Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

Algebra 1

Ewa Cygan, Maciej Ulas

Kraków, 2021

Spis treści

Wstęp

Oznaczenia i konwencje

1. Moc zbioru X oznaczamy przez $|X|$ lub $\#X$.
2. Funkcja „signum” jest określona na zbiorze liczb rzeczywistych, następująco

$$\operatorname{sgn}(a) := \begin{cases} -1, & \text{gdy } a < 0, \\ 0, & a = 0, \\ 1, & \text{gdy } a > 0. \end{cases}$$

Ponadto przyjmujemy oznaczenia:

$$\begin{aligned} \mathbb{N} &= \text{zbiór liczb naturalnych } = \{1, 2, \ldots\}, \\ \mathbb{N}_0 &= \text{zbiór liczb naturalnych z zerem } = \{0, 1, 2, \ldots\}, \\ \mathbb{Z} &= \text{zbiór liczb całkowitych}, \qquad \mathbb{Z}^\star = \mathbb{Z} \setminus \{0\}, \\ \mathbb{Q} &= \text{zbiór liczb wymiernych}, \qquad \mathbb{Q}^\star = \mathbb{Q} \setminus \{0\}, \\ \mathbb{R} &= \text{zbiór liczb rzeczywistych}, \quad \mathbb{R}^\star = \mathbb{R} \setminus \{0\}, \\ \mathbb{C} &= \text{zbiór liczb zespolonych}, \qquad \mathbb{C}^\star = \mathbb{C} \setminus \{0\}, \\ \mathbb{P} &= \text{zbiór liczb pierwszych } = \{2, 3, 5, \ldots\}, \\ A_{\geqslant k} &= \{a \in A : \ a \geqslant k\}, \text{ gdzie } A \text{ jest ustalonym zbiorem liczbowym.} \end{aligned}$$

Rozdział 1

Podstawy teorii liczb

Celem tego rozdziału jest zaznajomienie Czytelnika z podstawowymi wynikami teorii liczb, które są interesujące nie tylko same w sobie, ale znajdą również zastosowanie w dalszych rozdziałach i niejednokrotnie będą motywacją do wprowadzenia nowych pojęć (i badania ich własności).

1.1 Podzielność w $\mathbb{Z}$

Definicja 1.1.1 (podzielność w $\mathbb{Z}$)**.** Niech a, $b \in \mathbb{Z}$. Mówimy, że b **dzieli** a (lub inaczej b jest dzielnikiem a), gdy istnieje taka liczba $c \in \mathbb{Z}$, że $a = bc$.

W dalszej części wykładu dla oznaczenia podzielności a przez b, będziemy krótko pisać: $b|a$; dla oznaczenia braku podzielności pisać będziemy: $b \nmid a$.

Zauważmy, że wprost z definicji wynika zestaw poniższych, podstawowych własności podzielności, których uzasadnienie jest dobrym ćwiczeniem – pozostawiamy je więc Czytelnikowi.

Uwaga 1.1.2 (własności podzielności w $\mathbb{Z}$)**.** Niech $a, b, c, m, n \in \mathbb{Z}$. Wtedy:

(1) $1|a$, $a|0$,

(2) jeśli $0|a$, to $a = 0$,

(3) relacja podzielności rozważana na $\mathbb{Z}^\star$ jest zwrotna i przechodnia,

(4) ($b|a$ i $a|b$) wtedy i tylko wtedy, gdy $|a| = |b|$,

(5) jeśli $c|a$, $c|b$, to $c|(am + nb)$,

(6) jeśli $a|b$ i $b \neq 0$, to $1 \leqslant |a| \leqslant |b|$.

Przedstawimy poniżej dwie wersje twierdzenia o algorytmie dzielenia z resztą w zbiorze liczb całkowitych. Pierwsza z tych wersji (wersja A) stanowi przygotowanie do przyszłego uogólnienia omawianej własności do bardziej abstrakcyjnej sytuacji pierścienia euklidesowego (por. 4.6.1). Druga – szerzej znana wersja (wersja B), jest szczególnie wygodna w zastosowaniach.

Twierdzenie 1.1.3 (algorytm dzielenia z resztą – wersja A)**.** *Niech a, b – liczby całkowite, $b \neq 0$. Wtedy istnieje para $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ spełniająca następujące warunki:*

(1) $a = bq + r$, (2) $|r| < |b|$.

*Liczbę q nazywamy **wynikiem** dzielenia, zaś liczbę r – **resztą** z dzielenia.*

Zaletą tej wersji twierdzenia jest pewna „kanoniczność wypowiedzi" drugiej z własności. Zauważmy bowiem, że mówi ona o sposobie „porównania" ze sobą reszty z dzielenia i dzielnika występującego w założeniach: nie odwołujemy się tu do żadnych innych własności tych elementów jak to będzie we wspomnianym dalej ogólniejszym rezultacie, z którego pierwszej części bezpośrednim wnioskiem jest twierdzenie 1.1.3.

Twierdzenie 1.1.4 (algorytm dzielenia z resztą – wersja B)**.** *Niech $a, b \in \mathbb{Z}$ gdzie $b \neq 0$. Wtedy:*

(•) *istnieje dokładnie jedna taka para $(q, r) \in \mathbb{Z} \times \mathbb{Z}$, że:*

(1) $a = bq + r$, *(2)* $0 \leqslant r < |b|$,

(•) *jeśli dodatkowo $b \nmid a$, to istnieją dokładnie dwie takie pary (q, r) dla których:*

(1) $a = bq + r$, *(2)* $|r| < |b|$.

Dowód. Udowodnimy pierwszą część twierdzenia 1.1.4.

Istnienie reszty. Niech $S := \{a - kb,\ k \in \mathbb{Z},\ a - kb \geqslant 0\}$. Wtedy S jest niepustym podzbiorem $\mathbb{N}_0$, wobec tego ma element najmniejszy, który oznaczymy jako r. Element ten jest postaci $r = a - qb$ dla pewnego $q \in \mathbb{Z}$, zaś z jego określenia widzimy, że spełniona jest nierówność $0 \leqslant r$ oraz zależność $a = qb + r$.

