Q}_+, \cdot)$. Wtedy dla pewnego $a \in \mathbb{Q}$ mamy $f(a) = 2$. f jest homomorfizmem, więc

$$2 = f(a) = f\left(\frac{a}{2} + \frac{a}{2}\right) = f\left(\frac{a}{2}\right)^2.$$

Równość powyższa nie może jednak zachodzić, gdyż równanie $x^2 = 2$ nie posiada rozwiązań w zbiorze liczb wymiernych. Dlatego $(\mathbb{Q}, +) \ncong (\mathbb{Q}_+, \cdot)$.

Twierdzenie 4.30 *Zbiór automorfizmów dowolnej grupy z działaniem składania przekształceń stanowi grupę.*

Dowód. Niech G będzie grupą, zaś $\circ$ składaniem przekształceń w zbiorze $Aut(G)$. Działanie $\circ$ jest oczywiście łączne w $Aut(G)$.

Przekształcenie identycznościowe z G w G (oznaczenie: Id_G) jest automorfizmem grupy G. Co więcej, jeśli $f \in Aut(G)$, to $f \circ Id_G = Id_G \circ f = f$, czyli Id_G jest elementem neutralnym działania $\circ$.

Załóżmy, że $f, g \in Aut(G)$. Wtedy f, g są homomorfizmami oraz są bijekcjami. To zaś imlikuje, że również $f \circ g$ jest homomorfizmem oraz bijekcją. A więc $f \circ g \in Aut(G)$.

Jeśli $f \in Aut(G)$, to postępując jak w dowodzie twierdzenia 4.29(b) pokazujemy, że również f^{-1} (odwzorowanie odwrotne do f) jest automorfizmem grupy G.

W ten sposób wykazaliśmy, że $(Aut(G), \circ)$ jest grupą. ■

Definicja 4.31 *Niech $f : G \longrightarrow H$ będzie homomorfizmem grup. Zbiór*

$$Ker(f) = \{a \in G : f(a) = e_H\}$$

nazywamy jądrem homomorfizmu f. W przypadku, gdy $Ker(f) = \{e_G\}$, mówimy, że homomorfizm f ma trywielne jądro. Zbiór

$$Im(f) = \{f(a) : a \in G\}$$

nazywamy obrazem homomorfizmu f.

Twierdzenie 4.32 *Jeśli $f : G \longrightarrow H$ jest homomorfizmem grup, to*

(a) $Ker(f)$ jest dzielnikiem normalnym (a więc również podgrupą) grupy G,

(b) $Im(f)$ jest podgrupą grupy H.

(c) Dla każdego $b \in Im(f)$, $f^{-1}(b) = \{a \in G : f(a) = b\}$ jest warstwą podgrupy $Ker(f)$.

Dowód. Niech $f : G \longrightarrow H$ będzie homomorfizmem grup.

(a) Pokażemy najpierw, że $Ker(f)$ jest podgrupą grupy G. $f(e_G) = e_H$, więc $e_G \in Ker(f)$. Jeśli $a, b \in Ker(f)$, to

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)f(b)^{-1} = e_H e_H^{-1} = e_H,$$

skąd wynika, że $ab^{-1} \in Ker(f)$. Zatem, wobec warunku (e) twierdzenia 4.2, $Ker(f) < G$.

Dla wykazania, że $Ker(f)$ jest dzielnikiem normalnym grupy G, udowodnimy warunek (b) twierdzenia 4.23. Załóżmy, że $a \in G$ i $h \in Ker(f)$. Wtedy:

$$f(a^{-1}ha) = f(a^{-1})f(h)f(a) = f(a)^{-1}e_H f(a) = f(a)^{-1}f(a) = e_H,$$

a więc $a^{-1}ha \in Ker(f)$. Oznacza to, że $Ker(f) \lhd G$.

(b) Równość $f(e_G) = e_H$ oznacza, że $e_H \in Im(f)$. Jeśli $a \in Im(f)$, to istnieje element $b \in G$ taki, że $f(b) = a$. Wtedy $f(b^{-1}) = f(b)^{-1} = a^{-1}$ i $a^{-1} \in Im(f)$. Jeśli $a_1, a_2 \in Im(f)$, to $a_1 = f(b_1)$ i $a_2 = f(b_2)$ dla pewnych $b_1, b_2 \in G$. Stąd wynika, że $f(b_1b_2) = f(b_1)f(b_2) = a_1a_2$, czyli $a_1a_2 \in Im(f)$. Zatem $Im(f)$ jest podgrupą grupy G.

(c) Niech $b \in Im(f)$. Wtedy $f(a) = b$ dla pewnego $a \in G$. Pokażemy, że $f^{-1}(b) = aKer(f)$. Zauważmy, że

$$\begin{aligned} x \in f^{-1}(b) &\iff f(x) = b = f(a) \iff f(x)f(a)^{-1} = e_H \iff f(xa^{-1}) = e_H \\ &\iff xa^{-1} \in Ker(f) \iff x \in Ker(f)a = aKer(f). \end{aligned}$$

To kończy dowód. ■

Nietrudno podać przykład homomorfizmu grup $f : G \longrightarrow H$, którego obraz nie jest dzielnikiem normalnym grupy H. Rozważmy odwzorowanie $f : \mathbb{Z}_2 \longrightarrow S_3$ zadane wzorami: $f(0) = e$ i $f(1) = (1, 2)$. $Im(f) = \{e, (1, 2)\}$ nie jest dzielnikiem normalnym grupy S_3 (przykład 10, strona 42).

Twierdzenie 4.33 *Niech $f : G \longrightarrow H$ będzie homomorfizmem grup. Wówczas f jest monomorfizmem wtedy i tylko wtedy, gdy $Ker(f) = \{e_G\}$.*

Dowód. Załóżmy, że $f : G \longrightarrow H$ jest monomorfizmem grup. Jeśli $g \in Ker(f)$, to $f(g) = e_H = f(e_G)$. f jest odwzorowaniem różnowartościowm, więc $g = e_G$. Tak więc $Ker(f) = \{e_G\}$.

W celu wykazania implikacji przeciwnej, załóżmy, że $f : G \longrightarrow H$ jest homomorfizmem grup, którego jądro jest trywialne, tzn. $Ker(f) = \{e_G\}$. Wtedy dla dowolnych $g, h \in G$ otrzymujemy:

$$\begin{aligned} f(g) = f(h) &\implies f(g)f(h)^{-1} = e_H \implies f(gh^{-1}) = e_H \implies \\ &\implies gh^{-1} \in Ker(f) = \{e_G\} \implies gh^{-1} = e_G \implies g = h, \end{aligned}$$

co oznacza, że f jest odwzorowaniem różnowartościowym.

Twierdzenie 4.34 *Niech $f : G \longrightarrow H$ będzie homomorfizmem grup skończonych.*

(a) Jeśli f jest monomorfizmem, to $|G|$ dzieli $|H|$.

(b) Jeśli f jest epimorfizmem, to $|H|$ dzieli $|G|$.

Dowód. (a) Na mocy twierdzenia 4.32(b), $Im(f)$ jest podgrupą grupy H. Z twierdzenia Lagrange'a (twierdzenie 4.13) wynika, że

$$|H| = [H : Im(f)] \cdot |Im(f)|,$$

czyli $|Im(f)|$ dzieli $|H|$. f jest odwzorowaniem różnowartościowym, więc $|Im(f)| = |G|$ i dostajemy tezę.

(b) Niech $f : G \longrightarrow H$ będzie epimorfizmem. $Ker(f)$ jest podgrupą grupy G, więc na mocy twierdzenia Lagrange'a,

$$|G| = [G : Ker(f)] \cdot |Ker(f)|.$$

Jeśli $a \in H$, to zbiór $f^{-1}(a) = \{b \in G : f(b) = a\}$ jest warstwą podgrupy $Ker(f)$. Ponadto różnym elementom grupy H odpowiadają różne warstwy. Oznacza to, że indeks $Ker(f)$ w grupie G jest równy H, czyli $|G| = |H| \cdot |Ker(f)|$. Zatem $|H|$ dzieli $|G|$. ■

Twierdzenie 4.35 *(twierdzenie Cayleya[4]) Dowolna grupa G jest izomorficzna z pewną podgrupą grupy permutacji zbioru G. W szczególności dowolna grupa n-elementowa jest izomorficzna z pewną podgrupą grupy S_n.*

Dowód. Niech G będzie grupą. Dla elementu $g \in G$ przez F_g oznaczmy funkcję ze zbioru G w zbiór G daną wzorem $F_g(x) = gx$. Jak łatwo sprawdzić, dla dowolnego $g \in G$, F_g jest permutacją zbioru G: surjektywność F_g wynika z równości $F_g(g^{-1}h) = h$ prawdziwej dla dowolnych $g, h \in G$, zaś injektywność jest konsekwencją prawa skracań (twierdzenie 2.4). Tak więc odwzorowanie $\alpha : G \longrightarrow S_G$ (S_G oznacza grupę permutacji zbioru G) zdefiniowane wzorem $\alpha(g) = F_g$ jest dobrze określone. Pokażemy jeszcze, że α jest monomorfizmem.

Niech g i h będą dowolnymi elementami grupy G. Wtedy dla dowolnego $x \in G$:

$$\alpha(gh)(x) = F_{gh}(x) = (gh)x = g(hx) = F_g(F_h(x)) = (F_g \circ F_h)(x) = (\alpha(g) \circ \alpha(h))(x),$$

czyli $\alpha(gh) = \alpha(g) \circ \alpha(h)$, skąd wynika, że α jest homomorfizmem grup. Zauważmy ponadto, że

$$\alpha(g) = \alpha(h) \Longrightarrow F_g = F_h \Longrightarrow F_g(e) = F_h(e) \Longrightarrow g \circ e = h \circ e \Longrightarrow g = h,$$

czyli α jest odwzorowaniem różnowartościowym. ■

Przykład 15. Dla zilustrowania dowodu twierdzenia Cayleya znajdziemy zanurzenie grupy D_4 (tzn. grupy izometrii własnych kwadratu) w grupę S_8. Z przykładu 17 ze strony 26 wiemy, że

$$D_4 = \{I, R, R^2, R^3, S, RS, R^2S, R^3S\},$$

gdzie I jest przekształceniem identycznościowym, R obrotem o kąt 90 stopni, zaś S symetrią osiową względem symetralnej pary przeciwległych boków. Przyjmijmy ozmaczenia:

$$g_1 = I, g_2 = R, g_3 = R^2, g_4 = R^3, g_5 = S, g_6 = RS, g_7 = R^2S \text{ i } g_8 = R^3S.$$

Tak jak w dowodzie twierdzenia Cayleya, dla dowolnego $g \in D_4$, przez F_g oznaczamy odwzorowanie z grupy D_4 w grupę D_4 określone wzorem $F_g(x) = gx$. Biorąc pod uwagę, że

$$SR = R^3S, SR^2 = R^2S \text{ i } SR^3 = RS,$$

możemy łatwo wyznaczyć $F_{g_i}(g_j) = g_ig_j$ dla dowolnych $i, j \in \{1, \ldots, 8\}$. Wyniki zamieszczone są w poniższej tabeli.

x	$F_{g_1}(x)$	$F_{g_2}(x)$	$F_{g_3}(x)$	$F_{g_4}(x)$	$F_{g_5}(x)$	$F_{g_6}(x)$	$F_{g_7}(x)$	$F_{g_8}(x)$
g_1	g_1	g_2	g_3	g_4	g_5	g_6	g_7	g_8
g_2	g_2	g_3	g_4	g_1	g_8	g_5	g_6	g_7
g_3	g_3	g_4	g_1	g_2	g_7	g_8	g_5	g_6
g_4	g_4	g_1	g_2	g_3	g_6	g_7	g_8	g_5
g_5	g_5	g_6	g_7	g_8	g_1	g_2	g_3	g_4
g_6	g_6	g_7	g_8	g_5	g_4	g_1	g_2	g_3
g_7	g_7	g_8	g_5	g_6	g_3	g_4	g_1	g_2
g_8	g_8	g_5	g_6	g_7	g_2	g_3	g_4	g_1

Przyporządkowując elementowi $g_i \in D_4$ permutację $\sigma_i \in S_8$ taką, że

$$\sigma_i(j) = k \Longleftrightarrow F_{g_i}(g_j) = g_k \text{ dla } i, j, k \in \{1, \ldots, 8\},$$

dostajemy poszukiwane zanurzenie.

[4] Arthur Cayley (1821-1895), matematyk angielski

Rozdział 5

Grupa ilorazowa

Niech G będzie grupą, zaś H jej dzielnikiem normalnym. Wówczas warstwa lewostronna dowolnego elementu $a \in G$ względem H jest równa warstwie prawostronnej a względem H. Zbiór warstw dzielnika normalnego H w grupie G będziemy oznaczać przez G/H:

$$G/H = \{aH : a \in G\} = \{Ha : a \in G\}.$$

W zbiorze tym określimy pewne działanie i pokażemy, że G/H z tak zdefiniowanym działaniem jest grupą.

Twierdzenie 5.1 *Niech G będzie grupą, zaś H jej dzielnikiem normalnym. Wówczas wzór:*

$$aH \circ bH = (ab)H$$

definiuje działanie w zbiorze warstw G/H. G/H z tak określonym działaniem stanowi grupę.

Dowód. Sprawdzimy najpierw, że powyższy wzór określa działanie w G/H, to znaczy, że każdej uporządkowanej parze warstw względem podgrupy H przyporządkowana jest jednoznacznie pewna warstwa względem podgrupy H. Innymi słowy, pokażemy, że wynik działania $\circ$ na warstwach aH i bH nie zależy od wyboru reprezentantów a i b.

Załóżmy więc, że a, a_1, b, b_1 są takimi elementami grupy G, że $aH = a_1H$ i $bH = b_1H$. Pokażemy, że $(ab)H = (a_1b_1)H$. Z założenia $aH = a_1H$ i $bH = b_1H$, więc $a = a_1h_1$ i $b = a_2h_2$ dla pewnych $h_1, h_2 \in H$. Stąd $ab = a_1h_1b_1h_2$. $Hb_1 = b_1H$, więc $h_1b_1 = b_1h_3$ dla pewnego $h_3 \in H$. Po podstawieniu otrzymujemy: $x = (a_1b_1)(h_3h_2)$, co oznacza, że $ab \in (a_1b_1)H$, czyli $(ab)H = (a_1b_1)H$.

Udowodnimy teraz, że zbiór G/H z działaniem $\circ$ stanowi grupę. W tym celu sprawdzimy, że spełnione są aksjomaty teorii grup.

Działanie $\circ$ jest łączne:

$$(aH \circ bH) \circ cH = (ab)H \circ cH = ((ab)c)H = (a(bc))H = aH \circ (bc)H = aH \circ (bH \circ cH).$$

Elementem neutralnym działania $\circ$ jest warstwa $eH = H$:

$$aH \circ eH = (ae)H = aH.$$

Tak samo dowodzi się, że $eH \circ aH = aH$.

Elementem odwrotnym do warstwy aH jest warstwa $a^{-1}H$:

$$aH \circ a^{-1}H = (aa^{-1})H = eH.$$

Podobnie $aH \circ a^{-1}H = eH$. ■

W związku z powyższym twierdzeniem przyjmujemy następującą definicję.

Definicja 5.2 *Niech H będzie dzielnikiem normalnym grupy G. Grupę warstw G/H, w której działanie jest określone wzorem z twierdzenia 5.1 nazywamy grupą ilorazową grupy G modulo H.*

Poniższe twierdzenie zwane jest pierwszym twierdzeniem o izomorfizmie lub zasadniczym twierdzeniem o homomorfizmach grup[1].

Twierdzenie 5.3 *Niech $\varphi : G \longrightarrow H$ będzie homomorfizmem grup. Wtedy odwzorowanie $\psi : G/Ker(\varphi) \longrightarrow H$ określone wzorem:*

$$\psi(aKer(\varphi)) = \varphi(a) \text{ dla } a \in G$$

jest monomorfizmem grup i grupa ilorazowa $G/Ker(\varphi)$ jest izomorficzna z $Im(\varphi)$.

Dowód. Pokażemy najpierw, że odwzorowanie ψ jest dobrze określone. Innymi słowy, pokażemy, że jego wynik na warstwie $aKer(\varphi)$ zależy jedynie od tej warstwy, a nie zależey od wyboru jej reprezentanta a.

Załóżmy, że $aKer(\varphi) = bKer(\varphi)$. Wtedy $a^{-1}b \in Ker(\varphi)$. Tak więc mamy:

$$\varphi(a^{-1}b) = e_H \Longrightarrow \varphi(a)^{-1}\varphi(b) = e_H \Longrightarrow \varphi(a) = \varphi(b).$$

Zatem ψ jest dobrze określone.

ψ jest homomorfizmem grup, ponieważ dla dowolnych $a, b \in G$,

$$\psi(aKer(\varphi) \circ bKer(\varphi)) = \psi(abKer(\varphi)) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aKer(\varphi))\psi(bKer(\varphi)).$$

ψ jest odwzorowaniem różnowartościowym. Załóżmy bowiem, że $\psi(aKer(\varphi)) = \psi(bKer(\varphi))$, gdzie $a, b \in G$. Wtedy (z definicji ψ) dostajemy $\varphi(a) = \varphi(b)$. φ jest homomorfizmem, więc $\varphi(a^{-1}b) = \varphi(a)^{-1}\varphi(b) = e_H$. Oznacza to, że $a^{-1}b \in Ker(\varphi)$. Stąd zaś wynika, że $aKer(\varphi) = bKer(\varphi)$. W ten sposób udowodniliśmy, że ψ jest monomorfizmem.

Aby zakończyć dowód twierdzenia, pokażemy jeszcze, że $Im(\psi) = Im(\varphi)$. Inkluzja $\subseteq$ wynika wprost z określenia ψ. Przypuśćmy więc, że $b \in Im(\varphi)$. Wtedy $b = \varphi(a)$ dla pewnego $a \in G$, skąd wynika, że $\psi(aKer(\varphi)) = \varphi(a) = b$, czyli $b \in Im(\psi)$. ■

Wniosek 5.4 *Jeśli $\varphi : G \longrightarrow H$ jest epimorfizmem grup, to grupa ilorazowa $G/Ker(\varphi)$ jest izomorficzna z grupą H.*

Zilustrujemy teraz pojęcie grupy ilorazowej kilkoma przykładami.

Przykład 1. Jeśli G jest dowolną grupą, to $G/\{e\} \cong G$. Izomorfizmem jest tu odwzorowanie przyporządkowujące elementowi $a \in G$ warstwę $a\{e\} = \{a\}$. Ponadto $G/G \cong \{e\}$, co wynika z tego, że grupa ilorazowa składa się tutaj tylko z jednej warstwy.

Przykład 2. Pokażemy, że dla dowolnego $n \geq 2$, $S_n/A_n \cong \mathbb{Z}_2$ (A_n oznacza zbiór permutacji parzystych). Niech $f : S_n \longrightarrow \mathbb{Z}_2$ będzie odwzorowaniem określonym następująco:

$$f(\sigma) = \begin{cases} 0 & \text{gdy } \sigma \in A_n \\ 1 & \text{gdy } \sigma \in S_n \setminus A_n \end{cases}$$

Zauważmy, że:

(a) jeśli $\sigma, \tau \in A_n$, to $\sigma\tau \in A_n$ i $f(\sigma) = f(\tau) = f(\sigma\tau) = 0$,

(b) jeśli $\sigma, \tau \in S_n \setminus A_n$, to $\sigma\tau \in A_n$ i $f(\sigma) = f(\tau) = 1$, $f(\sigma\tau) = 0$,

[1] w literaturze angielskojęzycznej: first isomorphism theorem

(c) jeśli $\sigma \in A_n$ i $\tau \in S_n \setminus A_n$, to $\sigma\tau \in S_n \setminus A_n$ i $f(\sigma) = 0$, $f(\tau) = 1$, $f(\sigma\tau) = 1$,
(d) jeśli $\sigma \in S_n \setminus A_n$ i $\tau \in A_n$, to $\sigma\tau \in S_n \setminus A_n$ i $f(\sigma) = 1$, $f(\tau) = 0$, $f(\sigma\tau) = 1$.
We wszystkich czterech przypadkach otrzymujemy $f(\sigma\tau) = f(\sigma) +_2 f(\tau)$, co oznacza, że f jest homomorfizmem grup. f jest oczywiście surjekcją. Co więcej, $Ker(f) = A_n$. Na mocy wniosku 5.4 oznacza to, że $S_n/A_n \cong \mathbb{Z}_2$.

Jeśli $(G, \circ)$ jest grupą, zaś A i B jej podzbiorami, to przez AB będziemy rozumieli zbiór wszystkich iloczynów $a \circ b$, gdzie $a \in B$, zaś $b \in B$.

Twierdzenie 5.5 *(Drugie twierdzenie o izomorfizme) Jeśli H i K są podgrupami grupy G, przy czym $K \lhd G$, to*
(a) $HK = KH < G$,
(b) $K \lhd HK$,
(c) $H \cap K \lhd H$,
(d) $H/H \cap K \cong HK/K$.

Dowód. Załóżmy, że $H < G$ i $K \lhd G$. Ustalmy element $a \in HK$. Wtedy $a = hk$, przy czym $h \in H$ i $k \in K$. $hK = Kh$, więc $hk = k_1h$ dla pewnego $k_1 \in K$, co oznacza, że $hk \in KH$. W ten sposób pokazaliśmy, że $HK \subseteq KH$. Podobnie dowodzi się inkluzji przeciwnej.

Oczywiście $HK \neq \emptyset$, ponieważ $e \in HK$. Ustalmy elementy $a, b \in HK$. Pokażemy, że $ab^{-1} \in HK$. Wtedy $a = hk$ i $b = h'k'$ dla pewnych $h, h' \in H$ oraz $k, k' \in K$. Oczywiście

$$ab^{-1} = hk(h'k')^{-1} = hkk'^{-1}h'^{-1} = hh'^{-1}k_1$$

dla pewnego $k_1 \in K$, co oznacza, że $ab^{-1} \in HK$. Tak więc $HK < G$.

Punkt (b) twierdzenia wynika bezpośrednio z tego, że $K \lhd G$ oraz $K \subseteq HK < G$.

W celu udowodnienia (c), ustalmy $g \in H \cap K$ oraz $h \in H$. Ponieważ $g, h \in H$, mamy $h^{-1}gh \in H$. Z tego, że $K \lhd G$ i $g \in K$ wynika, że $h^{-1}gh \in K$. Tak więc $h^{-1}gh \in H \cap K$. W ten sposób, wobec twierdzenia 4.23, wykazaliśmy, że $H \cap K \lhd H$.

Dowód punktu (d) przeprowadzimy w oparciu o wniosek 5.4. Rozważmy odwzorowanie $\varphi : H \longrightarrow HK/K$ przyporządkowujące elementowi $h \in H$ warstwę $hK \in HK/K$. φ jest homomorfizmem grup, gdyż dla dowolnych $h_1, h_2 \in H$ mamy:

$$\varphi(h_1h_2) = (h_1h_2)K = (h_1K) \circ (h_2K).$$

Ponadto:

$$Ker(\varphi) = \{h \in H : hK = K\} = \{h \in H : h \in K\} = H \cap K.$$

Dla wykazania, że φ jest surjekcją, ustalmy element $a \in HK/K$. Wtedy $a = (hk)K$ dla pewnych $h \in H$ oraz $k \in K$. Mamy oczywiście

$$\varphi(h) = hK = (hK) \circ K = (hK) \circ (kK) = (hk)K = a.$$

Z wniosku 5.4 dostajemy izomorfizm $H/H \cap K \cong HK/K$, co kończy dowód. ■

Twierdzenie 5.6 *(Trzecie twierdzenie o izomorfizmie) Jeżeli H i K są dzielnikami normalnymi grupy G, przy czym K jest podgrupą H, to:*
(a) K jest dzielnikiem normalnym H,
(b) H/K jest dzielnikiem normalnym G/K,
(c) $(G/K)/(H/K) \cong G/H$.

Dowód. (a) Z założenia $K \lhd G$ i $K < H \lhd G$. Stąd $K \lhd H$.

W celu wykazania (b) i (c) wskażemy homomorfizm z grupy G/K na grupę G/H, którego jądrem jest H/K.

Niech odwzorowanie $f : G/K \longrightarrow G/H$ będzie zdefiniowane wzorem: $f(aK) = aH$.

Odwzorowanie f jest dobrze określone. Przypuśćmy bowiem, że $a, b \in G$ i $aK = bK$. Wtedy $a^{-1}b \in K \subseteq H$, a więc $aH = bH$.

f jest homomorfizmem grup. Mamy bowiem:

$$f((aK) \circ (bK)) = f((ab)K) = (ab)H = (aH) \circ (bH)$$

(dla uproszczenia działania w grupach G/K i G/H oznaczone zostały tym samym symbolem $\circ$). f jest oczywiście surjekcją.

Zauważmy, że

$$Ker(f) = \{aK \in G/K : f(aK) = H\} = \{aK \in G/K : aH = H\} = \{aK \in G/K : a \in H\} = H/K.$$

Na mocy twierdzenia 4.32(a), $H/K \lhd G/K$. Wniosek 5.4 implikuje, że $(G/K)/(H/K) \cong G/H$. ■

Rozdział 6

O klasyfikacji grup

Jednym z ważniejszych problemów zarówno algebry jak i innych dziedzin matematyki jest klasyfikacja obiektów określonego typu z dokładnością do pewnej równoważności (na przykład klasyfikacja określonego rodzaju grup z dokładnością do izomorfizmu). W niniejszym rozdziale opiszemy z dokładnością do izomorfizmu następujące klasy grup:

(a) grupy cykliczne (definicja 6.1),
(b) grupy rzędów p i p^2, gdzie p jest liczbą pierwszą,
(c) skończone grupy abelowe i
(d) grupy rzędu ≤ 10.

Niektóre dowody przy tym pominiemy.

Definicja 6.1 *Grupę G nazywamy cykliczną, jeśli ma ona zbiór generatorów złożony z jednego elementu. Element ten nazywamy wówczas generatorem grupy G.*

Przykładami grup cyklicznych są: $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +_n)$ dla $n \in \mathbb{N}_+$, grupa obrotów n-kąta foremnego, grupa zespolonych pierwiastków z jedności ustalonego stopnia $n \in \mathbb{N}_+$. Trzy ostatnie spośród wymienionych grup są dla danego $n \geq 3$ izomorficzne.

Jeśli a jest generatorem grupy G, to zgodnie z definicją ze strony 37,

$$G = \{a^{\varepsilon_1} \dots a^{\varepsilon_n} : n \in \mathbb{N}_+, \varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}\} \cup \{e_G\} = \{a^n : n \in \mathbb{Z}\}.$$

Fakt 6.2 *Każda grupa cykliczna jest abelowa, ale nie na odwrót.*

Dowód. Niech G będzie grupą cykliczną. Wtedy $G = \{a^n : n \in \mathbb{Z}\}$ dla pewnego $a \in G$. Zgodnie ze wzorem z twierdzenia 2.5(a) mamy $a^m a^n = a^{m+n} = a^n a^m$ dla dowolnych $m, n \in \mathbb{Z}$, co dowodzi abelowości grupy G.

Przykładem grupy abelowej niecyklicznej jest grupa czwórkowa Kleina K_4 (przykład 13, str. 23). ■

Poniższe twierdzenie opisuje wszystkie grupy cykliczne z dokładnością do izomorfizmu.

Twierdzenie 6.3 *Każda nieskończona grupa cykliczna jest izomorficzna z grupą $(\mathbb{Z}, +)$, zaś każda skończona grupa cykliczna z grupą $(\mathbb{Z}_k, +_k)$ dla pewnego $k \in \mathbb{N}_+$.*

Dowód. Niech G będzie grupą cykliczną. Wtedy $G = \{a^n : n \in \mathbb{Z}\}$ dla pewnego $a \in G$. Rozważymy 2 przypadki.

Przypadek 1. Dla dowolnych $m, n \in \mathbb{Z}$, $a^m \neq a^n$. Definiujemy odwzorowanie $f : G \longrightarrow \mathbb{Z}$ wzorem $f(a^m) = m$ dla $m \in \mathbb{Z}$. Wprost z okreŕślenia f wynika, że f jest bijekcją. Dla dowolnych $m, n \in \mathbb{Z}$,

$$f(a^m a^n) = f(a^{m+n}) = m + n = f(a^m) + f(a^n),$$

co oznacza, że f jest homomorfizmem. Zatem $G \cong (\mathbb{Z}, +)$.

Przypadek 2. Istnieją liczby całkowite m i n takie, że $m < n$ i $a^n = a^m$. Mnożąc obie strony tej równości przez a^{-m} dostajemy $a^{n-m} = e$ (z założenia $n - m > 0$). Niech teraz k będzie najmniejszą liczbą naturalną dodatnią taką, że $a^k = e$. Wtedy oczywiście $a^n = a^{n \bmod k}$ dla wszystkich $n \in \mathbb{Z}$, co implikuje, że $G = \{a^n : 0 \leq n < k\}$. Pokażemy, że odwzorowanie $f : G \longrightarrow \mathbb{Z}_k$ określone wzorem $f(a^n) = n$ $(0 \leq k \leq n-1)$ jest izomorfizmem grup.

Dla dowolnych $m, n \in \mathbb{Z}_k$,

$$f(a^m a^n) = f(a^{m+n}) = f(a^{(m+n) \bmod k}) = (m+n) \bmod k = m +_k n = f(a^m) +_k f(a^n).$$

Oczywiście f jest bijekcją, co kończy dowód. ■

Wniosek 6.4 *Każda grupa cykliczna rzędu n jest izomorficzna z $(\mathbb{Z}_n, +_n)$.*

Na oznaczenie grupy cyklicznej rzędu n używa się też symbolu C_n.

Twierdzenie 6.5 *Jeśli p jest liczbą pierwszą, to każda grupa rzędu p jest izomorficzna z grupą $(\mathbb{Z}_p, +_p)$, a więc jest cykliczna.*

Dowód. Niech G będzie grupą rzędu p, gdzie p jest liczbą pierwszą. Ustalmy element $a \in G \setminus \{e\}$ i niech H będzie podgrupą grupy G generowną przez a. Zgodnie z twierdzeniem Lagrange'a (twierdzenie 4.13), $|H|$ dzieli $|G|$, ale $|H| > 1$ i $|G| = p$ jest liczbą pierwszą. Dlatego $|H| = p$, co oznacza, że $H = G$ i a jest generatorem grupy G. W ten sposób wykazaliśmy, że grupa G jest cykliczna. Na mocy wniosku 6.4, $G \cong (\mathbb{Z}_p, +_p)$. ■

Twierdzenie 6.6 *Jeśli G i H są grupami skończonymi rzędów m i n (odpowiednio), to następujące warunki są równoważne.*

(a) Grupa $G \oplus H$ jest cykliczna.

(b) $NWD(m, n) = 1$ i grupy G, H są obie cykliczne.

Dowód. (a)$\Longrightarrow$ (b). Załóżmy, że grupa $G \oplus H$ jest cykliczna. Niech $\langle a, b\rangle$ będzie jej generatorem. Oczywiście $\mathrm{rz}(\langle a, b\rangle) = mn$. Na mocy twierdzenia 4.15, $\mathrm{rz}(a)|m$ i $\mathrm{rz}(b)|n$, czyli $\mathrm{rz}(a)\mathrm{rz}(b) \leq mn$. Z drugiej strony jednak

$$\langle a, b\rangle^{\mathrm{rz}(a)\mathrm{rz}(b)} = \langle (a^{\mathrm{rz}(a)})^{\mathrm{rz}(b)}, (b^{\mathrm{rz}(b))^{\mathrm{rz}_{(a)}}}\rangle = \langle e_G, e_H\rangle,$$

co oznacza, że $mn = \mathrm{rz}(\langle a, b\rangle) \leq \mathrm{rz}(a)\mathrm{rz}(b)$. W ten sposób

$$(*)\ mn = \mathrm{rz}(a)\mathrm{rz}(b).$$

Z równości $(*)$, wobec $\mathrm{rz}(a) \leq m$ i $\mathrm{rz}(b) \leq n$, dostajemy $\mathrm{rz}(a) = m = |G|$ i $\mathrm{rz}(b) = n = |H|$, co oznacza, że grupy G i H są cykliczne.

Przypuśćmy nie wprost, że $NWD(m, n) = d > 1$. Istnieją $m_1, n_1 \in \mathbb{N}_+$ takie, że $m = m_1 d$ i $n = n_1 d$. Mamy wówczas:

$$\langle a, b\rangle^{m_1 n_1 d} = \langle (a^m)^{n_1}, (b^n)^{m_1}\rangle = \langle e_G, e_H\rangle,$$

skąd wynika, że

$$\mathrm{rz}(\langle a, b\rangle) \leq m_1 n_1 d = m_1 n < mn,$$

sprzeczność z założeniem.

(b)$\Longrightarrow$(a). Załóżmy, że grupy G i H są cykliczne oraz $NWD(m, n) = 1$. Niech a będzie generatorem grupy G, zaś b generatorem grupy H. W celu wykazania cykliczności grupy $G \oplus H$ wystarczy dowieść, że $\mathrm{rz}(\langle a, b\rangle) = mn$. Oczywiście $\mathrm{rz}(\langle a, b\rangle) \leq |G \oplus H| = mn$. Oznaczmy przez k rząd elementu $\langle a, b\rangle$ w grupie $G \oplus H$. Wtedy

$$\langle a^k, b^k\rangle = \langle , b\rangle^k = \langle e_G, e_H\rangle,$$

czyli $a^k = e_G$ i $b^k = e_H$. Ponieważ $\mathrm{rz}(a) = m$ i $\mathrm{rz}(b) = n$, na mocy twierdzenia 4.15 dostajemy $m|k$ i $n|k$. $NWD(m, n) = 1$, więc $mn|k$ i $mn \leq k$, co kończy dowód. ■

Wniosek 6.7 *Jeśli $m, n \in \mathbb{N}_+$ i $NWD(m,n) = 1$, to $\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$.*

Twierdzenie 6.8 *Jeśli p jest liczbą pierwszą, to każda grupa rzędu p^2 jest abelowa.*

Dowód. Niech G będzie grupą rzędu p^2, gdzie p jest liczbą pierwszą. Wtedy rząd dowolnego elementu grupy G jest dzielnikiem liczby p^2, a więc jest równy 1, p lub p^2. Jeżeli G posiada element rzędu p^2, to G jest grupą cykliczną, a więc abelową (fakt 6.2).

Załóżmy więc, że w G nie ma elementu rzędu p^2. Oznacza to, że każdy element grupy G, różny od e, ma rząd p. Ustalmy element $a \in G \setminus \{e\}$. Wtedy oczywiście $H = \{e, a, \ldots, a^{p-1}\}$ jest podgrupą grupy G. H ma rząd p, więc na mocy twierdzenia Lagrange'a, $[G : H] = p$. Pokażemy, że H jest dzielnikiem normalnym G dowodząc, że $bH = Hb$ dla $b \in G$.

Równość powyższa jest oczywista, gdy $b \in H$. Przypuśćmy, więc, że $b \in G \setminus H$. Wtedy $Hb \cap H = \emptyset$. Niech $b_1H, \ldots, b_{p-1}H$ będą wszystkimi (różnymi) warstwami lewostronnymi podgrupy H zawartymi w $G \setminus H$. Ponieważ $Hb \subseteq b_1H \cup \ldots \cup b_{p-1}H$, istnieje $i \in \{1, \ldots, p-1\}$ takie, że $|Hb \cap b_iH| \geq 2$. Niech $c \in Hb \cap b_iH$. Wtedy $Hb = Hc$ i $b_iH = cH$, a więc $|Hc \cap cH| \geq 2$. Stąd $|H \cap c^{-1}Hc| \geq 2$. Na mocy twierdzenia 4.3, $c^{-1}Hc$ jest podgrupą grupy G. Z twierdzenia 4.5, również $H \cap c^{-1}Hc < G$. Zatem $|H \cap c^{-1}Hc|$ dzieli p^2. Ale $H \cap c^{-1}Hc$ nie jest zbiorem jednoelementowym i zawiera się w H. Dlatego $|H \cap c^{-1}Hc| = p$ i $H \cap c^{-1}Hc = H$. To zaś oznacza, że $H = c^{-1}Hc$, czyli $Hc = cH$. Biorąc pod uwagę wcześniejsze rozważania dostajemy:

$$Hb = Hc = cH = b_iH \Longrightarrow b \in b_iH \Longrightarrow b_iH = bH \Longrightarrow Hb = bH.$$

Tak więc H jest dzielnikiem normalnym grupy G.

Ustalmy element $b \in G \setminus H$. Z tego, że $H \lhd G$ wynika, że $ba = a^k b$ dla pewnego $k \in \{1, \ldots, p\}$. Oczywiście $k \neq p$. W przeciwnym wypadku mielibyśmy $ba = b$, czyli $a = e$, wbrew założeniu. Pokażemy, że $k = 1$.

Zauważmy, że

$$\begin{aligned}(ab)^2 &= a(ba)b = aa^k bb = a^{1+k}b^2,\\ (ab)^3 &= (ab)^2 ab = a^{1+k}bbab = a^{1+k}ba^k bb = a^{1+k}a^{k^2}bbb = a^{1+k+k^2}b^3.\end{aligned}$$

Przez indukcję względem l nietrudno wykazać, że

$$(ab)^l = a^{1+k+\ldots+k^{l-1}}b^l \text{ dla } l \in \mathbb{N}_+.$$

Stąd

$$e = (ab)^p = a^{1+k+\ldots+k^{p-1}}b^p = a^{1+k+\ldots+k^{p-1}}.$$

a jest elementem rzędu p, więc na mocy twierdzenia 2.8, $p|1 + k + \ldots + k^{p-1}$. Z małego twierdzenia Fermata wynika, że $p|k^{p-1} - 1$, a więc również

$$p|(k-1)(1 + k + \ldots + k^{p-1}) - (k^{p-1} - 1).$$

Stąd $p|k^{p-1}(k-1)$. k nie dzieli się przez p, więc $p|k-1$, co wobec $k \in \{1, \ldots, p-1\}$ oznacza, że $k = 1$. W ten sposób wykazaliśmy, że $ba = ab$.

Ponieważ $b \in G \setminus H$, z twierdzenia Lagrange'a łatwo wynika, że jedynym elementem wspólnym podgrup $H = \{e, a, \ldots, a^{p-1}\}$ i $\{e, b, \ldots, b^{p-1}\}$ jest e.

Zauważmy, że jeśli $i, j, k, l \in \{0, \ldots, p-1\}$ i $\langle i, j\rangle \neq \langle k, l\rangle$, to $a^i b^j \neq a^k b^l$. W przeciwnym wypadku mielibyśmy $a^{i-k} = b^{l-j}$, co świadczyłoby o tym, że przekrój podgrup H i $\{e, b, \ldots, b^{p-1}\}$ składa się z więcej niż jednego elementu.

Tak więc $G = \{a^i b^j : 0 \leq i, j \leq p-1\}$. Z tego, że $ab = ba$ wynika, że grupa G jest abelowa. ■

Wniosek 6.9 *Jeśli p jest liczbą pierwszą, to każda grupa rzędu p^2 jest izomorficzna z $\mathbb{Z}_{p^2}$ lub z $\mathbb{Z}_p \oplus \mathbb{Z}_p$.*

Dowód. Niech G będzie grupą rzędu p^2, gdzie p jest liczbą pierwszą. Jeśli w G istnieje element rzędu p^2, to G jest cykliczna, a więc izomorficzna z grupą $\mathbb{Z}_{p^2}$.