Pozostaje jedynie pytanie, czy $r < |b|$? Udowodnimy tę część nie wprost. Gdyby $r \geqslant |b|$, to $r - |b| \geqslant 0$ oraz $r - |b| = a - qb - |b| = a - (q + \operatorname{sgn}(b))b$, więc $r - |b| \in S$ oraz $r - |b| < r$ (skoro $b \neq 0$, to $|b| \geqslant 1$). Dostajemy sprzeczność z wyborem r.

Jednoznaczność reszty nieujemnej. Ponownie dla dowodu nie wprost załóżmy, że $a = bq_1 + r_1 = bq_2 + r_2$, $0 \leqslant r_1 < |b|$, $0 \leqslant r_2 < |b|$ i na przykład $r_1 < r_2$, czyli oczywiście $q_1 - q_2 \neq 0$. Ponieważ $b(q_1 - q_2) = r_2 - r_1$ otrzymujemy w konsekwencji $|b| \leqslant |b||q_1 - q_2| = |r_2 - r_1| = (r_2 - r_1) < |b|$, co prowadzi do sprzeczności. W analogiczny sposób rozumujemy w przypadku, gdy $r_2 < r_1$.

Zachęcamy do udowodnienia we własnym zakresie drugiej części twierdzenia 1.1.4. □

1.2 NWD i NWW w $\mathbb{Z}$

Pojęcia największego wspólnego dzielnika i najmniejszej wspólnej wielokrotności liczb całkowitych są fundamentalne w teorii liczb. Ich podstawowa definicja jest ściśle związana z istnieniem porządku w zbiorze liczb całkowitych. Należy jednak zaznaczyć, że istnieje definicja tych pojęć w ogólniejszych strukturach algebraicznych, w których na ogół nie możemy mówić o pojęciu „najmniejszy" czy „największy". Wspomnianą definicję przedstawimy w dalszej części naszych rozważań (4.7.13), gdy spojrzymy na zbiór liczb całkowitych przez pryzmat kanonicznie zadanej struktury pierścienia.

Definicja 1.2.1 (NWD, NWW, względna pierwszość)**.**

(1) **Największym wspólnym dzielnikiem** liczb $a_1, \ldots, a_r \in \mathbb{Z}$ (zakładamy, że przynajmniej jedna z liczb jest niezerowa), nazywamy największą liczbę całkowitą, która dzieli każdą z liczb $a_1, \ldots, a_r$.[1]

Oznaczenie: $\operatorname{NWD}(a_1, \ldots, a_r)$ (w literaturze również: $(a_1, \ldots, a_r)$)

(2) **Najmniejszą wspólną wielokrotnością** niezerowych liczb całkowitych $a_1, \ldots, a_r$ nazywamy najmniejszą liczbę całkowitą dodatnią, która jest podzielna przez każdą z liczb $a_1, \ldots, a_r$.

Oznaczenie: $\operatorname{NWW}(a_1, \ldots, a_r)$ (w literaturze również: $[a_1, \ldots, a_r]$)

(3) Liczby $a_1, \ldots, a_r \in \mathbb{Z}$, z których przynajmniej jedna jest niezerowa, nazywamy **względnie pierwszymi**, gdy $\operatorname{NWD}(a_1, \ldots, a_r) = 1$.

Uwaga 1.2.2. Zauważmy, że z określenia $\operatorname{NWD}(a, b)$ wynika, że dla $a, b \in \mathbb{Z}^\star$ prawdziwe są równości:

$$\operatorname{NWD}(a, b) = \operatorname{NWD}(b, a) = \operatorname{NWD}(\pm a, \pm b),$$

dla dowolnej kombinacji znaków $\pm$.

Przedstawimy teraz metodę wyznaczania największego wspólnego dzielnika dwóch liczb całkowitych a i b, która nosi nazwę **algorytmu Euklidesa**[2]. Oczywiście, jeśli $a \in \mathbb{Z}^\star$, $b = 0$, to $\operatorname{NWD}(a, b) = |a|$. W dalszej części naszych rozważań zakładamy więc, że obie liczby są niezerowe.

[1] Zauważmy, że stwierdzenie największa liczba ma tutaj sens: rozważamy naturalny porządek w zbiorze liczb całkowitych, zaś potencjalne dzielniki są ograniczone z góry przez każde $|a_i|$.

[2] Euklides: matematyk grecki, głównie działający w Aleksandrii (ok. 364–300 p.n.e. dokładne daty nie są znane), autor m.in. jednego z najbardziej znanych dzieł matematycznych pt. *Elementy*.

Algorytm Euklidesa[3]

Ustalmy dwie liczby całkowite $a, b \in \mathbb{Z}^\star$. Przyjmijmy: $r_{-1} := a$, $r_0 := |b|$.

Krok 1: Zgodnie z algorytmem dzielenia z resztą (1.3.(B) (•)) istnieją takie liczby całkowite $q_1, r_1 \in \mathbb{Z}$ dla których:

(1) $a = r_{-1} = q_1|b| + r_1$,

(2) $0 \leqslant r_1 < |r_0| = |b|$.

Jeśli $r_1 = 0$, to kończymy algorytm. Jeśli $r_1 \neq 0$, to wykonujemy Krok 2.

Krok 2: Ponownie na podstawie algorytmu dzielenia z resztą tak dobieramy liczby całkowite $q_2, r_2 \in \mathbb{Z}$ aby:

(1) $r_0 = q_2 r_1 + r_2$,

(2) $0 \leqslant r_2 < r_1 < |r_0| = |b|$.

Jeśli $r_2 = 0$, to kończymy algorytm. Jeśli $r_2 \neq 0$, to kontynuujemy analogicznie jak wyżej.

Ogólnie, mając r_{i-2}, r_{i-1} takie, że $r_{i-1} \neq 0$, wykonujemy kolejny krok:

Krok (i >1): Istnieją liczby całkowite $q_i, r_i \in \mathbb{Z}$:

(1) $r_{i-2} = q_i r_{i-1} + r_i$,

(2) $0 \leqslant r_i < r_{i-1}$.

Ze względu na nierówności: $0 \leqslant r_i < r_{i-1}$ istnieje takie $N(a,b) \in \mathbb{N}_0$ dla którego $r_{N(a,b)+1} = 0$, ale $r_{N(a,b)} \neq 0$.

Liczbę $N(a,b) \in \mathbb{N}_0$ będziemy nazywać dalej **długością algorytmu Euklidesa** dla liczb a i b (długość może być równa zero, gdy $b|a$), zaś $r(a,b) := r_{N(a,b)}$ **wynikiem** tego algorytmu.

Zanim przedstawimy związek algorytmu Euklidesa z wyznaczaniem największego wspólnego dzielnika liczb $a, b \in \mathbb{Z}^\star$ potrzebny nam będzie jeszcze jeden wynik.

Lemat 1.2.3. *Niech dla liczb $a, b \in \mathbb{Z}^\star$ zachodzi $a = qb + r$, gdzie $q, r \in \mathbb{Z}$ i $0 \leqslant r < |b|$. Wtedy zachodzi równość* $\mathrm{NWD}(a,b) = \mathrm{NWD}(b,r)$.

Dowód. Oznaczmy: $d := \mathrm{NWD}(a,b)$ i $d' := \mathrm{NWD}(b,r)$ – wykażemy, że $d = d'$. Ponieważ $d|a$ i $d|b$, więc istnieją takie liczby $k_1, k_2 \in \mathbb{Z}$, że $a = dk_1$, $b = dk_2$. Z założenia otrzymujemy równość $r = a - qb = d(k_1 - qk_2)$. Oznacza to, że $d|r$ i w konsekwencji $d|d'$ (bo $d' = \mathrm{NWD}(b,r)$). W szczególności $d \leqslant d'$. Niech teraz $k_3, k_4 \in \mathbb{Z}$ będą takie, że $b = d'k_3$, $r = d'k_4$. Stąd $a = qb + r = d'(qk_3 + k_4)$ i dostajemy, że $d'|a$. Oznacza to, że d' jest wspólnym dzielnikiem a, r i prawdziwa jest nierówność $d' \leqslant d$ (bo $d = \mathrm{NWD}(a,b)$). Otrzymujemy zatem $d = d'$, co daje tezę. □

Wykażemy teraz, że prawdziwe jest następujące twierdzenie.

Twierdzenie 1.2.4. *Dla dowolnych dwóch niezerowych liczb całkowitych a, b zachodzi* $\mathrm{NWD}(a,b) = r_{N(a,b)}$.

Dowód. Dla uproszczenia oznaczmy $n := N(a,b)$. By dowieść naszego twierdzenia wykażemy równość $\mathrm{NWD}(a,b) = r_n$. Z określenia algorytmu Euklidesa wynika, że istnieją takie ciągi liczb całkowitych r_i, $i = 1, \ldots, n$, q_i, $i = 1, \ldots, n+1$, że spełnione są równości

$$a = q_1|b| + r_1,\ |b| = q_2 r_1 + r_2, \ldots, r_{n-2} = q_n r_{n-1} + r_n,\ r_{n-1} = q_{n+1} r_n,$$

gdzie $0 < r_n < r_{n-1} < \ldots < r_2 < r_1$. W konsekwencji, z lematu 1.2.3, otrzymujemy ciąg równości

$$\begin{aligned}\mathrm{NWD}(a,b) &= \mathrm{NWD}(|b|, r_1) = \mathrm{NWD}(r_1, r_2) = \ldots = \mathrm{NWD}(r_{n-2}, r_{n-1}) \\ &= \mathrm{NWD}(r_{n-1}, r_n) = \mathrm{NWD}(q_{n+1} r_n, r_n) = r_n,\end{aligned}$$

co dowodzi tezy. □

[3] Nazwa algorytm pochodzi od brzmienia fragmentu nazwiska arabskiego matematyka Muhammada ibn Musa al.-Chorezmiego, którego uznaje się za prekursora metod obliczeniowych w matematyce. Żył on na przełomie VIII i IX wieku, przyczynił się do upowszechnienia systemu dziesiętnego oraz wprowadził stosowanie zera jako symbolu oznaczającego „nic".

Gdy już wiemy, że dla danej pary liczb $a, b \in \mathbb{Z}^\star$ można łatwo wyznaczyć ich największy wspólny dzielnik pojawia się naturalne pytanie: jak duża jest liczba kroków konieczna do wyznaczenia $\mathrm{NWD}(a, b)$? Innymi słowy interesuje nas rozsądne oszacowanie liczby $N(a, b)$. Odpowiedź na tak sformułowane pytanie daje rezultat otrzymany przez Gabriela Lamégo.[4] Zanim go sformułujemy przypomnijmy pojęcie liczb Fibonacciego. By określić n-tą liczbę Fibonacciego F_n przyjmijmy $F_0 = 0$, $F_1 = 1$, zaś dla $n \geqslant 2$ połóżmy $F_n = F_{n-1} + F_{n-2}$. Jeśli oznaczymy teraz przez ϕ dodatni pierwiastek równania $x^2 - x - 1 = 0$, tzn. $\phi = \frac{1}{2}(1 + \sqrt{5})$, to można wykazać, że n-ta liczba Fibonacciego wyraża się tzw. wzorem Bineta postaci (dowód por. [5])

$$F_n = \frac{1}{\sqrt{5}} \left(\phi^n - \frac{1}{(-\phi)^n} \right).$$

Stosując indukcję ze względu na n oraz zależność rekurencyjną $F_n = F_{n-1} + F_{n-2}$ bez trudu można wykazać, że $F_n > \phi^{n-2}$.