W przeciwnym wypadku możemy wybrać elementy $a, b \in G \setminus \{e\}$ takie, że przekrój podgrup generowanych przez te elementy jest jednoelementowy. Oczywiście w tej sytuacji

$$G = \{a^i b^j : 0 \leq i, j \leq p-1\} \text{ oraz } ab = ba.$$

Nietrudno sprawdzić, że odwzorowanie $f : G \longrightarrow \mathbb{Z}_p \oplus \mathbb{Z}_p$ określone wzorem $f(a^i b^j) = \langle i, j \rangle$ jest izomorfizmem grup. ■

Podobnie jak we wniosku 6.9 można sklasyfikować grupy abelowe, których rzędy są dowolnymi potęgami liczb pierwszych.

Twierdzenie 6.10 *Jeśli p jest liczbą pierwszą, zaś n liczbą naturalną dodatnią, to każda grupa abelowa rzędu p^n jest izomorficzna z $\mathbb{Z}_{p^n}$ lub z sumą prostą postaci $\mathbb{Z}_{p^{\alpha_1}} \oplus \ldots \oplus Z_{p^{\alpha_k}}$, gdzie $\langle \alpha_1, \ldots, \alpha_k \rangle$ jest niemalejącym ciągiem liczb naturalnych dodatnich takim, że $\alpha_1 + \ldots + \alpha_k = n$.*

Z powyższego twierdzenia wynika na przykład, że z dokładnością do izomorfizmu istnieją dokładnie 3 grupy abelowe rzędu 8, mianowicie: $\mathbb{Z}_8$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4 \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Jeśli p jest liczbą pierwszą i $n \in \mathbb{N}_+$, to liczba nieizomorficznych grup abelowych rzędu p^n jest równa liczbie niemalejęcych ciągów liczb naturalnych postaci $\langle \alpha_1, \ldots, \alpha_k \rangle$, przy czym $k \in \{1, \ldots, n\}$ i $\alpha_1 + \ldots + \alpha_k = n$.

Twierdzenie 6.11 *Niech $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, gdzie $p_1, \ldots, p_k$ są różnymi liczbami pierwszymi, zaś $\alpha_1, \ldots, \alpha_k \in \mathbb{N}_+$. Jeśli G jest grupą abelową rzędu n to $G \cong G_1 \oplus \ldots \oplus G_k$, gdzie $G_1, \ldots, G_k$ są grupami abelowymi rzędów $p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$ (odpowiednio).*

Z twierdzeń 6.10 i 6.11 wynikają następujące wnioski.

Wniosek 6.12 *Każda skończona grupa abelowa jest sumą prostą grup cyklicznych.*

Wniosek 6.13 *Jeśli G jest skończoną grupą abelową, która nie jest cykliczna, to G zawiera podgrupę izomorficzną z $\mathbb{Z}_p \oplus \mathbb{Z}_p$ dla pewnej liczby pierwszej p.*

Wniosek 6.14 *Jeśli G jest skończoną grupą abelową rzędu n, zaś m liczbą naturalną taką, że $m|n$, to G posiada podgrupę rzędu m.*

Poniżej przedstawiamy klasyfikację wszystkich grup rzędu co najwyżej 10 (z dokładnością do izomorfizmu).

n	Grupy rzędu n (z dokładnością do izomorfizmu)
1	$\mathbb{Z}_1$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_4$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong K_4$ (grupa czwórkowa Kleina)
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$ $S_3 \cong D_3$ (D_3 – grupa izometrii własnych trójkąta równobocznego)
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8$ $\mathbb{Z}_2 \oplus \mathbb{Z}_4$ $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ D_4 (grupa izometrii własnych kwadratu) Q_8 (grupa kwaternionów)
9	$\mathbb{Z}_9$ $\mathbb{Z}_3 \oplus \mathbb{Z}_3$
10	$\mathbb{Z}_{10} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_5 \oplus \mathbb{Z}_2$ D_5 (grupa izometrii własnych pięciokąta foremnego)

Rozdział 7

Pierścienie i ciała – zagadnienia wstępne

W poprzednich rozdziałach zajmowaliśmy się przede wszystkim strukturami algebraicznymi z jednym działaniem, w szczególności grupami. W matematyce często mamy do czynienia ze zbiorami, w których określone są dwa działania. Przykładami takich zbiorów są:

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ze zwykłymi działaniami dodawania i mnożenia,
- zbiór macierzy kwadratowych wymiaru 2×2 o wyrazach rzeczywistych z działaniemi dodawania i mnożenia macierzy.

Definicja 7.1 *Zbiór R, w którym określone są działania $\oplus$ i $\odot$ (oznaczenie: $(R, \oplus, \odot)$) nazywamy pierścieniem, jeśli spełnione są nastę pujące warunki:*
(a) $(R, \oplus)$ jest grupą abelową,
(b) działanie $\odot$ jest łączne
(c) działanie $\odot$ jest rozdzielne względem działania $\oplus$.

Działania $\oplus$ i $\odot$ z powyższej definicji nazywamy odpowiednio dodawaniem i mnożeniem pierścienia $(R, \oplus, \odot)$, zaś warunki (a)–(c) aksjomatami teorii pierścieni (lub aksjomatami pierścienia).

Dla oznaczenia dodawania i mnożenia w pierścieniu będziemy najczęściej używać symboli $+$ i $\cdot$ (odpowiednio). Iloczyn $a \cdot b$ zapisujemy na ogół jako ab. Jeśli nie prowadzi to nieporuzumień, zamiast $(R, +, \cdot)$ piszemy R mając na myśli pierścień $(R.+, \cdot)$.

Jeśli $(R, +, \cdot)$ jest pierścieniem, to grupę $(R, +)$ nazywamy jego grupą addytywną. Element neutralny tej grupy nazywamy zerem pierścienia $(R, +, \cdot)$ i oznaczamy przez 0_R lub po prostu przez 0. Element odwrotny do a względem działania $+$ nazywamy elementem przeciwnym do a i oznaczamy przez $-a$. Zamiast $a + (-b)$ będziemy pisać $a - b$. Zgodnie z terminologią wprowadzoną w rozdziale drugim dla grup abelowych, stosujemy oznaczenia: $na = \underbrace{a + \ldots + a}_{n \text{ razy}}$ i $(-n)a = n(-a)$ dla $n \in \mathbb{N}_+$ oraz $0_R a = 0_R$. Pisząc a^n (dla $n \in \mathbb{N}_+$) mamy na myśli $\underbrace{a \cdot \ldots \cdot a}_{n \text{ razy}}$.

Pierścień, w którym mnożenie jest przemienne nazywamy **pierścieniem przemiennym**. Element neutralny pierścienia $(R, +, \cdot)$ względem mnożenia (jeżeli takowy istnieje) oznaczamy przez 1_R lub po prostu przez 1 i nazywamy jednością tego pierścienia. Pierścień, w którym istnieje element neutralny względem mnożenia nazywamy **pierścieniem z jednością**. Oczywiście zero pierścienia może być równe jego jedności. Sytuacja taka zachodzi w pierścieniu $(\mathbb{Z}, +_1, \cdot_1)$. Jeśli R jest pierścieniem z jednością i $a \in R$, to piszemy $a^0 = 1_R$.

Poniżej dowodzimy kilku własności działań w pierścieniach. W sformułowaniu twierdzenia 7.2 została zastosowana konwencja, zgodnie z którą dla elementów a, b, c, d pierścienia $(R, +, \cdot)$ piszemy $ab + cd$ oraz $ab - cd$ zamiast odpowiednio $(a \cdot b) + (c \cdot d)$ i $(a \cdot b) + (-(c \cdot d))$.

Twierdzenie 7.2 *Niech $(R, +, \cdot)$ będzie pierścieniem i niech $a, b, c \in R$. Wtedy*
(a) $0_R \cdot a = a \cdot 0_R = 0_R$,
(b) $-(-a) = a$,
(c) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
(d) $(-a) \cdot (-b) = ab$,
(e) $a(b - c) = ab - ac$, $(b - c)a = ba - ca$,
(f) $(a - b) \cdot (c - d) = ac - ad - bc + bd$,
(g) jeśli R jest pierścieniem z jednością, to $(-1_R) \cdot a = -a$.

Dowód. (a) $0_R \cdot a = (0_R + 0_R) \cdot a = 0_R \cdot a + 0_R \cdot a$. Stąd, na mocy prawa skracań w grupie $(R, +)$ dostajemy $0_R = 0_R \cdot a$. Podobnie pokazujemy, że $0_R = a \cdot 0_R$.

(b) wynika z odpowiedniej własności dla grup (twierdzenie 2.3).

(c) $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0_R \cdot b = 0_R$, więc $(-a) \cdot b = -(a \cdot b)$. Podobnie dowodzi się, że $a \cdot (-b) = -(a \cdot b)$.

(d) Korzystając z (b) i (c) dostajemy $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = ab$.

(e) $a(b - c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$. Dowód drugiej równości jest podobny.

Dowód równości (f) pozostawiamy jako ćwiczenie dla Czytelnika.

(g) Na mocy (c) dostajemy $(-1) \cdot a = -(1 \cdot a) = -a$. ■

Podamy teraz kilka przykładów pierścieni.

Przykład 1. Zbiór liczb całkowitych ze zwykłymi działaniami dodawania i mnożenia (oznaczenie: $(\mathbb{Z}, +, \cdot)$) jest pierścieniem przemiennym z jednością.

Przykład 2. Niech n będzie liczbą naturalną większą od 1. Zbiór liczb podzielnych przez n (oznaczenie: $n\mathbb{Z}$) ze zwykłymi działaniami dodawania i mnożenia jest pierścieniem przemiennym bez jedności.

Przykład 3. Niech $n \in \mathbb{N}_+$. Zbiór $\mathbb{Z}_n$ wyposażony w działania dodawania i mnożenia modulo n jest pierścieniem przemiennym z jednością (dla $n = 1$ jednością jest liczba 0, zaś dla $n > 0$, liczba 1). Pierścień $(\mathbb{Z}_n, +_n, \cdot_n)$ nazywamy pierścieniem reszt modulo n.

Przykład 4. Niech $n \in \mathbb{N}_+$. Zbiór macierzy kwadratowych wymiaru $n \times n$ o wyrazach rzeczywistych z działaniami dodawania i mnożenia macierzy stanowi pierścień z jednością, który oznaczamy przez $M_{n\times n}(\mathbb{R})$. Jednością w tym pierścieniu jest macierz jednostkowa mająca jedynki na przekątnej i zera poza przekątną. Pierścień $M_{n\times n}(\mathbb{R})$ jest nieprzemienny dla $n \geq 2$. Analogicznie można rozważać pierścień macierzy o wyrazach z dowolnego pierścienia.

Przykład 5. Niech X będzie zbiorem niepustym, zaś $(R, +, \cdot)$ pierścieniem. Wtedy R^X (zbiór funkcji z X w R) z działaniami dodawania i mnożenie funkcji zdefiniowanymi następująco:

$$(f + g)(x) = f(x) + g(x) \text{ i } (fg)(x) = f(x)g(x)$$

jest pierścieniem. Jeśli R jest pierścieniem przemiennym [pierścieniem z jednością], to również R^X jest pierścieniem przemiennym [odpowiednio: pierścieniem z jednością].

Przykład 6. Niech I oznacza przedział zawarty w zbiorze liczb rzczywistych. $C(I)$ (zbiór funkcji

ciągłych z I w $\mathbb{R}$) z działaniami dodawania i mnożenia funkcji jest pierścieniem przemiennym z jednością. Zerem [odpowiednio: jednością] tego pierścienia jest funkcja stała przyporządkowująca każdej liczbie z przedziału I liczbę 0 [odpowiednio: 1]. Analogicznie dla $n \in N_+$ zbiór funkcji n-krotnie różniczkowalnych z I w $\mathbb{R}$ jest pierścieniem przemiennym z jednością.

Przykład 7. Zbiór funkcji wielomianowych z $\mathbb{R}$ w $\mathbb{R}$ (tzn. funkcji postaci $f(x) = a_0 + a_1x + \ldots + a_nx^n$, gdzie $a_0, \ldots, a_n \in \mathbb{R}$ i $n \in \mathbb{N}_+$) z działaniami dodawania i mnożenia funkcji jest pierścieniem przemiennym z jednością.

Przykład 8. Zbiór $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ ze zwykłymi działaniami dodawania i mnożenia jest pierścieniem przemiennym z jednością. Pierścień ten nazywamy pierścieniem Gaussa[1].

Przykład 9. Załóżmy, że n jest liczbą naturalną nie będącą kwadratem żadnej liczby naturalnej. Niech

$$R_n = \left\{ a + b\frac{1+\sqrt{n}}{2} : a, b \in \mathbb{Z} \right\}.$$

Pokażemy, że R_n ze zwykłymi działaniami dodawania i mnożenia jest pierścieniem z jednością wtedy i tylko wtedy, gdy $n-1$ dzieli się przez 4.

Załóżmy wpierw, że $(R_n, +, \cdot)$ jest pierścieniem. W szczególności oznacza to, że zbiór R_n jest zamknięty względem mnożenia. Tak więc

$$\frac{n-1}{4} = \frac{\sqrt{n}+1}{2} \cdot \frac{\sqrt{n}-1}{2} = \frac{\sqrt{n}+1}{2} \cdot (-1 + \frac{\sqrt{n}+1}{2}) \in R_n.$$

Zatem

$$\frac{n-1}{4} = a + b\frac{1+\sqrt{n}}{2}$$

dla pewnych $a, b \in \mathbb{Z}$. Stąd wynika, że

$$b\sqrt{n} = \frac{n-1}{2} - 2a - b.$$

n jednak nie jest kwadratem żadnej liczby naturalnej. Wynika stąd, że n nie jest kwadratem żadnej liczby wymiernej, a więc musi być $b = 0$. Tak więc $\frac{n-1}{4} = a \in \mathbb{Z}$, co oznacza, że $n-1$ dzieli się przez 4.

Przypuśćmy teraz, że liczba $4|n-1$. Wtedy dla dowolnych $a, b, c, d \in \mathbb{Z}$ zachodzą równości:

$$(a + b\frac{1+\sqrt{n}}{2}) + (c + d\frac{1+\sqrt{n}}{2}) = (a+c) + (b+d)\frac{1+\sqrt{n}}{2} \text{ oraz}$$
$$(a + b\frac{1+\sqrt{n}}{2}) \cdot (c + d\frac{1+\sqrt{n}}{2}) = ac + bd\left(\frac{1+\sqrt{n}}{2}\right)^2 + (ad+bc)\frac{1+\sqrt{n}}{2} =$$
$$= ac + bd\left(\frac{n-1}{4} + \frac{1+\sqrt{n}}{2}\right) + (ad+bc)\frac{1+\sqrt{n}}{2} = ac + bd\frac{n-1}{4} + (ab+bc+bd)\frac{1+\sqrt{n}}{2}.$$

Wynika stąd, że dodawanie i mnożenie są działaniami w zbiorze R_n. Nietrudno zauważyć, że $0 \in R_n$ i dla każdego $x \in R_n$, również $-x \in R_n$. Dodawanie w R_n jest działaniem łącznym i przemiennym, ponieważ dodawanie liczb rzeczywistych jest łączne i przemienne. Podobnie mnożenie w R_n jest łączne i rozdzielne względem dodawania. Tak więc $(R_n, +, \cdot)$ jest pierścieniem.

[1] Carl Friedrich Gauss (1777-1855), matematyk niemiecki

Przy badaniu pierścieni rozważa się pewne szczególne rodzaje elementów. Należą do nich elementy odwracalne oraz dzielniki zera.

Definicja 7.3 *Niech R będzie pierścieniem z jednością. Element $a \in R$ nazywamy elementem odwracalnym (lub jednostką) pierścienia R, jeśli $ab = ba = 1$ dla pewnego $b \in R$.*

Oczywiście, jeśli R jest pierścieniem przemiennym, to element $a \in R$ jest odwracalny wtedy i tylko wtedy, gdy $a \cdot b = 1$ dla pewnego $b \in R$.

Ponieważ mnożenie w pierścieniu jest łączne, z twierdzenia 1.8 wynika, że jeśli a jest elementem odwracalnym pierścienia R, to w R istnieje dokładnie jeden element odwrotny do a. Element ten będziemy oznaczali przez a^{-1}. W przypadku elementów odwracalnych definiujemy potęgę o wykładniku ujemnym: $a^{-n} = (a^{-1})^n$, gdzie $n \in \mathbb{N}_+$.

Zbiór elementów odwracalnych pierścienia R oznaczamy przez $U(R)$.

Twierdzenie 7.4 *Zbiór elementów odwracalnych dowolnego pierścienia z jednością jest grupą względem mnożenia w tym pierścieniu.*

Dowód. Niech $(R, +, \cdot)$ będzie pierścieniem z jednością. Oczywiście 1 jest jego elementem odwracalnym. Jeśli $a, b \in U(R)$, to

$$aa^{-1} = a^{-1}a = 1 \text{ i } (ab)(b^{-1}a^{-1}) = (b^{-1}a^{-1})(ab) = 1_R,$$

co oznacza, że również a^{-1} i ab są elementami odwracalnymi pierścienia R. Oczywiście $(a^{-1})^{-1} = a$ i $(ab)^{-1} = b^{-1}a^{-1}$. Działanie $\cdot$ jest łączne w $U(R)$, gdyż jest ono łączne w R. Tak więc $(U(R), \cdot)$ jest grupą. ■

Grupę $(U(R), \cdot)$, o której mowa w twierdzeniu 7.4, nazywamy grupą elementów odwracalnych lub grupą jednostek pierścienia R. Elementem neutralnym grupy $(U(R), \cdot)$ jest oczywiście jedność pierścienia R.

Przykład 10. W pierścieniu liczb całkowitych jedynymi elementami odwracalnymi są 1 i -1. W pierścieniach $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ każdy element różny od 0 jest odwracalny. Z przykładu 9 ze strony 23 wynika, że jeśli p jest liczbą pierwszą, to również każdy niezerowy element pierścienia $(\mathbb{Z}_p, +_p, \cdot_p)$ jest odwracalny.

Przykład 11. Pokażemy, że jedynymi elementami odwracalnymi pierścienia Gaussa $\mathbb{Z}[i]$ są $1, -1, i, -i$. Załóżmy, że $a + bi$ $(a, b \in \mathbb{Z})$ jest elementem odwracalnym pierścienia $\mathbb{Z}[i]$. Wtedy istnieję $c, d \in \mathbb{Z}$ takie, że $(a+bi)(c+di) = 1$. Stąd wynika, że $|a+bi|^2 \cdot |c+di|^2 = 1$, czyli $(a^2+b^2)(c^2+d^2) = 1$. Tak więc $a^2 + b^2 \in \mathbb{N}_+$ i $a^2 + b^2 | 1$. Warunki te implikują, że $a^2 + b^2 = 1$. Zbiorem rozwiązań otrzymanego równania jest

$$\{\langle 1, 0\rangle, \langle -1, 0\rangle, \langle 0, 1\rangle, \langle 0, -1\rangle\}.$$

Stąd $a + bi \in \{1, -1, i, -i\}$. Bezpośrednie sprawdzenie pokazuje, że każdy z elementów $1, -1, i, -i$ jest odwracalny w pierścieniu $\mathbb{Z}[i]$.

Przykład 12. Niech n będzie liczbą naturalną dodatnią nie będącą kwadratem żadnej żadnej liczby naturalnej. Wówczas $\sqrt{n}$ jest liczbą niewymierną. Pokażemy, że jedynymi elementami odwracalnymi pierścienia $\mathbb{Z}[\sqrt{n}i] = \{a + b\sqrt{n}i : a, b \in \mathbb{Z}\}$ ze zwykłymi działaniami dodawania i mnożenia są 1 i -1.

Niech $a + b\sqrt{n}i$, gdzie $a, b \in \mathbb{Z}$, będzie elementem odwracalnym w pierścieniu $\mathbb{Z}[\sqrt{n}i]$. Wtedy

$$(a + b\sqrt{n}i)(c + d\sqrt{n}i) = 1$$

dla pewnych $c, d \in \mathbb{Z}$. Stąd otrzymujemy:

$$(a^2 + b^2 n)(c^2 + d^2 n) = 1.$$

Ponieważ $a^2 + b^2 n$ jest liczbą naturalną dodatnią, musi być $a^2 + b^2 n = 1$. Z założenia n nie jest kwadratem żadnej liczby naturalnej, więc $n > 1$. To zaś implikuje, że $b = 0$ i $a \in \{-1, 1\}$. Tak więc $a + b\sqrt{n}i \in \{-1, 1\}$. Oczywiście, zarówno 1 jak i -1 są elementami odwracalnymi w rozważanym pierścieniu.

Przykład 13. Pokażemy, że $a + b\sqrt{2}$ $(a, b \in \mathbb{Z})$ jest elementem odwracalnym pierścienia $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ (ze zwykłymi działaniami dodawania i mnożenia) wtedy i tylko wtedy, gdy $|a^2 - 2b^2| = 1$. W tym celu wprowadzimy pomocniczą funkcję $N : \mathbb{Z}[\sqrt{2}] \longrightarrow \mathbb{N}$ określoną wzorem: $N(a+b\sqrt{2}) = a^2 - 2b^2$. Oczywiście $N(1) = 1$. Ponadto, jeśli $x = a+b\sqrt{2}$ i $y = c+d\sqrt{2}$ $(a, b, c, d \in \mathbb{Z})$, to

$$\begin{aligned} N(xy) &= N(ac + 2bd + (ad + bc)\sqrt{2}) = (ac + 2bd)^2 - 2(ad + bc)^2 = \\ &= a^2c^2 + 4b^2b^2 - 2a^2d^2 - 2b^2c^2 = (a^2 - 2b^2)(c^2 - 2d^2) = N(x)N(y). \end{aligned}$$

Przypuśćmy, że element $a + b\sqrt{2}$ $(a, b \in \mathbb{Z})$ jest odwracalny w pierścieniu $\mathbb{Z}[\sqrt{2}]$. Wtedy

$$(a + b\sqrt{2})(c + d\sqrt{2}) = 1$$

dla pewnych $c, d \in \mathbb{Z}$. Wobec wcześniejszych rozważań otrzymujemy:

$$N(a + b\sqrt{2})N(c + \sqrt{2}d) = 1,$$

czyli $(a^2 - 2b^2)(c^2 - 2d^2) = 1$. Stąd zaś wynika, że $a^2 - 2b^2 \in \{1, -1\}$, czyli $|a^2 - 2b^2| = 1$.

Załóżmy, że $a, b \in \mathbb{Z}$ oraz $|a^2 - 2b^2| = 1$. Jeśli $a^2 - 2b^2 = 1$, to

$$(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = 1.$$

Jeśli natomiast $a^2 - 2b^2 = -1$, to

$$(a + b\sqrt{2})(-a + b\sqrt{2}) = -a^2 + 2b^2 = 1.$$

W obu przypadkach $a + b\sqrt{2}$ jest elementem odwracalnym pierścienia $\mathbb{Z}[\sqrt{2}]$.

Przykład 14. Niech $n \in \mathbb{N}_+$. W przykładzie 15 ze strony 17 pokazaliśmy, że dla elementu $k \in \mathbb{Z}_n$ istnieje w $\mathbb{Z}_n$ element odwrotny względem $\cdot_n$ wtedy i tylko wtedy, gdy $NWD(k, n) = 1$. Tak więc liczba $k \in \mathbb{Z}_n$ jest elementem odwracalnym pierścienia $(\mathbb{Z}_n, +_n, \cdot_n)$ wtedy i tylko wtedy, gdy $NWD(k, n) = 1$.

Twierdzenie 7.5 *Niech R i S będą pierścieniami z jednością. Wówczas $\langle a, b\rangle$ jest elementem odwracalnym pierścienia $R \oplus S$ wtedy i tylko wtedy, gdy a, b są elementami odwracalnymi w pierścieniach R i S (odpowiednio).*

Dowód. Zauważmy, że

$$\begin{aligned} \langle a, b\rangle \text{ jest odwracalny w } R \oplus S \iff & (\exists c \in R)(\exists d \in S)(\langle a, b\rangle \cdot \langle c, d\rangle = \langle c, d\rangle \cdot \langle a, b\rangle = \langle 1_R, 1_S\rangle) \iff \\ & (\exists c \in R)(\exists d \in S)(\langle ac, bd\rangle = \langle ca, db\rangle = \langle 1_R, 1_S\rangle) \iff \\ & (\exists c \in R)(ac = ca = 1_R) \wedge (\exists d \in S)(bd = db = 1_S) \iff \\ & a \text{ jest odwracalny w } R \text{ i } b \text{ jest odwracalny w } S. \end{aligned}$$

To kończy dowód twierdzenia.

Definicja 7.6 *Niezerowy element a pierścienia R nazywamy dzielnikiem zera tego pierścienia, jeśli $ab = ca = 0$ dla pewnych niezerowych elementów $b, c \in R$.*

Jeśli R jest pierścieniem przemiennym, to niezerowy element $a \in R$ jest odwracalny wtedy i tylko wtedy, gdy $ab = 0_R$ dla pewnego niezerowego elementu $b \in R$.

Twierdzenie 7.7 *Niech R będzie pierścieniem przemiennym i niech $a, b \in R$. Jeżeli a, b nie są dzielnikami zera pierścienia R, to również ich iloczyn nie jest dzielnikeim zera pierścienia R.*

Dowód. Załóżmy, że ab jest dzielnikiem zera pierścienia R. Wtedy
(a) $ab \neq 0$ i
(b) $abc = 0$ dla pewnego $c \in R \setminus \{0_R\}$.
Z warunku (a) wynika, że a i b są elementami różnymi od 0. Jeśli $bc = 0$, to wobec przemienności pierścienia R, b jest dzielnikiem zera w R. W przeciwnym wypadku, na mocy warunku (b), a jest dzielnikiem zera pierścienia R. ■

Twierdzenie 7.8 *Niech R będzie pierścieniem z jednością i niech $a \in R$. Wtedy a nie może być jednocześnie dzielnikiem zera i elementem odwracalnym.*

Dowód. Załóżmy, że a jest zarówno dzielnikiem zera jak i elementem odwracalnym pierścienia R. Wtedy dla pewnych $b, c \in R$, $b \neq 0_R$ prawdziwe są równości: $ab = 0_R$ oraz $ca = 1_R$.

Z równości tych otrzymujemy:

$$b = 1_R \cdot b = cab = c \cdot 0_R = 0_R,$$

sprzeczność. ■

Lemat 7.9 *Niech R będzie pierścieniem przemiennym i niech $a \in R \setminus \{0_R\}$. Jeśli a nie jest dzielnikiem zera pierścienia R, to dla dowolnego $n \in \mathbb{N}_+$:*
(a)$_n$ $a^n \neq 0_R$,
(b)$_n$ a^n nie jest dzielnikiem zera pierścienia R.

Dowód. (Indukcja względem n) Dla $n = 1$ twierdzenie jest prawdziwe z założenia. Przypuśćmy więc, że dla pewnego $n \in \mathbb{N}_+$ prawdziwe są warunki (a)$_n$ i (b)$_n$.

Gdyby element a^{n+1} był równy 0, mielibyśmy $a^n \cdot a = 0$, skąd, wobec $a \neq 0_R$ i $a^n \neq 0_R$, wynikałoby, że a jest dzielnikiem zera pierścienia R. Tak więc $a^{n+1} \neq 0$.

Gdyby element a^{n+1} był dzielnikiem zera pierścienia R, mielibyśmy $a^{n+1}b = 0$ dla pewnego $b \neq 0$. Stąd zaś wynika, że

$$(*)\ a^n(ab) = 0_R.$$

a nie jest dzielnikiem zera w R, więc $ab \neq 0_R$. Ponieważ $a^n \neq 0_R$, $(*)$ implikuje, że a^n jest dzielnikiem zera pierścienia R, co jest sprzeczne z warunkiem (b)$_n$. ■

Twierdzenie 7.10 *Niech R będzie skończonym pierścieniem przemiennym z jednością zaś a jego niezerowym elementem. Wtedy następujące warunki są równoważne:*
(a) a jest elementem odwracalnym pierścienia R,
(b) a nie jest dzielnikiem zera pierścienia R,
(c) $a^n = 1_R$ dla pewnego $n \in \mathbb{N}_+$.

Dowód. Implikacja $(a) \Longrightarrow (b)$ wynika wprost z twierdzenia 7.8 Aby dowieść, że (b) implikuje (c), przypuśćmy, że element $a \in R$ nie jest dzielnikiem zera pierścienia R. Ponieważ R jest skończony, istnieją $m, n \in \mathbb{N}_+$ takie, że $a^{m+n} = a^m$, czyli $a^m(a^n - 1_R) = 0_R$. Na mocy lematu 7.9, $a^m \neq 0$ i a^m nie jest dzielnikiem zera pierścienia R. Oznacza to, że $a^n - 1_R = 0_R$, czyli $a^n = 1_R$.

W celu wykazania implikacji (c)$\Longrightarrow$(a), załóżmy, że $a^n = 1_R$ dla pewnego $n \in \mathbb{N}_+$. Jeśli $n = 1$, to $a = 1_R$, a więc jest elementem odwracalnym pierścienia R. Jeśli $n > 1$, to $a \cdot a^{n-1} = a^{n-1} \cdot a = 1_R$, skąd wynika, że a jest elementem odwracalnym pierścienia R. ■

Poniższe twierdzenie może posłużyć do wyznaczania dzielników zera w pierścieniach postaci $R \oplus S$.

Twierdzenie 7.11 *Niech R i S będą pierścieniami przemiennymi. Element $\langle a, b\rangle \in R \oplus S$ jest dzielnikiem zera pierścienia $R \oplus S$ wtedy i tylko wtedy, gdy spełniony jest któryś z warunków (a)–(d):*

(a) $a = 0_R$ i $b \neq 0_S$,

(b) $a \neq 0_R$ i $b = 0_S$,

(c) a jest dzielnikiem zera w R,

(d) b jest dzielnikiem zera w S.

Dowód. Przypuśćmy, że zachodzi warunek (a). Ustalmy $c \in R \setminus \{0_R\}$. Wtedy

$$\langle a, b\rangle \cdot \langle c, 0_S\rangle = \langle 0_R \cdot c, b \cdot 0_S\rangle = \langle 0_R, 0_S\rangle,$$

co oznacza, że $\langle a, b\rangle$ jest dzielnikiem zera pierścienia $R \oplus S$. Podobnie rozumujemy wychodząc od warunku (b).

Przypuśćmy teraz, że zachodzi warunek (c). Wtedy istnieje $c \in R \setminus \{0_R\}$ takie, że $ac = 0_R$. Stąd wynika, że

$$\langle a, b\rangle \cdot \langle c, 0_S\rangle = \langle a \cdot c, b \cdot 0_S\rangle = \langle 0_R, 0_S\rangle,$$

co oznacza, że $\langle a, b\rangle$ jest dzielnikiem zera pierścienia $R \oplus S$. Podobnie rozumujemy wychodząc od warunku (d).

Aby zakończyć dowód twierdzenia, załóżmy, że dla elementów $a \in R$ i $b \in S$ nie jest spełniony żaden z warunków (a)–(d). Wtedy

- $\langle a, b\rangle = \langle 0_R, 0_S\rangle$ lub
- $a \neq 0_R, b \neq 0_R$, a nie jest dzielnikiem zera w R i b nie jest dzielnikiem zera w S.

Jak łatwo zauważyć, w żadnym przypadku $\langle a, b\rangle$ nie jest dzielnikiem zera pierścienia $R \oplus S$. ■

Definicja 7.12 *Pierścień przemienny z jednością, w którym $0 \neq 1$, nie mający dzielników zera, nazywamy pierścieniem całkowitym lub dziedziną całkowitości.*

Przykładami pierścieni całkowitych są $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ i $\mathbb{Z}[i]$ ze zwykłymi działaniami dodawania i mnożenia. Pierścień $(\mathbb{Z}_6, +_6, \cdot_6)$ nie jest całkowity, gdyż posiada dzielniki zera: 2,3 i 4.

Definicja 7.13 *Niech R będzie pierścieniem z jednością. Mówimy, że charakterystyka pierścienia R wynosi 0, jeśli $\underbrace{1_R + \ldots + 1_R}_{n\text{razy}} \neq 0_R$ dla dowolnego $n \neq 0$. W przeciwnym wypadku, charakterystyką pierścienia R nazywamy najmniejszą liczbę naturalną dodatnią n taką, że $\underbrace{1_R + \ldots + 1_R}_{n\text{razy}} = 0_R$. Charakterystykę pierścienia R oznaczamy przez $\chi(R)$.*

Lemat 7.14 *Niech R będzie pierścieniem z jednością o charakterystyce $k > 0$. Jeżeli n jest liczbą całkowitą podzielną przez k, to dla dowolnego $a \in R$, $na = 0_R$.*

Dowód. Ustalmy element $a \in R$. Z założenia $n = lk$ dla pewnego $l \in \mathbb{Z}$. Stąd

$$na = (lk)a = l(ka) = l(\underbrace{a + \ldots + a}_{k\text{razy}}) = l[(\underbrace{1_R + \ldots + 1_R}_{k\text{razy}})a] = l(0_R \cdot a) = l0_R = 0_R.$$

■

Twierdzenie 7.15 *Jeśli R jest pierścieniem przemiennym z jednością o charakterystyce p, gdzie p jest liczbą pierwszą, to $(a+b)^p = a^p + b^p$ dla dowolnych $a, b \in R$.*

Dowód. Ustalmy $a, b \in R$. Wtedy

$$(a+b)^p = a^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} + b^p.$$

Ponieważ dla $i \in \{1, \ldots, p-1\}$, liczba $\binom{p}{i}$ dzieli się przez p, na mocy lematu 7.14, otrzymujemy:

$$\binom{p}{i} a^i b^{p-i} = 0_R \text{ dla } i \in \{1, \ldots, p-1\}.$$

Stąd wynika, że $(a+b)^p = a^p + b^p$. ■

Twierdzenie 7.16 *Charakterystyka dowolnego pierścienia całkowitego wynosi 0 lub jest liczbą pierwszą.*

Dowód. Niech R będzie pierścieniem całkowitym, którego charakterystyka jest różna od 0. Wtedy $\chi(R) \neq 1$, gdyż zero i jedność w pierścieniu całkowitym są różne. Przypuśćmy, że $\chi(R) = mn$, gdzie m i n są liczbami naturalnymi większymi od 1. Wtedy

$$0_R = \underbrace{1_R + \ldots + 1_R}_{mn \text{ razy}} = (\underbrace{1_R + \ldots + 1_R}_{m \text{ razy}}) \cdot (\underbrace{1_R + \ldots + 1_R}_{n \text{ razy}}).$$

Ponadto $\underbrace{1_R + \ldots + 1_R}_{m \text{ razy}} \neq 0_R$ i $\underbrace{1_R + \ldots + 1_R}_{n \text{ razy}} \neq 0_R$. Oznacza to, że pierścień R posiada dzielnik zera, a więc nie jest całkowity. Sprzeczność. ■

Definicja 7.17 *Pierścień przemienny z jednością $(R, +, \cdot)$ nazywamy ciałem przemiennym (lub po prostu ciałem), jeśli $0_R \neq 1_R$ i każdy jego element różny od 0_R jest odwracalny.*

Jeśli K jest ciałem, to $U(K) = K \setminus \{0_K\}$. Jak wiemy z twierdzenia 7.4, $(K \setminus \{0_K\}, \cdot)$ jest grupą. Grupę tę nazywamy grupą multyplikatywną ciała K.

Przykład 15. Zbiory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ze zwykłymi działaniami dodawania i mnożenia są ciałami. Pierścień $(\mathbb{Z}, +, \cdot)$ nie jest ciałem.

Przykład 16. Pokażemy, że pierścień $(\mathbb{Z}_n, +_n, \cdot_n)$ jest ciałem wtedy i tylko wtedy, gdy n jest liczbą pierwszą.

Pierścień $\mathbb{Z}_1$ nie jest ciałem, gdyż jego zero i jedność są sobie równe.

Jeśli $n = km$, gdzie $k, m > 1$, to $NWD(k, n) = k > 1$, a więc w myśl przykładu 14 ze str. 59 k jest elementem nieodwracalnym pierścienia $\mathbb{Z}_n$. Oznacza to, że $\mathbb{Z}_n$ nie jest ciałem.

Jeśli n jest liczbą pierwszą, to $(\mathbb{Z}_n, +_n, \cdot_n)$ jest pierścieniem przemiennym z jednością, w którym zero i jedność są różne. Z przykładu 9, str. 23 wynika, że, $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ jest grupą. Tak więc dowolny niezerowy element pierścienia $\mathbb{Z}_n$ jest odwracalny i $\mathbb{Z}_n$ jest ciałem.

Przykład 17. Zbiory $\mathbb{Q}$, W czteroelementowym zbiorze $K = \{0, 1, a, b\}$ definiujemy działania $\oplus$ i $\odot$ przy pomocy tabelek.

$\oplus$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\odot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Nietrudno przekonać się o tym, że $(K, \oplus, \cdot)$ jest ciałem.

Twierdzenie 7.18 *Każde ciało jest pierścieniem całkowitym.*

Dowód. Niech K będzie ciałem. Wtedy, na mocy definicji 7.17, K jest pierścieniem przemiennym z jednością, w którym zero i jedność są różne. Pokażemy, że K nie ma dzielników zera.

Załóżmy, że a i b są niezerowymi elementami ciała K, dla których $ab = 0$. a jest elementem odwracalnym, więc $b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. Sprzeczność. ■

Wniosek 7.19 *Charakterystyka dowolnego ciała jest równa 0 lub jest liczbą pierwszą.*

Wniosek 7.20 *Jeśli K jest ciałem o charakterystyce $p > 0$, to $(a + b)^p = a^p + b^p$ dla dowolnych $a, b \in K$.*

Definicja 7.21 *Pierścień z jednością, który nie jest przemienny i w którym każdy element różny od zera jest odwracalny nazywamy ciałem nieprzemiennym.*

Przykład 18. W zbiorze $\mathbb{H} = \mathbb{C} \times \mathbb{C}$ definiujemy działania $\oplus$ i $\odot$:

$$\langle a, b\rangle \oplus \langle c, d\rangle = \langle a + c, b + d\rangle, \text{ oraz } \langle a, b\rangle \odot \langle c, d\rangle = \langle ac - b\overline{d}, ad + b\overline{c}\rangle.$$

Łatwo można sprawdzić, że $(\mathbb{H}, \oplus, \odot)$ jest pierścieniem. Elementy $\langle 0, 0\rangle$ i $\langle 1, 0\rangle$ są odpowiednio zerem i jednością tego pierścienia. Działanie $\odot$ nie jest przemienne, gdyż

$$\langle i, 0\rangle \odot \langle 0, 1\rangle = \langle 0, i\rangle, \text{ ale } \langle 0, 1\rangle \odot \langle i, 0\rangle = \langle 0, -i\rangle.$$

Każdy niezerowy element pierścienia $(\mathbb{H}, \oplus, \odot)$ jest odwracalny. Tak więc $(\mathbb{H}, \oplus, \odot)$ jest ciałem nieprzemiennym. Nazywamy je ciałem kwaternionów lub ciałem Hamiltona.

Rozdział 8

Podpierścienie, ideały i homomorfizmy pierścieni

Definicja 8.1 *Podzbiór S pierścienia $(R, +, \cdot)$ nazywamy jego podpierścieniem, jeśli S z działaniami $+$ i $\cdot$ ograniczonymi do zbioru S jest pierścieniem. Pierścień $(R, +, \cdot)$ nazywamy wówczas rozszerzeniem pierścienia $(S, +, \cdot)$.*

Z powyższej definicji wynika natychmiast, że zbiór $S \subseteq R$ jest podpierścieniem pierścienia $(R, +, \cdot)$ wtedy i tylko wtedy, gdy $0_R \in S$ oraz

$$(\forall a, b \in S)(a - b \in S \wedge ab \in S).$$

Innymi słowy, jeśli $(R, +, \cdot)$ jest pierścieniem i $S \subseteq R$, to $(S, +, \cdot)$ jest pierścieniem wtedy i tylko wtedy, gdy $0_R \in S$ i S jest zbiorem zamkniętym względem odejmowania i mnożenia.

Oczywiście, w przypadku gdy S jest podpierścieniem pierścienia R, to $0_R = 0_S$.

Przykład 1. Rozważmy podzbiór $S = \{\langle n, n\rangle : n \in \mathbb{Z}\}$ pierścienia $\mathbb{Z} \oplus \mathbb{Z}$. Oczywiście $\langle 0, 0\rangle \in S$. Jeśli $a, b \in S$, to $a = \langle m, m\rangle$ i $b = \langle n, n\rangle$ dla pewnych $m, n \in \mathbb{Z}$. Stąd

$$\begin{aligned} a - b &= \langle m, m\rangle - \langle n, n\rangle = \langle m - n, m - n\rangle \in S \\ a \cdot b &= \langle m, m\rangle \cdot \langle n, n\rangle = \langle m \cdot n, m \cdot n\rangle \in S. \end{aligned}$$

Tak więc S jest podpierścieniem pierścienia $\mathbb{Z} \oplus \mathbb{Z}$.

Definicja 8.2 *Podzbiór L ciała $(K, +, \cdot)$ nazywamy jego podciałem, jeśli L z działaniami $+$ i $\cdot$ ograniczonymi do L jest ciałem. Ciało $(K, +, \cdot)$ nazywamy wówczas rozszerzeniem ciała $(L, +, \cdot)$.*

Jak łatwo zauważyć, zbiór $L \subseteq K$ jest podciałem ciała K wtedy i tylko wtedy, gdy spełnione są następujące warunki:

(a) $0_K, 1_K \in L$,

(b) $(\forall a, b \in L)(a - b \in L \wedge ab \in L)$,

(c) $(\forall a \in L \setminus \{0_K\})(a^{-1} \in L)$.

Oznacza to, że jeśli $(K, +, \cdot)$ jest ciałem i $L \subseteq K$, to $(L, +, \cdot)$ jest ciałem wtedy i tylko wtedy, gdy spełnione są warunki (a)–(c).

Czytelnikowi powinna być znana teoria przestrzeni liniowych nad ciałem liczb rzeczywistych. Analogiczną teorię można rozwinąć nad dowolnym ciałem wprowadzając pojęcie przestrzeni liniowej nad ciałem, liniową niezależność wektorów, bazy, macierze, wyznaczniki itd. Dla przykładu podajemy definicję przestrzeni liniowej nad ciałem.

Definicja 8.3 *Niech K będzie ciałem. Zbiór V z działaniem $+$ (oznaczenie: $(V,+)$) nazywamy przestrzenią liniową nad ciałem K, jeśli $(V,+)$ jest grupą abelową i określone jest odwzorowanie $f : K \times V \longrightarrow V$, przyporządkowujące każdemu $\alpha \in K$ i każdemu $x \in V$ element $f(\alpha, x) \in V$, który oznaczamy przez αx, spełniające dla dowolnych $\alpha, \beta \in K$ i dowolnych $x, y \in V$ następujące warunki:*

(1) $1_K x = x$,
(2) $\alpha(x + y) = \alpha x + \alpha y$,
(3) $(\alpha + \beta)x = \alpha x + \beta x$,
(4) $(\alpha\beta)x = \alpha(\beta x)$.

Jeśli K jest rozszerzeniem ciała L, to K jest przestrzenią liniową nad ciałem L. Wymiar tej przestrzeni liniowej nazywamy stopniem tego rozszerzenia i oznaczamy przez $[K : L]$.

Twierdzenie 8.4 *Jeśli ciało K jest rozszerzeniem ciała L, zaś L rozszerzeniem ciała M, przy czym stopnie obu rozszerzeń są skończone, to skończony jest również stopień rozszerzenia K nad M i zachodzi równość.*

$$[K : M] = [K : L] \cdot [L : M].$$

Wprost z definicji ciała, podciała i przestrzeni liniowej nad ciałem wynika następujące twierdzenie.

Twierdzenie 8.5 *Jeśli K jest podciałem ciała L, to L jest przestrzenią liniową nad ciałem K.*

Przykład 2. Ciało liczb wymiernych jest podciałem ciała liczb rzeczywistych i podciałem ciała liczb zespolonych. Ciało liczb rzeczywistych jest podciałem ciała liczb zespolonych.

Przykład 3. Niech K będzie podciałem ciała $\mathbb{Q}$. Pokażemy, że $K = \mathbb{Q}$.

Z definicji podciała wynika, że 0 i 1 należą do K. Ponieważ K jest zbiorem zamkniętym względem dodawania,

$$n = \underbrace{1 + \ldots + 1}_{n \text{ razy}} \in K \text{ dla } n \in \mathbb{N}_+.$$

Tak więc $\mathbb{N} \subseteq K$. K jest zbiorem zamkniętym względem odejmowania, więc $\mathbb{Z} \subseteq K$. Jeśli $m, n \in \mathbb{Z}$, $n \neq 0$, to $\frac{m}{n} = m \cdot n^{-1} \in K$. Zatem $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}$, czyli $K = \mathbb{Q}$. W ten sposób wykazaliśmy, że jedynym podciałem ciała $\mathbb{Q}$ jest $\mathbb{Q}$.

Nietrudno też pokazać, że jedynym podciałem ciała $\mathbb{F}_p = (\mathbb{Z}_p, +_p, \cdot_p)$ (p: liczba pierwsza)jest $\mathbb{Z}_p$.

Ciało K, którego jedynym podciałem jest K nazywamy ciałem prostym. Tak więc z powyższego przykładu wynika, że $\mathbb{Q}$ i $\mathbb{F}_p$ (p jest liczbą pierwszą) są ciałami prostymi.

Rozumując podobnie jak w przypadku grup i podgrup, możemy udowodnić następujące dwa twierdzenia.

Twierdzenie 8.6 *Jeśli R_1 jest podpierścieniem pierścienia R_2 i R_2 jest podpierściniem pierścienia R_3, to R_1 jest podpierścieniem pierścinia R_3. Podobnie dla ciał i podciał.*

Twierdzenie 8.7 *Przekrój dowolnej rodziny podpierścieni danego pierścienia jest jego podpierścieniem. Przekrój dowolnej rodziny podciał danego ciała jest jego podciałem.*

Definicja 8.8 *Podzbiór I pierścienia $(R, +, \cdot)$ nazywamy jego ideałem, jeśli I jest podgrupą grupy $(R, +)$ oraz*

$$(\forall a \in I)(\forall b \in R)(ab \in I \wedge ba \in I).$$

Nietrudno zauważyć, że I jest ideałem pierścienia R wtedy i tylko wtedy, gdy spełnione są poniższe warunki (a), (b) i (c):

(a) $0_R \in I$,

(b) $(\forall a, b \in I)(a - b \in I)$,

(c) $(\forall a \in I)(\forall b \in R)(ab \in I \wedge ba \in I)$.

Oczywiście, w przypadku, gdy pierścień R jest przemienny, warunek (c) możemy zastąpić następującym:

(c') $(\forall a \in I)(\forall b \in R)(ab \in I)$.

Jeśli R jest pierścieniem, to $\{0_R\}$ i R są jego ideałami. Ideał $\{0_R\}$ zwany jest ideałem zerowym. Jeśli I jest ideałem pierścienia R, to I jest podpierścieniem pierścienia R. Odwrotna implikacja nie jest prawdziwa (przykład 6, str. 66).

Przykład 4. Jeśli $n \in \mathbb{N}_+$, to zbiór liczb całkowitych podzielnych przez n (oznaczenie: $n\mathbb{Z}$) jest ideałem pierścienia liczb całkowitych. Mamy bowiem:

(a) $0 = n \cdot 0 \in n\mathbb{Z}$,

(b) dla dowolnych $a, b \in \mathbb{Z}$, $na - nb = n(a - b) \in n\mathbb{Z}$ i

(c) dla dowolnych $a, b \in \mathbb{Z}$, $(na)b = n(ab) \in n\mathbb{Z}$.

Przykład 5. Jeśli $d, n \in \mathbb{N}_+$ i $d|n$, to $\{x \in \mathbb{Z}_n : d|x\}$ jest ideałem pierścienia $\mathbb{Z}_n$.

Przykład 6. Jak wiemy z przykładu 1 ze strony 64, zbiór $S = \{\langle n, n\rangle : n \in \mathbb{Z}\}$ jest podpierścieniem pierścienia $\mathbb{Z} \oplus \mathbb{Z}$. S nie jest jednak ideałem pierścienia $\mathbb{Z} \oplus \mathbb{Z}$, ponieważ $\langle 1, 1\rangle \in S$, ale $\langle 1, 1\rangle \cdot \langle 1, 0\rangle = \langle 1, 0\rangle \notin S$.

Twierdzenie 8.9 *Jeśli R i S są pierścieniami z jednością to I jest ideałem pierścienia $R \oplus S$ wtedy i tylko wtedy, gdy $I = I_1 \times I_2$ dla pewnych ideałów I_1, I_2 w pierścieniach R i S (odpowiednio).*

Dowód. Niech I będzie ideałem pierścienia $R \oplus S$. Definiujemy

$$I_1 = \{x \in R : (\exists y \in S)(\langle x, y\rangle \in I)\} \text{ oraz } I_2 = \{y \in S : (\exists x \in R)(\langle x, y\rangle \in I)\}.$$

Zauważmy, że $0_R \in I_1$, ponieważ $\langle 0_R, 0_S\rangle \in I$. Jeśli $a, b \in I_1$, to $\langle a, c\rangle, \langle b, d\rangle \in I$ dla pewnych $c, d \in S$. Stąd $\langle a - b, c - d\rangle = \langle a, c\rangle - \langle b, d\rangle \in I$, a więc $a - b \in I_1$. Jeśli dodatkowo $r \in R$, to $\langle ar, 0_S\rangle = \langle a, b\rangle \cdot \langle r, 0_S\rangle \in I$, a więc $ar \in I_1$. Analogicznie pokazujemy, że $ra \in I_1$. Tak więc I_1 jest ideałem pierścienia R. Podobnie dowodzi się, że I_2 jest ideałem pierścienia S.

Pokażemy teraz, że $I = I_1 \times I_2$. Wprost z określenia ideałów I_1, I_2 wynika, że $I \subseteq I_1 \times I_2$. W celu wykazania implikacji przeciwnej załóżmy, że $\langle a, b\rangle \in I_1 \times I_2$. Wtedy $a \in I_1$ i $b \in I_2$. Stąd $\langle a, b_1\rangle \in I$ oraz $\langle a_1, b\rangle \in I$ dla pewnych $a_1 \in R$ i $b_1 \in S$. Oczywiście $\langle a, 0_S\rangle = \langle a, b_1\rangle \cdot \langle 1_R, 0_S\rangle \in I$. Podobnie $\langle 0_R, b\rangle \in I$. I jest zbiorem zamkniętym względem dodawania w $R \oplus S$, więc $\langle a, b\rangle = \langle a, 0_S\rangle + \langle 0_R, b\rangle \in I$. Ostatecznie $I = I_1 \times I_2$.

Nietrudno pokazać, że jeśli I_1, I_2 są ideałami pierścieni R i S (odpowiednio), to $I_1 \times I_2$ jest ideałem pierścienia $R \oplus S$. ■

Przykład 7. Jeżeli a jest elementem pierścienia przemiennego R, to zbiór $aR = \{ar : r \in R\}$ jest ideałem pierścienia R. Istotnie, $0_R = a \cdot 0_R \in aR$. Ponadto, jeśli $x, y \in aR$, to $x = ax_1$ i $y = ay_1$ dla pewnych $x_1, y_1 \in R$, skąd wynika, że $x - y = ax_1 - ax_2 = a(x_1 - x_2) \in aR$. Jeśli $z \in R$, to $xz = ax_1z \in aR$. Tak więc aR jest ideałem pierścienia R.

Definicja 8.10 *Niech R będzie pierścieniem przemiennym. Ideał postaci aR, gdzie $a \in R$ nazywamy ideałem głównym generowanym przez element a. Zamiast aR czasami piszemy (a).*

Oczywiście w dowolnym pierścieniu przemiennym R, $\{0_R\} = \{0_R \cdot x : x \in R\}$ jest ideałem głównym pierścienia R. Jeśli dodatkowo R jest pierścieniem z jednością, to również $R = \{1_R \cdot x : x \in R\}$ jest ideałem głównym.

Definicja 8.11 *Pierścień przemienny, którego wszystkie ideały są główne nazywamy pierścieniem ideałów głównych (lub dziedziną ideałów głównych).*

Przykład 8. Pierścień liczb całkowitych jest pierścieniem ideałów głównych.

Jak już wiemy, $\{0\}$ jest ideałem głównym w $\mathbb{Z}$. Rozważmy ideał I pierścienia $\mathbb{Z}$ zawierający pewną liczbę $a \neq 0$. Wtedy również $-a \in I$, a więc I zawiera pewną liczbę naturalną dodatnią. Oznaczmy przez n najmniejszą liczbę naturalną dodatnią należącą do I. Pokażemy, że $n\mathbb{Z} = I$.

Inkluzja $n\mathbb{Z} \subseteq I$ wynika bezpośrednio z definicji ideału. W celu wykazania inkluzji przeciwnej załóżmy nie wprost, że istnieje liczba $b \in I \setminus n\mathbb{Z}$. Innymi słowy, liczba b nie dzieli się przez n. Wtedy $nk < b < n(k+1)$ dla pewnego $k \in \mathbb{Z}$. Stąd $0 < b - nk < n$. Wiemy, że $b, n \in I$, zatem $b - nk \in I$. W ten sposób znaleśmy w ideale I liczbę naturalną dodatnią mniejszą od n. Sprzeczność

Przykład 9. Pierścień Gaussa $\mathbb{Z}[i]$ jest pierścieniem ideałów głównych.

Rozważmy ideał I pierścienia $\mathbb{Z}[i]$ różny od $\{0\}$. Wybierzmy element $a \in I \setminus \{0\}$ o najmniejszym module, to znaczy taki, że $|x| \geq |a|$ dla dowolnego $x \in I \setminus \{0\}$. Pokażemy, że $a\mathbb{Z}[i] = I$.

Inkluzja $aZ[i] \subseteq I$ jest oczywista. Aby udowodnić inkluzję przeciwną, załóżmy nie wprost, że istnieje element $b \in I \setminus a\mathbb{Z}[i]$. Wtedy b należy do kwadratu K o wierzchołkach: $a(n+mi)$, $a(n+1+mi)$, $a(n+(m+1)i)$, $a(n+1+(m+1)i)$, gdzie $m, n \in \mathbb{Z}$, ale nie jest żadnym z wierzchołków. Niech c będzie wierzchołkiem kwadratu K leżącym najbliżej b. Odległość pomiędzy b a c (równa $|b-c|$) jest nie większa niż połowa długości przekątnej kwadratu K. Oznacza to, że

$$0 < |b - c| \leq \frac{\sqrt{2}|a|}{2} < |a|.$$

Z założenia $b, c \in I$, więc również $b - c \in I$. W ten sposób znaleźliśmy w ideale I niezerowy element o module mniejszym od $|a|$. Sprzeczność.

Definicja 8.12 *Ideał I pierścienia R nazywamy pierwszym, jeśli $I \neq R$ oraz*

$$(\forall a, b \in R)(ab \in I \Longrightarrow a \in I \vee b \in I).$$

Przykład 10. Pokażemy, że ideał I pierścienia $(\mathbb{Z}, +, \cdot)$ jest pierwszy wtedy i tylko wtedy, gdy $I = \{0\}$ lub $I = p\mathbb{Z}$, gdzie p jest liczbą pierwszą.

Niech I będzie ideałem pierścienia $\mathbb{Z}$. Wtedy $I = nZ$ dla pewnego $n \in \mathbb{N}$. Jeśli $n = 0$, to $I = \{0\} \neq \mathbb{Z}$. Wtedy dla dowolnych $a, b \in \mathbb{Z}$ mamy

$$ab \in I \Longrightarrow ab = 0 \Longrightarrow a = 0 \vee b = 0 \Longrightarrow a \in I \vee b \in I,$$

co oznacza, że ideał I jest pierwszy.

Jeśli $n = 1$, to $I = \mathbb{Z}$, a więc nie jest ideałem pierwszym.

Jeśli n jest liczbą pierwszą, to dla dowolnych $a, b \in \mathbb{Z}$ mamy

$$ab \in I \Longrightarrow n|ab \Longrightarrow n|a \vee n|b \Longrightarrow a \in I \vee b \in I.$$

Tak więc I jest ideałem pierwszym.

Jeśli $n = kl$, gdzie $k, l \in \mathbb{N}_+$, $k, l > 1$, to $kl \in I$, ale żadna z liczb k, l nie należy do I. Oznacza to, że I nie jest ideałem pierwszym.

Twierdzenie 8.13 *Niech R będzie pierścieniem przemiennym z jednością. Wówczas R jest pierścieniem całkowitym wtedy i tylko wtedy, gdy $\{0_R\}$ jest ideałem pierwszym pierścienia R.*

Dowód. Niech R będzie pierścieniem całkowitym. Wtedy $0_R \neq 1_R$, więc $\{0_R\} \neq R$. Przypuśćmy, że $a, b \in R$ i $ab \in \{0_R\}$. Wtedy $ab = 0_R$. Pierścień R nie posiada dzielników zera, więc $a = 0_R$ lub $b = 0_R$. To zaś oznacza, że $a \in \{0_R\}$ lub $b \in \{0_R\}$. A więc $\{0_R\}$ jest ideałem pierwszym pierścienia R.

Załóżmy teraz, że $\{0_R\}$ jest ideałem pierwszym pierścienia R. Wtedy $\{0_R\} \neq R$, co implikuje, że $0_R \neq 1_R$. Pokażemy jeszcze, że R nie posiada dzielników zera. Przypuśćmy, że $a, b \in R$ i $ab = 0_R$. Wtedy $ab \in \{0_R\}$. $\{0_R\}$ jest ideałem pierwszym więc przynajmniej jeden z elementów a, b należy do $\{0_R\}$. Stąd $a = 0_R$ lub $b = 0_R$. Tak więc R jest pierścieniem całkowitym.

Definicja 8.14 *Ideał I pierścienia R nazywamy maksymalnym, jeśli $I \neq R$ i nie istnieje ideał J pierścienia R taki, że $I \subsetneq J \subsetneq R$.*

Twierdzenie 8.15 *Niech R będzie pierścieniem przemiennym z jednością. Każdy ideał maksymalny pierścienia R jest jego ideałem pierwszym.*

Dowód. Niech I będzie idełem maksymalnym pierścienia R i niech $ab \in I$, gdzie $a, b \in R$. Załóżmy, że $a \notin I$. Pokażemy, że wtedy $b \in I$.

Niech $J = \{x + ay : x \in I, y \in R\}$. Oczywiście J jest ideałem pierścienia R zawierającym $I \cup \{a\}$. Z maksymalności idału I wynika zatem, że $J = R$. W szczególności $1_R \in J$ i mamy $1_R = x_0 + ay_0$ dla pewnych $x_0 \in I$, $y_0 \in R$. Stąd $b = x_0 b + aby_0$. Wiemy, że $x_0, ab \in I$. Tak więc $b = x_0 b + aby_0 \in I$.

W ten sposób wykazaliśmy, że I jest ideałem pierwszym pierścienia R. ■

Nie każdy ideał pierwszy jest maksymalny. Na przykład $\{0\}$ jest ideałem pierwszym w pierścieniu $\mathbb{Z}$, ale nie jest ideałem maksymalnym.

Twierdzenie 8.16 *Niech R będzie pierścieniem przemiennym z jednością. Następujące warunki są równoważne:*

(a) R jest ciałem,

(b) $\{0_R\}$ jest ideałem maksymalnym pierścienia R,

(c) R posiada dokładnie dwa ideały: $\{0_R\}$ oraz R.

Dowód. (a)$\Longrightarrow$(b): Niech R będzie ciałem, zaś I jego ideałem zawierającym niezerowy element a. Na mocy założenia, a jest elementem odwracalnym w R. Oczywiście $1_R = a \cdot a^{-1} \in I$, co oznacza, że $I = R$. W ten sposób wykazaliśmy, że $\{0_R\}$ jest ideałem maksymalnym ciała R.

(b)$\Longrightarrow$(c): Jeśli $\{0_R\}$ jest ideałem maksymalnym pierścienia R, to $\{0_R\} \neq R$ oraz nie istnieje ideał J taki, że $\{0_R\} \subsetneq J \subsetneq R$. Stąd wynika (c).

(c)$\Longrightarrow$(a): Załóżmy, $\{0_R\}$ i R są jedynymi ideałami pierścienia R, przy czym $\{0_R\} \neq R$. Wtedy $0_R \neq 1_R$.

Ustalmy niezerowy element $a \in R$. Ideał aR zawiera element a, więc jest różny od $\{0_R\}$. Na mocy założenia, musi być $aR = R$, co znacza, że $1_R \in aR$. Tak więc $1_R = ab$ dla pewnego $b \in R$ i element a jest odwracalny. Stąd wynika, że R jest ciałem. ■

Twierdzenie 8.17 *Niech R będzie pierścieniem z jednością. Każdy ideał pierścienia R, różny od R, zawiera się w pewnym ideale maksymalnym tego pierścienia.*

Dowód. Niech I będzie ideałem pierścienia przemiennego R różnym od R. Wtedy oczywiście $1_R \notin I$. Definiujemy rodzinę ideałów pierścienia R zawierających I, do których nie należy 1_R:

$$\mathcal{R} = \{J \lhd R : I \subseteq J, 1_R \notin J\}.$$

Rodzina ta jest niepusta, gdyż ideał I do niej należy. Ponadto relacja $\subseteq$ jest częściowym porządkiem w $\mathcal{R}$.

Załóżmy, że $\mathcal{S}$ jest niepustą podrodziną rodziny $\mathcal{R}$ liniowo uporządkowaną przez relację inkluzji. Pokażemy, że $I_1 = \bigcup_{J\in\mathcal{S}} J$ jest ideałem należącym do rodziny $\mathcal{R}$ i ograniczającym z góry rodzinę $\mathcal{S}$.

- $0_R \in J$ dla każdego $J \in \mathcal{S}$, więc $0_R \in I_1$;
- Jeśli $a, b \in I_1$, to istnieją ideały $J_1, J_2 \in \mathcal{S}$ takie, że $a \in J_1$ i $b \in J_2$; ponieważ rodzina $\mathcal{S}$ jest liniowo uporządkowana przez relacją inkluzji, $J_1 \subseteq J_2$ lub $J_2 \subseteq J_1$. W pierwszym przypadku mamy $a - b \in J_2$, zaś w drugim $a - b \in J_1$. Stąd $a - b \in I_1$.
- Jeśli $a \in I_1$ i $b \in R$, to $a \in J$ dla pewnego $J \in \mathcal{S}$. Stąd $ab \in J \subseteq I_1$. Podobnie $ba \in J \subseteq I_1$.
- Z definicji rodziny $\mathcal{S}$, $I \subseteq J$ i $1_R \notin J$ dla $J \in \mathcal{S}$. To oznacza, że $I \subseteq I_1$ i $1 \notin I_1$, a więc $I_1 \in \mathcal{R}$.
- Wprost z określeni rodziny $\mathcal{S}$ wynika, że $J \subseteq I_1$ dla wszystkich $J \in \mathcal{S}$. Innymi słowy, ideał I_1 ogranicza rodzinę $\mathcal{S}$ z góry.

W ten sposób wykazaliśmy, że porządek częściowy $(\mathcal{R}, \subseteq)$ spełnia założenia lematu Kuratowskiego – Zorna. Z lematu tego wynika, że w rodzinie $\mathcal{R}$ istnieje element maksymalny względem relacji inkluzji. Element ten jest ideałem maksymalnym pierścienia R zawierającym ideał I. ■

Wniosek 8.18 *Każdy pierścień z jednością, w którym zero i jedność są różne posiada pewien ideał maksymalny.*

Dowód. Stosujemy twierdzenie 8.17 dla ideału zerowego. ■

Definicja 8.19 *Niech $(R, +, \cdot)$ będzie pierścieniem, zaś I, J jego ideałami.*

(a) Sumą idałów I i J nazywamy zbiór

$$I + J = \{a + b : a \in I, b \in J\}.$$

(b) Iloczynem ideałów I i J nazywamy zbiór

$$I \cdot J = \{a_1b_1 + \ldots + a_nb_n : a_1, \ldots, a_n \in I, b_1, \ldots, b_n \in J, n \in \mathbb{N}_+\}.$$

(c) Ilorazem ideałów I i J nazywamy zbiór

$$I : J = \{a \in R : (\forall b \in J)(ab \in I)\}.$$

Twierdzenie 8.20 *Niech I i J będą ideałami pierścienia $(R, +, \cdot)$. Wtedy $I + J$ i $I \cdot J$ są ideałami pierścienia R. Jeśli dodatkowo pierścień R jest przemienny, to również $I : J$ jest ideałem pierścienia R.*

Dowód. Niech $(R, +, \cdot)$ będzie pierścieniem, zaś I, J jego ideałami. Pokażemy najpierw, że $I + J$ jest ideałem pierścienia R.

- $0_R \in I$ i $0_R \in J$, więc $0_R = 0_R + 0_R \in I + J$.
- Załóżmy, że $a, b \in I + J$. Wtedy $a = a_1 + a_2$ i $b = b_1 + b_2$ dla pewnych $a_1, b_1 \in I$ oraz $b_1, b_2 \in J$. Oczywiście $a_1 - b_1 \in I$ i $a_2 - b_2 \in J$. Dlatego $a - b = (a_1 - b_1) + (a_2 - b_2) \in I + J$.
- Rozważmy elementy $a \in I + J$ i $r \in R$. Tak jak poprzednio, $a = a_1 + a_2$, gdzie $a_1 \in I$ i $a_2 \in J$. Oczywiście $a_1r \in I, a_2r \in J$. Stąd $ar = (a_1 + a_2)r = a_1r + a_2r \in I + J$. Podobnie $ra \in I + J$.

Tak więc $I + J$ jest ideałem pierścienia R.

Dalej udowodnimy, że $I \cdot J$ jest ideałem pierścienia R.

- 0_R należy do każdego z ideałów I, J, więc $0_R = 0_R \cdot 0_R \in I \cdot J$.
- Załóżmy teraz, że $a, b \in I \cdot J$. Wtedy $a = a_1a'_1 + \ldots + a_ma'_m$ i $b = b_1b'_1 + \ldots + b_nb'_n$, gdzie $a_1, \ldots, a_m, b_1, \ldots, b_n \in I$ i $a'_1, \ldots, a'_m, b'_1, \ldots, b'_n \in J$. Stąd:
$$\begin{aligned} a - b &= (a_1a'_1 + \ldots + a_ma'_m) - (b_1b'_1 + \ldots + b_nb'_n) = \\ &= a_1a'_1 + \ldots + a_ma'_m + (-b_1)b'_1 + \ldots + (-b_n)b'_n \in I \cdot J. \end{aligned}$$
- Przypuśćmy, że $a \in I \cdot J$ oraz $r \in R$. Istnieją elementy $a_1, \ldots, a_m \in I$ oraz $a'_1, \ldots, a'_m \in J$, dla których $a = a_1a'_1 + \ldots + a_ma'_m$. Oczywiście $ra_1, \ldots, ra_m \in I$ i $a'_1r, \ldots, a'_mr \in J$. Stąd
$$ra = r(a_1a'_1 + \ldots + a'_ma_m) = (ra_1)a'_1 + \ldots + (ra_m)a'_m \in I \cdot J.$$
Podobnie
$$ar = (a_1a'_1 + \ldots + a_ma'_m)r = a_1(a'_1r) + \ldots + a_m(a'_mr) \in I \cdot J.$$

W ten sposób wykazaliśmy, że $I \cdot J$ jest ideałem pierścienia R.

Przypuśćmy teraz, pierścień R jest przemienny. Wykażemy, że $I : J$ jest jego ideałem.

- $0_R \in I$. Stąd $(\forall b \in J)(0_R \cdot b = 0_R \in I)$. Zatem $0_R \in I : J$.
- Załóżmy, że $a, a' \in I : J$. Wtedy $ab, a'b \in I$ dla dowolnego $b \in J$. Stąd $ab - a'b = (a - a')b \in I$ dla dowolnego $b \in J$. To zaś oznacza, że $a - a' \in I : J$.
- Ustalmy elementy $a \in I$ i $r \in R$. Pokażemy, że $ra \in I : J$. Z definicji ilorazu ideałów, $ab \in I$ dla dowolnego $b \in J$. Stąd $(ra)b \in I$ dla dowolnego $b \in J$. Tak więc $ra \in I : J$.

To kończy dowód faktu, iż $I : J$ jest ideałem pierścienia R. ■

Definicja 8.21 *Niech I będzie ideałem pierścienia R. Radykałem ideału I nazywamy zbiór*
$$rad(I) = \{a \in R : (\exists n \in \mathbb{N}_+)(a^n \in I)\}.$$

Twierdzenie 8.22 *Jeżeli I jest ideałem pierścienia przemiennego R, to $rad(I)$ również jest ideałem pierścienia R.*

Dowód. I jest ideałem w pierścieniu R, więc $0^1 = 0 \in I$. To zaś oznacza, że $0 \in \mathrm{rad}(I)$.

Załóżmy, że $a, b \in \mathrm{rad}(I)$. Wtedy $a^m, b^n \in I$ dla pewnych $m, n \in \mathbb{N}_+$ dla pewnych $m, n \in \mathbb{N}_+$. Zauważmy, że
$$(a-b)^{m+n} = a^{m+n} + \sum_{k=1}^{m+n-1} \binom{m+n}{k} a^k(-b)^{m+n-k} + b^{m+n}.$$
Jeżeli $1 \leq k \leq m+n-1$, to $k \geq m$ lub $m+n-k \geq n$. Zatem dla dowolnego $k \in \{1, \ldots, m+n-1\}$, $a^k \in I$ lub $(-b)^{m+n-k} \in I$. Stąd
$$\binom{m+n}{k} a^k(-b)^{m+n-k} \in I.$$
Ponadto $a^{m+n}, (-b)^{m+n} \in I$. Dlatego $(a-b)^{m+n} \in I$, co implikuje, że $a - b \in \mathrm{rad}(I)$. ■

Przykład 11. W pierścieniu liczb całkowitych rozważmy ideały: $I_1 = 8\mathbb{Z}$, $I_2 = 6\mathbb{Z}$ i $I_3 = 108\mathbb{Z}$. Pokażemy, że

(a) $I_1 + I_2 = 2\mathbb{Z}$,

(b) $I_1 \cdot I_2 = 48\mathbb{Z}$,

(c) $I_3 : I_2 = 18\mathbb{Z}$ i
(d) $\mathrm{rad}(I_3) = 6\mathbb{Z}$.

Oczywiście, $8\mathbb{Z}, 6\mathbb{Z} \subseteq 2\mathbb{Z}$, skąd wynika, że $8\mathbb{Z} + 6\mathbb{Z} \subseteq 2\mathbb{Z}$. Ponadto $2 = 8 + 6 \cdot (-1) \in I_1 + I_2$, a więc również $2\mathbb{Z} \subseteq I_1 + I_2$. To kończy dowód (a).

Załóżmy, że $a \in I_1 \cdot I_2$. Wtedy $a = b_1c_1 + \ldots + b_nc_n$ dla pewnych $b_1, \ldots, b_n \in I_1$ i $c_1, \ldots, c_n \in I_2$. Każda z liczb $b_1, \ldots, b_n$ dzieli się przez 8, zaś każda z liczb $c_1, \ldots, c_n$ dzieli się przez 6. Stąd wynika, że a dzieli się przez 48, czyli $a \in 48\mathbb{Z}$. Z drugiej strony, jeśli $a \in 48\mathbb{Z}$, to $a = 48b = (6 \cdot 1) \cdot (8 \cdot b)$ dla pewnego $b \in \mathbb{Z}$. Stąd $a \in I_1 \cdot I_2$. W ten sposób wykazaliśmy, że $I_1 \cdot I_2 = 48\mathbb{Z}$.

Zauważmy, że jeśli $a \in \mathbb{Z}$, to

$$a \in I_3 : I_2 \iff (\forall b \in I_2)(ab \in I_3) \iff (\forall b \in \mathbb{Z})(6|b \implies 108|ab) \iff 18|a \iff a \in 18\mathbb{Z}.$$

Tak więc $I_3 : I_2 = 18\mathbb{Z}$.

W celu wykazania (d) zauważmy, że jeśli a jest liczbą całkowitą podzielną przez 6, to a^3 dzieli się przez 108. W przypadku, gdy a nie dzieli się przez 6, a^n nie dzieli się przez 6 dla żadnego $n \in \mathbb{N}_+$, a więc tym bardziej a^n nie dzieli się przez 108. Stąd otrzymujemy:

$$a \in \mathrm{rad}(I_3) \iff (\exists n \in \mathbb{N}_+)(a^n \in I_3) \iff (\exists n \in \mathbb{N}_+)(108|a^n) \iff 6|a.$$

Definicja 8.23 *Niech $(R, +, \cdot)$ i $(S, \oplus, \odot)$ będą pierścieniami. Odwzorowanie $f : R \longrightarrow S$ nazywamy*
(a) homomorfizmem, jeśli f zachowuje działania dodawania i mnożenia, to znaczy

$$f(a + b) = f(a) \oplus f(b) \text{ i } f(a \cdot b) = f(a) \odot f(b)$$

dla dowolnych $a, b \in G$,
(b) monomorfizmem lub zanurzeniem, jeśli f jest homomorfizmem różnowartościowym,
(c) epimorfizmem, jeśli f jest homomorfizmem oraz surjekcją,
(d) izomorfizmem, jeśli f jest homomorfizmem oraz bijekcją.

Przykład 12. Niech $n \in \mathbb{N}_+$. Przyporządkowanie liczbie całkowitej jej reszty z dzielenia przez n jest epimorfizmem z pierścienia $(\mathbb{Z}, +, \cdot)$ na pierścień $(\mathbb{Z}_n, +_n, \cdot_n)$.

Definicja 8.24 *Niech $(R, +, \cdot)$ będzie pierścieniem. Dowolny homomorfizm pierścienia R w siebie nazywamy jego endomorfizmem. Izomorfizm $f : R \longrightarrow R$ nazywamy automorfizmem pierścienia R. Zbiór automorfizmów pierścienia R oznaczamy przez $Aut(R)$.*

Z definicji 8.24 natychmiast wynika, że każdy izomorfizm pierścieni jest monomorfizmem oraz epimorfizmem. To samo można powiedzieć o automorfizmie dowolnego pierścienia.

Twierdzenie 8.25 *Niech f będzie homomorfizmem z pierścienia $(R, +, \cdot)$ w pierścień $(S, \oplus, \odot)$ i niech $a \in R$. Wtedy:*
(a) $f(0_R) = 0_R$,
(b) $f(-a) = -f(a)$,
(c) $f(na) = nf(a)$ dla $n \in \mathbb{Z}$,
(d) $f(a^n) = f(a)^n$ dla $n \in \mathbb{N}_+$.

Dowód. Punkty (a), (b) i (c) są konsekwencją twierdzenia 4.26 oraz tego, że f jest homomorfizmem z grupy $(R, +)$ w grupę $(S, \oplus)$. (d) dowodzi się tak samo jak w przypadku grup. ■

Jeśli $f : R \longrightarrow S$ jest homomorfizmem pierścieni z jednością, to obrazem jedności nie musi być jedność. Na przykład dla homomorfizmu $f : \mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z}$ określonego wzorem $f(n) = \langle n, 0\rangle$, $f(1) = \langle 1, 0\rangle$. Jeśli jednak $1_S = f(a)$ dla pewnego $a \in R$, to $f(1_R) = 1_S$. Mamy bowiem:

$$f(1_R) = f(1_R) \cdot 1_S = f(1_R) \cdot f(a) = f(1_R \cdot a) = f(a) = 1_S.$$

Podobnie jak w przypadku grup możemy wykazać następujące twierdzenie.

Twierdzenie 8.26 *Złożenie dwóch homomorfizmów pierścieni jest homomorfizmem pierścieni. To samo dla monomorfizmów, epimorfizmów i izomorfizmów pierścieni.*

Definicja 8.27 *Mówimy, że pierścienie R i S są izomorficzne, jeśli istnieje izomorfizm $f : R \longrightarrow S$. Piszemy wtedy: $R \cong S$.*

Poniższe dwa twierdzenia dowodzi się podobnie jak w przypadku grup.

Twierdzenie 8.28 *Niech R, S i T będą pierścieniami. Wtedy:*
(a) $R \cong R$,
(b) jeśli $R \cong S$, to $S \cong R$,
(c) jeśli $R \cong S$ i $S \cong T$, to $R \cong T$.

Twierdzenie 8.29 *Zbiór automorfizmów dowolnego pierścienia z działaniem składania przekształceń stanowi grupę.*

Definicja 8.30 *Niech $f : R \longrightarrow S$ będzie homomorfizmem pierścieni. Zbiór*

$$Ker(f) = \{a \in R : f(a) = 0_S\}$$

nazywamy jądrem homomorfizmu f. Jeśli $Ker(f) = \{0_R\}$, to mówimy, że homomorfizm f ma trywialne jądro. Zbiór

$$Im(f) = \{f(a) : a \in R\}$$

nazywamy obrazem homomorfizmu f.

Twierdzenie 8.31 *Jeśli $f : R \longrightarrow S$ jest homomorfizmem pierścieni, to*
(a) $Ker(f)$ jest ideałem pierścienia R,
(b) $Im(f)$ jest podpierścieniem pierścienia S.

Dowód. Niech $f : R \longrightarrow S$ będzie homomorfizmem pierścieni. Wówczas f jest homomorfizmem grup addytywnych rozważanych pierścieni, a więc na mocy twierdzenia 4.32(a), $Ker(f)$ jest podgrupą grupy $(R, +)$.

Aby zakończyć dowód punktu (a), rozważmy $a \in Ker(f)$ i $b \in R$. Wtedy

$$f(ab) = f(a) \cdot f(b) = 0_S \cdot f(b) = 0_S.$$

Zatem $ab \in Ker(f)$. Podobnie $ba \in Ker(f)$. Tak więc $Ker(f)$ jest ideałem pierścienia R.