Twierdzenie 1.2.5 (o liczbie kroków w algorytmie Euklidesa)**.** *Niech $a, b \in \mathbb{N}$ i niech $N(a, b)$ oznacza liczbę kroków w algorytmie Euklidesa wyznaczania* $\mathrm{NWD}(a, b)$*. Załóżmy, że $b < a$. Wtedy $N(a, b) \leqslant 5(\lfloor \log_{10} b \rfloor + 1)$.*

Dowód. Dla $a, b \in \mathbb{N}, b < a$, oznaczmy $n := N(a, b)$. Z twierdzenia 1.2.4 wiemy, że spełniona jest równość $\mathrm{NWD}(a, b) = r_n$. Z określenia algorytmu Euklidesa wynika, że istnieją takie ciągi liczb całkowitych r_i, $i = 1, \ldots, n$, q_i, $i = 1, \ldots, n + 1$, że spełnione są równości:

$$a = q_1 b + r_1,\ b = q_2 r_1 + r_2, \ldots, r_{n-2} = q_n r_{n-1} + r_n,\ r_{n-1} = q_{n+1} r_n,$$

$0 < r_n < r_{n-1} < \ldots < r_2 < r_1$. Ponadto, dla $i = 1, \ldots, n$, mamy, że $q_i \geqslant 1$ oraz $q_{n+1} \geqslant 2$. Otrzymujemy zatem, że

$$\begin{aligned}
r_n &\geqslant 1 = F_1, \\
r_{n-1} &\geqslant 2r_n \geqslant 2F_1 = F_2, \\
r_{n-2} &\geqslant r_{n-1} + r_n \geqslant F_2 + F_1 = F_3, \\
r_{n-3} &\geqslant r_{n-2} + r_{n-1} \geqslant F_3 + F_2 = F_4, \\
&\vdots \\
r_2 &\geqslant r_3 + r_2 \geqslant F_{n-2} + F_{n-3} = F_{n-1}, \\
r_1 &\geqslant r_2 + r_1 \geqslant F_{n-1} + F_{n-2} = F_n, \\
r_0 = b &\geqslant r_1 + r_0 \geqslant F_n + F_{n-1} = F_{n+1}.
\end{aligned}$$

W szczególności prawdziwa jest nierówność $b \geqslant F_{n+1}$ i jeśli $n \geqslant 2$, to otrzymujemy $b \geqslant \phi^{n-1}$. Ponieważ $\log_{10} \phi = 0.208988\ldots > \frac{1}{5}$, więc $\log_{10} b > \frac{1}{5}(n - 1)$ lub równoważnie

$$n \leqslant 5 \log_{10} b + 1.$$

Zauważmy teraz, że jeśli b ma m cyfr w zapisie dziesiętnym, to $b \leqslant 10^m$ i stąd $\log_{10} b < m$. W konsekwencji $n < 5m+1$ i ostatecznie $n \leqslant 5m$. Ponieważ prawdziwa jest równość $m = \lfloor \log_{10} b \rfloor + 1$, dostajemy tezę. □

Uwaga 1.2.6. Należy zauważyć, że teza w powyższym twierdzeniu nie może być wzmocniona. Istotnie, z dowodu wynika, jeśli $a = F_{n+1}, b = F_n$, to w nierównościach wiążących reszty r_{n-i} z liczbami Fibonacciego F_{i+1} dla $i = 0, \ldots, n$, mamy tak naprawdę równości, co jest konsekwencją rekurencji spełnianej przez liczby Fibonacciego.

Przejdziemy teraz do dowodu tak zwanej identyczności Bacheta–Bézouta (dalej w skrócie: BB), która dla ustalonych liczb całkowitych $a_1, \ldots, a_n$, umożliwia przedstawienie liczby $\mathrm{NWD}(a_1, \ldots, a_n)$ jako kombinacji liniowej liczb $a_1, \ldots, a_n$.

Twierdzenie 1.2.7 (identyczność Bacheta–Bézouta)**.** *Niech $a_1, \ldots, a_n \in \mathbb{Z}$ i załóżmy, że co najmniej jedna z tych liczb jest niezerowa. Wtedy istnieją takie liczby $k_1, \ldots, k_n \in \mathbb{Z}$, że spełniona jest równość*

$$\mathrm{NWD}(a_1, \ldots, a_n) = k_1 a_1 + \ldots + k_n a_n.$$

[4] Gabriel Lamé: matematyk i inżynier francuski, żyjący w latach 1795–1870, znany m.in. z prac w zakresie geometrii różniczkowej i wkładu w dowód Wielkiego Twierdzenia Fermata, które wykazał dla $n = 7$.

Dowód. Najpierw udowodnimy tezę dla dwóch liczb a, b z których co najmniej jedna jest niezerowa. W tym celu rozważmy zbiór $D = \{ax + by : ax + by > 0, x, y \in \mathbb{Z}\}$. Oczywiście, jedna z liczb $\pm a$, $\pm b$ należy do naszego zbioru, wobec tego zbiór ten jest niepusty. Ponieważ D zawiera wyłącznie liczby naturalne, to posiada element najmniejszy, powiedzmy $d > 0$. Istnieją więc takie liczby x_0, $y_0 \in \mathbb{Z}$, że $d = ax_0 + by_0$. Udowodnimy, że d jest poszukiwanym największym wspólnym dzielnikiem a i b.

Udowodnimy najpierw, że $d|a$. Z algorytmu dzielenia z resztą (1.1.4) wiemy, że istnieją takie liczby q, r, że $a = dq + r$ i $0 \leqslant r < d$. Wobec tego

$$r = a - dq = a(1 - qx_0) - bqy_0.$$

Jeśli $r > 0$, to $r \in D$ i jest to element mniejszy od d – sprzeczność. W takim razie $r = 0$ i w konsekwencji dostajemy $d|a$. W analogiczny sposób dowodzimy, że $d|b$.

Załóżmy teraz, że $0 < t$ jest taką liczbą całkowitą, która dzieli i a i b. To oznacza, że $a = tm$, $b = tn$, dla pewnych liczb całkowitych m, n, skąd $d = ax_0 + by_0 = t(mx_0 + ny_0)$ czyli $t|d$, wobec czego $t \leqslant d$. Tym samym każdy wspólny dzielnik liczb a i b jest dzielnikiem d, czyli wobec dodatniości d mamy $d = \mathrm{NWD}(a, b)$.

Przypuśćmy teraz, że $n > 2$ i nasze twierdzenie jest prawdziwe dla każdego układu mniej niż n liczb, spełniającego założenia.

Wprowadźmy następujące oznaczenia:

$$d_0 := \mathrm{NWD}(a_1, \ldots, a_{n-1}) > 0, \qquad d := \mathrm{NWD}(\mathrm{NWD}(a_1, \ldots, a_{n-1}), a_n) > 0.$$

Zgodnie z założeniem indukcyjnym wiemy, że istnieją takie liczby $l_1, \ldots, l_{n-1}, k, l \in \mathbb{Z}$, że

$$(\star) \qquad d_0 = l_1a_1 + \ldots + l_{n-1}a_{n-1}, \qquad d = kd_0 + la_n.$$

Udowodnimy, że d jest największym wspólnym dzielnikiem liczb $a_1, \ldots, a_n$ (a przy okazji udowodnimy własność rekurencyjnego obliczania NWD).