Ponieważ f jest homomorfizmem grup addytywnych pierścieni R i S, na mocy twierdzenia 4.34(b) $Im(f)$ jest podgrupą grupy $(S, +)$. Pokażemy jeszcze, że $Im(f)$ jest zbiorem zamkniętym względem mnożenia. W tym celu ustalmy elementy $a, b \in Im(f)$. Wtedy istnieją $c, d \in R$ takie, że $f(c) = a$ i $f(d) = b$. Stąd $f(cd) = f(c)f(d) = ab$, co oznacza, że $ab \in Im(f)$. ■

Nietrudno podać przykład homomorfizmu pierścieni $f : R \longrightarrow S$, którego obraz nie jest ideałem pierścienia S. Rozważmy odwzorowanie $f : \mathbb{Z} \longrightarrow \mathbb{Z} \oplus \mathbb{Z}$ zadane wzorem $f(x) = \langle x, x\rangle$. f jest homomorfizmem pierścieni (łatwy dowód pozostawiamy Czytelnikowi). Jednak jego obraz

$$Im(f) = \{\langle x, x\rangle : x \in \mathbb{Z}\}$$

nie jest ideałem pierścienia $\mathbb{Z} \oplus \mathbb{Z}$. Mamy bowiem: $\langle 1, 1\rangle \in Im(f)$, ale $\langle 1, 1\rangle \cdot \langle 1, 0\rangle = \langle 1, 0\rangle \notin Im(f)$.

Twierdzenie 8.32 *Homomorfizm pierścieni jest monomorfizmem wtedy i tylko wtedy, gdy jego jądro jest trywialne.*

Dowód. Niech $f : R \longrightarrow S$ będzie homomorfizmem pierścieni. Wtedy f jest homomorfizmem z grupy $(R, +)$ w grupę $(S, +)$, a więc na mocy twierdzenia 4.33 otrzymujemy tezę. ■

Twierdzenie 8.33 *Dowolny niezerowy homomorfizm ciał jest monomorfizmem.*

Dowód. Niech $f : K \longrightarrow L$ będzie homomorfizmem ciał, który nie jest monomorfizmem. Wtedy istnieją $a, b \in K$ takie, że $a \neq b$ i $f(a) = f(b)$. Stąd dla dowolnego $c \in K$ otrzymujemy:

$$\begin{aligned} f(c) &= f(c \cdot 1_K) = f(c \cdot (a-b)^{-1} \cdot (a-b)) = f(c \cdot (a-b)^{-1}) f(a-b) = \\ &= f(c \cdot (a-b)^{-1})(f(a) - f(b)) = f(c \cdot (a-b)^{-1}) \cdot 0_L = 0_L, \end{aligned}$$

co oznacza, że f jest homomorfizmem zerowym. ■

Twierdzenie 8.34 *Niech $f : R \longrightarrow S$ będzie homomorfizmem pierścieni skończonych.*
(a) Jeśli f jest monomorfizmem, to $|R|$ dzieli $|S|$.
(b) Jeśli f jest epimorfizmem, to $|S|$ dzieli $|R|$.

Dowód. Twierdzenie to wynika z twierdzenia 4.34 i z tego, że f jest homomorfizmem grup addytywnych rozpatrywanych pierścieni. ■

Rozdział 9

Pierścienie wielomianów

Pojęcie wielomianu jednej zmiennej o współczynnikach rzeczywistych powinno być znane Czytelnikowi ze szkoły średniej czy też z kursu algebry liniowej. Przez wielomian jednej zmiennej o współczynnikach rzeczywistych rozumie się zwykle funkcję $f : \mathbb{R} \longrightarrow \mathbb{R}$ określoną wzorem postaci

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n,$$

gdzie $a_0, \ldots, a_n$ są pewnymi liczbami rzeczywistymi. W algebrze stosowniejsze jest jednak określenie wielomianu jako pewnego ciągu. O słuszności takiego podejścia może przekonać Czytelnika następujący przykład. Niech $f(x)$ i $g(x)$ będą funkcjami z pierścienia $\mathbb{Z}_2$ w siebie określonymi wzorami: $f(x) = 1+x$ i $g(x) = 1+x^3$. Wtedy $f(0) = g(0) = 1$ i $f(1) = g(1) = 0$. Zatem ta sama funkcja może być określona różnymi wzorami postaci $f(x) = a_0 + a_1 x + \ldots + a_n x^n$.

Poniżej definiujemy pojęcie wielomianu nad pierścieniem przemiennym. W całym rozdziale rozpatrujemy wyłącznie wielomiany nad pierścieniami przemiennymi.

Definicja 9.1 *Niech $(R, +, \cdot)$ będzie pierścieniem przemiennym. Wielomianem jednej zmiennej nad pierścieniem R nazywamy dowolny ciąg nieskończony $f = \langle a_0, a_1, a_2, \ldots\rangle$ elementów pierścienia R, w którym wszystkie wyrazy począwszy od pewnego miejsca są równe 0_R.*

Wyrazy ciągu $f = \langle a_0, a_1, a_2, \ldots\rangle$ nazywamy współczynikami wielomianu f. Wyraz a_0 zwie się wyrazem wolnym wielomianu f. Wielomian jednej zmiennej nad pierścieniem R, którego wszystkie współczynniki są równe 0_R nazywamy wielomianem zerowym. Jeśli R jest pierścieniem z jednością, w którym $0_R \neq 1_R$, to wielomian nad pierścieniem R, którego wyraz wolny jest równy 1_R, zaś pozostałe wyrazy są równe 0_R, nazywamy jednostkowym.

Jak wynika z definicji wielomianu, jeśli $f = \langle a_0, a_1, a_2, \ldots\rangle$ i $g = \langle b_0, b_1, b_2, \ldots\rangle$, to $f = g$ wtedy i tylko wtedy, gdy $a_i = b_i$ dla $i \in \mathbb{N}$.

Jeśli $f = \langle a_0, a_1, a_2, \ldots\rangle$ jest niezerowym wielomianem jednej zmiennej nad pierścieniem R, $a_n \neq 0_R$ i $a_k = 0_R$ dla $k > n$, to f nazywamy wielomianem stopnia n, zaś liczbę n stopniem wielomianu f (oznaczenie: $n = \mathrm{st}(f)$). a_n nazywamy najstarszym (lub najwyższym) współczynnikiem wielomianu f. Dla wielomianu zerowego stopnia nie określamy. Wielomian nad pierścieniem R z jednością, w którym $1_R \neq 0_R$ nazywa się wielomianem unormowanym, jeśli jego najstarszy współczynnik jest równy 1_R.

Zbiór wszystkich wielomianów jednej zmiennej nad pierścieniem przemiennym R oznaczamy przez $R[x]$. W $R[x]$ definiujemy działania dodawania i mnożenia w następujący sposób. Niech $f = \langle a_0, a_1, a_2, \ldots\rangle$ i $g = \langle b_0, b_1, b_2, \ldots\rangle$ będą wielomianami nad R. Przyjmujemy:

$$f \oplus g = \langle a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots\rangle \text{ oraz}$$

$$f \odot g = \langle c_0, c_1, c_2, \ldots\rangle, \text{ gdzie } c_k = \sum_{i=0}^{k} a_i b_{k-i} \text{ dla } k \in \mathbb{N}.$$

W szczególności $c_0 = a_0b_0$, $c_1 = a_0b_1 + a_1b_0$ i $c_2 = a_0b_2 + a_1b_1 + a_2b_0$.

Łatwo sprawdzić, że $(R[x], \oplus, \odot)$ jest pierścieniem przemiennym, którego zerem jest wielomian zerowy. Własności działań w $(R[x], \oplus, \odot)$ wynikają z odpowiednich własności działań w $(R, +, \cdot)$. Udowodnimy dla przykładu łączność mnożenia w $R[x]$. Niech $f = \langle a_0, a_1, a_2, \ldots\rangle$, $g = \langle b_0, b_1, b_2, \ldots\rangle$ i $h = \langle c_0, c_1, c_2, \ldots\rangle$ będą wielomianami nad R. Przyjmijmy oznaczenia: $(f \odot g) \odot h = \langle d_0, d_1, d_2, \ldots\rangle$ i $f \odot (g \odot h) = \langle d'_0, d'_1, d'_2, \ldots\rangle$. Wtedy dla dowolnego $k \in \mathbb{N}$ mamy:

$$d_k = \sum_{j=0}^{k} \left(\sum_{i=0}^{j} a_i b_{j-i} \right) c_{k-j} = \sum_{j=0}^{k} \sum_{i_1+i_2=j} a_{i_1} b_{i_2} c_{k-j} = \sum_{i_1+i_2+i_3=k} a_{i_1} b_{i_2} c_{i_3}.$$

Analogicznie pokazujemy, że d'_k równa się ostatniej z napisanych sum. Tak więc mnożenie w $R[x]$ jest działaniem łącznym.

Nietrudno sprawdzić, że jeśli R jest pierścieniem przemiennym z jednością to $R[x]$ jest pierścieniem przemiennym z jednością. Jednością pierścienia $R[x]$ jest wówczas wielomian $\langle 1_R, 0_R, 0_R, \ldots\rangle$, którego wyraz wolny jest równy 1_R (jedność pierścienia R), zaś pozostałe wyrazy są równe 0_R.

Pierścień $R[x]$ nazywamy pierścieniem wielomianów jednej zmiennej nad pierścieniem R. Pierścień n zmiennych nad pierścieniem R (oznaczenie: $R[x_1, \ldots, x_n]$) definiujemy indukcyjnie:

$$R[x_1] = R[x],\ R[x_1, \ldots, x_{n+1}] = R[x_1, \ldots, x_n][x_{n+1}].$$

Twierdzenie 9.2 *Jeśli R jest pierścieniem, to $R[x]$ ma podpierścień izomorficzny z pierścieniem R.*

Dowód. Niech R będzie pierścieniem. Definiujemy odwzorowanie $f : R \longrightarrow R[x]$ wzorem $f(c) = \langle c, 0, 0, \ldots\rangle$. Wtedy dla dowolnych $a, b \in R$,

$$f(a + b) = \langle a + b, 0, 0, \ldots\rangle = \langle a, 0, 0 \ldots\rangle \oplus \langle b, 0, 0, \ldots\rangle = f(a) \oplus f(b).$$

Analogicznie pokazujemy, że $f(a \cdot b) = f(a) \odot f(b)$. Zatem f jest homomorfizmem pierścieni. Oczywiście f jest odwzorowaniem różnowartościowym, dlatego $Im(f)$ jest podpierścieniem pierścienia $R[x]$ izomorficznym z R. ■

Jak wynika z dowodu powyższego twierdzenia, zbiór wielomianów stopnia 0 wraz z wielomianem zerowym stanowi podpierścień pierścienia $R[x]$ izomorficzny z R. Z tego powodu dowolny wielomian postaci $\langle a, 0_R, 0_R \ldots\rangle$ w praktyce utożsamia się z elementem $a \in R$. Można wtedy pierścień R uważać za podpierścień pierścienia $R[x]$. Wielomian $\langle 0_R, a, 0_R, 0_R \ldots\rangle$ oznaczamy przez ax, wielomian $\langle 0_R, 0_R, a, 0_R, 0_R \ldots\rangle$ przez ax^2, i ogólnie, wielomian $f = \langle a_0, a_1, a_2, \ldots\rangle$ zapisujemy jako $a_0 + a_1x + a_2x^2 + \ldots$. Stosujemy też zapis $a_0 + \sum_{k=1}^{\infty} a_k x^k$ lub $\sum_{k=0}^{\infty} a_k x^k$ (w przypadku pierścieni z jednością, przy czym przyjmujemy, że $x^0 = 1_R$). Jest to tak zwana postać algebraiczna wielomianu f. Jeśli R jest pierścieniem przemiennym z jednością i $1_R \neq 0_R$, to zamiast $1_R x^n$ piszemy zazwyczaj x^n.

Wielomian, którego wszystkie współczynniki poza jednym są równe 0_R nazywamy jednomianem. Zauważmy, że wielomian $a_0 + a_1x + a_2x^2 + \ldots$ jest równy sumie jednomianów: $a_0 \oplus a_1x \oplus a_2x^2 + \ldots$, zaś suma i iloczyn jednomianów a i b stopnia 0 wynoszą odpowiednio $a + b$ i ab. Z tego powodu dalej będziemy używać tych samych symboli do oznaczenia działań w R i w $R[x]$.

Wielomian o zmiennych $x_1, \ldots, x_n$ nad pierścieniem R zapisujemy jako sumę jednomianów, to znaczy wyrażeń postaci $ax_1^{k^1} \ldots x_n^{k_n}$, gdzie $a \in R$.

Twierdzenie 9.3 *Jeśli R jest pierścieniem całkowitym, to $R[x]$ jest pierścieniem całkowitym. W szczególności, jeśli R jest ciałem, to $R[x]$ jest pierścieniem całkowitym.*

Dowód. Niech R będzie pierścieniem całkowitym. Z wcześniejszych rozważań wynika, że $R[x]$ jest pierścieniem przemiennym z jednością. Ponieważ zero i jedność pierścienia R są z założenia różne, także zero i jedność pierścienia $R[x]$ są różne.

Pokażemy jeszcze, że pierścień $R[x]$ nie ma dzielników zera. Niech $f = a_0 + \ldots + a_n x^n$ i $g = b_0 + \ldots + b_m x^m$ będą niezerowymi wielomianami z $R[x]$ takimi, że $a_n \neq 0$ i $b_m \neq 0$. Wtedy najstarszy współczynnik wielomianu fg jest równy $a_n b_m$. Ponieważ pierścień R jest całkowity, mamy $a_n b_m \neq 0$. Wynika stąd, że fg nie jest wielomianem zerowym. W ten sposób wykazaliśmy, że pierścień $R[x]$ nie ma dzielników zera. ■

Twierdzenie 9.4 *Niech R będzie pierścieniem przemiennym i niech $f, g \in R[x]$. Wtedy:*
(a) jeśli $f + g \neq 0$, to $st(f + g) \leq \max(st(f), st(g))$,
(b) jeśli $fg \neq 0$, to $st(fg) \leq st(f) + st(g)$,
(b) jeśli R jest całkowity i $f, g \neq 0$, to $st(fg) = st(f) + st(g)$.

Łatwy dowód tego twierdzenia pozostawiamy Czytelnikowi jako ćwiczenie. Zauważmy, że równość z punktu (c) nie musi zachodzić dla wielomianów nad pierścieniami z dzielnikami zera. Na przykład dla $f = 2x \in \mathbb{Z}_6[x]$, $g = 3x + 1 \in \mathbb{Z}_6[x]$ mamy $\mathrm{st}(fg) = \mathrm{st}(2x) = 1 < \mathrm{st}(f) + \mathrm{st}(g) = 2$.

Niech $f = a_0 + \ldots + a_n x^n$ będzie wielomianem nad pierścieniem przemiennym R i niech $c \in R$. Wartością wielomianu f dla argumentu c nazywamy element $a_0 + \ldots + a_n c^n$ tego pierścienia. Wartość wielomianu f dla argumentu c oznaczamy przez $f(c)$. Łatwo zauważyć, że jeśli f, g są wielomianami nad pierścieniem przemiennym R oraz $c \in R$, to $(f + g)(c) = f(c) + g(c)$ i (fg)(c)=f(c)g(c).

Ustalmy wielomian f nad pierścieniem przemiennym R. Przyporządkowanie każdemu elementowi $c \in R$ wartości $f(c)$ nazywamy funkcją wielomianową wielomianu f i oznaczamy przez $f(x)$. Tak więc wartość wielomianu f dla argumentu c jest równa wartości funkcji wielomianowej wielomiau f w dla argumentu c.

Oczywiście równość wielomianów $f, g \in R[x]$ implikuje równość funkcji wielomianowych $f(x) = g(x)$. Przykład rozważany na początku niniejszego rozdziału pokazuje, że implikacja odwrotna nie zachodzi.

Niech $\Phi : R[x] \longrightarrow R^R$ oznacza przyporządkowanie wielomianowi jego funkcji wielomianowej (funkcja wielomianowa wielomianu $f \in R[x]$ jest pewną funkcją z R w R). W zbiorze R^R w naturalny sposób określone są działania dodawania i mnożenia (przykład 5 ze strony 56). Z wcześniejszych rozważań wynika, że jeśli R jest pierścieniem przemiennym, to Φ jest homomorfizmem pierścieni. Obraz homomorfizmu Φ jest podpierścieniem, pierścienia R^R (twierdzenie 8.31). Dalej zobaczymy, że jeśli R jest nieskończonym pierścieniem całkowitym, to $R[x] \cong Im(\Phi)$ (twierdzenie 9.14).

Definicja 9.5 *Element c pierścienia R nazywamy pierwiastkiem wielomianu $f \in R[x]$, jeśli $f(c) = 0$.*

Zauważmy że wielomian stopnia 0 nie ma pierwiasków i że każdy element pierścienia R jest pierwiastkiem wielomianu zerowego.

Niech R będzie pierścieniem przemiennym i niech $f, g \in R[x]$. Mówimy, że wielomian g dzieli wielomian f (równoważnie: f jest podzielny przez g), jeśli $f = gh$ dla pewnego $h \in R[x]$.

Twierdzenie 9.6 *(Twierdzenie Bézouta[1]) Niech R będzie pierścieniem całkowitym i niech $f \in R[x]$. Element $c \in R$ jest pierwiastkiem wielomianu f wtedy i tylko wtedy, gdy $x - c$ dzieli f.*

Dowód. $\Longrightarrow$. Niech R będzie pierścieniem całkowitym, zaś $f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$ mającym pierwiastek $c \in R$. Wówczas

$$f = a_0 - f(c) + a_1 x + \ldots + a_n x^n = a_1(x - c) + \ldots + a_n(x^n - c^n).$$

Jak łatwo sprawdzić, wielomian $x^k - c^k$ jest podzielny przez $x - c$ dla dowolnego $k \in \mathbb{N}_+$. Zatem wielomian f dzieli się przez $x - c$.

$\Longleftarrow$. Załóżmy, że $x - c$ dzieli wielomian f. Wtedy $f = (x - c)g$ dla pewnego $g \in R[x]$. Stąd dostajemy: $f(c) = (c - c) \cdot g(c) = 0_R \cdot g(c) = 0_R$, co kończy dowód twierdzenia. ■

[1] Etienne Bézout (1730-1783), matematyk francuski

W dowodzie twierdzenia Bézouta nie korzystaliśmy z faktu iż rozpatrywany pierścień nie ma dzielników zera. Zatem jest ono prawdziwe dla wielomianu nad dowolnym pierścieniem przemiennym z jednością, w którym zero i jedność są różne. W związku z twierdzeniem Bézuota przyjmujemy następującą definicję.

Definicja 9.7 *Niech R będzie pierścieniem całkowitym zaś f niezerowym wielomianem z $R[x]$. Element $c \in R$ nazywamy k-krotnym ($k \in \mathbb{N}_+$) pierwiastkiem wielomianu f, jeśli $(x-c)^k$ dzieli f, ale $(x-c)^{k+1}$ nie dzieli f. Liczbę k nazywamy wtedy krotnością pierwiastka c wielomianu f. Krotności pierwiastków wielomianu zerowego nie określamy.*

Wprowadzimy teraz pojęcie pochodnej wielomianu, które dalej wykorzystamy do badania krotności pierwiastków wielomianów nad pierścieniemi całkowitymi.

Niech R będzie pierścieniem przemiennym i niech $f = a_0 + a_1x + a_2x^2 + \ldots \in R[x]$. Przyjmujemy $f' = a_1 + 2a_2x + 3a_3x^2 + \ldots$ (tzn. współczynnik przy x^k dla $k \in \mathbb{N}_+$ w wielomianie f' jest równy $(k+1)a_{k+1}$, wyraz wolny wielomianu f' jest równy a_1). Przypomnijmy, że dla $a \in R$ i $k \in \mathbb{N}_+$, ka oznacza $\underbrace{a + \ldots + a}_{k \text{ razy}}$. Wielomian f' nazywamy pochodną (pierwszego rzędu) wielomianu f. Bezpośrednio z definicji pochodnej wielomianu wynika, że jeśli $f = 0$ lub f jest wielomianem stopnia 0, to $f' = 0$. Odwrotna implikacja nie zachodzi, gdyż na przykład pochodna wielomianu $f = x^3 \in \mathbb{Z}_3[x]$ wynosi 0.

Niech teraz

$$f^{(0)} = f,\ f^{(1)} = f' \text{ i } f^{(n+1)} = (f^{(n)})' \text{ dla } n \in \mathbb{N}.$$

Wielomian $f^{(n)}$ ($n \in \mathbb{N}$) nazywamy pochodną wielomianu f rzędu n lub n-tą pochodną wielomianu f. Czasami zamiast $f^{(2)}, f^{(3)}$ piszemy f'' i f''' (odpowiednio).

Jak łatwo zauważyć, dla wielomiaów nad ciałem liczb rzeczywistych, wprowadzone wyżej pojęcie pochodnej zgadza się z pojęciem pochodej rozważanym w analizie matematycznej.

Przykład 1. Niech $f = 2 + x + 2x^2 + x^4 \in \mathbb{Z}_3[x]$. Wtedy $f' = 1 + x + x^3$, $f^{(2)} = 1$ i $f^{(n)} = 0$ dla $n \geq 3$.

W poniższym twierdzeniu zostały zebrane najważniejsze własności pochodnych wielomianów nad pierścieniami. $f \circ g$ w punkcie (f) oznacza złożenie wielomianów f i g. Ściślej mówiąc, jeśli $f, g \in R[x]$ i $f = a_0 + a_1x + a_2x^2 + \ldots$, to $f \circ g = a_0 + a_1g + a_2g^2 + \ldots$.

Twierdzenie 9.8 *Niech R będzie pierścieniem przemiennym i niech $f, g \in R[x]$. Wtedy*

(a) $(f+g)' = f' + g'$, $(f-g)' = f' - g'$,

(b) $(cf)' = cf'$ *dla* $c \in R$,

(c) $(fg)' = f'g + fg'$,

(d) $(fg)^{(n)} = \sum_{k=0}^{n} \binom{n}{k} f^{(k)}g^{(n-k)}$ *dla* $n \in \mathbb{N}$,

(e) $(f^n)' = nf^{n-1}f'$ *dla* $n \geq 2$,

(f) $(f \circ g)' = (f' \circ g) \cdot g'$,

(g) $(f^{(m)})^{(n)} = (f^n)^{(m)} = f^{m+n}$ *dla* $m, n \in \mathbb{N}$.

Dowód. Niech $f = a_0 + a_1x + a_2x^2 + \ldots$ i $g = b_0 + b_1x + b_2x^2 + \ldots$ będą wielomianami nad pierścieniem przemiennym R i niech $c \in R$. Wtedy $f + g = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots$, skąd wynika, że

$$\begin{aligned}(f+g)' &= (a_1 + b_1) + 2(a_2 + b_2)x + 3(a_3 + b_3)x^2 + \ldots) = \\ &= (a_1 + 2a_2x + 3a_3x^2 + \ldots) + (b_1 + b_2x + b_3x^2 + \ldots) = f' + g'.\end{aligned}$$

Analogicznie dowodzi się, że $(f-g)' = f' - g'$.

$$\begin{aligned}(cf)' &= [c(a_0 + a_1x + a_2x^2 + \ldots)]' = (ca_0 + ca_1x + ca_2x^2 + \ldots)' = \\ &= ca_1 + 2ca_2x + 3ca_3x^2 + \ldots = c(a_1 + 2a_2x + 3a_3x^2 + \ldots) = cf'.\end{aligned}$$

Dla dowodu (c) przyjmijmy, że

$$f \cdot g = c_0 + c_1x + c_2x^2 + \ldots \text{ i } f'g + fg' = d_0 + d_1x + d_2x^2 + \ldots,$$

z definicji iloczynu wielomianów oraz definicji pochodnej dla $n \in \mathbb{N}$ otrzymujemy:

$$\begin{aligned}c_n &= \sum_{k=0}^{n} a_k b_{n-k}, \\ d_n &= \sum_{k=0}^{n}(k+1)a_{k+1}b_{n-k} + \sum_{k=0}^{n} a_k(n+1-k)b_{n+1-k} = \sum_{k=1}^{n+1} ka_kb_{n+1-k} + \sum_{k=0}^{n} a_k(n+1-k)b_{n+1-k} = \\ &= (n+1)a_{n+1}b_0 + \sum_{k=1}^{n}(n+1)a_kb_{n+1-k} + (n+1)a_0b_{n+1} = (n+1)\sum_{k=0}^{n+1} a_kb_{n+1-k} = (n+1)c_{n+1}.\end{aligned}$$

W ten sposób wykazaliśmy części (a), (b) i (c) twierdzenia.

(d) i (e) udowodnimy przez indukcję względem n. Oczywiście

$$(fg)^{(0)} = fg = f^{(0)}g^{(0)} = \sum_{k=0}^{0} \binom{0}{k} f^{(k)}g^{(0-k)},$$

co oznacza, że (d) zachodzi dla $n = 0$. Zakładając, że (d) zachodzi dla pochodnych rzędu $n \in \mathbb{N}$ otrzymujemy:

$$\begin{aligned}(fg)^{(n+1)} &= ((fg)^{(n)})' = \left(\sum_{k=0}^{n} \binom{n}{k} f^{(k)}g^{(n-k)}\right)' = \sum_{k=0}^{n} \binom{n}{k} (f^{(k)}g^{(n-k)})' = \\ &= \sum_{k=0}^{n} \binom{n}{k} (f^{(k+1)}g^{(n-k)} + f^{(k)}g^{n+1-k}) = \\ &= \sum_{k=1}^{n+1} \binom{n}{k-1} f^{(k)}g^{(n+1-k)} + \sum_{k=0}^{n} \binom{n}{k} f^{(k)}g^{(n+1-k)} = \\ &= f^{(0)}g^{(n+1)} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k}\right) f^{(k)}g^{(n+1-k)} + f^{(n+1)}g^{(0)} = \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} f^{(k)}g^{(n+1-k)}.\end{aligned}$$

Z (c) łatwo wynika, że $(f^2)' = 2ff'$. Zakładając, że (e) zachodzi dla liczby naturalnej $n \geq 2$, otrzymujemy:

$$(f^{n+1})' = (f \cdot f^n)' = f'f^n + fnf^{n-1}f' = (n+1)f^{n+1}f'.$$

W celu wykazania (f) załóżmy, że $f = a_0 + a_1x + a_2x^2 + \ldots$. Wtedy na mocy (a) i (e) otrzymujemy:

$$(f \circ g)' = (a_0 + a_1g + a_2g^2 + a_3g^3 + \ldots)' = a_1g' + 2a_2gg' + 3a_3g^2g' + \ldots = (f' \circ g)g'.$$

Dowód punktu (g) zostawiamy jako ćwiczenie dla Czytelnika. ■

Twierdzenie 9.9 *Niech R będzie pierścieniem całkowitym o charakterystyce równej 0 i niech $f \in R[x]$. Wtedy dla dowolnych $k \in \mathbb{N}_+$ i $c \in R$, c jest k-krotnym pierwiastkiem wielomianu f wtedy i tylko wtedy gdy $f^{(i)}(c) = 0$ dla $i < k$ oraz $f^{(k)}(c) \neq 0$.*

Dowód. Załóżmy, że R jest pierścieniem całkowitym o charakterystyce równej 0 i $c \in R$. Aby udowodnić twierdzenie, wystarczy wykazać, że dla dowolnego $k \in \mathbb{N}_+$ spełniony jest warunek:

$$(*)_k \text{ jeśli } f \in R[x], \text{to } (x-c)^k | f \iff f^{(i)}(c) = 0 \text{ dla } i < k.$$

Dowód przeprowadzimy metodą indukcji matematycznej. Dla $k = 1$ powyższy warunek wynika z twierdzenia Bézouta (twierdzenie 9.6). Załóżmy, że udowodniliśmy już warunek $(*)_k$ ($k \in \mathbb{N}_+$). W celu wykazania $(*)_{k+1}$, ustalmy dowolny wielomian $f \in R[x]$. Udowodnimy, że

$$(x-c)^{k+1} | f \iff f^{(i)}(c) = 0 \text{ dla } i \leq k.$$

$\Longrightarrow$. Załóżmy, że $(x-c)^{k+1} | f$. Wtedy $f = (x-c)^{k+1}h$ dla pewnego $h \in R[x]$. Zgodnie z twierdzeniem 9.8(c),

$$f' = (k+1)(x-c)^k h + (x-c)^{k+1}h' = (x-c)^k[(k+1)h + (x-c)h'].$$

Tak więc $(x-c)^k | f'$. Stąd, na mocy warunku $(*)_k$ wynika, że $(f')^{(i)}(c) = 0$ dla $i < k$, czyli, wobec twierdzenia 9.8(g), $f^{(i)}(c) = 0$ dla $1 \leq i \leq k$. Ponieważ $f^{(0)}(c) = f(c) = 0$, dostajemy $f^{(i)}(c) = 0$ dla $i \leq k$.

$\Longleftarrow$. Załóżmy, że $f^{(i)}(c) = 0$ dla $i \in \{0, 1, \ldots k\}$. Wtedy $f^{(i)}(c) = 0$ i $(f')^{(i)}(c) = 0$ dla $i < k$. W myśl warunku $(*)_k$ oznacza to, że wielomiany f i f' są podzielne przez $(x-c)^k$. Istnieją zatem wielomiany $h_1, h_2 \in R[x]$ takie, że $f = (x-c)^k h_1$ i $f' = (x-c)^k h_2$. Zauważmy, że $f' = k(x-c)^{k-1}h_1 + (x-c)^k h_1'$. Stąd

$$(x-c)^k h_2 = k(x-c)^{k-1}h_1 + (x-c)^k h_1'.$$

$R[x]$ jest pierścieniem całkowitym (twierdzenie 9.3), więc można zastosować prawo skracań. Otrzymujemy: $(x-c)h_2 = kh_1 + (x-c)h_1'$, co dla $x = c$ daje $kh_1(c) = 0$.

$$kh_1(c) = \underbrace{h_1(c) + \ldots + h_1(c)}_{k \text{ razy}} = (\underbrace{1_R + \ldots + 1_R}_{k \text{ razy}}) \cdot h_1(c).$$

Ponieważ charakterystyka pierścienia R wynosi 0, $\underbrace{1_R + \ldots + 1_R}_{k \text{ razy}} \neq 0_R$. Stąd, na mocy całkowitości pierścienia R dostajemy $h_1(c) = 0$. Z twierdzenia Bézouta istnieje wielomian $h_3 \in R[x]$ taki, że $h_1 = (x-c)h_3$. Tak więc

$$f = (x-c)^k h_1 = (x-c)^{k+1} h_3,$$

co oznacza, że wielomian f dzieli się przez $(x-c)^{k+1}$. ■

Przykład 2. Zastosujemy twierdzenie 9.9 do określenia krotności pierwiastka wielomianu o współczynnikach całkowitych (jak wiemy, $(\mathbb{Z}, +, \cdot)$ jest pierścieniem całkowitym o charakterystyce równej 0). Niech $f = x^5 + 5x^4 + 13x^3 + 19x^2 + 14x + 4$. $f(-1) = -1 + 5 - 13 + 19 - 14 + 4 = 0$, więc -1 jest pierwiastkiem wielomianu f. Dalej obliczamy: $f' = 5x^4 + 20x^3 + 39x^2 + 38x + 14$, $f'(-1) = 5 - 20 + 39 - 38 + 14 = 0$, $f'' = 20x^3 + 60x^2 + 78x + 38$, $f''(-1) = -20 + 60 - 78 + 38 = 0$, $f''' = 60x^2 + 120x + 78$, $f'''(-1) = 60 - 120 + 78 \neq 0$ Tak więc na mocy twierdzenia 9.9, -1 jest trzykrotnym pierwiastkiem wielomianu f. Innymi słowy, wielomian f dzieli się przez $(x+1)^3$, ale nie dzieli się przez $(x+1)^4$.

Metoda określania krotności pierwiastka wielomianu wynikająca z twierdzenia 9.9 zawodzi dla wielomianów nad pierścieniami całkowitymi o charakterystyce dodatniej. Rozważmy na przykład

wielomian $g = x^4 + x^2 \in \mathbb{Z}_2[x]$. Wtedy $g(0) = g'(0) = g''(0) = 0$, ale g nie dzieli się przez x^3. Załóżmy bowiem, że $x^4 + x^2 = x^3 h$ dla pewnego $h \in \mathbb{Z}_2[x]$. Wtedy h jest wielomianem stopnia 1, co oznacza, że $h = x$ lub $h = x + 1$. Oba przypadki łatwo prowadzą do sprzeczności.

Twierdzenie 9.10 *Jeśli liczba całkowita m jest pierwiastkiem wielomianu $f = a_0 + \ldots + a_n x^n \in \mathbb{Z}[x]$, to m dzieli a_0.*

Dowód. Załóżmy, że $f(m) = 0$. Wtedy

$$a_0 = (-a_1 m) + \ldots + (-a_n m^n) = -m(a_1 + \ldots a_n m^{n-1}),$$

co oznacza, że m dzieli a_0. ■

Twierdzenie 9.11 *Jeśli liczba wymierna $\frac{p}{q}$ $(p, q \in \mathbb{Z}, q \neq 0, NWD(p, q) = 1)$ jest pierwiastkiem wielomianu $f = a_0 + \ldots + a_n x^n$ stopnia przynajmniej 1, to $p|a_0$ i $q|a_n$.*

Dowód. Załóżmy, że $f(\frac{p}{q}) = 0$. Wtedy

$$a_0 + a_1 \frac{p}{q} + \ldots + a_n \left(\frac{p}{q}\right)^n = 0,$$

skąd wynika, że

$$a_0 q^n = (-a_1 p q^{n-1}) + \ldots + (-a_n p^n) = -p \cdot \sum_{k=1}^{n} a_k p^{k-1} q^{n-k} \text{ oraz}$$

$$a_n p^n = (-a_0 q^n) + \ldots + (-a_{n-1} p^{n-1} q) = -q \sum_{k=1}^{n} a_k p^{k-1} q^{n-k}.$$

Mamy więc $p|a_0 q^n$ i $q|a_n p^n$. Ponieważ liczby p i q są względnie pierwsze, $p|a_0$ i $q|a_n$. ■

Twierdzenie 9.12 *Jeśli R jest pierścieniem całkowitym, to wielomian $f \in R[x]$ stopnia $n \in \mathbb{N}$ ma w pierścieniu R co najwyżej n pierwiastków (liczonych z krotnościami).*

Dowód. Niech R będzie pierścieniem całkowitym. Twierdzenie jest oczywiste dla wielomianów stopnia 0 (wielomian stopnia 0 jest z definicji niezerowy). Przypuśćmy zatem, że $n \in \mathbb{N}$ i twierdzenie jest słuszne dla wielomianów stopnia mniejszego lub równego n. Rozważmy wielomian $f \in R[x]$ stopnia $n + 1$. Pokażemy, że f ma w pierścieniu R co najwyżej $n + 1$ pierwiastków.

Oczywiście, w przypadku gdy f nie posiada żadnych pierwiastków w R, nie trzeba niczego dowodzić. Załóżmy więc, że a jest pierwiastkiem k-krotnym wielomianu f. Wtedy $(x - a)^k | f$, ale $(x - a)^{k+1}$ nie dzieli f. Mamy więc $f = (x - a)^k g$, przy czym $g \in R[x]$ i $g(a) \neq 0$. Oczywiście $\mathrm{st}(g) = \mathrm{st}(f) - k = n + 1 - k \leq n$. Z całkowitości pierścienia R wynika, że każdy pierwiastek wielomianu f różny od a jest pierwiastkiem wielomianu g. Na mocy założenia indukcyjnego, wielomian g posiada co najwyżej $n + 1 - k$ pierwiastków (liczonych z krotnościami). Dlatego wielomian f posiada co najwyżej $k + (n + 1 - k) = n + 1$ pierwiastków, co kończy dowód. ■

Twierdzenie 9.13 *Niech R będzie pierścieniem całkowitym, zaś f i g wielomianami nad R stopnia co najwyżej n. Jeżeli istnieją różne elementy $c_1, \ldots, c_{n+1} \in R$ takie, że $f(c_i) = g(c_i)$ dla wszystkich $i = 1, \ldots, n + 1$, to $f = g$.*

Dowód. Załóżmy nie wprost, że wielomiany f i g są różne. Wtedy $f - g$ jest wielomianem niezerowym stopnia co najwyżej n. Tak więc na mocy twierdzenia 9.12, $f - g$ posiada co najwyżej n pierwiastków (liczonych z krotnościami). Tymczasem, na mocy założenia, $(f - g)(c_i) = f(c_i) - g(c_i) = 0$ dla $i = 0, \ldots n + 1$. Sprzeczność. ■

Twierdzenie 9.14 *Jeżeli R jest nieskończonym pierścieniem całkowitym i $f, g \in R[x]$, to*

$$f = g \iff f(x) = g(x).$$

Dowód. Implikacja $\Longrightarrow$ jest oczywista. W celu wykazania implikacji przeciwnej, rozważmy wielomiany f i g nad pierścieniem całkowitym R, których funkcje wielomianowe $f(x)$ i $g(x)$ są równe. Niech $n = \max(\mathrm{st}(f), \mathrm{st}(g))$. Wybierzmy różne elementy $c_1, \ldots, c_{n+1} \in R$ (można to uczynić, gdyż R jest nieskończony). Z założenia mamy wówczas $f(c_i) = g(c_i)$ dla $i \in \{1, \ldots, n+1\}$. Stąd, na mocy twierdzenia 9.13, wynika że $f = g$. ■

Wniosek 9.15 *Jeśli R jest nieskończonym pierścieniem całkowitym, to pierścień $R[x]$ jest izomorficzny z pierścieniem funkcji wielomianowych nad R.*

Dowód. Niech R będzie nieskończonym pierścieniem całkowitym, zaś S pierścieniem funkcji wielomianowych nad R. Definiujemy odwzorowanie $F : R[x] \longrightarrow S$ wzorem $F(f) = f(x)$ (tzn. wielomianowi przyporządkowujemy jego funkcję wielomianową). Pokażemy, że F jest izomorfizmem.

Oczywiście $(f + g)(c) = f(c) + g(c)$ i $(fg)(c) = f(c)g(c)$ dla $c \in R$. Oznacza to, że funkcje wielomianowe wielomianów $f+g$ i fg są równe $f(x)+g(x)$ i $f(x)g(x)$ (odpowiednio). Stąd dostajemy:

$$\begin{aligned} F(f+g) &= (f+g)(x) = f(x) + g(x) = F(f) + F(g) \\ F(fg) &= (fg)(x) = f(x)g(x) = F(f)F(g). \end{aligned}$$

Tak więc F jest homomorfizmem pierścieni. Oczywiście F jest surjekcją. Różnowartościowość F jest konsekwencją twierdzenia 9.14. W ten sposób wykazaliśmy, że F jest izomorfizmem pierścieni. ■

Twierdzenie 9.16 *Niech R będzie pierścieniem całkowitym, zaś $f = a_n x^n + \ldots + a_1 x + a_0$ wielomianem stopnia $n \geq 1$. Jeśli $c_1, \ldots, c_n$ są wszystkimi pierwiastkami wielomianu f (w ciągu tym pierwiastek k-krotny wymieniamy k razy), to $f = a_n(x - c_1) \cdot \ldots \cdot (x - c_n)$.*

Dowód. (Indukcja względem n) Niech R będzie pierścieniem całkowitym. Załóżmy najpierw, że $f \in R[x]$ jest wielomianem stopnia 1 mającym pierwiastek c_1. Wtedy $f = a_1 x + a_0$ dla pewnych $a_0, a_1 \in R$, przy czym $a_1 \neq 0_R$.

$$f = a_1 x + a_0 = a_1(x - c_1) + (a_1 c_1 + a_0) = a_1(x - c_1) + f(c_1) = a_1(x - c_1) + 0 = a_1(x - c_1).$$

Przypuśćmy teraz, że twierdzenie jest prawdziwe dla wielomianów stopni $1, \ldots, n$ ($n \in \mathbb{N}_+$) nad pierścieniem R. Rozważmy wielomian $f = a_{n+1}x^{n+1} + \ldots + a_1 x + a_0 \in R[x]$ stopnia $n+1$, mający pierwiastki $c_1, \ldots, c_{n+1}$. Niech c_1 będzie pierwiastkiem k-krotnym wielomianu f. Wtedy f dzieli się przez $(x - c_1)^k$ ale nie dzieli się przez $(x - c_1)^{k+1}$. Oczywiście $f = (x - c_1)^k g$ dla pewnego $g \in R[x]$, przy czym $g(c_1) \neq 0$.