Z definicji wynika, że d dzieli d_0 oraz a_n. Ponieważ d_0 dzieli każde a_i dla $i = 1, \ldots, n-1$, więc z przechodniości relacji podzielności d jest wspólnym dzielnikiem wszystkich liczb $a_1, \ldots, a_n$.

Z drugiej strony, jeśli $\tilde{d} \in \mathbb{N}$ jest wspólnym dzielnikiem $a_1, \ldots, a_n$, to z $(\star)$ mamy, że $\tilde{d}|d_0$, a tym samym, wobec dodatniości d, liczba $\tilde{d}$ dzieli d. Oznacza to, że $\tilde{d} \leqslant d$ i wobec tego $d = \mathrm{NWD}(a_1, \ldots, a_n)$.

Jednocześnie, ponownie dzięki $(\star)$, wiemy, że $d = kd_0 + la_n = k(l_1a_1 + \ldots + l_{n-1}a_{n-1}) + la_n$ i przyjmując $k_i := kl_i$ dla $i = 1, \ldots, n-1$ i $k_n := l$ otrzymujemy tezę. □

Z twierdzenia 1.2.7 i jego dowodu otrzymujemy następujące wnioski.

Wniosek 1.2.8 (wnioski z BB)**.** *Niech $a_1, \ldots, a_r$ – liczby całkowite, spośród których co najmniej jedna jest niezerowa, $a, b, c \in \mathbb{Z}$. Wtedy zachodzą następujące własności:*

(1) liczby $a_1, \ldots, a_r$ są względnie pierwsze wtedy i tylko wtedy, gdy istnieją takie liczby całkowite $k_1, \ldots, k_r$, że:

$$(\star) \qquad 1 = k_1a_1 + \ldots + k_ra_r,$$

(2) jeśli $r > 2$, to $\mathrm{NWD}(\mathrm{NWD}(a_1, \ldots, a_{r-1}), a_r) = \mathrm{NWD}(a_1, \ldots, a_r)$,

(3) jeśli $(a, b) = 1$ i $a|bc$, to $a|c$.

Odnotujmy jeszcze w tym miejscu fakt, że znajomość rozkładu liczb całkowitych a, b na czynniki pierwsze umożliwia szybkie wyznaczenie $\mathrm{NWD}(a, b)$ bez wykorzystania algorytmu Euklidesa. Istotnie, jeśli

$$a = \mathrm{sgn}(a)p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}, \quad b = \mathrm{sgn}(b)p_1^{l_1} \cdot \ldots \cdot p_s^{l_s},$$

to $\mathrm{NWD}(a, b) = p_1^{t_1} \cdot \ldots \cdot p_s^{t_s}$ gdzie $t_i = \min(k_i, l_i)$ przy czym zakładamy, że $p_i \neq p_j$ dla $i \neq j$ oraz $t_i \geqslant 0$. Nie wspominamy dokładniej o tej metodzie, gdyż odwołuje się ona do zasadniczego twierdzenia arytmetyki, o którym opowiemy w dalszej części naszych rozważań. Należy jednak zwrócić uwagę, że ta metoda wyznaczania $\mathrm{NWD}(a, b)$ ma istotną słabość, gdyż wymaga znajomości rozkładu liczb a, b. Dla małych wartości a, b nie jest to problem, ale gdy liczby a, b są duże, powiedzmy $> 10^{100}$, i wybrane w sposób losowy, to problem ich rozkładu na czynniki pierwsze jest trudny.

Z podstawowych informacji odnotujmy na zakończenie zależność łączącą $\mathrm{NWD}(a, b)$ i $\mathrm{NWW}(a, b)$, której dowód pozostawiamy jako ćwiczenie. Zwróćmy przy okazji uwagę, na fakt, że równość z poniższego wniosku nie jest prawdziwa, gdy rozważamy więcej niż dwie liczby całkowite.

Wniosek 1.2.9 (zależność między NWD i NWW)**.** *Dla liczb $a, b \in \mathbb{N}$ zachodzi równość:* $\mathrm{NWD}(a,b)\cdot\mathrm{NWW}(a,b) = ab$.

Przedstawimy teraz proste zastosowanie tożsamości BB: metodę, która umożliwia rozwiązywanie tak zwanych liniowych równań diofantycznych. Dokładniej, przez **liniowe równanie diofantyczne** będziemy rozumieć równanie postaci:

$$ax + by = c,$$

gdzie a, b, c są ustalonymi liczbami całkowitymi, zaś rozwiązań x, y poszukujemy również w zbiorze liczbach całkowitych.

Twierdzenie 1.2.10 (istnienie i postać rozwiązań liniowego równania diofantycznego)**.** *Niech $a, b, c \in \mathbb{Z}$ takie, że $ab \neq 0$. Zachodzą następujące własności:*

(1) liniowe równanie diofantyczne $ax + by = c$ posiada rozwiązanie w liczbach całkowitych x, y, wtedy i tylko wtedy, gdy $d := \mathrm{NWD}(a,b)|c$,

(2) jeśli (x_0, y_0) jest dowolnym rozwiązaniem równania $ax + by = c$, to każde inne rozwiązanie jest postaci

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t,$$

dla pewnego $t \in \mathbb{Z}$.

Dowód. Pierwsza część naszego twierdzenia jest natychmiastowym wnioskiem z twierdzenia 1.2.7.

By dowieść drugiej części na początek zauważmy, że dla dowolnej liczby całkowitej t mamy równość

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 = c.$$

Oznacza to, że para $\left(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t\right)$ również jest rozwiązaniem naszego równania.

Niech teraz para $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$ będzie rozwiązaniem równania $ax + by = c$, tzn. $aX + bY = c$. Mamy zatem, że $aX + bY = c = ax_0 + by_0$ i w konsekwencji

$$a(X - x_0) = b(y_0 - Y) \text{ lub równoważnie } \frac{a}{d}(X - x_0) = \frac{b}{d}(y_0 - Y).$$

Ponieważ $\mathrm{NWD}(a/d, b/d) = 1$, więc $\frac{a}{d}|(y_0 - Y)$ oraz $\frac{b}{d}|(X - x_0)$. Oznacza to, że istnieje taka liczba całkowita t, że spełnione są równości

$$t = \frac{y_0 - Y}{\frac{a}{d}} = \frac{X - x_0}{\frac{b}{d}}.$$

Innymi słowy $X = x_0 + \frac{b}{d}t, Y = y_0 - \frac{a}{d}t$, co kończy dowód naszego twierdzenia. □

Przykład 1.2.11. By pokazać teraz działanie (rozszerzonej wersji, która pozwala jednocześnie wyliczać też współczynniki w przedstawieniu Bézouta z 1.2.7) algorytmu Euklidesa w akcji rozwiążemy liniowe równanie diofantyczne

$$1716x + 420y = 24.$$

By rozwiązać powyższe równanie wyznaczymy najpierw $\mathrm{NWD}(1716, 420)$ oraz takie liczby całkowite x_0, y_0, że $\mathrm{NWD}(1716, 420) = 1716x_0 + 4206y_0$. Zanim jednak to zrobimy zauważmy, że przedstawienie NWD dwóch liczb za pomocą kombinacji liczb wyjściowych można oczywiście uzyskać „wracając" krok po kroku drogą wykonywanego algorytmu Euklidesa. Jest to jednak czasochłonne, gdyż wymaga wielu operacji arytmetycznych. Procedurę tę można uprościć wyrażając w każdym kroku powstałą resztę jako kombinację liniową (o współczynnikach całkowitych) liczb 1716 i 420.

Chcemy wyliczyć $\mathrm{NWD}(1716, 420)$ oraz jednocześnie przedstawić tę liczbę w postaci Bézouta (tak nazywać będziemy poszukiwaną kombinację).

Wypiszmy, dla przejrzystości kolejne kroki w tabeli

	1716	420
1716	1	0
420	0	1

.

Wiemy teraz, że $1716 = 4 \cdot 420 + 36$. Mnożąc drugi wiersz przez 4 i odejmując go od pierwszego dostajemy

	1716	420
420	0	1
36	1	-4

.

Otrzymaliśmy zatem przedstawienie reszty: $36 = 1 \cdot 1716 + (-4) \cdot 420$ w postaci kombinacji wyjściowych liczb. Dalej powtarzamy procedurę zgodnie z algorytmem Euklidesa i otrzymujemy równość $420 = 11 \cdot 35 + 24$. Ponownie więc mnożymy drugi wiersz ostatniej tabeli przez 11 i odejmujemy od pierwszego otrzymując

	1716	420
36	1	-4
24	-11	45

,

i w konsekwencji dostajemy równość $24 = (-11) \cdot 1716 + 45 \cdot 420$. Kontynuujemy nasze rozumowanie wykorzystując równość $36 = 1 \cdot 24 + 12$ i otrzymujemy

	1716	420
24	-11	45
12	12	-49

.

Po wydzieleniu 24 przez 12 jako resztę otrzymamy zero, wobec tego $\mathrm{NWD}(1716, 420) = 12$ i otrzymaliśmy też przedstawienie $12 = 12 \cdot 1716 + (-49) \cdot 420$. Mamy zatem, że para $(X_0, Y_0) = (12, -49)$ jest rozwiązaniem równania $1716X + 420Y = 12$. W konsekwencji, para $(x_0, y_0) = (24, -98)$ jest szczególnym rozwiązaniem naszego wyjściowego równania, zaś zgodnie z 1.2.10 ogólne rozwiązanie ma postać

$$x = 24 + 35t, \quad y = -98 - 143t, \quad t \in \mathbb{Z}.$$

1.3 O liczbach pierwszych i ich własnościach

W niniejszym podrozdziale podamy podstawowe informacje i własności dotyczące liczb pierwszych. Liczby pierwsze można widzieć jako podstawowe składniki, z których zbudowane są wszystkie liczby całkowite. Choć wspominaliśmy o nich luźno wcześniej, zakładając znajomość tego pojęcia ze szkoły postawmy teraz formalną definicję liczby pierwszej.

Definicja 1.3.1 (liczba pierwsza)**.** Liczbę całkowitą $p \in \mathbb{Z}$ nazywamy **liczbą pierwszą,** jeśli spełnione są następujące warunki:

(1) $p > 1$;

(2) $\forall\, d \in \mathbb{N} :\ d|p \implies d = 1 \ \text{ lub } \ d = p.$

Zbiór wszystkich liczb pierwszych oznaczamy dalej przez $\mathbb{P}$. Każdą liczbę naturalną większą od jedynki, nie będącą liczbą pierwszą nazywamy **liczbą złożoną**.

Pamiętajmy dalej o umowie, iż liczba jeden nie jest ani liczbą pierwszą ani też liczbą złożoną.

Definicja liczby pierwszej i proste zastosowanie identyczności Bézouta prowadzi nas do następującego wniosku.

Własność 1.3.2 (podstawowe własności liczb pierwszych)**.**

(1) Jeśli $p \in \mathbb{P}$, $k \in \mathbb{Z}$, *to* $\mathrm{NWD}(p, k) = 1$ *lub* $\mathrm{NWD}(p, k) = p$.

(2) Jeśli $p \in \mathbb{P}$, $k_1, \ldots, k_n \in \mathbb{Z}$, $p|k_1 \cdot \ldots \cdot k_n$, *to* $p|k_i$ *dla pewnego* $i = 1, \ldots, n$.

Warto zaznaczyć, że własność 1.3.2(2) charakteryzuje liczby pierwsze. Dokładniej, stosując tę własność można wprowadzić równoważną definicję liczby pierwszej. Jest to o tyle ciekawe z naszego punktu widzenia, że w przyszłości własność „braku istotnego rozkładu" elementu (jak to jest w przypadku liczby pierwszej, gdzie rozkłada się ona wyłącznie na iloczyn $p \cdot 1$, względnie $(-p) \cdot (-1)$) oraz 1.3.2(2) okażą się być nierównoważne w ogólniejszych strukturach. Te problemy doprowadzą nas do definicji odpowiednio elementów nierozkładalnych i elementów pierwszych (4.7.3).