Jeśli $k = n + 1$, to $c_1 = c_i$ dla $i \in \{1, \ldots, n+1\}$. Ponadto g jest wielomianem stopnia 0. Ponieważ najstarszy współczynnik wielomianu f jest równy a_{n+1}, dostajemy $f = a_{n+1}(x - c_1)^{n+1} = a_{n+1}(x - c_1) \cdot \ldots \cdot (x - c_{n+1})$.

Jeśli $1 \leq k \leq n$, to $1 \leq \mathrm{st}(g) \leq n$. Niech c_i będzie pierwiastkiem wielomianu f różnym od c_1. Wtedy $(c_i - c_1)^k g(c_i) = 0$. Stąd, na mocy całkowitości pierścienia R wynika, że $g(c_i) = 0$. Tak więc wielomian g posiada dokładnie $n + 1 - k$ pierwiastków (liczonych z krotnościami). $n + 1 - k \leq n$, więc na mocy założenia indukcyjnego,

$$g = a_{n+1} \prod_{\{i : c_i \neq c_1\}} (x - c_i) \Longrightarrow f = a_{n+1}(x - c_1)^k \prod_{\{i : c_i \neq c_1\}} (x - c_i) = a_{n+1}(x - c_1) \cdot \ldots \cdot (x - c_{n+1}).$$

■

Wniosek 9.17 *(Wzory Viety[2]) Jeśli R jest pierścieniem całkowitym, zaś $f = a_n x^n + \ldots + a_1 x + a_0 \in R[x]$ wielomianem stopnia $n \geq 1$ mającym pierwiastki $c_1, \ldots, c_n$, to*

$$\begin{aligned} a_{n-1} &= -a_n(c_1 + \ldots + c_n) \\ a_{n-2} &= a_n \sum_{1 \leq i_1 < i_2 \leq n} c_{i_1} c_{i_2} \\ &\ldots \\ a_{n-k} &= (-1)^k a_n \sum_{1 \leq i_1 < \ldots < i_k \leq n} c_{i_1} \ldots c_{i_k} \\ &\ldots \\ a_0 &= (-1)^n a_n c_1 \ldots c_n. \end{aligned}$$

Dowód. Z twierdzenia 9.16 wynika, że $f = a_n(x - x_1) \cdot \ldots \cdot (x - x_n)$. Stąd po wymnożeniu wszystkich czynników otrzymujemy:

$$f = a_n x^n - a_n(c_1 + \ldots + c_n)x^{n-1} + a_n \left(\sum_{1 \leq i_1 < i_2 \leq n} c_{i_1} c_{i_2} \right) x^{n-2} + \ldots + (-1)^n a_n c_1 \ldots c_n.$$

W ten sposób współczynnik przy x^{n-k} jest równy $(-1)^k a_n \sum_{1 \leq i_1 < \ldots < i_k \leq n} c_{i_1} \ldots c_{i_k}$. Z drugiej strony wiemy, że współczynnik przy x^{n-k} wynosi a_{n-k}. Stąd dostajemy wzory Viety. ■

Twierdzenie 9.18 *(Schemat Hornera) Niech $f = a_0 x^n + \ldots + a_{n-1} x + a_n$ będzie wielomianem stopnia $n \geq 1$ nad pierścieniem całkowitym R i niech $a \in R$. Wtedy istnieją: wielomian $g = b_0 x^{n-1} + \ldots + b_{n-1} \in R[x]$ oraz element $c \in R$ takie, że $f = (x - a)g + c$, przy czym*

$$\begin{aligned} b_0 &= a_0 \\ b_k &= a_k + a b_{k-1} \text{ gdy } 1 \leq k \leq n-1 \\ c &= a_n + a b_{n-1}. \end{aligned}$$

g i c są określone jednoznacznie.

Dowód. Mając dane współczynniki $a_0, \ldots, a_n$, definiujemy $b_0, \ldots, b_{n-1}$ i c wzorami: $b_0 = a_0$, $b_{k+1} = a_k + a b_{k-1}$ gdy $0 \leq k \leq n-2$ i $c = a_n + a b_{n-1}$. Wtedy:

$$\begin{aligned} f &= a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = \\ &= b_0 x^n + (b_1 - a b_0) x^{n-1} + \ldots + (b_{n-1} - a b_{n-2}) x + (c - a b_{n-1}) = \\ &= b_0 x^{n-1}(x - a) + b_1 x^{n-2}(x - a) + \ldots + b_{n-1}(x - a) + c = (b_0 x^{n-1} + \ldots + b_{n-1})(x - a) + c, \end{aligned}$$

co kończy dowód istnienia wielomianu g i elementu c.

Przypuśćmy teraz, że $f = (x - a)g_1 + c_1 = (x - a)g_2 + c_2$, gdzie $g_1, g_2 \in R[x]$ i $c_1, c_2 \in R$. Wtedy $(x - a)(g_1 - g_2) = c_1 - c_2$. Jeśli $c_1 \neq c_2$, to $g_1 \neq g_2$ i stopień lewej strony jest większy od 0. Sprzeczność. Zatem musi być $c_1 = c_2$. Wtedy $(x - a)(g_1 - g_2) = 0$, a więc również $g_1 = g_2$. ■

Przykład 3. Niech $f = 2x^4 + 6x^2 - 10x + 12 \in \mathbb{Z}[x]$. Posługując się schematem Hornera znajdziemy wielomian $g \in \mathbb{Z}[x]$ oraz liczbę całkowitą c takie, że $f = (x - 2)g + c$.

[2]Francis Vieta (1540-1603), matematyk i prawnik francuski

Przyjmijmy oznaczenia: $f = a_0x^4 + a_1x^3 + a_2x^2 + a_1x + a_0$ (to znaczy $a_0 = 2$, $a_1 = 0$, $a_2 = 6$, $a_3 = -10$ i $a_4 = 12$) i $a = 2$. Szukamy wielomianu g postaci $b_0x^3 + b_1x^2 + b_2x + b_3$. Obliczamy:

$$\begin{aligned} b_0 &= a_0 = 2 \\ b_1 &= a_1 + ab_0 = 0 + 2 \cdot 2 = 4 \\ b_2 &= a_2 + ab_1 = 6 + 2 \cdot 4 = 14 \\ b_3 &= a_3 + ab_2 = -10 + 2 \cdot 14 = 18 \\ c &= a_4 + ab_3 = 12 + 2 \cdot 18 = 48. \end{aligned}$$

Posługując się schematem Hornera, można, zamiast pisać powyższe równości, umieszczać wyniki obliczeń w następującej tabeli:

2	0	6	-10	12
2	4	14	18	48

W pierwszym wierszu znajdują się kolejno dane współczynniki a_0, a_1, a_2, a_3 i a_4, zaś w drugim obliczone b_0, b_1, b_2, b_3 oraz c. Tak więc $f = (x - 2)(2x^3 + 4x^2 + 14x + 18) + 48$.

Twierdzenie 9.19 *Niech R będzie pierścieniem całkowitym. Dla dowolnego wielomianu $f \in R[x]$ i dowolnego unormowanego wielomianu $g \in R[x]$, istnieją wielomiany $q, r \in R[x]$ takie, że $f = qg + r$, przy czym $r = 0$ lub $st(r) < st(g)$. Wielomiany q i r są określone jednoznacznie.*

Dowód. Ustalmy wielomian unormowany $g \in R[x]$. Jeśli $f = 0$ lub $\mathrm{st}(f) < \mathrm{st}(g)$, to przyjmując $q = 0$ i $r = f$ otrzymujemy odpowiednie przedstawienie wielomianu f. Dlatego wystarczy dowieść, że dla dowolnego $n \in \mathbb{N}$ spełniony jest warunek:

$$(*)_n \quad (\forall f \in R[x])\,[\mathrm{st}(f) = n \geq \mathrm{st}(g) \Longrightarrow (\exists q, r \in R[x])[f = qg + r \wedge (r = 0 \vee \mathrm{st}(r) < \mathrm{st}(g))]].$$

Dowód przeprowadzimy stosując indukcję względem n. Załóżmy, że $f \in R[x]$ i $\mathrm{st}(f) = 0 \geq \mathrm{st}(g)$. Wtedy $g = 1$, gdyż z założenia g jest wielomianem unormowanym. Tak więc $f = f \cdot g + 0$, co oznacza, że $(*)_0$ zachodzi.

Niech $n \in \mathbb{N}_+$. Przypuśćmy, że dla liczb naturalnych $k < n$ prawdziwy jest warunek $(*)_k$. W celu wykazania $(*)_n$, załóżmy, że $f \in R[x]$ jest wielomianem stopnia n, przy czym $n \geq \mathrm{st}(g)$. Wtedy $f = a_nx^n + f_1$, przy czym $f_1 = 0$ lub $\mathrm{st}(f_1) < \mathrm{st}(f)$. Z założenia indukcyjnego i wstępnych uwag wynika, że $f_1 = q_1g + r_1$ dla pewnych wielomianów $q_1, r_1 \in R[x]$, przy czym $r_1 = 0$ lub $\mathrm{st}(r_1) < \mathrm{st}(g)$. Tak więc $f = a_nx^n + (q_1g + r_1)$. g jest wielomianem unormowanym, więc

$$a_nx^n = a_nx^{n-\mathrm{st}(g)}g + (-a_nx^{n-\mathrm{st}(g)}g + a_nx^n),$$

przy czym

$$-a_nx^{n-\mathrm{st}(g)}g + a_nx^n = 0 \text{ lub } \mathrm{st}(-a_nx^{n-\mathrm{st}(g)}g + a_nx^n) < \mathrm{st}(f).$$

Zatem na mocy założenia indukcyjnego oraz uwag wstępnych, $-a_nx^{n-\mathrm{st}(g)}g + a_nx^n = q_2g + r_2$ dla pewnych $q_2, r_2 \in R[x]$, przy czym $r_2 = 0$ lub $\mathrm{st}(r_2) < \mathrm{st}(g)$. Ostatecznie otrzymujemy

$$f = a_nx^n + f_1 = (a_nx^{n-\mathrm{st}(g)}g + q_2g + r_2) + (q_1g + r_1) = (a_nx^{n-\mathrm{st}(g)} + q_1 + q_2)g + (r_1 + r_2).$$

Oczywiście $r_1 + r_2 = 0$ lub $\mathrm{st}(r_1 + r_2) < \mathrm{st}(g)$.

Dla wykazania jednoznaczności, załóżmy, że $f = q_1g + r_1 = q_2g + r_2$, gdzie $q_1, q_2, r_1, r_2 \in R[x]$, przy czym ($r_1 = 0$ lub $\mathrm{st}(r_1) < \mathrm{st}(g)$) i ($r_2 = 0$ lub $\mathrm{st}(r_2) < \mathrm{st}(g)$). Wtedy $(q_1 - q_2)g = r_1 - r_2$. Jeśli $r_1 \neq r_2$, to $q_1 \neq q_2$ i stopień lewej strony jest większy od stopnia prawej strony. Sprzeczność. Zatem musi być $r_1 = r_2$. Wtedy $(q_1 - q_2)g = 0$, a więc $q_1 = q_2$. ■

Wniosek 9.20 *Niech K będzie ciałem. Dla dowolnego wielomianu $f \in K[x]$ i dowolnego niezerowego wielomianu $g \in K[x]$, istnieją wielomiany $q, r \in K[x]$ takie, że $f = qg + r$, przy czym $r = 0$ lub $st(r) < st(g)$. Wielomiany q i r są określone jednoznacznie.*

Dowód. Twierdzenie jest oczywiste, gdy wielomian f jest zerowy. Załóżmy, więc, że $f \neq 0$. Ponieważ K jest ciałem, wielomian g możemy zapisać w postaci $g = ag_1$, gdzie $a \in K$, zaś g_1 jest wielomianem unormowanym. Zgodnie z twierdzeniem 9.19, w pierścieniu $K[x]$ istnieje dokładnie jedna para wielomianów $\langle q_1, r_1 \rangle$ taka, że $f = q_1 g_1 + r_1$ i ($\mathrm{st}(r_1) < \mathrm{st}(g_1)$ lub $r_1 = 0$). Zatem $f = (a^{-1}q_1)g + r_1$ i wielomiany $q = a^{-1}q_1$ i $r = r_1$ spełniają tezę twierdzenia. ■

Lemat 9.21 *Załóżmy, że K jest podciałem ciała L oraz $f, g \in K[x]$. Jeśli $f = gh \neq 0$, gdzie $h \in L[x]$, to $h \in K[x]$.*

Dowód. Przypuśćmy nie wprost, że $f = gh \neq 0$, przy czym $f, g \in K[x]$ i $h \in L[x] \setminus K[x]$. Wtedy mamy: $g \neq 0$ i $h = h_1 + h_2$, gdzie $h_1 \in K[x]$, zaś najstarszy współczynnik wielomianu h_2 należy do $L \setminus K$. Ponieważ g jest niezerowym wielomianem z $K[x]$, najstarszy współczynnik wielomianu gh_2 należy do $L \setminus K$, czyli $gh_2 \notin K[x]$. Z drugiej strony

$$gh_2 = g(h - h_1) = f - gh_1 \in K[x].$$

Otrzymana sprzeczność kończy dowód twierdzenia. ■

Definicja 9.22 *Niech K będzie ciałem, zaś $f \in K[x]$ wielomianem stopnia ≥ 1. Wielomian f nazywamy rozkładalnym nad K, jeśli istnieją wielomiany $g, h \in K[x]$ stopnia przynajmniej 1 takie, że $f = gh$. W przeciwnym wypadku wielomian f nazywamy nierozkładalnym lub nieprzywiedlnym nad K.*

Bezpośrednio z definicji wynika, że każdy wielomian stopnia 1 o współczynnikach z ciała jest nierozkładalny nad tym ciałem. Przy badaniu rozkładalności wielomianów nad $\mathbb{Q}$ pomocne bywa tzw. kryterium Eisensteina[3]-Schönemanna (twierdzenie 9.25). Udowodnimy najpierw dwa pomocnicze fakty o wielomianach nad $\mathbb{Z}$ i nad $\mathbb{Q}$.

Lemat 9.23 *(Lemat Gaussa) Niech $f = a_0 + a_1 x + \ldots$ i $g = b_0 + b_1 x + \ldots$ będą niezerowymi wielomianami nad $\mathbb{Z}$ takimi, że $NWD(a_0, a_1, \ldots) = 1$ i $NWD(b_0, b_1, \ldots) = 1$. Wtedy największy wspólny dzielnik współczynników wielomianu fg wynosi 1.*

Dowód. Niech $fg = c_0 + c_1 x + \ldots$. Wtedy $c_n = \sum_{i=0}^{n} a_i b_{n-i}$ dla $n \in \mathbb{N}$. Załóżmy nie wprost, że $NWD(c_0, c_1, \ldots) > 1$. Wtedy istnieje liczba pierwsza p taka, $p | c_i$ dla wszystkich $i \in \mathbb{N}$. Niech m będzie najmniejszą liczbą naturalną taką, że p nie dzieli a_m, zaś n najmniejszą liczbą naturalną taką, że p nie dzieli b_n. Zauważmy, że

$$c_{m+n} = \sum_{i=0}^{m+n} a_i b_{m+n-i} = \sum_{i<m} a_i b_{m+n-i} + a_m b_n + \sum_{j<n} a_{m+n-j} b_j.$$

Z założenia $p | c_{m+n}$, $p | a_i$ dla $i < m$ oraz $p | b_j$ dla $j < n$. Zatem $p | a_m b_n$, co oznacza, że $p | a_m$ lub $p | b_n$. Sprzeczność. ■

Lemat 9.24 *Jeśli $f, g \in \mathbb{Q}[x]$ i $fg \in \mathbb{Z}[x]$, to istnieją wielomiany $f_1, g_1 \in \mathbb{Z}[x]$ takie, że $fg = f_1 g_1$. Jeśli $fg \neq 0$, to f_1 i g_1 można wybrać tak, aby $st(f_1) = st(f)$ i $st(g_1) = st(g)$.*

[3]Ferdinand Gotthold Eisenstein (1823-1852), matematyk niemiecki

Dowód. Przyjmijmy oznaczenia:

$$f = a_0 + a_1x + \ldots \in \mathbb{Q}[x],\ g = b_0 + b_1x + \ldots \in \mathbb{Q}[x].$$

Jeśli $fg = 0$, to można przyjąć, że $f_1 = g_1 = 0$. Załóżmy więc, że $fg \neq 0$. Niech m będzie liczbą naturalną dodatnią taką, że $mf \in \mathbb{Z}[x]$, zaś n liczbą naturalną dodatnią taką, że $ng \in \mathbb{Z}[x]$. Niech $\alpha = NWD(ma_0, ma_1, \ldots)$ i $\beta = NWD(nb_0, nb_1, \ldots)$. Wtedy

$$mf = \alpha f_0 \text{ i } ng = \beta g_0 \text{ dla pewnych } f_0, g_0 \in \mathbb{Z}[x].$$

Stąd $mnfg = \alpha\beta f_0 g_0$ i $mn|\alpha\beta f_0 g_0$. Oczywiście współczynniki każdego z wielomianów f_0, g_0 są względnie pierwsze. Na mocy lematu 9.23, również współczynniki wielomianu f_0g_0 są względnie pierwsze. Oznacza to, że $mn|\alpha\beta$, czyli $\alpha\beta = \gamma mn$ dla pewnego $\gamma \in \mathbb{Z}$. Tak więc mamy $mnfg = \gamma mnf_0g_0$. Stąd $fg = \gamma f_0g_0$. Wielomiany $f_1 = \gamma f_0$ i $g_1 = g_0$ spełniają tezę twierdzenia. ■

Twierdzenie 9.25 *(Kryterium Eisensteina - Schönemanna) Niech $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$, $n \in \mathbb{N}_+$. Jeżeli istnieje liczba pierwsza p taka, że*

(a) p nie dzieli a_n,

(b) p dzieli a_i dla $i = 0, \ldots, n-1$ oraz

(c) p^2 nie dzieli a_0,

to wielomian f jest nierozkładalny nad $\mathbb{Q}$.

Dowód. Załóżmy nie wprost, że wielomian $f = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ stopnia ≥ 1 spełnia założenia twierdzenia, ale jest rozkładalny nad $\mathbb{Q}$. Wtedy, zgodnie z lematem 9.24, istnieją wielomiany $g, h \in \mathbb{Z}[x]$ stopnia ≥ 1 takie, że $f = gh$. Niech $g = b_0 + b_1x + \ldots + b_kx^k$ i $h = c_0 + c_1x + \ldots + c_lx^l$. Oczywiście $a_0 = b_0c_0$. Z założenia liczba a_0 dzieli się przez p, ale nie przez p^2. Dlatego dokładnie jedna z liczb b_0, c_0 dzieli się przez p. Przyjmijmy, że $p|b_0$ i p nie dziel c_0. Indukcyjnie względem i pokażemy, że $p|b_i$ dla $i \leq k$.

Załóżmy, że $1 \leq i \leq k$ oraz $p|b_j$ dla $j < i$. $\mathrm{st}(g), \mathrm{st}(h) \geq 1$, więc $i < n$. Z założenia $p|a_i$, czyli $p|b_ic_0 + b_{i-1}c_1 + \ldots + b_0c_i$. Z założenia indukcyjnego liczby $b_0, \ldots, b_{i-1}$ są podzielne przez p, zatem $p|b_ic_0$. Przyjęliśmy, że c_0 nie dzieli się przez p, więc $p|b_i$, co było do udowodnienia.

Z powyższego rozumowania wynika, że $p|b_k$. $a_n = b_kc_l$, więc $p|a_n$. Sprzeczność z założeniem twierdzenia. ■

Przykład 4. Z kryterium Eisensteina - Schönemanna wynika, że wielomian $f = 4x^6 + 3x^5 - 9x^3 + 12x^2 + 3x + 21 \in \mathbb{Z}[x]$ jest nierozkładalny nad $\mathbb{Q}$, ponieważ wszystkie jego współczynniki oprócz najstarszego dzielą się przez 3, zaś wyraz wolny nie dzieli się przez 9. Z nierozkładalności wielomianu f nad $\mathbb{Q}$ wynika jego nierozkładalność nad $\mathbb{Z}$.

Przykład 5. Pokażemy, że wielomian $f = 1 + x + x^2 + x^3 + x^4$ jest nierozkładalny nad $\mathbb{Q}$. Do wielomianu tego nie da się zastosować kryterium Eisensteina - Schönemanna. Rozważmy więc pomocniczy wielomian:

$$f_1 = 1 + (1+x) + (1+x)^2 + (1+x)^3 + (1+x)^4 = 5 + 10x + 10x^2 + 5x^3 + x^4.$$

Wszystkie współczynniki wielomianu f_1 oprócz najstarszego dzielą się przez 5. Ponadto wyraz wolny nie dzieli się przez 25. Dlatego, na mocy kryterium Eisensteina - Schönemanna, wielomian f_1 jest nierozkładalny nad $\mathbb{Q}$.

Przypuśćmy teraz, że wielomian f jest rozkładalny nad $\mathbb{Q}$. Wtedy istnieją wielomiany $g = a_0 + a_1x + \ldots + a_mx^m \in \mathbb{Q}[x]$ i $h = b_0 + b_1x + \ldots + b_nx^n \in \mathbb{Q}[x]$ stopnia ≥ 1 takie, że $f = gh$. Wtedy jednak

$$f_1 = (a_1 + a_1(1+x) + \ldots + a_m(1+x)^m)(b_0 + b_1(1+x) + \ldots + b_n(1+x)^n).$$

Oba wielomiany występujące w powyższym rozkładzie mają stopień dodatni, więc f_1 jest rozkładalny. Sprzeczność. Tak więc wielomian f jest nierozkładalny nad $\mathbb{Q}$.

Lemat 9.26 *Jeśli K jest ciałem, zaś $f \in K[x]$ wielomianem stopnia ≥ 1, to f jest nierozkładalny lub jest iloczynem wielomianów nierozkładalnych z $K[x]$.*

Dowód. Niech K będzie ciałem. Indukcyjnie względem n pokażemy, że dla $n \in \mathbb{N}_+$ zachodzi $(*)_n$:

$(*)_n$ Jeśli $f \in K[x]$ jest wielomianem stopnia n, to f jest nierozkładalny nad K lub jest iloczynem wielomianów nierozkładalnych z $K[x]$.

Dowolny wielomian stopnia 1 jest nierozkładalny nad K, więc $(*)_1$ zachodzi. Ustalmy liczbę naturalną dodatnią i załóżmy, że udowodniśmy już $(*)_1, \ldots, (*)_n$. W celu wykazania $(*)_{n+1}$ rozważmy wielomian $f \in K[x]$ stopnia $n+1$. Jeśli f jest nierozkładalny, to oczywiście spełnie tezę $(*)_{n+1}$. W przeciwnym wypadku mamy $f = gh$, gdzie g i h są wielomianami stopnia ≥ 1 z $K[x]$. Ponieważ $\mathrm{st}(g) + \mathrm{st}(h) = \mathrm{st}(f) = n+1$, mamy $1 \leq \mathrm{st}(g) \leq n$ i $1 \leq \mathrm{st}(h) \leq n$. Na mocy założenia indukcyjnego, każdy z wielomianów g, h jest nierozkładalny lub jest iloczynem wielomianów nierozkładalnych. Wynika stąd, że f jest iloczynem wielomianów nierozkładalnych. ■

Lemat 9.27 *Niech K będzie ciałem, zaś $f \in K[x]$ wielomianem nierozkładalnym stopnia ≥ 1. Jeśli $g, h \in K[x]$ są wielomianami takimi, że $f|gh$, to $f|g$ lub $f|h$.*

Dowód. Ustalmy wielomian nierozkładalny $f \in K[x]$ stopnia ≥ 1. Udowodnimy, że

$$(*)\ (\forall g, h \in K[x])(f|gh \Longrightarrow f|g \vee f|h).$$

Jeśli $gh = 0$, to implikacja $f|gh \Longrightarrow f|g \vee f|h$ jest oczywiście prawdziwa (mamy bowiem $g = 0 \vee h = 0$). Tak więc w celu udowodnienia $(*)$ wystarczy wykazać, że dla dowolnego $n \in \mathbb{N}$ zachodzi

$$(*)_n \text{ Jeśli } g, h \in K[x], gh \neq 0, \mathrm{st}(gh) \leq n \text{ i } f|gh, \text{ to } f|g \vee f|h.$$

Załóżmy, że $g, h \in K[x]$ i $\mathrm{st}(gh) = 0$. Wtedy f nie dzieli gh. Tak więc implikacja $f|gh \Longrightarrow f|g \vee f|h$ jest prawdziwa i $(*)_0$ zachodzi.

Ustalmy liczbę naturalną n i przypuśćmy, że udowodniliśmy już $(*)_0, \ldots, (*)_n$. Niech $g, h \in K[x]$, $\mathrm{st}(gh) = n+1$ i $f|gh$.

Przypadek 1. $\mathrm{st}(f) \leq \mathrm{st}(g)$. Wtedy istnieją $q, r \in K[x]$ takie, że

$$(\triangle)\ f = qg + r,$$

przy czym $r = 0$ lub $\mathrm{st}(r) < \mathrm{st}(f)$. Jeśli $r = 0$, to $g = qf$ i $f|g$. Jeśli natomiast $r \neq 0$, to $\mathrm{st}(r) < \mathrm{st}(g) \leq \mathrm{st}(f)$. Mnożąc równość $(\triangle)$ przez h dostajemy $gh = gfh + rh$. $f|gh$ i $f|qfh$, więc również $f|rh$. Oczywiście

$$\mathrm{st}(rh) = \mathrm{st}(r) + \mathrm{st}(h) < \mathrm{st}(g) + \mathrm{st}(h) = \mathrm{st}(gh) = n+1.$$

Na mocy założenia indukcyjnego, $f|r$ lub $f|h$. Ponieważ $r \neq 0$ i $\mathrm{st}(f) > \mathrm{st}(r)$, f nie może dzielić r. Tak więc $f|h$.

Przypadek 2. $\mathrm{st}(f) > \mathrm{st}(g)$. Wtedy istnieją $q, r \in K[x]$ takie, że

$$(\triangle\triangle)\ f = qg + r,$$

przy czym $r = 0$ lub $\mathrm{st}(r) < \mathrm{st}(g)$.

Przypadek 2a. $r = 0$. Wtedy $f = qg$ i, ponieważ wielomian f jest nierozkładalny, mamy $g = af$ lub $g = a$ dla pewnego $a \in K \setminus \{0\}$. Jeśli $g = af$, $a \in K \setminus \{0\}$, to oczywiście $f|g$. Jeśli natomiast $g = a$, $a \in K \setminus \{0\}$, to wobec $f|gh$ mamy $f|ah$, skąd wynika, że $f|h$.

Przypadek 2b. $r \neq 0$. Wtedy $\mathrm{st}(r) < \mathrm{st}(g)$. Mnożąc obustronnie równość $\triangle\triangle$ przez h otrzymujemy $fh = qgh + rh$, skąd wobec $f|gh$, otrzymujemy $f|rh$. Zauważmy, że

$$\mathrm{st}(rh) = \mathrm{st}(r) + \mathrm{st}(h) < \mathrm{st}(g) + \mathrm{st}(h) = \mathrm{st}(gh) = n + 1.$$

Na mocy założenia indukcyjnego, $f|r$ lub $f|h$. Ponieważ $\mathrm{st}(r) < \mathrm{st}(g) < \mathrm{st}(f)$, wielomian r nie może dzielić się przez r. Tak więc $f|h$, co kończy dowód. ■

Lemat 9.28 *Niech K będzie ciałem, zaś $f \in K[x]$ wielomianem nierozkładalnym stopnia ≥ 1. Jeśli $g_1, \ldots, g_n \in K[x]$ są wielomianami takimi, że $f|g_1 \cdot \ldots \cdot g_n$, to $f|g_i$ dla pewnego $i \in \{1, \ldots, n\}$.*

Twierdzenie 9.29 *Niech K będzie ciałem, zaś $f \in K[x]$ wielomianem stopnia ≥ 1. Jeżeli $f = f_1 \cdot \ldots \cdot f_k$ i $f = g_1 \cdot \ldots \cdot g_l$ są dwoma rozkładami wielomianu f na czynniki nierozkładalne stopnia przynajmniej 1, to $k = l$ i istnieje permutacja $\sigma \in S_k$ taka, że: $f_1 = a_1 g_{\sigma(1)}, \ldots, f_k = a_k g_{\sigma(k)}$ dla pewnych $a_1, \ldots, a_k \in K \setminus \{0\}$.*

Dowód. (Indukcja względem stopnia wielomianu f) Twierdzenie jest oczywiście prawdziwe dla wielomianów nierozkładalnych, w szczególności zachodzi ono dla wielomianów stopnia 1.

Załóżmy teraz prawdziwość twierdzenia dla wielomianów stopnia co najwyżej n, gdzie $n \in \mathbb{N}_+$. Ustalmy wielomian f stopnia $n+1$. Jeśli f jest nierozkładalny, to oczywiście spełnia tezę twierdzenia. W przeciwnym wypadku rozważmy dwa rozkłady wielomianu f na czynniki nierozkładalne stopnia ≥ 1:

$$(*)\ f = f_1 \cdot \ldots \cdot f_k = g_1 \cdot \ldots \cdot g_l.$$

W każdym z napisanych rozkładów występują przynajmniej 2 czynniki. Z równości $(*)$ wynika, że $f_1|g_1 \cdot \ldots \cdot g_l$. Na mocy wniosku 9.28, $f_1|g_i$ dla pewnego $i \in \{1, \ldots, l\}$. g_i jest wielomianem nierozkładalnym, więc $g_i = af_1$ dla pewnego $a \in K \setminus \{0\}$. Stąd

$$f_2 \cdot \ldots \cdot f_k = ag_1 \cdot \ldots g_{i-1} g_{i+1} \cdot g_l.$$

Stopień wielomianu $f_2 \cdot \ldots \cdot f_k$ jest mniejszy lub równy n, więc na mocy założenia indukcyjnego $k = l$ i istnieje bijekcja $\tau : \{2, \ldots, k\} \longrightarrow \{1, \ldots, l\} \setminus \{i\}$ taka, że $f_j = a_j g_{\tau(j)}$ dla pewnych $a_2, \ldots, a_k \in K \setminus \{0\}$. Stąd łatwo wynika teza twierdzenia. ■

Niech $\mathcal{U}$ będzie równaniem postaci $w(x_1, \ldots, x_n) = 0$, gdzie w oznacza pewien wielomian n zmiennych o współczynnikach całkowitych i niech $m \in \mathbb{N}_+$. Zastępując każdy współczynnik a równania $\mathcal{U}$ przez $a \bmod m$ otrzymamy równanie o współczynnikach z pierścienia $\mathbb{Z}_m$. Równanie to będziemy oznaczać przez $\mathcal{U}_m$ i nazywać redukcją równania $\mathcal{U}$ według modułu m.

Poniższe twierdzenie łatwo wynika z faktu iż przyporządkowanie liczbie całkowitej jej reszty z dzielenia przez n jest homomorfizmem z pierścienia $(\mathbb{Z}, +, \cdot)$ w pierścień $(\mathbb{Z}_m, +_m, \cdot_m)$.

Twierdzenie 9.30 *Jeśli równanie $\mathcal{U}$ o współczynnikach całkowitych ma rozwiązanie w zbiorze liczb całkowitych, to dla każdego $n \in \mathbb{N}_+$, redukcja równania $\mathcal{U}$ modulo n ma rozwiązanie w $\mathbb{Z}_n$.*

Twierdzenie odwrotne do twierdzenia 9.30 nie jest prawdziwe. Rozważmy na przykład równanie

$$(*)\ 6x^2 + 5x + 1 = 0.$$

Równanie to oczywiście nie posiada rozwiązań w pierścieniu $\mathbb{Z}$. Używając rozkładu $6x^2 + 5x + 1 = (3x + 1)(2x + 1)$ oraz chińskiego twierdzenia o resztach (twierdzenie 0.12), można wykazać, że dla dowolnego $n \in \mathbb{N}_+$ redukcja równania $(*)$ według modułu n ma rozwiązanie w pierścieniu $\mathbb{Z}_n$.

Z twierdzenia 9.30 wynika ważny wniosek, który pozwala dla wielu równań o współczynnikach całkowitych udowodnić, że nie mają one rozwiązania w $\mathbb{Z}$.

Wniosek 9.31 *Jeżeli istnieje liczba naturalna $m > 1$ taka, że redukcja równania $\mathcal{U}$ według modułu m nie posiada rozwiązania w pierścieniu $\mathbb{Z}_m$, to równanie $\mathcal{U}$ nie ma rozwiązania w $\mathbb{Z}$.*

Przykład 6. Rozważmy równanie:

$$10x^2 + 7y^2 + 5z + 9 = 0 \ (\mathcal{U})$$

Będziemy rozpatrywać redukcje równania $\mathcal{U}$ według modułów $2, 3, 4, \ldots$ i badać ich rozwiązalność w odpowiednich pierścieniach.

Redukcją powyższego równania według modułu 2 jest równanie

$$0x^2 + y^2 + z^2 + 1 = 0 \ (\mathcal{U}_2)$$

Nietrudno zauważyć, że trójka $\langle 0, 0, 1\rangle$ jest jego rozwiązaniem w $\mathbb{Z}_2$. Nie można więc skorzystać z wniosku 9.31. Podobnie, redukcja równania $\mathcal{U}$ według modułu 3:

$$x^2 + y^2 + 2z^2 = 0 \ (\mathcal{U}_3)$$

ma w $\mathbb{Z}_3$ rozwiązanie $\langle 0, 1, 1\rangle$, zaś redukcja $\mathcal{U}$ według modułu 4:

$$2x^2 + 3y^2 + z^2 + 1 = 0 \ (\mathcal{U}_4)$$

ma w $\mathbb{Z}_4$ rozwiązanie $\langle 0, 1, 0\rangle$.

Rozważmy więc redukcję równania $\mathcal{U}$ według modułu 5:

$$0x^2 + 2y^2 + 0z^2 + 4 = 0 \ (\mathcal{U}_5)$$

Obliczając wartości wyrażenia $2y^2 + 4$ w pierścieniu $\mathbb{Z}_5$ dla $y = 0, 1, 2, 3, 4$ otrzymujemy kolejno: 4,1,2,2,1. Tak więc równanie $\mathcal{U}_5$ nie posiada rozwiązania w $\mathbb{Z}_5$, a to na mocy wniosku 9.31 oznacza, że równanie $\mathcal{U}$ nie ma rozwiązania w $\mathbb{Z}$.

Czytelnikowi może w tym momencie nasunąć się pytanie, czy istnieje jakaś metoda pozwalająca na wskazanie dla danego równania diofantycznego takiej liczby $m \in \mathbb{N}_+$, że redukcja $\mathcal{U}_m$ nie posiada rozwiązania w $\mathbb{Z}_m$ bądź wykazanie, że liczba taka nie istnieje. Odpowiedź na to pytanie jest negatywna. Ogólniej, nie istnieje algorytm pozwalający dla dowolnego równania diofantycznego rozstrzygnąć czy ma ono rozwiązanie w zbiorze liczb całkowitych.

Twierdzenie 9.32 *(Twierdzenie Wilsona[4]) Jeśli p jest liczbą pierwszą, to liczba $(p-1)! + 1$ jest podzielna przez p.*

Dowód. Jest oczywiste, że $2|(2-1)! + 1$ i $3|(3-1)! + 1$, zatem twierdzenie jest prawdziwe dla $p \in \{2, 3\}$. Załóżmy więc, że p jest liczbą pierwszą większą od 4.

Ponieważ p jest liczbą pierwszą, $(\mathbb{Z}_p, +_p, \cdot_p)$ jest ciałem. Liczby 1 i $p-1$ są pierwiastkami wielomianu $f = x^2 - 1$ w tym ciele. Zgodnie z twierdzeniem 9.12, f, jako wielomian stopnia 2, nie posiada innych pierwiastków w $\mathbb{Z}_p$. Oznacza to, że dla dowolnego $a \in \mathbb{Z}_p \setminus \{0, 1, p-1\}$, $a \cdot_p a \neq 1$. Innymi słowy, jeśli $a \in \mathbb{Z}_p \setminus \{0, 1, p-1\}$, to element odwrotny do a względem działania $\cdot_p$ jest różny od a. Co więcej, $a^{-1} \notin \{0, 1, p-1\}$. Tak więc zbiór $\mathbb{Z}_p \setminus \{0, 1, p-1\}$ (złożony z $p-3$ elementów) można podzielić na $\frac{p-3}{2}$ podzbiorów dwuelementowych postaci $\{a, a^{-1}\}$. Oczywiście iloczyn modulo p elementów należących do każdego takiego podzbioru jest równy 1. Oznacza to, że $2 \cdot_p \ldots \cdot_p (p-2) = 1$. Stąd:

$$1 \cdot_p 2 \cdot_p \ldots \cdot_p (p-2) \cdot_p (p-1) +_p 1 = (p-1) +_p 1 = 0.$$

Stąd wynika, że p dzieli $(p-1)! + 1$. ■

[4]Pierwszy dowód tego twierdzenia podał J. L. Lagrange w roku 1771

Rozdział 10

Pierścień ilorazowy

Niech I będzie ideałem pierścienia $(R, +, \cdot)$. Wówczas I jest podgrupą grupy $(R, +)$. Ponieważ grupa ta jest z definicji abelowa, I jest dzielnikiem normalnym grupy $(R, +)$. W zbiorze warstw R/I można wtedy określić w naturalny sposób działanie $\oplus$ (zwane dalej dodawaniem warstw):

$$(a + I) \oplus (b + I) = (a + b) + I.$$

Jak wiadomo z rozdziału 5, zbiór R/I z tak określonym działaniem stanowi grupę abelową.

Wprowadzimy teraz w zbiorze warstw R/I jeszcze jedno działanie, zwane mnożeniem warstw, i pokażemy, że zbiór ten jest pierścieniem względem wymienionych działań.

Twierdzenie 10.1 *Jeśli I jest ideałem pierścienia R, to wzór*

$$(a + I) \odot (b + I) = ab + I$$

określa w zbiorze warstw względem I jako dzielnika normalnego grupy addytywnej pierścienia R działanie, które nazwiemy mnożeniem warstw. Zbiór warstw R/I tworzy pierścień względem ich dodawawania i mnożenia.

Dowód. R/I z działaniem dodawania warstw (oznaczenie: $\oplus$) jest grupą abelową. Sprawdzimy najpierw, że powyższy wzór określa działanie w zbiorze warstw, to znaczy, że każdej parze uporządkowanej warstw względem ideału I przyporządkowana jest jednoznacznie warstwa względem I. Innymi słowy pokażemy, że wynik działania $\odot$ nie zależy od wyboru reprezentantów z każdej z warstw.