Własność 1.3.2 (2) w wersji dla $n = 2$ to tak zwany lemat Euklidesa, który pojawia się w VII Księdze Elementów w sformułowaniu dla przypadku dwóch liczb. Carl Friedrich Gauss[5] w swoim dziele *Disquisitiones arithmeticae* wypowiada lemat Euklidesa i dowodzi przy jego pomocy twierdzenie o rozkładzie liczb całkowitych na liczby pierwsze, z którego to twierdzenia bezpośrednio wynika też gaussowskie uogólnienie lematu Euklidesa. Jak się często podkreśla lemat ten pojawia się już jednak wcześniej w tekście *Nouveaux éléments de mathématiques* Jeana Presteta.[6]

Definicja, którą teraz wprowadzimy może razić przerostem formy nad treścią. Znów wytłumaczeniem niech będą nasze przyszłe zamierzenia, gdzie słowo „jedność" oznaczać będzie znacznie szerszą klasę elementów niż jest to w przypadku zbioru $\mathbb{Z}$.

Definicja 1.3.3 (jedność w $\mathbb{Z}$)**. Jednościami w** $\mathbb{Z}$ nazywamy liczby -1 i 1. Zbiór jedności w $\mathbb{Z}$ będziemy oznaczać przez $U(\mathbb{Z}) := \{-1, 1\}$.

Definicja 1.3.4 (rozkład jednoznaczny)**.** Niech $k \in \mathbb{Z}^\star$. Mówimy, że k posiada jednoznaczny rozkład na iloczyn liczb pierwszych, jeśli

(1) istnieją $p_1, \ldots, p_r \in \mathbb{P}$, $u \in U(\mathbb{Z})$ takie, że $k = u \cdot p_1 \cdot \ldots \cdot p_r$;

(2) dla dowolnych dwóch układów $p_1, \ldots, p_r \in \mathbb{P}$, $q_1, \ldots, q_s \in \mathbb{P}$, $u, v \in U(\mathbb{Z})$ takich, że

$$k = u \cdot p_1 \cdot \ldots \cdot p_r = v \cdot q_1 \cdot \ldots \cdot q_s$$

mamy $r = s$ oraz istnieje taka funkcja σ – bijekcja zbioru $\{1, \ldots, r\}$ na siebie, że: $\forall\ i \in \{1, \ldots, r\} :\ p_i = q_{\sigma(i)}$.

Twierdzenie 1.3.5 (Zasadnicze twierdzenie arytmetyki)**.** *Każda niezerowa liczba całkowita, nie będąca jednością w $\mathbb{Z}$, posiada jednoznaczny rozkład na iloczyn liczb pierwszych.*

Dowód. Wystarczy oczywiście wykazać twierdzenie dla liczb naturalnych większych od jedynki. W naturalny sposób dowód rozbija się na dwie części: wykazanie istnienia rozkładu i wykazanie jego jednoznaczności.
Istnienie. Indukcja względem n: dla $n = 2$ teza jest spełniona.

Załóżmy, że teza jest spełniona dla takich liczb naturalnych m, że $1 < m < n$. Jeśli n jest liczbą pierwszą, to dowód jest zakończony. Jeśli n nie jest liczbą pierwszą, to $n = ab$, gdzie $1 < a < n$ i $1 < b < n$. Wobec tego, z założenia indukcyjnego liczby a i b są liczbami pierwszymi bądź iloczynami liczb pierwszych. W konsekwencji n również jest iloczynem liczb pierwszych.
Jednoznaczność. Ponownie indukcja względem n.

Dla $n = 2$ jednoznaczność rozkładu jest oczywista ze względu na pierwszość tej liczby. Gdyby bowiem było $n = p_1 \cdot \ldots \cdot p_r$ gdzie $p_i \in \mathbb{P}$ i $r > 1$, to 2 musiałaby dzielić jedną z liczb p_i, a tym samym być jej równa (wobec pierwszości). Wtedy dzieląc obie strony przez 2 mielibyśmy, że pozostałe liczby pierwsze p_j dzielą jedynkę co jest niemożliwe. Wobec tego $r = 1$ i $p_1 = 2$.

Zakładając tezę dla liczb mniejszych lub równych $(n-1)$, gdzie $n > 2$, przypuśćmy, że dla n, mamy dwa rozkłady:

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s,$$

gdzie $p_i, q_j \in \mathbb{P}$ oraz $p_1 \leqslant \ldots \leqslant p_r$, $q_1 \leqslant \ldots \leqslant q_s$. Oczywiście możemy przyjąć, że $r > 1$. Istotnie, w przeciwnym razie mamy do czynienia z liczbą pierwszą i teza zachodzi. Niech zatem p będzie najmniejszą liczbą pierwszą dzielącą n. Oznacza to, że p dzieli p_i dla pewnego i (1.3.2(2)). W konsekwencji $p = p_i$ i z minimalności p otrzymujemy równość $p = p_1$. Rozumując analogicznie dostajemy $p = q_1$.

Niech teraz $m := \frac{n}{p} < n$. Wobec tego mamy rozkład:

$$m = p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s.$$

Z założenia indukcyjnego otrzymujemy $r = s$ i istnieje taka bijekcja $\widetilde{\sigma}$ zbioru $\{2, \ldots, n\}$ na siebie (permutacja tego zbioru), że $\forall\ i \in \{2, \ldots, r\}\ p_i = q_{\widetilde{\sigma}(i)}$. Przyjmując $\sigma(1) = 1$, $\sigma(i) = \widetilde{\sigma}(i)$, dla $i > 1$ otrzymujemy poszukiwaną permutację zbioru $\{1, \ldots, n\}$. □

Twierdzenie 1.3.6 (Euklides)**.** *Istnieje nieskończenie wiele liczb pierwszych.*

[5] Carl Friedrich Gauss: matematyk, fizyk i astronom niemiecki, (1777–1855), nazywany „księciem matematyków".