Załóżmy, że $a + I = a' + I$ oraz $b + I = b' + I$. Wtedy $a - a' \in I$ oraz $b - b' \in I$. Zauważmy, że

$$ab + I = (a'b' + a(b - b') + (a - a')b') + I = (a'b' + I) \oplus (a(b - b') + (a - a')b' + I).$$

Z definicji ideału: $a(b - b') + (a - a')b' \in I$, czyli $a(b - b') + (a - a')b' + I = I$. Tak więc

$$ab + I = (a'b' + I) \oplus I = a'b' + I.$$

Pokażemy jeszcze, że mnożenie warstw jest łączne i rozdzielne względem ich dodawania:

$$\begin{aligned}
[(a + I) \odot (b + I)] \odot (c + I) &= (ab + I) \odot (c + I) = (ab)c + I = a(bc) + I = \\
&= (a + I) \odot (bc + I) = (a + I) \odot [(b + I) \odot (c + I)]; \\
(a + I) \odot [(b + I) \oplus (c + I)] &= (a + I) \odot ((b + c) + I) = a(b + c) + I = \\
&= (ab + ac) + I = (ab + I) \oplus (ac + I) = \\
&= [(a + I) \odot (b + I)] \oplus [(a + I) \odot (c + I)].
\end{aligned}$$

Podobnie dowodzi się, że $[(b + I) \oplus (c + I)] \odot (a + I) = [(b + I) \odot (a + I)] \oplus [(c + I) \odot (a + I)]$. ■

Definicja 10.2 *Niech I będzie ideałem pierścienia R. Pierścień warstw względem ideału I, w którym działaniami są dodawanie warstw i mnożenie warstw, nazywamy pierścieniem ilorazowym pierścienia R względem ideału I i oznaczamy symolem R/I. Warstwy grupy addytywnej pierścienia R nazywamy klasami reszt względem ideału I lub klasami reszt modulo I.*

Przykład 1. Niech I będzie ideałem pierścienia $\mathbb{R}[x]$ generowanym przez wielomian $1+x^2$, to znaczy $I=(1+x^2)=\{(1+x^2)\cdot f : f\in\mathbb{R}[x]\}$. Pokażemy, że pierścień ilorazowy $\mathbb{R}[x]/I$ jest izomorficzny z ciałem liczb zespolonych.

Z definicji pierścienia ilorazowego wynika, że $\mathbb{R}[x]/I=\{f+I : f\in\mathbb{R}[x]\}$. Niech $f\in\mathbb{R}[x]$. Na mocy twierdzenia 9.19 istnieją wielomiany $q\in\mathbb{R}[x]$ i $r=a+bx\in\mathbb{R}[x]$ takie, że $f=(1+x^2)q+ax+b$. Wielomiany q i r są określone jednoznacznie. To zaś oznacza, że warstwa $f+I$ ma dokładnie jedno przedstawienie w postaci $a+bx+I$.

Niech $F:\mathbb{R}[x]/I\longrightarrow\mathbb{C}$ będzie odwzorowaniem określonym wzorem:

$$F(a+bx+I)=a+bi.$$

Odwzorowanie F jest dobrze określone, gdyż każda warstwa ideału I jednoznacznie przedstawia się w postaci $a+bx+I$. Zauważmy, że dla dowolnych $a,b,c,d\in\mathbb{R}$,

$$\begin{aligned}
&F((a+bx+I)\oplus(c+dx+I))=F(a+c+(b+d)x+I)=\\
&=a+c+(b+d)i=(a+bi)+(c+di)=F(a+bx+I)+F(c+dx+I),\\
&F((a+bx+I)\odot(c+dx+I))=F((a+bx)(c+dx)+I)=\\
&=F((ac-bd)+(ad+bc)x+bd(1+x^2)+I)=F((ac-bd)+(ad+bc)x+I)=\\
&=(ac-bd)+(ad+bc)i=(a+bi)\cdot(c+di)=F(a+bx+I)\cdot F(c+dx+I).
\end{aligned}$$

Oznacza to, że F jest homomorfizmem pierścieni.

Oczywiście F jest surjekcją. W celu wykazania różnowartościowości F, załóżmy, że $F(a+bx+I)=F(c+dx+I)$. Wtedy $a+bi=c+di$, co oznacza, że $a=c$ i $b=d$, a więc $a+bx+I=c+dx+I$. W ten sposób udowodniliśmy, że F jest izomorfizmem pierścieni.

Twierdzenie 10.3 *Niech I będzie ideałem pierścienia R.*

(a) Jeśli R jest pierścieniem przemiennym, to R/I jest pierścieniem przemiennym.

(b) Jeśli pierścień R posiada jedność 1_R, to warstwa 1_R+I jest jednością w pierścieniu R/I.

Dowód. (a) Niech R będzie pierścieniem przemiennym, zaś I jego ideałem. Wtedy dla dowolnych $a,b\in R$ mamy:

$$(a+I)\odot(b+I)=ab+I=ba+I=(b+I)\odot(a+I),$$

gdzie $\odot$ jest mnożeniem w pierścieniu ilorazowym R/I.

(b) Jeśli I jest ideałem w pierścieniu R z jednością 1_R, to

$$(a+I)\odot(1_R+I)=a\cdot 1_R+I=a+I$$

dla dowolnego $a\in R$. Podobnie $(1+I)\odot(a+I)=a+I$. Tak więc warstwa 1_R+I jest jednością pierścienia ilorazowego R/I. ■

Lemat 10.4 *Niech R będzie pierścieniem z jednością, zaś I jego ideałem. Wówczas następujące warunki są równoważne:*

(a) $I=R$,

(b) R/I jest pierścieniem jednoelementowym,

(c) zero i jedność pierścienia R/I są sobie równe.

Dowód. (a)$\Longrightarrow$(b). Jeżeli $I = R$, to $R/I = \{I\}$, a więc jest zbiorem jednoelementowym.

Implikacja (b)$\Longrightarrow$(c) jest trywialna.

(c)$\Longrightarrow$(a). Warunek (c) oznacza, że $1_R + I = I$, czyli $1_R \in I$. Ale wtedy dla każdego $a \in R$, $a = 1_R \cdot a \in I$. Tak więc $I = R$. ■

Twierdzenie 10.5 *Niech R będzie pierścieniem przemiennym z jednością, zaś I jego ideałem. Wówczas następujące warunki są równoważne.*

(a) Ideał I jest pierwszy.

(b) Pierścień ilorazowy R/I jest całkowity.

Dowód. Załóżmy, że R jest pierścieniem przemiennym z jednością, zaś I jego ideałem.

(a)$\Longrightarrow$(b). Niech I będzie ideałem pierwszym. Z twierdzenia 10.3 wynika, że R/I jest pierścieniem przemiennym z jednością. Wtedy $I \neq R$ i na mocy lematu 10.4, zero i jedność w pierścieniu ilorazowym R/I są różne.

Pokażemy teraz, że pierścień R/I nie ma dzielników zera. Załóżmy nie wprost, że istnieją elementy $a, b \in R$ takie, że $a + I \neq I$, $b + I \neq I$ oraz $(a + I) \odot (b + I) = ab + I = I$. Oznacza to, że $a, b \notin I$, ale $ab \in I$, a więc ideał I nie jest pierwszy. Sprzeczność z założeniem.

(b)$\Longrightarrow$(a). Załóżmy, że pierścień ilorazowy R/I jest całkowity. Wtedy zero i jedność w R/I są różne, a więc $I \neq R$.

Niech a i b będą elementami pierścienia R takimi, że $ab \in I$. Wtedy $(a + I) \odot (b + I) = ab + I = I$. Pierścień R/I nie ma dzielników zera, więc $a + I = I$ lub $b + I = I$. To zaś oznacza, że $a \in I$ lub $b \in I$. W ten sposób wykazaliśmy, że ideał I jest pierwszy. ■

Twierdzenie 10.6 *Niech R będzie pierścieniem przemiennym z jednością, zaś I jego ideałem. Wówczas następujące warunki są równoważne.*

(a) Ideał I jest maksymalny.

(b) Pierścień ilorazowy R/I jest ciałem.

Dowód. (a)$\Longrightarrow$(b). Załóżmy, że I jest ideałem maksymalnym pierścienia R. Z twierdzenia 10.3 wynika, że R/I jest pierścieniem przemiennym z jednością. $I \neq R$, więc na mocy lematu 10.4, zero i jedność pierścienia R/I są różne. Pokażemy jeszcze, że każdy element pierścienia R/I, różny od I jest odwracalny.

Niech $a \in R$ i $a + I \neq I$. Wtedy $a \notin I$, a więc I jest właściwym podzbiorem ideału $aR + I$. Ideał I jest maksymalny, więc $aR + I = R$. Stąd $ab + c = 1_R$ dla pewnych $b \in R$ i $c \in I$. Zauważmy, że

$$ab + I = \{ab + x : x \in I\} = \{1_R - c + x : x \in I\} = \{1_R + (x - c) : x \in I\} = 1_R + I.$$

Tak więc $a + I$ jest elementem odwracalnym w pierścieniu R/I.

(b)$\Longrightarrow$(a) Załóżmy, że R/I jest ciałem. Wtedy $1_R + I \neq I$, a więc $I \neq R$. Niech J będzie ideałem pierścienia R, którego właściwym podzbiorem jest I. Pokażemy, że $J = R$. Wybierzmy w tym celu element $a \in J \setminus I$. Wtedy $a + I \neq I$. Ponieważ R/I jest ciałem, $a + I$ jest elementem odwracalnym w R/I. Oznacza to, że $ab + I = 1_R + I$ dla pewnego $b \in R$. Stąd $1_R \in aR + I \subseteq J$ i mamy $J = R$. W ten sposób wykazaliśmy, że I jest ideałem maksymalnym pierścienia R. ■

Twierdzenie 10.7 *Jeśli I jest ideałem pierścienia R, to odwzorowanie $\nu : R \longrightarrow R/I$, przyporządkowujące każdemu elementowi pierścienia R klasę reszt tego elementu modulo I jest homomorfizmem pierścienia R na pierścień ilorazowy R/I. Jądrem homomorfizmu ν jest I.*

Dowód. Niech I będzie ideałem pierścienia R, zaś $\nu : R \longrightarrow R/I$ odwzorowaniem zdefiniowanym wzorem $\nu(a) = a + I$. Z definicji dodawania i mnożenia w pierścieniu ilorazowym R/I wynika, że

$$\begin{aligned} \nu(a + b) &= (a + b) + I = (a + I) \oplus (b + I) = \nu(a) \oplus \nu(b), \\ \nu(a \cdot b) &= a \cdot b + I = (a + I) \odot (b + I) = \nu(a) \odot \nu(b). \end{aligned}$$

Tak więc ν jest homomorfizmem pierścieni. Oczywiście ν jest surjekcją. Ponadto

$$Ker(\nu) = \{a \in R : \nu(a) = I\} = \{a \in R : a + I = I\} = I,$$

co kończy dowód. ■

Homomorfizm $\nu : R \longrightarrow R/I$, o którym mowa w twierdzeniu 10.7 nazywamy homomorfizmem kanonicznym. Z powyższego twierdzenia i z twierdzenia 8.31 wynika następujący wniosek.

Wniosek 10.8 *Zbiór $I \subseteq R$ jest ideałem pierścienia R wtedy i tylko wtedy, gdy I jest jądrem pewnego homomorfizmu pierścieni.*

Twierdzenie 10.9 *(Zasadnicze twierdzenie o homomorfizmach pierścieni) Niech $\varphi : (R, +, \cdot) \longrightarrow (S, +, \cdot)$ będzie homomorfizmem pierścieni. Wtedy odwzorowanie $\psi : R/Ker(\varphi) \longrightarrow S$ określone wzorem:*

$$\psi(a + Ker(\varphi)) = \varphi(a) \text{ dla } a \in R$$

jest monomorfizmem pierścieni.

Dowód. Z założeń twierdzenia wynika, że φ jest homomorfizmem z grupy addytywnej pierścienia R w grupę addytywną pierścienia S. Ponadto $Ker(\varphi)$ jest dzielnikiem normalnym grupy $(R, +)$. Na mocy twierdzenia 5.3, odwzorowanie ψ zdefiniowane w sformułowaniu twierdzenia jest dobrze określone i jest ono monomorfizmem z grupy $(R/Ker(\varphi), \oplus)$ w grupę $(S, +)$ ($\oplus$ oznacza dodawanie w pierścieniu ilorazowym $R/Ker(\varphi)$).

Zauważmy, że jeśli $a, b \in G$, to

$$\begin{aligned}\psi((a + Ker(\varphi)) \odot (b + Ker(\varphi))) &= \psi(ab + Ker(\varphi)) = \varphi(ab) = \varphi(a)\varphi(b) = \\ &= \psi(a + Ker(\varphi))\psi(b + Ker(\varphi)).\end{aligned}$$

Tak więc odwzorowanie ψ jest monomorfizmem pierścieni i pierścień ilorazowy $R/Ker(\varphi)$ jest izomorficzny z pierścieniem $(Im(\varphi), +, \cdot)$. ■

Wniosek 10.10 *Jeśli $\varphi : R \longrightarrow S$ jest epimorfizmem pierścieni, to pierścień ilorazowy $R/Ker(\varphi)$ jest izomorficzny z pierścieniem S.*

Przykład 2. Tak jak w przykładzie 1 ze strony 90, niech I oznacza ideał pierścienia $\mathbb{R}[x]$ generowany przez wielomian $1 + x^2$. Używając zasadniczego twierdzenia o homomorfizmach pierścieni pokażemy, że pierścień ilorazowy $\mathbb{R}[x]/I$ jest izomorficzny z ciałem liczb zespolonych. Niech $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ będzie funkcją określoną wzorem $\varphi(f) = f(i)$ (i oznacza tutaj jedność urojoną). φ jest homomorfizmem pierścieni, gdyż dla dowolnych $f, g \in \mathbb{R}[x]$ mamy:

$$\varphi(f + g) = (f + g)(i) = f(i) + g(i) = \varphi(f) + \varphi(g) \text{ oraz } \varphi(fg) = (fg)(i) = f(i)g(i) = varphi(f)\varphi(g).$$

Ponadto dla dowolnych $a, b \in \mathbb{R}$, mamy $\varphi(a + bx) = a + bi$, więc φ jest surjekcją.

Pokażemy teraz, że $I = Ker(\varphi)$. Jeśli $f \in I$, to $f = (1 + x^2)g$ dla pewnego $g \in \mathbb{R}[x]$. Stąd $\varphi(f) = f(i) = 0$, czyli $f \in Ker(\varphi)$. Tak więc $I \subseteq Kerf$. W celu wykazania inkluzji przeciwnej ustalmy wielomian $f \in Ker(\varphi)$. Wtedy $f(i) = \varphi(f) = 0$, co wobec twierdzenia Bézouta (twierdzenie 9.6) daje $f = (x - i)g$ dla pewnego $g \in \mathbb{C}[x]$. Współczynniki wielomianu f są rzeczywiste, więc musi być $f(-i) = 0$. To zaś oznacza, że $(-i - i) \cdot g(i) = 0$, czyli $g(-i) = 0$. Stosując ponownie twierdzenie Bézouta dostajemy $g = (x + i)h$ dla pewnego $h \in \mathbb{C}[x]$. Tak więc

$$f = (x - i)(x + i)h = (x^2 + 1)h.$$

Ponieważ $\mathbb{R}$ jest podciałem ciała liczb zespolonych, $h \in \mathbb{C}[x]$ zaś wielomiany x^2+1 i f mają współczynniki rzeczywiste, na mocy lematu 9.21, również h ma współczynniki rzeczywiste. Tak więc $f \in I$ i mamy $Ker(\varphi) \subseteq I$.

Pokazaliśmy w ten sposób, że odwzorowanie $\varphi : \mathbb{R}[x] \longrightarrow \mathbb{C}$ jest epimorfizmem pierścieni, którego jądrem jest I. Zatem, na mocy wniosku 10.10, $\mathbb{R}[x]/I \cong \mathbb{C}$.

Udowodnimy teraz twierdzenie będące uogólnieniem chińskiego twierdzenia o resztach (twierdzenie 0.12). Wcześniej jednak będzie potrzebny następujący lemat.

Lemat 10.11 *Jeśli R jest pierścieniem z jednością, zaś $I, I_1, \ldots, I_n$ jego ideałami takimi, że $I + I_k = R$ dla $k = 1, \ldots, n$, to $I + I_1 \cap \ldots \cap I_k = R$.*

Dowód. Ponieważ $I_1 \cdot \ldots \cdot I_n \subseteq I_1 \cap \ldots \cap I_n$, wystarczy udowodnić, że $I + I_1 \cdot \ldots \cdot I_n = R$. Niech $x_1, \ldots, x_n \in I$, $y_1 \in I_1, \ldots, y_n \in I_n$ będą elementami takimi, że $x_k + y_k = 1$ dla $k = 1, \ldots, n$. Wtedy

$$1_R = (x_1 + y_1) \cdot \ldots \cdot (x_n + y_n) = r + y_1 \cdot \ldots \cdot y_n.$$

gdzie r jest sumą $2^n - 1$ iloczynów, przy czym w każdym z nich jako czynnik występuje element ideału I. Mamy więc $r \in I$ oraz $y_1 \cdot \ldots \cdot y_n \in I_1 \cdot \ldots \cdot I_n$. Tak więc $1_R = r + y_1 \cdot \ldots \cdot y_n \in I + I_1 \cdot \ldots \cdot I_n$, skąd wynika, że $I + I_1 \cdot \ldots \cdot I_n = R$. ■

Twierdzenie 10.12 *Niech R będzie pierścieniem z jednością, zaś $I_1, \ldots, I_n$ ($n \geq 2$) jego ideałami takimi, że $I_i + I_j = R$ dla $1 \leq i < j \leq n$. Wtedy odwzorowanie $f : R \longrightarrow R/I_1 \oplus \ldots \oplus R/I_n$ określone wzorem $f(x) = \langle x + I_1, \ldots, x + I_n \rangle$ jest epimorfizmem pierścieni. Innymi słowy, dla dowolnych $x_1, \ldots, x_n \in R$, istnieje element $x \in R$ taki, że $x - x_i \in I_i$ dla $i = 1, \ldots, n$.*

Dowód. Udowodnimy twierdzenie przez indukcję względem n. Niech I_1, I_2 będą ideałami pierścienia R (z jednością) takimi, że $I_1 + I_2 = R$ i niech $x_1, x_2 \in R$. Wówczas istnieją elementy $a_1 \in I_1$ oraz $a_2 \in I_2$ takie, że $a_1 + a_2 = 1$. Przyjmijmy $x = x_1a_2 + x_2a_1$. Wtedy

$$\begin{aligned} x - x_1 &= x_1a_2 + x_2a_1 - x_1(a_1 + a_2) = (x_2 - x_1)a_1 \in I_1, \\ x - x_2 &= x_1a_2 + x_2a_1 - x_2(a_1 + a_2) = (x_1 - x_2)a_2 \in I_2. \end{aligned}$$

W ten sposób wykazaliśmy prawdziwość twierdzenia dla dwóch ideałów.

Niech teraz $x_1, \ldots, x_{n+1} \in R$ i niech $I_1, \ldots, I_{n+1}$ będą ideałami pierścienia R takimi, że $I_i + I_j = R$ dla $1 \leq i < j \leq n+1$. Przypuśćmy, że znaleźliśmy już element $y \in R$ taki, że $y - x_i \in I_i$ dla $i = 1, \ldots, n$. Na mocy założenia $I_k + I_{n+1} = R$ dla $k = 1, \ldots, n$. Z lematu 10.11 wynika, że $I_1 \cap \ldots \cap I_n + I_{n+1} = R$. Stosując twierdzenie hdla przypadku dwóch ideałów $I_1 \cap \ldots \cap I_n$, I_{n+1} i elementów $y, x_{n+1} \in R$ znajdujemy element $x \in R$ taki, że $x - y \in I_1 \cap \ldots \cap I_n$ i $x - x_{n+1} \in I_{n+1}$. Ponieważ dla $i = 1, \ldots, n$ mamy $x - y, y - x_i \in I_i$, otrzymujemy

$$x - x_i = (x - y) + (y - x_i) \in I_i \text{ dla } i = 1, \ldots, n.$$

Tak więc element x spełnia żądane warunki. ■

Przyjmując w założeniach powyższego twierdzenia, że $R = \mathbb{Z}$ oraz $I_1 = k_1\mathbb{Z}, \ldots, I_n = k_n\mathbb{Z}$, gdzie liczby $k_1, \ldots, k_n \in \mathbb{N}_+$ są parami względnie pierwsze, otrzymujemy chińskie twierdzenie o resztach, które zostało udowodnione elementarnie w rozdziale 0.

Rozdział 11

Teoria podzielności w pierścieniach całkowitych

W niniejszym rozdziele zajmiemy się relacją podzielności w pierścieniach całkowitych, będącą uogólnieniem relacji podzielności w pierścieniu liczb całkowitych. Wszędzie zakładamy, że rozpatrywany pierścień R jest **całkowity**.

Definicja 11.1 *Niech $a, b \in R$. Mówimy, że element a dzieli element b (oznaczenie: $a|b$), jeśli istnieje element $c \in R$ taki, że $b = ac$.*

Gdy $a|b$, to mówimy, że *a jest dzielnikiem elementu b*, zaś *b jest wielokrotnością elementu a*. Mówimy też, że element b jest podzielny przez a (lub dzieli się przez a).

Na przykład w pierścieniu $\mathbb{Z}$, $-5|20$, ale 6 nie dzieli 25. W pierścieniu $\mathbb{Q}[x]$, wielomian $x-2$ dzieli wielomian x^3-8. W pierścieniu Gaussa $\mathbb{Z}[i]$, $2+i|5$, gdyż $5 = (2+i)(2-i)$. Dowolny element ciała jest podzielny przez dowolny niezerowy element tego ciała.

Poniższe twierdzenie mówi o najprostszych własnościach relacji podzielności w pierścieniu całkowitym. Łatwe dowody pomijamy, zostawiając je jako ćwiczenie dla Czytelnika.

Twierdzenie 11.2 *Niech $a, b, c, d \in R$. Wtedy*
(a) $1|a$,
(b) $a|a$,
(c) $a|b \Longrightarrow a|bc$,
(d) $(a|b \wedge a|c) \Longrightarrow (a|b+c \wedge a|b-c)$,
(e) $a|b \Longrightarrow ac|bc$,
(f) $(a|b \wedge c|d) \Longrightarrow ac|bd$,
(g) $a|b \wedge b|c \Longrightarrow a|c$,
(h) $0|a \Longleftrightarrow a = 0$.

Wniosek 11.3 *Jeśli $a, b_1, \ldots, b_k, c_1, \ldots, c_k \in R$ i $a|b_i$ dla $i = 1, \ldots, k$, to $a| \sum_{i=1}^{k} b_i c_i$.*

Twierdzenie 11.4 *Dla dowolnych $a, b \in R$, $a|b$ wtedy i tylko wtedy, gdy $bR \subseteq aR$.*

Dowód. Załóżmy, że $a|b$ i ustalmy $x \in bR$. Wtedy $b = ac$ i $x = bd$ dla pewnych $c, d \in R$. Stąd $x = acd$, co oznacza, że $x \in aR$. Tak więc $bR \subseteq aR$.

W celu wykazania implikacji przeciwnej, załóżmy, że $bR \subseteq aR$. Pierścień R posiada jedność, więc $b = b \cdot 1 \in bR \subseteq aR$. To zaś oznacza, że $b = ac$ dla pewnego $c \in R$, czyli $a|b$. ■

Definicja 11.5 *Mówimy, że elementy $a, b \in R$ są stowarzyszone (oznaczenie: $a \sim b$), jeśli $a|b$ i $b|a$.*

Przykład 1. Elementy 10 i -10 pierścienia $\mathbb{Z}$ są stowarzyszone.

Przykład 2. Elementy $\sqrt{3}+1$ i $\sqrt{3}-1$ pierścienia $\mathbb{Z}[\sqrt{3}]]$ są stowarzyszone, gdyż $\sqrt{3}+1 = (\sqrt{3}-1)(\sqrt{3}+2)$ i $\sqrt{3}-1 = (\sqrt{3}+1)(-\sqrt{3}+2)$.

Przykład 3. Jeśli K jest ciałem, $a \in K \setminus \{0\}$ i $f \in K[x]$, to wielomiany f i af są elementami stowarzyszonymi pierścienia $K[x]$.

Twierdzenie 11.6 *Relacja stowarzyszenia $\sim$ jest równoważnością w dowolnym pierścieniu całkowitym.*

Dowód. Niech a, b, c będą dowolnymi elementami pierścienia całkowitego R.

Oczywiście $a|a$, więc $a \sim a$. Jeśli $a \sim b$, to $a|b$ i $b|a$. Stąd $b \sim a$.

Załóżmy teraz, że $a \sim b$ i $b \sim c$. Wtedy $a|b$, $b|a$, $b|c$ i $c|b$. Stąd, na mocy twierdzenia 11.2(7) wynika, że $a|c$ i $c|a$. Tak więc $a \sim c$.

W ten sposób pokazaliśmy, że relacja $\sim$ jest zwrotna, symetryczna i przechodnia, a więc jest to relacja równoważności. ■

Twierdzenie 11.7 *Element pierścienia R jest odwracalny wtedy i tylko wtedy, gdy jest stowarzyszony z jednością tego pierścienia.*

Dowód. Niech $a \in R$ będzie elementem odwracalnym. Wtedy $ab = 1_R$ dla pewnego $b \in R$, co oznacza, że $a|1_R$. Oczywiście również $1_R|a$, skąd wynika, że $a \sim 1_R$.

Jeśli $a \sim 1_R$, to $a|1_R$, czyli $1_R = ab$ dla pewnego $b \in R$. Tak więc a jest elementem odwracalnym. ■

Twierdzenie 11.8 *Niech $a, b \in R$. Wtedy następujące warunki są równoważne.*

(a) $a \sim b$,

(b) $a = bc$, gdzie c jest elementem odwracalnym pierścienia R,

(c) $aR = bR$

Dowód. (a)$\Longrightarrow$(b). Załóżmy, że $a \sim b$. Wtedy $a = bc$ i $b = ad$ dla pewnych $c, d \in R$. Zatem $a = acd$, czyli $a(1_R - cd) = 0_R$. Pierścień R nie ma dzielników zera, więc $a = 0_R$ lub $cd = 1_R$. Jeśli $a = 0_R$, to $b = ad = 0_R \cdot d = 0_R$ i mamy $a = 1_R \cdot b$ (1_R jest elementem odwracalnym w R). Jeśli natomiast $cd = 1_R$, to c jest elementem odwracalnym w R. Ponieważ $a = bc$, dowód implikacji od (a) do (b) jest zakończony.

(b)$\Longrightarrow$(a). Załóżmy, że $a = bc$, gdzie c jest elementem odwracalnym pierścienia R. Wtedy $b = ac^{-1}$, a więc $a|b$ i $b|a$. To oznacza, że $a \sim b$.

Równoważność warunków (a) i (c) wynika łatwo z twierdzenia 11.4 ■

Lemat 11.9 *Jeśli $a, b, c, d \in R$, $a \sim b$ i $c \sim d$, to $ac \sim bd$.*

Dowód. Załóżmy, że $a \sim b$ i $c \sim d$. Wtedy $a|b$, $b|a$, $c|d$ i $d|c$. Stąd wynika, że $ac|bd$ i $bd|ac$, a więc $ac \sim bd$. ■

Niech a będzie różnym od 0_R elementem pierścienia całkowitego R. Rozkładem elementu a na czynniki nazywamy każde jego przedstawienie w postaci iloczynu: $a = a_1 \cdot \ldots \cdot a_n$, gdzie $a_1, \ldots, a_n \in R$. Jeśli dodatkowo $a_1, \ldots, a_n$ są nieodwracalne, to rozkład nazywamy właściwym.

Definicja 11.10 *Różny od zera element a pierścienia całkowitego R nazywamy elementem rozkładalnym (lub mówimy, że a ma rozkład właściwy), jeśli $a = a_1 a_2$, gdzie a_1, a_2 są pewnymi elementami nieodwracalnymi pierścienia R.*

Zauważmy, że element odwracalny ε pierścienia całkowitego R nie może być rozkładalny. Przypuśćmy bowiem, że element odwracalny ε pierścienia R jest równy iloczynowi a_1a_2 elementów tego pierścienia. Wtedy jednak $a_1(a_2\varepsilon^{-1}) = 1_R$, co oznacza, że element a_1 jest odwracalny.

Definicja 11.11 *Różny od zera element pierścienia całkowitego nazywamy nierozkładalnym, jeśli nie jest on elementem odwracalnym i nie jest elementem rozkładalnym.*

Przykład 4. Elementami nierozkładalnymi pierścienia $(\mathbb{Z}, +, \cdot)$ są liczby pierwsze i liczby przeciwne do liczb pierwszych. Liczby złożone i liczby przeciwne do liczb złożonych są elementami rozkładalnymi w $\mathbb{Z}$.

Przykład 5. 5 jest elementem rozkładalnym w pierścieniu Gaussa $\mathbb{Z}[i]$, gdyż $5 = (2 + i)(2 - i)$. Elementy $2+i, 2-i$ są nieodwracalne w $\mathbb{Z}[i]$ (przykład 11, str. 7), więc napisany rozkład jest właściwy.

Przykład 6. Wielomian x^2+1 jest elementem nierozkładalnym w pierćcieniu $\mathbb{R}[x]$, ale rozkładalnym w pierścieniach $\mathbb{C}[x]$ i $\mathbb{Z}_2[x]$. W pierścieniu $\mathbb{C}[x]$ mamy bowiem $x^2+1 = (x+i)(x-i)$, zaś w pierścieniu $\mathbb{Z}_2[x]$, $x^2 + 1 = (x + 1)(x + 1)$.

Przykład 7. Jeśli K jest ciałem, to dowolny wielomian stopnia 1 o współczynnikach z K jest elementem nierozkładalnym pierścienia $K[x]$.

Definicja 11.12 *Pierścień całkowity R nazywa się pierścieniem z rozkładem, jeśli każdy różny od zera nieodwracalny element tego pierścienia jest elementem nierozkładalnym lub ma rozkład, którego czynniki są nierozkładalne.*

Definicja 11.13 *Dwa rozkłady elementu $a \in R$ na czynniki nierozkładalne*

$$a = a_1 \cdot \ldots \cdot a_k = b_1 \cdot \ldots \cdot b_m$$

nazywamy rozkładami stowarzyszonymi, jeśli $k = m$ i jeśli w drugim (lub – co na jedno wychodzi – w pierwszym) rozkładzie można tak zmienić porządek czynników, by kolejne czynniki obu rozkładów były stowarzyszone.

Tak więc rozkłady $a = a_1 \cdot \ldots \cdot a_k = b_1 \cdot \ldots \cdot b_m$ są stowarzyszone, gdy $k = m$ i istnieje permutacja $\sigma \in S_k$, taka że $a_i \sim b_{\sigma(i)}$ dla $i = 1, \ldots, k$.

Definicja 11.14 *Pierścień R z rozkładem nazywamy pierścieniem z jednoznacznacznością rozkładu (lub dziedziną z jednoznacznością rozkładu), jeśli każde dwa rozkłady na czynniki nierozkładalne dowolnego różnego od zera elementu nieodwracalnego są stowarzyszone.*

Jak wynika z lematu 9.26 i twierdzenia 9.29, jeśli K jest ciałem, to $K[x]$ jest pierścieniem z jednoznacznością rozkładu. Dalej udowodnimy, że każdy pierścień ideałów głównych jest pierścieniem z jednoznacznością rozkładu (twierdzenie 11.31). Pozwoli to stwierdzić, że $\mathbb{Z}$ i $\mathbb{Z}[i]$ są pierścieniami z jednoznacznością rozkładu.

Przykład 8. Pokażemy, że pierścień $\mathbb{Z}[\sqrt{5}i]$ nie jest pierścieniem z jednoznacznością rozkładu. Rozważmy dwa rozkłady liczby 6:

$$6 = 2 \cdot 3 = (1 + \sqrt{5}i)(1 - \sqrt{5}i).$$

Ponieważ jedynymi elementami odwracalnymi w pierścieniu $\mathbb{Z}[\sqrt{5}i]$ są 1 i -1 (przykład 12 strona 58), napisane rozkłady są właściwe i nie są stowarzyszone.

Trzeba jeszcze wykazać, że $2, 3, 1+\sqrt{5}i$ i $1-\sqrt{5}i$ są elementami nierozkładalnymi pierścienia $\mathbb{Z}[\sqrt{5}i]$. Dla przykładu udowodnimy, że nierozkładalny jest element $1+\sqrt{5}i$. Przypuśćmy, że

$$1+\sqrt{5}i = (a+b\sqrt{5}i)(c+d\sqrt{5}i)$$

dla pewnych $a, b, c, d \in \mathbb{Z}$. Stąd otrzymujemy

$$|1+\sqrt{5}i|^2 = |(a+b\sqrt{5}i)(c+d\sqrt{5}i)|^2 = |a+b\sqrt{5}i|^2 \cdot |c+d\sqrt{5}i|^2,$$

co oznacza, że

$$6 = (a^2+5b^2)(c^2+5d^2).$$

$a^2+5b^2 \in \mathbb{N}_+$ i $a^2+5b^2|6$, więc $a^2+5b^2 \in \{1,2,3,6\}$.

- Jeśli $a^2+5b^2 = 1$, to $a \in \{1,-1\}$ i $b=0$, co oznacza, że $a+b\sqrt{5}i$ jest elementem odwracalnym.
- Jeśli $a^2+5b^2 = 2$, to $b=0$ i $a^2=2$, co nie jest możliwe dla żadnego $a \in \mathbb{Z}$.
- Jeśli $a^2+5b^2 = 3$, to $c^2+5d^2 = 2$ i jak wcześniej dostajemy sprzeczność.
- Jeśli $a^2+5b^2 = 6$, to $c^2+5d^2 = 1$ skąd wynika, że $c+d\sqrt{5}i$ jest elementem odwracalnym.

W ten sposób pokazaliśmy, że element $1+\sqrt{5}i$ nie posiada właściwego rozkładu w pierścieniu $\mathbb{Z}[\sqrt{5}i]$, a więc jest on nierozkładalny.

Niech R będzie pierścieniem z jednoznacznością rozkładu. Załóżmy, że niezerowy i nieodwracalny element a pierścienia R posiada rozkład na czynniki nierozkładalne postaci $a = a_1 \cdot \ldots \cdot a_m$. W rozkładzie tym mogą występować elementy stowarzyszone. Jeśli na przykład $a_i \sim a_j$, to $a_i = \delta a_j$, gdzie $\delta \in U(R)$. Możemy więc iloczyn $a_i a_j$ zapisać w postaci δa_j^2. Postępując tak dalej, to znaczy grupując w iloczyny czynniki stowarzyszone, i pisząc je w postaci $\delta_i a_i^{k_i}$ ($\delta_i \in U(R)$), możemy napisać rozkład elementu a w następujący sposób:

$$a = \varepsilon b_1^{k_1} \cdot \ldots \cdot b_n^{k_n},$$

gdzie $\varepsilon \in U(R)$, $b_1, \ldots, b_n$ są elementami nierozkładalnymi pierścienia R, $k_1, \ldots, k_n \in \mathbb{N}_+$, b_i nie jest stowarzyszone z b_j dla $i \neq j$. Powyższą postać rozkładu elementu a na czynniki nazywać będziemy *postacią kanoniczną rozkładu* lub *rozkładem kanonicznym*.

Twierdzenie 11.15 *Niech $a, b \in R \setminus \{0\}$, gdzie R jest pierścieniem z jednoznacznością rozkładu. Jeśli a jest elementem nieodwracalnym i ma rozkład kanoniczny $a = \varepsilon a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$ ($\varepsilon \in U(R)$), to $b|a$ wtedy i tylko wtedy, gdy $b = \delta a_1^{h_1} \cdot \ldots \cdot a_n^{h_n}$, gdzie $\delta \in U(R)$, $0 \leq h_i \leq k_i$ dla $i = 1, \ldots, n$.*

Dowód. Implikacja $\Longleftarrow$ jest oczywista. Dla wykazania implikacji przeciwnej, załóżmy, że $a \in R \setminus \{0_R\}$ jest elementem nieodwracalnym o rozkładzie kanonicznym $a = \varepsilon a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$, w którym $\varepsilon \in U(R)$, $a_1, \ldots, a_n$ są elementami nierozkładalnymi, parami niestowarzyszonymi. Niech $b|a$. Wtedy $a = bc$ dla pewnego $c \in R$. Jeśli b jest elementem odwracalnym, to można przedstawić go w postaci: $b = b \cdot 1 = b a_1^0 \cdot \ldots \cdot a_n^0$.

Przypuśćmy teraz, że element b jest nieodwracalny. Niech $b = b_1 \cdot \ldots \cdot b_l$ będzie jego rozkładem na czynniki nierozkładalne. Ponieważ R jest pierścieniem z jednoznacznością rozkładu i

$$a = \varepsilon a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} = bc = b_1 \cdot \ldots \cdot b_l c,$$

każdy z nierozkładalnych elementów $b_1, \ldots, b_l$ jest stowarzyszony z którymś z czynników $a_1, \ldots, a_n$. Stąd wynika, że $b = b_1 \cdot \ldots \cdot b_l = \delta a_1^{h_1} \cdot \ldots \cdot a_n^{h_n}$, gdzie $\delta \in U(R)$ i $h_1, \ldots, h_n \in \mathbb{N}$. Zatem

$$\varepsilon a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} = \delta a_1^{h_1} \cdot \ldots \cdot a_n^{h_n} c.$$

Gdyby na przykład $h_1 > k_1$, to po skróceniu obu stron powyższej równości przez $a_1^{k_1}$, otrzymalibyśmy

$$\varepsilon a_1^0 \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n} = \delta a_1^{h_1 - k_1} \cdot \ldots \cdot a_n^{h_n} c,$$

a więc dla elementu a_1 występującego jako czynnik po prawej stronie nie byłoby stowarzyszonego z nim po lewej. Tak więc $h_1 \leq k_1$. Podobnie wykazuje się, że $h_i \leq k_i$ dla $i \in \{1, \ldots, n\}$. ■

Definicja 11.16 *Niech a, b będą elementami pierścienia całkowitego R. Element $d \in R$ nazywamy największym wspólnym dzielnikiem elementów a i b, jeśli*

(1) $d|a$ i $d|b$,

(2) dla dowolnego $c \in R$, jeśli $c|a$ i $c|b$, to $c|d$.

Największy wspólny dzielnik elementów pierścienia całkowitego na ogół nie jest określony jednoznacznie. Na przykład w pierścieniu $\mathbb{Z}[i]$ każdy z elementów: $2, -2, 2i, -2i$ jest największym wspólnym dzielnikem elementów 2 i $2 - 2i$.

Dla dwóch danych elementów a, b pierścienia całkowitego może nie istnieć ich największy wspólny dzielnik. Poniżej rozważamy przykład takiej sytuacji.

Przykład 9. Rozważmy elementy $a = 4$ i $b = 2 + 2\sqrt{3}i$ pierścienia $\mathbb{Z}[\sqrt{3}i]$. Pokażemy, że w pierścieniu $\mathbb{Z}[\sqrt{3}i]$ nie istnieje największy wspólny dzielnik elementów a i b. W tym celu wyznaczymy najpierw dzielniki rozważanych elementów.

Przypuśćmy, że $k, l \in \mathbb{Z}$ i $k + l\sqrt{3}i|4$. Wtedy istnieją $m, n \in \mathbb{Z}$ takie, że $(k + l\sqrt{3}i)(m + n\sqrt{3}i) = 4$. Stąd $|k + l\sqrt{3}i|^2 |m + n\sqrt{3}i|^2 = 16$. Wyliczając oba moduły otrzymujemy: $(k^2 + 3l^2)(m^2 + 3n^2) = 16$, a więc liczba naturalna $k^2 + 3l^2$ dzieli 16, co oznacza, że $k^2 + 3l^2 \in \{1, 2, 4, 8, 16\}$. Nietrudno sprawdzić, że:

(a) jeśli $k^2 + 3l^2 = 1$, to $\langle k, l\rangle \in \{\langle 1, 0\rangle, \langle -1, 0\rangle\}$,

(b) jeśli $k^2 + 3l^2 = 4$, to $\langle k, l\rangle \in \{\langle 2, 0\rangle, \langle -2, 0\rangle, \langle 1, 1\rangle, \langle -1, 1\rangle, \langle 1, -1\rangle, \langle -1, -1\rangle\}$,

(c) jeśli $k^2 + 3l^2 = 16$, to $m^2 + 3n^2 = 1$, co wobec (a) daje $n = 0$ i $m \in \{1, -1\}$. Zatem $\langle k, l\rangle \in \{\langle 4, 0\rangle, \langle -4, 0\rangle\}$,

(d) równania $k^2 + 3l^2 = 2$ i $k^2 + 3l^3 = 8$ nie mają rozwiązań w $\mathbb{Z}$.

Tak więc każdy dzielnik elementu $a = 4$ w pierścieniu $\mathbb{Z}[\sqrt{3}i]$ należy do zbioru

$$A = \{1, -1, 2, -2, 4, -4, 1 + \sqrt{3}i, 1 - \sqrt{3}i, -1 + \sqrt{3}i, -1 - \sqrt{3}i\}.$$

Bezpośrednio sprawdzamy, że każdy element zbioru A jest dzielnikiem elementu $a = 4$. Na przykład $1 + \sqrt{3}i|4$, gdyż $4 = (1 + \sqrt{3}i)(1 - \sqrt{3}i)$.

Podobnie pokazujemy, że zbiór dzielników elementu $b = 2 + 2\sqrt{3}i$ jest równy

$$B = \{1, -1, 2, -2, 1 + \sqrt{3}i, 1 - \sqrt{3}i, -1 + \sqrt{3}i, -1 - \sqrt{3}i, 2 + 2\sqrt{3}, -2 - 2\sqrt{3}\}.$$

Zbiór wspólnych dzielników elementów a i b jest równy

$$A \cap B = \{1, -1, 2, -2, 1 + \sqrt{3}i, 1 - \sqrt{3}i, -1 + \sqrt{3}i, -1 - \sqrt{3}i\}.$$

Gdyby w pierścieniu $\mathbb{Z}[\sqrt{5}i]$ istniał element będący największym wspólnym dzielnikiem a i b, to należał by on do $A \cap B$ i byłby podzielny przez każdy element zbioru $A \cap B$. Tymczasem:

(a) elementy $1, -1, 2, -2$ nie dzielą się przez $1 + \sqrt{3}i$

(b) elementy $1 + \sqrt{3}i, 1 - \sqrt{3}i, -1 + \sqrt{3}i, -1 - \sqrt{3}i$ nie dzielą się przez 2.

Oznacza to, że żaden z elementów zbioru $A \cap B$ nie spełnia warunku (2) definicji 11.16. Zatem w pierścieniu $\mathbb{Z}[\sqrt{3}i]$ nie istnieje największy wspólny dzielnik elementów 4 i $2 + 2\sqrt{3}i$.

Twierdzenie 11.17 *Jeśli d_1 i d_2 są największymi wspólnymi dzielnikami elementów a i b, to $d_1 \sim d_2$.*

Jeśli d_1 jest największym wspólnym dzielnikiem elementów a, b i $d_2 \sim d_1$, to d_2 też jest największym wspólnym dzielnikiem elementów a i b.

Dowód. Załóżmy, że d_1, d_2 są największymi wspólnymi dzielnikami elementów a i b. Wtedy $d_1|a$, $d_1|b$, $d_2|a$ i $d_2|b$. Wobec definicji największego wspólnego dzielnika oznacza to, że $d_1|d_2$ i $d_2|d_1$, a więc $d_1 \sim d_2$.

Przypuśćmy teraz, że d_1 jest największym wspólnym dzielnikiem elementów a, b i $d_2 \sim d_1$. Wtedy: (1) $d_1|a$, (2) $d_1|b$, (3) $d_1|d_2$ i (4) $d_2|d_1$. Z warunków (1), (2) i (4) na mocy przechodniości relacji podzielności wynika, że $d_2|a$ i $d_2|b$. Niech c będzie dowolnym wspólnym dzielnikiem elementów a i b. Z tego, że d_1 jest największym wspólnym dzielnikiem elementów a i b wynika, że $c|d_1$. Ale $d_1|d_2$, więc również $c|d_2$. Tak więc d_2 jest największym wspólnym dzielnikiem elementów a i b. ■

Twierdzenie powyższe pokazuje, że największy wspólny dzielnik dwóch elementów pierścienia, o ile istnieje, jest określony z dokładnością do stowarzyszenia.

Pojęcie największego wspólnego dzielnika dwóch elementów pierścienia uogólnia się na dowolną skończoną liczbę niezerowych elementów pierścienia.

Definicja 11.18 *Niech $a_1, \ldots, a_n$ będą elementami pierścienia całkowitego R. Element $d \in R$ nazywamy największym wspólnym dzielnikiem elementów $a_1, \ldots, a_n$, jeśli*

(1) $d|a_i$ dla $i = 1, \ldots, n$,

(2) dla dowolnego $c \in R$, jeśli $c|a_i$ dla $i = 1, \ldots, n$, to $c|d$.

Nietrudno wykazać następujący fakt.

Fakt 11.19 *Niech $a_1, \ldots, a_{k+1}$ będą elementami pierścienia całkowitego R. Jeżeli*

(a) c jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_k$,

(b) d_1 jest największym wspólnym dzielnikiem elementów c i a_{k+1},

(c) d_2 jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_{k+1}$,

to $d_1 \sim d_2$.

Definicja 11.20 *Elementy $a, b \in R \setminus \{0\}$ nazywamy względnie pierwszymi, jeśli jedność pierścienia R jest ich największym wspólnym dzielnikiem.*

Twierdzenie 11.21 *W pierścieniu z jednoznacznością rozkładu każde dwa różne od zera elementy mają największy wspólny dzielnik.*

Dowód. Niech R będzie pierścieniem z jednoznacznością rozkładu. Przedstawmy elementy a i b w postaci:

$$a = \delta a_1^{k_1} \cdot \ldots \cdot a^{k_n} \text{ i } b = \varepsilon a_1^{l_1} \cdot \ldots \cdot a_n^{l_n},$$

gdzie $\delta, \varepsilon \in U(R)$, $a_1, \ldots, a_n$ są elementami nierozkładalnymi, parami niestowarzyszonymi, zaś $k_1, \ldots, k_n$, $l_1, \ldots, l_n$ liczbami naturalnymi (niektóre z nich mogą być zerami). Wtedy $d = a_1^{\min(k_1,l_1)} \cdot \ldots \cdot a_n^{\min(k_n,l_n)}$ jest oczywiście dzielnikiem elementów a i b. Pokażemy, że d jest największym wspólnym dzielnikiem elementów a i b.

Załóżmy, że c jest dowolnym elementem takim, że $c|a$ i $c|b$. Wtedy, na mocy twierdzenia 11.15, $c = \eta a_1^{h_1} \cdot \ldots \cdot a_n^{h_n}$, gdzie $\eta \in U(R)$ oraz

$$h_i \leq k_i, h_i \leq l_i \text{ dla } i \in \{1, \ldots, n\}.$$

A więc $h_i \leq \min(k_i, l_i)$ dla $i \in \{1, \ldots, n\}$, co implikuje, że $c|d$. A więc d jest największym wspólnym dzielnikiem elementów a i b. ■

Z powyższego twierdzenia oraz faktu 11.19 wynika istnienie największego wspólnego dzielnika dowolnej skończonej liczby różnych od zera elementów pierścienia z jednoznacznością rozkładu. Łatwy dowód indukcyjny pozostawiamy Czytelnikowi jako ćwiczenie.

Definicja 11.22 *Niech a, b będą elementami pierścienia całkowitego R. Element $w \in R$ nazywamy najmniejszą wspólną wielokrotnością elementów a i b, jeśli*
(1) $a|w$ i $b|w$,
(2) dla dowolnego $c \in R$, jeśli $a|c$ i $b|c$, to $w|c$.

Podobnie jak w przypadku największego wspólnego dzielnika, najmniejsza wspólna wielokrotność pary elementów pierścienia całkowitego może nie istnieć lub też może być określona niejednoznacznie. Prawdziwy jest przy tym odpowiednik twierdzenia 11.17. Jego dowód pomijamy, gdyż jest bardzo podobny do dowodu twierdzenia 11.17.

Twierdzenie 11.23 *Jeśli w_1 i w_2 są najmniejszymi wspólnymi wielokrotnościami elementów a i b, to $w_1 \sim w_2$. Jeśli w_1 jest najmniejszą wspólną wielokrotnością elementów a, b i $w_2 \sim w_1$, to w_2 też jest najmniejszą wspólną wielokrotnością elementów a i b.*

Pojęcie najmniejszej wspólnej wielokrotności dwóch elementów pierścienia uogólnia się na dowolną skończoną liczbę niezerowych elementów pierścienia.

Definicja 11.24 *Niech $a_1, \ldots, a_n$ będą elementami pierścienia całkowitego R. Element $w \in R$ nazywamy najmniejszą wspólną wielokrotnością elementów $a_1, \ldots, a_n$, jeśli*
(1) $a_i|w$ dla $i = 1, \ldots, n$,
(2) dla dowolnego $c \in R$, jeśli $a_1|c, \ldots, a_n|c$ to $w|c$.

Nietrudno wykazać następujący fakt.

Fakt 11.25 *Niech $a_1, \ldots, a_{k+1}$ będą elementami pierścienia R. Jeżeli*
(a) c jest najmniejszą wspólną wielokrotnością elementów $a_1, \ldots, a_k$,
(b) w_1 jest najmniejszą wspólną wielokrotnością elementów $a_1, \ldots, a_{k+1}$,
(c) w_2 jest najmniejszą wspólną wielokrotnością elementów c i a_{k+1},
to $w_1 \sim w_2$.

Twierdzenie 11.26 *W pierścieniu R z jednoznacznością rozkładu każde dwa różne od zera elementy mają najmniejszą wspólną wielokrotność.*

Dowód. Przedstawmy elementy a i b w postaci:

$$a = \delta a_1^{k_1} \cdot \ldots \cdot a^{k_n} \text{ i } b = \varepsilon a_1^{l_1} \cdot \ldots \cdot a_n^{l_n},$$

gdzie $\delta, \varepsilon \in U(R)$, $a_1, \ldots, a_n$ są elementami nierozkładalnymi, parami niestowarzyszonymi, zaś $k_1, \ldots, k_n$, $l_1, \ldots, l_n$ liczbami naturalnymi (niektóre z nich mogą być zerami). Wtedy element $w = a_1^{\max(k_1,l_1)} \cdot \ldots \cdot a_n^{\max(k_n,l_n)}$ jest oczywiście podzielny przez a i przez b. Pokażemy, że w jest najmniejszą wspólną wielokrotnością elementów a i b.

Załóżmy, że c jest dowolnym elementem takim, że $a|c$ i $b|c$. Wtedy, na mocy twierdzenia 11.15, $c = \eta a_1^{h_1} \cdot \ldots \cdot a_n^{h_n}$, gdzie $\eta \in U(R)$ oraz

$$h_i \geq k_i, h_i \geq l_i \text{ dla } i = 1, \ldots, n.$$

A więc $h_i \geq \max(k_i, l_i)$ dla $i = 1, \ldots, n$, co implikuje, że $w|c$. Tym samym w jest najmniejszą wspólną wielokrotnością elementów a i b. ■

Z powyższego twierdzenia oraz faktu 11.25 wynika istnienie najmniejszej wspólnej wielokrotności dowolnej skończonej liczby różnych od zera elementów pierścienia z jednoznacznością rozkładu. Łatwy dowód indukcyjny pozostawiamy Czytelnikowi jako ćwiczenie.

W arytmetyce pod pojęciem największego wspólnego dzielnika liczb całkowitych m i n, z których przynajmniej jedna jest różna od 0 rozumiemy największą liczbę naturalną dodatnią d taką, że $d|m$ i

$d|n$ (definicja na stronie 5). Liczbę tę oznaczamy przez $NWD(m,n)$. Podobnie, mówiąc o najmniejszej wspólnej wielokrotności niezerowych liczb całkowitych m i n mamy na myśli najmniejszą liczbę naturalną dodatnią w taką, że $a|w$ i $b|w$ (definicja na stronie 4). Liczbę tę oznaczamy przez $NWW(m,n)$. Pojęcia największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności rozważane w arytmetyce różnią się od wprowadzonych w definicjach 11.16 i 11.22, ale są z nimi blisko związane. Następujące twierdzenie jest bezpośrednią konsekwencją twierdzeń 0.3 i 0.4.

Twierdzenie 11.27 *Niech $m,n \in \mathbb{Z}$ i ($m \neq 0$ lub $n \neq 0$). Załóżmy, że d jest największym wspólnym dzielnikiem liczb m i n (w sensie definicji 11.16), zaś w ich największą wspólną wielokrotnością (w sensie definicji 11.22). Wtedy $|d| = NWD(m,n)$ i $|w| = NWW(m,n)$.*

Twierdzenie 11.28 *Niech R będzie pierścieniem z jednoznacznością rozkładu i niech $a,b \in R \setminus \{0\}$. Jeśli d jest największym wspólnym dzielnikiem, zaś w najmniejszą wspólną wielokrotnością elementów a i b, to $dw \sim ab$.*

Dowód. Przedstawmy elementy a i b w postaci:

$$a = \delta a_1^{k_1} \cdot \ldots \cdot a^{k_n} \text{ i } b = \varepsilon a_1^{l_1} \cdot \ldots \cdot a_n^{l_n},$$

gdzie $\delta, \varepsilon \in U(R)$, $a_1, \ldots, a_n$ są elementami nierozkładalnymi, zaś $k_1, \ldots, k_n, l_1, \ldots, l_n$ liczbami naturalnymi (niektóre z nich mogą być zerami). Jak wynika z dowodów twierdzeń 11.21 i 11.26,

$$d \sim a_1^{\min(k_1,l_1)} \cdot \ldots \cdot a_n^{\min(k_n,l_n)} \text{ i } w \sim a_1^{\max(k_1,l_1)} \cdot \ldots \cdot a_n^{\max(k_n,l_n)}.$$

Stąd, na mocy lematu 11.9 otrzymujemy

$$dw \sim a_1^{\min(k_1,l_1)+\max(k_1,l_1)} \cdot \ldots \cdot a_n^{\min(k_n,l_n)+\max(k_n,l_n)} = a_1^{k_1+l_1} \cdot \ldots \cdot a_n^{k_n+l_n} = ab,$$

co kończy dowód. ■

Wniosek 11.29 *Jeśli $a,b \in \mathbb{Z} \setminus \{0\}$, to $NWD(a,b)NWW(a,b) = |ab|$.*

Twierdzenie 11.30 *Pierścień całkowity R jest pierścieniem z jednoznacznością rozkładu wtedy i tylko wtedy, gdy*

(1) R jest pierścieniem z rozkładem oraz

(2) jeśli $a,b,c \in R$ i a jest nierozkładalny, to $a|bc \Longrightarrow a|b \vee a|c$.

Dowód. Załóżmy, że R jest pierścieniem z jednoznacznością rozkładu. Wtedy na mocy definicji jest on pierścieniam z rozkładem. W celu udowodnienia warunku (2), ustalmy elementy $a,b,c \in R$ takie, że a jest nierozkładalny i $a|bc$. Wtedy $ad = bc$ dla pewnego $d \in R$. Jeśli $b = 0$, to oczywiście $a|b$. Jeśli $b \in U(R)$ to $adb^{-1} = c$, skąd wynika, że $a|c$. Podobnie postępujemy w przypadku, gdy $c = 0$ lub $c \in U(R)$. Załóżmy więc, że elementy b,c są nieodwracalne i różne od zera. Można je zatem przedstawić w postaci iloczynów elementów nierozkładalnych: $b = b_1 \cdot \ldots \cdot b_k$ i $c = c_1 \cdot \ldots \cdot c_m$. Tak więc otrzymujemy:

$$ad = b_1 \cdot \ldots \cdot b_k \cdot c_1 \cdot \ldots \cdot c_m.$$

Ponieważ R jest pierścieniem z jednoznacznością rozkładu, wśród czynników $b_1, \ldots, b_k, c_1, \ldots, c_m$ znajduje się czynnik stowarzyszony z elementem a. Jeśli jest to któryś z czynników $b_1, \ldots, b_k$, to $a|b$, jeśli zaś któryś z czynników $c_1, \ldots, c_m$, to $a|c$.

Załóżmy teraz, że R jest pierścieniem z rozkładem spełniającym warunek (2). Ustalmy element nieodwracalny $a \in R \setminus \{0_R\}$. Pokażemy, że dowolne dwa rozkłady elementu a na czynniki nierozkładalne są stowarzyszone.

Niech $a = b_1 \cdot \ldots \cdot b_k = c_1 \cdot \ldots \cdot c_m$, gdzie $b_1, \ldots, b_k, c_1, \ldots, c_m$ są elementami nierozkładalnymi pierścienia R. Oczywiście $b_1|c_1 \cdot \ldots \cdot c_m$, co na mocy warunku (2) oznacza, że $b_1|c_i$ dla pewnego $i \in \{1, \ldots, m\}$. Tak więc $c_i = \delta b_1$ dla pewnego $\delta \in R$. Ponieważ b_1 oraz c_i są elementami nierozkładalnymi,

element δ musi być odwracalny. Oznacza to, że elementy b_1 i c_i są stowarzyszone. Stąd na mocy prawa skracań (R jest całkowity) dostajemy

$$b_2 \cdot \ldots \cdot b_k = \delta \prod_{\{j:1\leq j\leq k, j\neq i\}} c_j.$$

Powtarzając przeprowadzone rozumowanie dla powyższych rozkładów, możemy określić funkcję różnowartościową $\sigma : \{1,\ldots,k\} \longrightarrow \{1,\ldots,m\}$ taką, żem $b_i \sim c_{\sigma(i)}$ dla $i = 1,\ldots,k$. W szczególności wynika stąd, że $k \leq m$. Podobnie pokazuje się, że $m \leq k$. Tak więc rozkłady $a = b_1 \cdot \ldots b_k = c_1 \cdot \ldots \cdot c_m$ są stowarzyszone. ■

Twierdzenie 11.31 *Każdy całkowity pierścień ideałów głównych jest pierścieniem z jednoznacznością rozkładu.*

Dowód. Niech R będzie całkowitym pierścieniem ideałów głównych. Pokażemy najpierw, że R jest pierścieniem z rozkładem. W tym celu załóżmy nie wprost, że $a \in R \setminus \{0_R\}$ jest elementem nieodwracalnym i rozkładalnym, przy czym nie ma rozkładu na iloczyn czynników nierozkładalnych. Skonstruujemy ciąg ideałów $I_1, I_2, \ldots$ oraz ciąg $a_1, a_2, \ldots$ elementów pierścienia R takich, że dla dowolnego $i \in \mathbb{N}_+$ spełnione są warunki:

(a) $a_i \in R \setminus \{0\}$ jest elementem nieodwracalnym i rozkładalnym w R,

(b) a_i nie ma rozkładu na iloczyn czynników nierozkładalnych,

(c) $I_i = a_i R$,

(d) I_i jest właściwym podzbiorem I_{i+1},

Niech $a_1 = a$ i $I_1 = aR$. Przypuśćmy, że znaleźliśmy już elementy $a_1, \ldots, a_n$ oraz ideały $I_1, \ldots, I_n$ czyniące zadość warunkom (a)-(d). Niech $a_n = bc$ będzie rozkładem elementu a_n na czynniki nieodwracalne. Oczywiście $b, c \neq 0$. Ponieważ a_n nie ma rozkładu na czynniki nierozkładalne, również jeden z elementów b, c nie ma takiego rozkładu. Załóżmy, że elementem tym jest b i przyjmijmy $a_{n+1} = b$, $I_{n+1} = a_{n+1}R$. Wtedy $I_n = a_nR = bcR \subseteq bR = I_{n+1}$. c jest elementem nieodwracalnym, więc elementy a_n i b nie są stowarzyszone. To zaś implikuje, że ideały I_n i I_{n+1} są różne.

Niech I będzie sumą mnogościową ideałów $I_1, I_2, I_3, \ldots$. Nietrudno sprawdzić, że I jest ideałem pierścienia R. Ponieważ R jest pierścieniem ideałów głównych, istnieje element $a \in R$ taki, że $I = aR$. Wtedy jednak $a \in I_n$ dla pewnego $n \in \mathbb{N}_+$, skąd wynika, że $I \subseteq I_n$. A więc mamy

$$I \subseteq I_n \subseteq I_{n+1} \subseteq I.$$

Stąd $I_n = I_{n+1}$, sprzeczność z warunkiem (d). W ten sposób wykazaliśmy, że R jest pierścieniem z rozkładem.

Załóżmy teraz, że $a, b, p \in R$, przy czym p jest elementem nierozkładalnym i $p|ab$. W myśl twierdzenia 11.30, wystarczy wykazać, że $p|a$ lub $p|b$.

R jest pierścieniem ideałów głównych, więc $aR+pR = cR$ dla pewnego $c \in R$. Ale $pR = \{0\}+pR \subseteq aR + pR = cR$, więc na mocy twierdzenia 11.4, $c|p$, czyli $p = cd$ dla pewnego $d \in R$. Ponieważ p jest elementem nierozkładalnym, jeden z elementów c, d musi być odwracalny.

Jeśli c jest elementem odwracalnym, to $1_R = cc^{-1} \in cR = aR + pR$, co oznacza, że $1_R = ax + py$ dla pewnych $x, y \in R$. Stąd $b = abx + bpy$. Z założenia $p|ab$, więc również $p|abx + bpy$, czyli $p|b$.

Jeśli d jest elementem odwracalnym, to $c = pd^{-1}$. Zatem

$$a = a \cdot 1 + p \cdot 0 \in aR + pR = cR = pd^{-1}R,$$

skąd wynika, że $p|a$. ■

Wniosek 11.32 *Jeśli R jest całkowitym pierścieniem ideałów głównych, to dla dowolnych dwóch niezerowych elementów tego pierścienia istnieją: największy wspólny dzielnik i najmniejsza wspólna wielokrotność.*

Twierdzenie 11.33 *Załóżmy, że R jest pierścieniem ideałów głównych i $a, b \in R \setminus \{0\}$. Jeśli d jest największym wspólnym dzielnikiem elementów a i b, to istnieją $u, v \in R$ takie, że $au + bv = d$.*

Dowód. R jest całkowitym pierścieniem ideałów głównych, więc $aR + bR = cR$ dla pewnego $c \in R$. Pokażemy, że $cR = dR$.

Z założenia d jest dzielnikiem elementów a i b. Oznacza to, że $aR \subseteq dR$ i $bR \subseteq dR$ (twierdzenie 11.4). Tak więc $aR + bR \subseteq dR$, czyli $cR \subseteq dR$.

W celu wykazania inkluzji przeciwnej, zauważmy, że:

$$a = a \cdot 1 + b \cdot 0 \in aR + bR = cR \Longrightarrow c|a.$$

Podobnie pokazuje się, że $c|b$. c jest wspólnym dzielnikiem elementów a i b, zaś d ich największym wspólnym dzielnikiem, więc $c|d$, co oznacza, że $dR \subseteq cR$.

W ten sposób wykazaliśmy, że $dR = cR = aR + bR$. Stąd wynika, że $d = d \cdot 1 \in aR + bR$, czyli $d = au + bv$ dla pewnych $u, v \in R$. ■

Twierdzenie 11.34 *Niech R będzie całkowitym pierścieniem ideałów głównych. Jeśli a jest elementem nierozkładalnym pierścienia R, to ideał aR jest maksymalny.*

Dowód. Niech R będzie całkowitym pierścieniem ideałów głównych, zaś a jego elementem nierozkładalnym. Ustalmy idał J pierścienia R, którego właściwym podzbiorem jest aR. Pokażemy, że $J = R$.

R jest pierścieniem ideałów głównych, więc $J = bR$ dla pewnego $b \in R$. $aR \subseteq bR$, więc $b|a$, czyli $a = bd$ dla pewnego $d \in R$. $aR \neq bR$, więc d jest elementem nieodwracalnym. Wobec nierozkładalności elementu a oznacza to, że element b jest odwracalny. Dlatego $J = bR = R$, co kończy dowód. ■

Rozdział 12

Pierścienie euklidesowe

W rozdziale 0 przedwstawiliśmy algorytm Euklidesa umożliwiający znalezienie największego wspólnego dzielnika dwóch liczb całkowitych, z których przynajmniej jedna nie jest zerem. W niniejszym rozdziale omawiamy klasę pierścieni, dla których możliwe jest stosowanie pewnego uogólnienia algorytmu Euklidesa.

Definicja 12.1 *Pierścień całkowity R nazywamy pierścieniem euklidesowym, jeśli istnieje funkcja $N : R \setminus \{0_R\} \longrightarrow \mathbb{N}$ (zwana normą) taka, że*

$$(\forall a \in R)(\forall b \in R \setminus \{0_R\})(\exists q, r \in R)\,[a = bq + r \wedge (N(r) < N(b) \vee r = 0_R)]\,.$$

Element r w powyższym wzorze nazywa się resztą. Mówimy też, że R jest pierścieniem euklidesowym względem normy[1] *N.*

Przykład 1. Pierścień liczb całkowirych jest pierścieniem euklidesowym względem normy $N(x) = |x|$, mamy bowiem:

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z} \setminus \{0\})(\exists q, r \in \mathbb{Z})\,[a = bq + r \wedge |r| < |b|]\,.$$

Przykład 2. Jeśli K jest ciałem, to pierścień $K[x]$ jest pierścieniem euklidesowym względem normy $N(f) = \mathrm{st}(f)$. Wynika to z wniosku 9.20, zgodnie z którym:

$$(\forall f \in K[x])(\forall g \in K[x] \setminus \{0\})(\exists q, r \in K[x])\,[f = qg + r \wedge (\mathrm{st}(r) < \mathrm{st}(g) \vee r = 0)]\,.$$

Przykład 3. Pierścień Gaussa $\mathbb{Z}[i] = \{m+ni : m, n \in \mathbb{Z}\}$ jest pierścieniem eklidesowym względem normy $N(m + ni) = \sqrt{m^2 + n^2} = |m + ni|$.

Dla wykazania tego faktu, załóżmy, że $a, b \in \mathbb{Z}[i]$ i $b \neq 0$. Wtedy a należy do pewnego kwadratu o boku długości $|b|$ i o wierzchołkach $(m + ni)b$, $(m + 1 + ni)b$, $(m + (n + 1)i)b$, $(m + 1 + (n + 1)i)b$, gdzie $m, n \in \mathbb{Z}$. Odległość punktu a od jednego z wierzchołków tego kwadratu nie przekracza połowy długości przekątnej. Innymi słowy, istnieje element $q \in \mathbb{Z}[i]$ taki, że $|a - bq| \leq \frac{|b|}{\sqrt{2}} < |b|$. Przyjmując, że $r = a - bq$, otrzymujemy $|r| < |b|$, czyli $N(r) < N(b)$.

Jak wiemy z wniosku 9.20, jeśli K jest ciałem, to przy dzieleniu wielomianu $f \in K[x]$ przez niezerowy wielomian $g \in K[x]$, iloraz i reszta są określone jednoznacznie.

[1] Czasmi dodatkowo zakłada się, że pojęcie normy spełnia tzw. warunek multyplikatywności, tzn. $N(ab) = N(a)N(b)$ dla $a, b \in R \setminus \{0_R\}$

Jeżeli R jest pierścieniem euklidesowym względem normy N, $a, b \in R$ i $b \neq 0$, to przedstawienie elemenetu a w postaci $a = bq + r$, gdzie $N(r) < N(b)$ lub $r = 0$ na ogół nie jest jednoznaczne.

Na przykład w pierścieniu liczb całkowitych, który jest pierścieniem euklidesowym względem wartości bezwzględnej, mamy: $17 = 3 \cdot 5 + 2 = 4 \cdot 5 + (-3)$. Wartość bezwzględna każdej z liczb 2 i -3 jest mniejsza od 5.

W pierścieniu Gaussa $\mathbb{Z}[i]$ dla $a = 12 + 3i$ oraz $b = 1 + 4i$ otrzymujemy:
$a = (1 - 2i)b + (3 - i)$,
$a = (1 - 3i)b + (-1 + 2i)$,
$a = (2 - 2i)b + (2 - 3i)$,
$a = (2 - 3i)b + (2 + 2i)$.
Oczywiście, moduł każdej z liczb $3 - i$, $-1 + 2i$, $2 - 3i$ i $2 + 2i$ jest mniejszy od $|b| = \sqrt{17}$.

Twierdzenie 12.2 *Każdy pierścień euklidesowy jest pierścieniem ideałów głównych.*

Dowód. Niech R będzie pierścieniem euklidesowym względem normy N, zaś I jego ideałem. Jeśli $I = \{0_R\}$, to oczywiście I jest ideałem głównym. Załóżmy więc, że $I \neq \{0_R\}$ i wybierzmy w I niezerowy element o najmniejszej normie, tzn. element $a \in I \setminus \{0_R\}$ taki, że $N(b) \geq N(a)$ dla dowolnego $b \in I \setminus \{0_R\}$. Pokażemy, że $I = aR$.

$a \in I$, więc $ax \in R$ dla dowolnego $x \in R$. To zaś oznacza, że $aR \subseteq I$. W celu wykazania inkluzji przeciwnej rozważmy $b \in I \setminus \{0\}$. R jest pierścieniem euklidesowym, więc dla pewnych $q, r \in R$ mamy:

$$(*)\ b = aq + r, \text{ przy czym } (N(r) < N(a) \text{ lub } r = 0).$$

Ponieważ $a, b \in I$, więc również $r = b - aq \in I$. a jest elementem ideału I o najmniejszej normie, więc warunek $N(r) < N(a)$ nie zachodzi. Na mocy $(*)$ oznacza to, że $r = 0$, czyli $b = aq \in aR$. Oczywiście również $0 \in aR$. Tak więc $I \subseteq aR$. ■

Poniższy wniosek jest bezpośrednią konsekwencją twierdzeń 12.2 i 11.31.

Wniosek 12.3 *Każdy pierścień euklidesowy jest pierścieniem z jednoznacznością rozkładu.*

Z powyższego wniosku wynika, że dowolna para niezerowych elementów pierścienia euklidesowego posiada największy wspólny dzielnik oraz najmniejszą wspólną wielokrotność. Przedstawimy teraz metodę będącą uogólnieniem klasycznego algorytmu Euklidesa i pozwalającą w skończenie wielu krokach znaleźć największy wspólny dzielnik pary niezerowych elementów pierścienia euklidesowego.

Niech dane będą różne od zera elementy pierścienia euklidesowego R z normą N. Istnieją wówczas elementy $q_1, r_1 \in R$ takie, że

$$a = bq_1 + r_1, \text{ przy czym } N(r_1) < N(b) \text{ lub } r_1 = 0_R.$$

Jeśli $r_1 = 0_R$, to $b|a$ i element b jest największym wspólnym dzielnikiem pary a, b. Jeśli $r_1 \neq 0$, to rozumujemy podobnie jak wyżej: istnieją elementy $q_2, r_2 \in R$ takie, że

$$b = r_1 q_2 + r_2, \text{ przy czym } N(r_2) < N(r_1) \text{ lub } r_2 = 0_R.$$

W przypadku, gdy $r_2 = 0_R$, największym wspólnym dzielnikiem pary a, b jest r_1. Jeśli natomiast $r_2 \neq 0_R$, wykonujemy kolejne dzielenie. Po skończonej liczbie kroków postępowanie to musi się skończyć, gdyż norma każdej kolejnej reszty jest mniejsza od normy reszty poprzedniej, a liczb naturalnych mniejszych od danej liczby jest skończenie wiele. Jest oczywiste, że postępowanie to skończy się,

gdy reszta otrzymana w danym kroku będzie równa 0, gdyż w przeciwnym razie moglibyśmy proces przedłużyć o następny krok. Otrzymamy w ten sposób układ równości:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ &\cdots\cdots \\ r_{k-2} &= r_{k-1}q_k + r_k \\ r_{k-1} &= r_kq_{k+1} + 0_R, \end{aligned}$$

gdzie r_k jest ostatnią resztą różną od 0_R. Oczywiście $N(r_k) = 0$. Przeprowadzone postępowanie nazywa się algorytmem Euklidesa.

Twierdzenie 12.4 *Ostatnia różna od zera reszta r_k w algorytmie Euklidesa jest największym wspólnym dzielnikiem niezerowych elementów a i b pierścienia euklidesowego R.*

Dowód. Aby udowodnić twierdzenie, wykażemy, że:

(a) elementy a i b są podzielne przez r_k oraz

(b) jeśli $d \in R$, $d|a$ i $d|b$, to $d|r_k$.

Przyjmijmy oznaczenia: $r_{-1} = a$, $r_0 = b$ i $r_{k+1} = 0_R$. Wtedy układ równości ze strony 106 można zapisać w postaci:

$$r_{k-j} = r_{k-j+1}q_{k-j+2} + r_{k-j+2}, \text{ gdzie } j \in \{1, \ldots, k+1\}.$$

Dla dowodu warunku (a), pokażemy indukcyjnie, że

$$(*)_j \; r_k|r_{k-j}$$

dla $j = -1, \ldots, k+1$. Oczywiście $r_k|r_{k+1}$ (bo $r_{k+1} = 0_R$) i $r_k|r_k$, więc warunek $(*)_j$ jest prawdziwy dla $j = -1$ oraz dla $j = 0$. Przypuśćmy teraz, że $1 \leq j \leq k+1$ i $(*)_i$ zachodzi dla $i < j$. Wynika stąd, że r_k dzieli $r_{k-(j-2)}$ i $r_{k-(j-1)}$. Ponieważ $r_{k-j} = r_{k-(j-1)}q_{k-j+2} + r_{k-(j-2)}$, również element r_{k-j} dzieli się przez r_k. W ten sposób przez indukcję pokazaliśmy, że $(*)_j$ zachodzi dla $j = -1, \ldots, k+1$. W szczególności $r_k|r_{-1}$ i $r_k|r_0$, co jest rónoważne z (a).

W celu wykazania (b) załóżmy, że $d|a$ i $d|b$. Pokażemy indukcyjnie, że d dzieli elementy $r_{-1}, r_0, \ldots, r_k$. Z założenia $d|r_{-1}$ i $d|r_0$. Przypuśćmy więc, że $1 \leq j \leq k$ i $d|r_i$ dla $-1 \leq i < j$. Ponieważ

$$r_j = r_{j-2} + r_{j-1}q_j,$$

również element r_j dzieli się przez d. Ostatecznie $d|r_k$, co kończy dowód warunku (b).

Koniunkcja warunków (a) i (b) oznacza, że r_k jest największym wspólnym dzielnikiem elementów a i b. ■

Wiemy, że każdy pierścień euklidesowy jest pierścieniem ideałów głównych (twierdzenie 12.2). Wynika stąd, że największy wspólny dzielnik pary niezerowych elementów a i b pierścienia euklidesowego R jest kombinacją liniową postaci $ua + vb$ dla pewnych $u, v \in R$ (twierdzenie 11.33).

Do wyznaczenia współczynników u i v tej kombinacji wykorzystamy algorytm Euklidesa. Załóżmy na przykład, że w wyniku zastosowania algorytmu Euklidesa do elementów a, b otrzymujemy układ równości:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ r_2 &= r_3q_4 + r_4 \\ r_3 &= r_4q_5, \end{aligned}$$

w którym r_4 jest ostatnią resztą różną od zera, a więc jest też największym wspólnym dzielnikiem elementów a i b. Przekształcając otrzymane równości dostajemy:

$$\begin{aligned} r_4 &= r_2 - r_3q_4 = r_2 - (r_1 - r_2q_3)q_4 = (1 + q_3q_4)r_2 - q_4r_1 = \\ &= (1 + q_3q_4)(b - r_1q_2) - q_4r_1 = -(q_2 + q_4 + q_2q_3q_4)r_1 + (1 + q_3q_4)b = \\ &= -(q_2 + q_4 + q_2q_3q_4)(a - bq_1) + (1 + q_3q_4)b = \\ &= -(q_2 + q_4 + q_2q_3q_4)a + (1 + q_3q_4 + q_1q_2 + q_1q_4 + q_1q_2q_3q_4)b. \end{aligned}$$

Zilustrujemy teraz działanie algorytmu Euklidesa w pierścieniu liczb całkowitych, w pierścieniu wielomianów i w pierścieniu Gaussa.

Przykład 4. Posługując się algorytmem Euklidesa znajdziemy największy wspólny dzielnik liczb 350 i -896 w pierścieniu $\mathbb{Z}$. Zauważmy, że:

$$\begin{aligned} -896 &= (-3) \cdot 350 + 154, \\ 350 &= 2 \cdot 154 + 42, \\ 154 &= 3 \cdot 42 + 28, \\ 42 &= 1 \cdot 28 + 14, \\ 28 &= 2 \cdot 14 + 0. \end{aligned}$$

Tak więc 14 jest najwiękdzszym wspólnym dzielnikiem liczb 350 i -896. Znajdziemy teraz liczby całkowite u i v takie, że $14 = 350u - 896v$. Z napisanych wyżej równości otrzymujemy:

$$\begin{aligned} 14 &= 42 - 28 = 42 - (154 - 3 \cdot 42) = 4 \cdot 42 - 154 = 4 \cdot (350 - 2 \cdot 154) - 154 = \\ &= 4 \cdot 350 - 9 \cdot 154 = 4 \cdot 350 - 9 \cdot (-896 + 3 \cdot 350) = (-9) \cdot (-896) + (-23) \cdot 350. \end{aligned}$$

Przykład 5. Przy pomocy algorytmu Euklidesa znajdziemy największy wspólny dzielnik wielomianów $f = x^5 - 2x^4 - 2x^3 + 8x^2 - 7x + 2$ i $g = x^4 - 4x + 3$ przyjmując, że $f, g \in \mathbb{Q}[x]$. Wykonując dzielenie z resztą wielomianu f przez g otrzymujemy

$$f = (x - 2)g + (-2x^3 + 12x^2 - 18x + 8),$$

przy czym $r_1 = -2x^3 + 12x^2 - 18x + 8$ jest resztą z tego dzielenia. Ponieważ największy wspólny dzielnik elementów pierścienia $\mathbb{Q}[x]$ jest wyznaczony z dokładnością do niezerowego czynnika z ciała $\mathbb{Q}$, możemy w następnym kroku algorytmu Euklidesa zamiast wielomianu r_1 rozważać wielomian unormowany $s_1 = -\frac{1}{2}r_1$. Wykonując dzielenie g przez s_1 otrzymujemy

$$g = (x + 6)s_1 + (27x^2 - 54x + 27).$$

W kolejnym kroku zamiast reszty $r_2 = 27x^2 - 54x + 27$ rozważamy wielomian unormowany $s_2 = \frac{1}{27}r_2$. Otrzymujemy $s_1 = (x - 4)s_2 + 0$. Tak więc wielomian $x^2 - 2x + 1$ jest największym wspólnym dzielnikiem wielomianów f i g.

Teraz znajdziemy wielomiany $u, v \in \mathbb{Q}[x]$ takie, że $x^2 - 2x + 1 = uf + vg$. Z przeprowadzonych wcześniej rozważań otrzymujemy:

$$\begin{aligned} x^2 - 2x + 1 &= s_2 = \frac{1}{27}r_2 = \frac{1}{27}(g - (x + 6)s_1) = \frac{1}{27}(g + \frac{1}{2}(x + 6)r_1) = \\ &= \frac{1}{27}g + \frac{1}{54}(x + 6)(f - (x - 2)g) = \frac{1}{54}(x + 6)f + (\frac{1}{27} - \frac{1}{54}(x + 6)(x - 2))g = \\ &= \frac{1}{54}(x + 6)f + \frac{1}{54}(-x^2 - 4x + 14)g. \end{aligned}$$

Przykład 6. Znajdziemy największy wspólny dzielnik elementów $a = 23 + 11i$ oraz $b = 24 - 2i$ pierścienia Gaussa $\mathbb{Z}[i]$. Zauważmy, że

$$\begin{aligned} 23 + 11i &= 1 \cdot (24 - 2i) + (-1 + 13i),\ |-1 + 13i| < |24 - 2i|, \\ 24 - 2i &= -2i(-1 + 13i) + (-2 - 4i),\ |-2 - 4i| < |-1 + 13i|, \\ -1 + 13i &= (-2 - i)(-2 - 4i) + (-1 + 3i),\ |-1 + 3i| < |-2 - 4i|, \\ -2 - 4i &= (-1 + i)(-1 + 3i) + 0 \end{aligned}$$

Tak więc największy wspólny dzielnik elementów a i b, z dokładnością do czynnika odwracalnego, wynosi $-1 + 3i$. Przypomnijmy, że elementami odwracalnymi pierścienia Gaussa są $1, -1, i, -i$. Dlatego $d \in \mathbb{Z}[i]$ jest największym wspólnym dzielnikiem elementów a i b wtedy i tylko wtedy, gdy

$$d \in \{-1 + 3i, 1 - 3i, -3 - i, 3 + i\}.$$

Rozdział 13

Ciało ułamków pierścienia całkowitego

W niniejszym rozdziale pokażemy, jak wychodząc od pierścienia całkowitego R skonstruować pewne ciało K, zwane ciałem ułamków tego pierścienia, mające tę własność, że pierścień R zanurza się w nim izomorficznie, to znaczy istnieje monomorfizm z R w K.

Twierdzenie 13.1 *Każdy pierścień całkowity można zanurzyć izomorficznie w pewnym ciele.*

Dowód. Niech $(R, +, \cdot)$ będzie pierścieniem całkowitym. W zbiorze $R \times R \setminus \{0_R\}$ określamy następującą relację $\sim$:

$$\langle a, b\rangle \sim \langle c, d\rangle \Longleftrightarrow ad = bc.$$

Tak określona relacja jest równoważnością. Jej zwrotność i symetryczność są oczywiste. Pokażemy, że jest ona przechodnia. Załóżmy, że $\langle a, b\rangle \sim \langle c, d\rangle$ i $\langle c, d\rangle \sim \langle g, h\rangle$. Wtedy

$$ad = bc \text{ i } ch = dg.$$

Mnożąc pierwszą równość przez h, a drugą przez b otrzymujemy:

$$adh = bch \text{ i } bch = bdg.$$

Stąd $adh = bdg$. $d \neq 0_R$, zaś w pierścieniu całkowitym można skracać przez element różny od zera. Dlatego $ah = bg$, co oznacza, że $\langle a, b\rangle \sim \langle g, h\rangle$.

Łatwo zauważyć, że relacja $\sim$ posiada następującą własność:

$$\langle a, b\rangle \sim \langle ac, bc\rangle \text{ dla dowolnych } a \in R \text{ i } b, c \in R \setminus \{0_R\}.$$

Wiedząc, że $\sim$ jest relacją równoważności w zbiorze $R \times R \setminus \{0_R\}$, możemy określić zbiór ilorazowy $\Delta(R) = (R \times R \setminus \{0_R\})/\sim$, to znaczy zbiór wszystkich klas abstrakcji relacji $\sim$. Klasę elementu $\langle a, b\rangle$ względem relacji $\sim$ oznacza się zwykle przez $[\langle a, b\rangle]_\sim$, jednak dla uproszczenia zapisu użyjemy oznaczenia $[a, b]$. Tak więc

$$\Delta(R) = \{[\langle a, b\rangle]_\sim : a, b \in R, b \neq 0_R\} = \{[a, b] : a, b \in R, b \neq 0_R\}.$$

W $\Delta(R)$ definiujemy działania $\oplus$ i $\odot$ (zwane odpowiednio dodawaniem i mnożeniem) w następujący sposób:

$$[a, b] \oplus [c, d] = [ad + bc, bd],\ [a, b] \odot [c, d] = [ac, bd].$$

Pokażemy najpierw, że działania $\oplus$ i $\odot$ są dobrze określone. Jeśli $[a, b], [c, d] \in \Delta(R)$, to b i d są niezerowymi elementami pierścienia R. Pierścień R nie ma dzielników zera, więc $bd \neq 0_R$, a to oznacza,

że pary uporządkowane $\langle ad+bc, bd\rangle$ oraz $\langle ac, bd\rangle$ wyznaczają klasy abstrakcji relacji $\sim$. Wykażemy, że wynik dodawania i mnożenia w $\Delta(R)$ nie zależy od wyboru reprezentantów klas w zbiorze $R\times R\setminus\{0_R\}$. Załóżmy, że $[a,b]=[a',b']$ i $[c,d]=[c',d']$. Wtedy $\langle a,b\rangle\sim\langle a',b'\rangle$ i $\langle c,d\rangle\sim\langle c',d'\rangle$, czyli $ab'=a'b$ i $cd'=c'd$. Ponadto bd i $b'd'$ są elementami niezerowymi. Stąd:

$$\begin{aligned}[a,b]\oplus[c,d] &= [ad+bc,bd]=[adb'd'+bcb'd',bdb'd']=\\ &= [a'dbd'+bc'b'd,bdb'd']=[a'd'+c'd',b'd']=[a',b']\oplus[c',d'].\end{aligned}$$

Podobnie

$$[a,b]\odot[c,d]=[ac,bd]=[acb'd',bdb'd']=[a'c'bd,bdb'd']=[a'c',b'd']=[a',b']\odot[c',d'].$$

Dalej udowodnimy, że $\Delta(R)$ jest ciałem względem działań $\oplus$ i $\odot$. Wykażemy po pierwsze, że $(\Delta(R),\oplus)$ jest grupą abelową.

Istotnie, działanie $\oplus$ jest łączne:

$$([a,b]\oplus[c,d])\oplus[g,h]=[ad+bc,bd]\oplus[g,h]=[adh+bch+bdg,bdh],$$

$$[a,b]\oplus([c,d]\oplus[g,h])=[a,b]\oplus[ch+dg,dh]=[adh+bch+bdg,bdh]$$

i przemienne:

$$[a,b]\oplus[c,d]=[ad+bc,bd]=[cb+da,db]=[c,d]\oplus[a,b].$$

Elementem neutralnym działania $\oplus$ jest klasa $[0_R,1_R]$, zaś elementem odwrotnym do klasy $[a,b]$ względem działania $\oplus$ klasa $[-a,b]$:

$$\begin{aligned}[a,b]\oplus[0_R,1_R] &= [a\cdot 1_R+b\cdot 0_R,a\cdot 1_R]=[a,b],\\ [a,b]\oplus[-a,b] &= [ab+b(-a),b^2]=[0_R,b^2]=[0_R,1_R].\end{aligned}$$

Działanie $\odot$ jest łączne:

$$\begin{aligned}([a,b]\odot[c,d])\odot[g,h] &= [ac,bd]\odot[g,h]=[acg,bdh]=[a,b]\odot[cg,dh]=\\ &= [a,b]\odot([c,d]\odot[g,h])\end{aligned}$$

i przemienne:

$$[a,b]\odot[c,d]=[ac,bd]=[ca,db]=[c,d]\odot[a,b].$$

Elementem neutralnym względem $\odot$ jest klasa $[1_R,1_R]$:

$$[a,b]\odot[1_R,1_R]=[a\cdot 1_R,b\cdot 1_R]=[a,b].$$

Jeśli $[a,b]\neq[0,1]$, to $ab\neq 0_R$ i elementem odwrotnym do klasy $[a,b]$ jest klasa $[b,a]$:

$$[a,b]\odot[b,a]=[ab,ba]=[1_R,1_R].$$

Działanie $\odot$ jest rozdzielne względem $\oplus$. Z jednej bowiem strony:

$$[a,b]\odot([c,d]\oplus[g,h])=[a,b]\odot[ch+dg,dh]=[ach+adg,bdh],$$

z drugiej zaś:

$$\begin{aligned}([a,b]\odot[c,d])\oplus([a,b]\odot[g,h]) &= [ac,bd]\oplus[ag,bh]=[acbh+bdag,bdbh]=\\ &= [(ach+adg)b,(bdh)b]=[ach+adg,bdh].\end{aligned}$$

Zero i jedność pierścienia R są różne, więc $\langle 0_R,1_R\rangle\not\sim\langle 1_R,1_R\rangle$, co oznacza, że $[0_R,1_R]\neq[1_R,1_R]$.

W ten sposób udowodniliśmy, że $(\Delta(R), \oplus, \odot)$ jest ciałem. Wykażemy teraz, że istnieje monomorfizm φ z pierścienia R w ciało $\Delta(R)$.

Odwzorowanie $\varphi : R \longrightarrow \Delta(R)$ określimy następująco:

$$\varphi(a) = [a, 1_R] \text{ dla } a \in R.$$

φ jest funkcją różnowartościową, gdyż dla dowolnych $a, b \in R$ mamy:

$$\varphi(a) = \varphi(b) \Longrightarrow [a, 1_R] = [b, 1_R] \Longrightarrow \langle a, 1_R\rangle \sim \langle b, 1_R\rangle \Longrightarrow a \cdot 1_R = 1_R \cdot b \Longrightarrow a = b.$$

φ jest homomorfizmem pierścieni, ponieważ

$$\begin{aligned} \varphi(a+b) &= [a+b, 1_R] = [a, 1_R] \oplus [b, 1_R] = \varphi(a) \oplus \varphi(b) \\ \varphi(ab) &= [ab, 1_R] = [a, 1_R] \odot [b, 1_R] = \varphi(a) \odot \varphi(b) \end{aligned}$$

dla dowolnych $a, b \in R$. ■

Skonstruowane w dowodzie twierdzenia 13.1 ciało zwane jest *ciałem ułamków pierścienia całkowitego* R. Elementy ciała ułamków, tzn. klasy $[a, b]$, zapisuje się zwykle w postaci $\frac{a}{b}$ i nazywa ułamkami. Zgodnie z określeniem działań w ciele $\Delta(R)$, ułamki dodaje się i mnoży według wzorów:

$$\frac{a}{b} \oplus \frac{c}{d} = \frac{ab+bc}{bd}, \quad \frac{a}{b} \odot \frac{c}{d} = \frac{ac}{bd}.$$

Pierścień R zanurza się izomorficznie w ciało $\Delta(R)$. Jego obrazem izomorficznym jest zbiór $R' = \left\{\frac{a}{1} : a \in R\right\}$. R' zazwyczaj identyfikuje się z R zapisując dowolny ułamek $\frac{a}{1} \in R'$ po prostu jako a. Dla oznaczenia działań w ciele ułamków używa się symboli dodawania i mnożenia w R. Nie prowadzi to do nieporozumień.

W niniejszym opracowaniu traktujemy pierścień $\mathbb{Z}$ i ciało $\mathbb{Q}$ jako znane twory. Natomiast w arytmetyce teoretycznej ciało liczb wymiernych definiuje się jako ciało ułamków pierścienia liczb całkowitych. Więcej informacji na ten temat można znaleźć na przykład w książce A. Grzegorczyka pt. *Zarys arytmetyki teoretycznej*.

Niech R będzie pierścieniem całkowitym. Wówczas pierścień wielomianów $R[x]$ też jest pierścieniem całkowitym. Jego ciało ułamków oznaczamy przez $R(x)$ i nazywamy *ciałem wyrażeń wymiernych* (lub *ciałem funkcji wymiernych*, mimo, że nie traktujemy elementów tego ciała jako funkcji). Wyrażenia wymierne mają więc postać:

$$\frac{f}{g} = \frac{a_0 + \ldots + a_n x^n}{b_0 + \ldots + b_m x^m},$$

gdzie $g = b_0 + \ldots + b_m x^m$ jest wielomianem niezerowym.

Przykład 1. Zdefiniujmy w zbiorze $\mathbb{Z}_6 \times \mathbb{Z}_6 \setminus \{0\}$ relację $\sim$ tak jak to uczyniliśmy przy konstrukcji ciała ułamków:

$$\langle a, b\rangle \sim \langle c, d\rangle \Longrightarrow ad = bc.$$

Jak łatwo sprawdzić, relacja ta jest zwrotna oraz symetryczna, ale nie jest przechodnia. Wynika stąd, że dla pierścienia $(\mathbb{Z}_6, +_6, \cdot_6)$ nie można skonstruować ciała ułamków.

Rozdział 14

Ciało algebraicznie domknięte

W niniejszym rozdziale wprowadzamy pojęcia ciała algebraicznie domkniętego i omawiamy jeden z najważniejszych przykładów takiego ciała – ciało liczb zespolonych.

Poniżej pokazujemy, że każde ciało posiada rozszerzenie będące ciałem algebraicznie domkniętym.

Lemat 14.1 *Niech K będzie ciałem, zaś $f \in K[x]$ wielomianem nierozkładalnym stopnia ≥ 1. Wtedy istnieje ciało L będące rozszerzeniem ciała K takie, że wielomian f ma pierwiastek w L.*

Dowód. oznaczmy przez I ideał pierścienia $K[x]$ generowany przez wielomian f. $K[x]$ jest całkowitym pierścieniem ideałów głównych, więc wobec twierdzenia 11.34, ideał I jest maksymalny. Na mocy twierdzenia 10.6, pierścień ilorazowy $K[x]/I$ jest ciałem. Jak łatwo zauważyć, odwzorowanie $\varphi : K \longrightarrow K[x]/I$ określone wzorem $\varphi(a) = a + I$ jest homomorfizmem pierścieni. φ jest ponadto różnowartościowe, albowiem dla dowolnych $a, b \in K$ mamy:

$$\varphi(a) = \varphi(b) \Longrightarrow a + I = b + I \Longrightarrow a - b \in I \Longrightarrow f | a - b \Longrightarrow a = b.$$

Ostatnia implikacja wynika stąd, że $\mathrm{st}(f) \geq 1$.

Rozważmy teraz zbiór $L = K \cup X$, gdzie X jest pewnym zbiorem rozłącznym z K oraz równolicznym ze zbiorem $(K[x]/I) \setminus Im(\varphi)$. Niech ponadto $G : L \longrightarrow K[x]/I$ będzie bijekcją taką, że $G(x) = \varphi(x)$ dla $x \in K$. W L definiujemy działania:

$$\begin{aligned} a \oplus b &= G^{-1}(G(a) + G(b)), \\ a \odot b &= G^{-1}(G(a) \cdot G(b)), \end{aligned}$$

przy czym $+$ i $\cdot$ oznaczają dodawanie i mnożenie (odpowiednio) w ciele $K[x]/I$. Nietrudno pokazać, że $(L, \oplus, \odot)$ jest ciałem izomorficznym z $K[x]/I$, zaś K jest podciałem ciała L. Ponadto G i G^{-1} są izomorfizmami ciał.

Na koniec pokażemy, że $a = G^{-1}(x + I) \in L$ jest pierwiastkiem wielomianu f.

$$\begin{aligned} f(a) &= f(G^{-1}(x + I)) = a_0 + a_1 G^{-1}(x + I) + \ldots + a_n [G^{-1}(x + I)]^n = \\ &= G^{-1}(G(a_0)) + G^{-1}(G(a_1)) G^{-1}(x + I) + \ldots + G^{-1}(G(a_n)) [G^{-1}(x + I)]^n = \\ &= G^{-1}((a_0 + I) + (a_1 + I)(x + I) + \ldots + (a_n + I)(x^n + I)) = \\ &= G^{-1}(a_0 + a_1 x + \ldots + a_n x^n + I) = G^{-1}(f + I) = G^{-1}(0 + I) = 0. \end{aligned}$$

■

Używając powyższego lematu można dowieść następujący lemat.

Lemat 14.2 *Niech K będzie ciałem. Wtedy istnieje ciało L będące rozszerzeniem ciała K takie, że każdy wielomian $f \in K[x]$ ma pierwiastek w L.*

Lemat 14.3 *Niech K będzie ciałem. Wtedy istnieje ciało L będące rozszerzeniem ciała K takie, że każdy wielomian $f \in L[x]$ ma pierwiastek w L.*

Dowód. Definiujemy indukcyjnie ciąg ciał: $K_0, K_1, K_2, \ldots$:

$K_0 = K$,

K_{n+1}: rozszerzenie ciała K_n takie, że każdy wielomian $f \in K_n[x]$ ma pierwiastek w K_{n+1}.

W ten sposób K_i jest podciałem ciała K_j dla $i \leq j$. Niech $L = \bigcup_{i=0}^{\infty} K_i$.

W zbiorze L definiujemy działania dodawania i mnożenia: Jeśli $a, b \in L$, to $a, b \in K_n$ dla pewnego $n \in \mathbb{N}$ i przyjmujemy $a \oplus b = a + b$ i $a \odot b = a \cdot b$, gdzie $+$ i $\cdot$ oznaczają dodawanie w K_n. Ponieważ K_i jest podciałem ciała K_j dla $i \leq j$, określenie działań $\oplus$ i $\odot$ nie zależy od wyboru n. Nietrudno sprawdzić, że $(L, \oplus, \odot)$ jest ciałem, zaś K jego podciałem.

Niech teraz $f \in L[x]$ będzie wielomianem stopnia ≥ 1. Ponieważ wielomian f posiada skończenie wiele współczynników i L jest sumą wstępującą ciał $K_0, K_1, K_2, \ldots$, istnieje $n \in \mathbb{N}$ takie, że $f \in K_n[x]$. Jak wiemy, f ma wówczas pierwiastek w K_{n+1}, a to oznacza, że ma pierwiastek w L. ■

Definicja 14.4 *Ciało K nazywamy algebraicznie domkniętym, jeśli dowolny wielomian $f \in K[x]$ stopnia ≥ 1 ma pierwiastek w K.*

Wniosek 14.5 *Każde ciało posiada rozszerzenie będące ciałem algebraicznie domkniętym.*

Twierdzenie 14.6 *Dowolne ciało algebraicznie domknięte jest nieskończone.*

Dowód. Niech K będzie ciałem skończonym. Rozważmy wielomian

$$f = (x - a_1) \cdot \ldots \cdot (x - a_n) + 1_K,$$

gdzie $a_1, \ldots, a_n$ są wszystkimi elementami ciała K. Wtedy $f(a) = 1_K \neq 0_K$ dla dowolnego $a \in K$, co oznacza, że wielomian f nie ma pierwiastka w ciele K. ■

Nietrudno zauważyć, że ciała $\mathbb{Q}$ i $\mathbb{R}$ nie są algebraicznie domknięte. Wynika to z faktu, iż wielomian $x^2 + 1$ nie ma pierwiastka w żadnym z nich. Poniżej udowodnimy, że ciało liczb zespolonych jest algebraicznie domknięte.

Lemat 14.7 *Jeśli $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$ jest wielomianem stopnia $n \geq 1$ oraz $A > 0$, to istnieje $r > 0$ takie, że*

$$(\forall z \in \mathbb{C})(|z| > r \Longrightarrow |f(z)| > A).$$

Dowód. Wybierzmy liczbę rzeczywistą $r > 0$ taką, że

$$r > 1, r > \frac{2A}{|a_n|} \text{ oraz } r > 2n \left| \frac{a_{n-k}}{a_n} \right| \text{ dla } k = 1, \ldots, n.$$

Wtedy dla $|z| \geq r$ oraz $k \in \{1, \ldots, n\}$ mamy:

$$\left| \frac{a_{n-k}}{a_n} \right| \frac{1}{|z|^k} \leq \left| \frac{a_{n-k}}{a_n} \right| \frac{1}{r^k} \leq \left| \frac{a_{n-k}}{a_n} \right| \frac{1}{r} \leq \frac{1}{2n}.$$

Używając tej zależności dla $|z| > r$ otrzymujemy:

$$\begin{aligned}|f(z)| &= \left|a_n z^n \left(1 + \frac{a_{n-1}}{a_n z} + \ldots + \frac{a_1}{a_n z^{n-1}} + \frac{a_0}{a_n z^n}\right)\right| \geq \\ &\geq |a_n| \cdot |z|^n \left(1 - \left|\frac{a_{n-1}}{a_n}\right| \cdot \frac{1}{|z|} - \ldots - \left|\frac{a_1}{a_n}\right| \frac{1}{|z|^{n-1}} - \left|\frac{a_0}{a_n}\right| \frac{1}{|z|^n}\right) \geq \\ &\geq |a_n| r^n \left(1 - \underbrace{\frac{1}{2n} - \ldots - \frac{1}{2n}}_{n\text{razy}}\right) = \frac{1}{2}|a_n| r^n \geq \frac{1}{2}|a_n| r > A.\end{aligned}$$

■

Poniższy lemat powinien być znany Czytelnikowi z kursu analizy matematycznej.

Lemat 14.8 *Dla liczby rzeczywistej dodatniej r definiujemy*

$$B_r = \{\langle x, y\rangle \in \mathbb{R}^2 : x^2 + y^2 \leq r\}$$

(koło domknięte o środku $\langle 0, 0\rangle$ i promieniu r). Jeśli $g : B_r \longrightarrow \mathbb{R}$ jest funkcją ciągłą, to istnieje para $\langle x_0, y_0\rangle \in B_r$ taka, że

$$g(x_0, y_0) = \inf_{\langle x,y\rangle \in B_r} g(x, y).$$

Z lematu 14.8 natychmiast wynika następujący wniosek.

Wniosek 14.9 *Niech $r > 0$ i $D_r = \{z \in \mathbb{C} : |z| \leq r\}$. Jeśli $f \in \mathbb{C}[x]$, to istnieje liczba zespolona $z_0 \in B$ taka, że*

$$|f(z_0)| = \inf_{z \in B} |f(z)|.$$

Lemat 14.10 *Niech $f = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{C}[x]$ będzie wielomianem stopnia $n \geq 1$, zaś z_0 liczbą zespoloną, która nie jest pierwiastkiem f. Wtedy istnieje $h \in \mathbb{C}$ takie, że $|f(z_0 + h)| < |f(z_0)|$.*

Dowód. Istnieją $b_0, b_1, \ldots, b_n \in \mathbb{C}$ takie, że

$$f(z_0 + h) = a_n(z_0 + h)^n + \ldots + a_1(z_0 + h) + a_0 = b_n h^n + \ldots + b_1 h + b_0 \text{ dla } h \in \mathbb{C}.$$

Stąd wynika, że $b_0 = f(z_0) \neq 0$ i $b_n = a_n \neq 0$. Zatem wśród współczynników $b_1, \ldots, b_n$ jest co najmniej jeden różny od zera. Niech b_k oznacza pierwszy z nich. Tak więc $f(z_0 + h) = b_0 + b_k h^k + \ldots + b_n h^n$.

Niech $c = -\frac{b_0|b_k|}{b_k|b_0|}$. Ustalmy liczbę $\alpha \in \mathbb{C}$ taką, że $\alpha^k = c$. $|c| = 1$, więc również $|\alpha| = 1$. Niech ϱ będzie dowolną liczbą rzeczywistą dodatnią taką, że:

$$\varrho < 1,\ \varrho < \frac{|b_0|}{|b_k|} \text{ i (gdy } k < n)\ \varrho < \frac{|b_k|}{|b_{k+1}| + \ldots + |b_n|}.$$

Przyjmijmy ponadto, że $h = \varrho\alpha$. Wtedy

$$\begin{aligned}|b_0 + b_k h^k| &= |b_0 + b_k \varrho^k \alpha^k| = |b_0| \cdot \left|1 + \frac{b_k \varrho^k c}{b_0}\right| = \\ &= |b_0| \cdot \left|1 - \varrho^k \frac{|b_k|}{|b_0|}\right| = |b_0| \cdot \left(1 - \varrho^k \frac{|b_k|}{|b_0|}\right) = |b_0| - \varrho^k |b_k|.\end{aligned}$$

Jeśli $k = n$, to

$$|f(z_0 + h)| = |b_0 + b_k h^k| = |b_0| - \varrho^k |b_k| < |b_0| = |f(z_0)|.$$

W przypadku, gdy $k < n$, mamy:

$$|b_{k+1}h^{k+1} + \ldots + b_n h^n| \leq |b_{k+1}| \cdot |h|^{k+1} + \ldots + |b_n| \cdot |h|^n = |b_{k+1}| \cdot \varrho^{k+1}|\alpha|^{k+1} + \ldots + |b_n|\varrho^n|\alpha|^n = |b_{k+1}|\varrho^{k+1} + \ldots + |b_n|\varrho^n \leq \varrho^{k+1}\left(|b_{k+1}| + \ldots + |b_n|\right) < \varrho^k|b_k|.$$

Zatem

$$|f(z_0 + h)| = |b_0 + b_k h^k + \ldots + b_n h^n| \leq |b_0 + b_k h^k| + |b_{k+1}h^{k+1} \ldots + b_n h^n| < < (|b_0| - |b_k|\varrho^k) + |b_k|\varrho^k = |b_0| = |f(z_0)|.$$

■

Twierdzenie 14.11 *(Zasadnicze twierdzenie algebry)* $(\mathbb{C}, +, \cdot)$ *jest ciałem algebraicznie domkniętym.*

Dowód. Załóżmy nie wprost, że ciało $(\mathbb{C}, +, \cdot)$ nie jest algebraicznie domknięte. Wtedy istnieje wielomian $f \in \mathbb{C}[x]$ stopnia przynajmniej 1 nie mający pierwiastka w $\mathbb{C}$. Niech $A = 1 + \inf\limits_{z\in\mathbb{C}} |f(z)|$. Tak więc $|A| \geq 1$. Na mocy lematu 14.7 istnieje $r > 0$ takie, że

$$(\forall z \in \mathbb{C})(|z| > r \Longrightarrow |f(z)| > A).$$

Zatem

$$\inf_{z\in\mathbb{C}} |f(z)| = \inf_{|z|\leq r} |f(z)|.$$

Na mocy wniosku 14.9 istnieje $z_0 \in \mathbb{C}$ takie, że $|z_0| \leq r$ i

$$|f(z_0)| = \inf_{|z|\leq r} |f(z)| = \inf_{z\in\mathbb{C}} |f(z)|.$$

Z założenia $f(z_0) \neq 0$, zatem wobec lematu 14.10 istnieje $h \in \mathbb{C}$ takie, że $|f(z_0 + h)| < |f(z_0)|$. To zaś oznacza, że

$$\inf_{z\in\mathbb{C}} |f(z)| < |f(z_0)|.$$

Otrzymana sprzeczność kończy dowód. ■

Rozdział 15

Ciała skończone

W rozdziale siódmym wykazaliśmy, że jeśli p jest liczbą pierwszą, to $(\mathbb{Z}_p, +_p, \cdot_p)$ jest ciałem (przykład 16, strona 62). Ponadto podaliśmy przykład ciała czteroelementowego (przykład 17, strona 63). Poniżej udowodnimy, że liczba elementów dowolnego ciała skończonego jest potęgą liczby pierwszej.

Lemat 15.1 *Jeśli K jest ciałem skończonym, to jego charakterystyka jest liczbą pierwszą.*

Dowód. Niech K będzie ciałem skończonym. Wiemy już, że charakterystyka dowolnego ciała wynosi 0 lub jest liczbą pierwszą (wniosek 7.19). Wystarczy zatem wykazać, że $\chi(K) \neq 0$.

Skończoność ciała K implikuje, że istnieją liczby naturalne dodatnie m i n takie, że $1 < m < n$ i

$$\underbrace{1_K + \ldots + 1_K}_{m \text{ razy}} = \underbrace{1_K + \ldots + 1_K}_{n \text{ razy}}.$$

Stąd zaś na mocy prawa skracań wynika, że

$$\underbrace{1_K + \ldots + 1_K}_{n-m \text{ razy}} = 0_K.$$

Tak więc $\chi(K) \neq 0$. ■

Twierdzenie 15.2 *Jeśli K jest ciałem skończonym o charakterystyce p (p jest liczbą pierwszą), to $|K| = p^n$ dla pewnej liczby naturalnej dodatniej n.*

Dowód. Załóżmy, że K jest ciałem skończonym o charakterystyce p. Wtedy

$$L = \{1_K, 1_K + 1_K, \ldots, \underbrace{1_K + \ldots + 1_K}_{p \text{ razy}}\}$$

jest podciałem ciała K, a więc K jest przestrzenią liniową nad L. Niech $\{x_1, \ldots, x_n\}$ będzie bazą tej przestrzeni liniowej. Każdy element $x \in K$ można jednoznacznie przedstawić w postaci kombinacji liniowej elementów $x_1, \ldots, x_n$:

$$x = \alpha_1 x_1 + \ldots + \alpha_n x_n,$$

gdzie $\alpha_1, \ldots, \alpha_n \in L$. Ponieważ każdy współczynnik powyższej kombinacji możemy wybrać na p sposobów, istnieje dokładnie p^n kombinacji liniowych elementów $x_1, \ldots, x_n$ o współczynnikach z ciała L. Tak więc liczba elementów ciała K wynosi p^n. ■

Twierdzenie 15.3 *Grupa multyplikatywna dowolnego ciała skończonego jest cykliczna.*

Dowód. Niech K będzie ciałem skończonym. Jego grupa multyplikatywna, $(K \setminus \{0_K\}, \cdot)$, jest skończoną grupą abelową, a więc na mocy wniosku 6.12 jest sumą prostą skończenie wielu grup cyklicznych. Załóżmy nie wprost, że grupa ta nie jest cykliczna. Wówczas zawiera ona pewną podgrupę H izomorficzną z $\mathbb{Z}_p \oplus \mathbb{Z}_p$ (twierdzenie 6.13), gdzie p jest liczbą pierwszą. Nietrudno sprawdzić, że każdy niezerowy element grupy $\mathbb{Z}_p \oplus \mathbb{Z}_p$ ma rząd równy p. Ponieważ $\mathbb{Z}_p \oplus \mathbb{Z}_p \cong (H, \cdot) < (K \setminus \{0_K\}, \cdot)$, każdy element grupy $(H, \cdot)$ różny od 1 ma rząd równy p. To zaś oznacza, że wielomian $f = x^p - 1$ ma w ciele K przynajmniej p^2 pierwiastków. Jak wiemy z twierdzenia 9.12, niezerowy wielomian o współczynnikach z ciała K nie może mieć w tym ciele więcej pierwiastów niż wynosi jego stopień. Otrzymana sprzeczność kończy dowód. ■

Wniosek 15.4 *Jeśli p jest liczbą pierwszą, to grupy $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ i $(\mathbb{Z}_{p-1}, +_{p-1})$ są izomorficzne.*

Dowód. Niech p będzie liczbą pierwszą. Z twierdzenia 15.3 wynika, że grupa $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ jest cykliczna. Na mocy twierdzenia 6.5 jest ona izomorficzna z grupą $(\mathbb{Z}_{p-1}, +_{p-1})$. ■

Twierdzenie 15.5 *Niech p będzie liczbą pierwszą . Jeśli K jest ciałem skończonym o charakterystyce p, to odwzorowanie $f : K \longrightarrow K$ określone wzorem $f(x) = x^p$ jest automorfizmem ciała K. Automorfizm ten nazywamy automorfizmem Frobeniusa*[1]*.*

Dowód. Niech K będzie ciałem skończonym o charakterystyce p i niech $f(x) = x^p$ dla $x \in K$. Na mocy twierdzenia 7.15 mamy: $f(x+y) = (x+y)^p = x^p + y^p = f(x) + f(y)$. Ponadto $f(xy) = (xy)^p = x^p y^p = f(x)f(y)$. Tak więc f jest homomorfizmem.

Pokażemy teraz, że f jest odwzorowaniem różnowartościowym. Załóżmy, że x i y są takimi elementami ciała K, dla których $f(x) = f(y)$. Wtedy $0 = f(x) - f(y) = f(x-y)$, co oznacza, że $(x-y)^p = 0$. Ponieważ ciało nie posiada dzielników zera, dostajemy stąd $x - y = 0$, czyli $x = y$. Dowiedliśmy w ten sposób, że f jest odwzorowaniem różnowartościowym. Ponieważ K jest zbiorem skończonym, f jest też surjekcją. Zatem f jest automorfizmem ciała K. ■

Poniższe dwa twierdzenia wraz z twierdzeniem 15.2 pozwalają na sklasyfikowanie wszystkich ciał skończonych.

Twierdzenie 15.6 *Jeśli $n > 1$ jest potęgą liczby pierwszej, to istnieje ciało n-elementowe.*

Twierdzenie 15.7 *Każde dwa ciała skończone o tej samej liczbie elementów są izomorficzne.*

[1] C. Frobenius (1849-1917), matematyk niemiecki

Spis oznaczeń

$\mathbb{N}$	zbiór liczb naturalnych
$\mathbb{N}_+$	zbiór liczb naturalnych dodatnich
$s(n)$	następnik liczby naturalnej n
$\mathbb{Z}$	zbiór liczb całkowitych
$\mathbb{Q}$	zbiór liczb wymiernych
$\mathbb{Q}_+$	zbiór liczb wymiernych dodatnich
$\mathbb{R}$	zbiór liczb rzeczywistych
$\mathbb{R}_+$	zbiór liczb rzeczywistych dodatnich
$\mathbb{C}$	zbiór liczb zespolonych
$\|z\|$	moduł liczby zespolonej z
NWD	największy wspólny dzielnik
NWW	najmniejsza wspólna wielokrotność
$a\|b$	a dzieli b
$m \bmod n$	reszta z dzielenia liczby m przez n
$+_n, \cdot_n$	dodawanie i mnożenie modulo n
$a \equiv b (\bmod n)$	a przystaje do b modulo n
$\|X\|$	moc (liczba elementów) zbioru X
$\mathcal{P}(X)$	zbiór podzbiorów zbioru X
$\langle a, b\rangle$	para uporządkowana
$\langle a_0, a_1, \dots a_n\rangle$	ciąg elementów
$\triangle$	różnica symetryczna zbiorów
Id_X	odwzorowanie identycznościowe w zbiorze X
Y^X	zbiór funkcji odwzorowujących X w Y
e_G	element neutralny w grupie G
a^{-1}	element odwrotny do a
$\mathbb{Z}_n, (\mathbb{Z}_n, +_n)$	grupa reszt modulo n
C_n	grupa cykliczna rzędu n
$M_{m\times n}(\mathbb{R})$	Zbiór macierzy wymiaru $m \times n$ o wyrazach z $\mathbb{R}$
$GL(n, \mathbb{R})$	Zbiór macierzy nieosobliwych wymiaru $n \times n$ o wyrazach z $\mathbb{R}$
$SL(n, \mathbb{R})$	Zbiór macierzy wymiaru $n \times n$ o wyrazach z $\mathbb{R}$ i wyznaczniku 1
K_4	grupa czwórkowa Kleina
Q_8	grupa kwaternionów
D_n	grupa izometrii własnych n-kąta foremnego
$G(n)$	$\{k \in \{0, \dots, n-1\} : NWD(k, n) = 1\}$
$\varphi(n)$	funkcja Eulera
$G \oplus H$, $R \oplus S$	suma prosta grup, pierścieni
$(a_1, \dots, a_k)$	cykl długości k
(i, j)	transpozycja zamieniająca miejscami liczby i, j
S_n	grupa permutacji zbioru $\{1, \dots, n\}$
S_X	grupa permutacji niepustego zbioru X

$H < G$	H jest podgrupą grupy G
$H \triangleleft G$	H jest dzielnikiem normalnym grupy G
aH	warstwa lewostronna podgrupy H zawierająca element a
Ha	warstwa prawostronna podgrupy H zawierająca element a
$\langle A \rangle_G$	podgrupa generowana przez zbiór A w grupie G
$0_R, 1_R$	zero i jedność pierścienia R
Ker(f)	jądro homomorfizmu f (grup, pierścieni)
Im(f)	obraz homomorfizmu f (grup pierścieni)
$Aut(G), Aut(R)$	grupa automorfizmów grupy G, pierścienia R
$G/H, R/I$	grupa ilorazowa, pierścień ilorazowy
$\cong$	relacja izomorfizmu
$\mathbb{Z}_n, (\mathbb{Z}_n, +_n, \cdot_n)$	pierścień reszt modulo n
$\mathbb{Z}[i]$	pierścień Gaussa
$\mathbb{F}_p$	ciało $(\mathbb{Z}_p, +_p, \cdot_p)$
$U(R)$	zbiór elementów odwracalnych pierścienia R
$I \triangleleft R$	I jest ideałem pierścienia R
$I + J$	suma ideałów
$I \cdot J$	iloczyn ideałów
$I : J$	iloraz ideałów
rad(I)	radykał idału I
aR, (a)	ideał generowany przez a w pierścieniu R
$a + I$	warstwa ideału I zawierająca element a
$R[x]$	pierścień wielomianów jednej zniennej nad R
$R[x_1, \ldots, x_n]$	pierścień wielomianów n zmiennych nad R
$f', f'', f^{(n)}$	pochodne wielomianu lub funkcji f rzędów $1, 2, n$

Indeks

Bibliografia

[BB1] A. Białynicki-Birula, *Algebra*, PWN, Warszawa 1976.

[BB2] A. Białynicki-Birula, *Zarys algebry*, PWN, Warszawa 1987.

[BJ] M. Bryński, J. Jurkiewicz, *Zbiór zadań z algebry*, PWN, Warszawa 1985.

[Ca] F. Cajori, *A History of Mathematics*, Chalsea Publishing Company, New York 1991.

[Gl] B. Gleichgewicht, *Algebra. Podręcznik dla kierunków nauczycielskich studiów matematycznych*, PWN, Warszawa 1976.

[Gr] A. Grzegorczyk, *Zarys arytmetyki teoretycznej*, PWN, Warszawa 1983.

[Ko] A.I. Kostrikin, *Wstęp do algebry*, PWN, Warszawa 1984.

[La] S. Lang, *Algebra*, PWN, Warszawa 1984.

[MS] A. Mostowski, M. Stark, *Elementy algebry wyższej*, PWN, Warszawa 1958.

[Si] W. Sierpiński, *Wstęp do teorii liczb*, WSiP, Warszawa 1987.

[Sz] K. Szymiczek, *Zbiór zadań z teorii grup*, PWN, Warszawa 1989.

[W1] W. Więsław, *Algebra geometryczna*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 1974.

[W2] W. Więsław, *Grupy, pierścienie, ciała*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 1983.