[6] Jean Prestet: ksiądz i matematyk francuski, (1648–1690), jego tekst *Elemens des mathematiques* był bardzo popularny w nauczaniu matematyki w szkołach francuskich XVII wieku – w szczególności z tej książki uczył się m.in. Abraham de Moivre. *Nouveaux éléments de mathématiques* to poprawione, drugie wydanie tego podręcznika.

Dowód. Dla dowodu nie wprost przypuśćmy, że $\mathbb{P} = \{p_1, \ldots, p_r\}$ i zdefiniujmy liczbę $M := p_1 \cdot \ldots \cdot p_r + 1$. Jest jasne, że żadna z liczby $p_1, \ldots, p_r$ nie dzieli M: w przeciwnym razie liczba 1 byłaby podzielna przez liczbę pierwszą. Niech zatem p będzie liczbą pierwszą dzielącą M (taka istnieje na mocy 1.3.5). Wobec tego $p \notin \mathbb{P}$ i p jest liczbą pierwszą, co prowadzi do sprzeczności. □

W tej chwili znamy wiele dowodów nieskończoności zbioru wszystkich liczb pierwszych. Zaprezentowany wyżej w dość podobnej wersji jak w Elementach, jest uznawany za pierwszy zapisany dowód przeprowadzony metodą nie wprost i choćby z tego powodu jest tym dowodem, z którym warto się zapoznać.

Skoro już wiemy, że liczb pierwszych jest nieskończenie wiele powstaje naturalne pytanie: jak wiele jest liczb pierwszych niewiększych od x, gdzie x jest ustaloną liczbą rzeczywistą? Innymi słowy interesuje nas szybkość wzrostu funkcji

$$\pi(x) = |\{p : \ p \leqslant x \ \text{ oraz } \ p \in \mathbb{P}\}|.$$

Funkcja π nazywana jest funkcją zliczającą liczby pierwsze. Gauss przypuszczał, zaś J. Hadamard[7] i Ch. J. de la Vallée-Poussin[8] udowodnili niezależnie tzw. Twierdzenie o liczbach pierwszych, tj. równość

$$\lim_{x \to +\infty} \frac{\pi(x) \log x}{x} = 1.$$

Dowód tego twierdzenia wymaga zastosowania zaawansowanego aparatu funkcji analitycznych. Można jednak podać zupełnie elementarny dowód dolnego oszacowania na wartość $\pi(x)$, które wymaga tylko podstawowych własności liczb całkowitych. Dokładniej, przedstawimy dowód Erdősa[9] następującego twierdzenia.

Twierdzenie 1.3.7. *Dla $n \in \mathbb{N}$ prawdziwa jest nierówność*

$$\pi(n) \geqslant \frac{\log n}{2 \log 2}.$$

Dowód. Zanim rozpoczniemy dowód przypomnijmy, że liczba naturalna nazywana jest bezkwadratową, jeśli nie jest podzielna przez kwadrat żadnej liczby pierwszej. Oznaczmy zbiór liczb bezkwadratowych przez B.

Dla $n \in \mathbb{N}$ rozważmy zbiór

$$A(n) = \{(a, b) \in \mathbb{N} \times B : \ a^2 b \leqslant n\}$$

i zauważmy, że $|A(n)| = n$. Istotnie, każdą liczbą naturalną m można jednoznacznie zapisać w postaci $m = a^2 b$, gdzie $a \in \mathbb{N}$ i $b \in B$.

Jeśli $(a, b) \in A(n)$, to mamy oczywiście $a^2 \leqslant n$ i $b \leqslant n$, i w konsekwencji $a \leqslant \sqrt{n}$. Ponadto liczba b jest bezkwadratowa, więc jest iloczynem różnych liczb pierwszych, z których każda jest $\leqslant n$. Oznacza to, że b daje się zapisać jako iloczyn liczb ze zbioru $\{p_1, p_2, \ldots, p_{\pi(n)}\}$. Możliwych iloczynów mamy tyle ile podzbiorów rozważanego zbioru, czyli $2^{\pi(n)}$. Podsumowując nasze rozważania widzimy, że jeśli $(a, b) \in A(n)$, to mamy co najwyżej $\sqrt{n}$ możliwych wyborów liczby a oraz $2^{\pi(n)}$ możliwych postaci liczby b. Stąd $|A(n)| < \sqrt{n} 2^{\pi(n)}$, ale $|A(n)| = n$, więc ostatecznie $n \leqslant \sqrt{n} 2^{\pi(n)}$ i w konsekwencji

$$\pi(n) \geqslant \frac{\log n}{2 \log 2}.$$ □

Liczby pierwsze obecnie to punkt wyjścia do analizy całego bogactwa problemów nie tylko stricte teorioliczbowych, o których nie sposób opowiedzieć w kilku słowach. Wspomnieć jednak wypada o wciąż udoskonalanych testach pierwszości, których celem jest zbadanie pierwszości zadanej liczby (nie zaś jej rozkład na liczby pierwsze co jest zagadnieniem znacznie trudniejszym). Już w okolicach 200 p.n.e. grecki matematyk Eratosthenes[10] wprowadził metodę wyznaczania liczb pierwszych nie większych od ustalonej liczby n zwaną odtąd „sitem Eratosthenesa". Jej działanie jest niezwykle proste – wypisujemy wszystkie liczby od 2 do n następnie zakreślamy 2 jako liczbę pierwszą i wykreślamy jej wszystkie wielokrotności. Potem zakreślamy pierwszą pozostałą liczbę i wykreślamy wszystkie jej wielokrotności i tak kontynuujemy aż nie ma „nietkniętych" liczb mniejszych lub równych od $\sqrt{n}$. W ten sposób otrzymamy tablicę liczb pierwszych nie większych od liczby wyjściowej.

[7] Jacques Hadamard: matematyk francuski (1865–1963).

[8] Charles Jean de la Vallée-Poussin: matematyk francuski (1866–1962).

[9] Paul Erdős: matematyk węgierski, jeden z najwybitniejszych matematyków XX w. Autor ponad 1500 artykułów dotyczących głównie teorii liczb, kombinatoryki i teorii grafów (1913–1996).

[10] Eratosthenes: grecki matematyk, poeta, geograf, astronom i filozof (276–194 p.n.e.).

Obecne, o wiele bardziej zaawansowane metody testowania pierwszości dzielą się na dwa rodzaje: testy deterministyczne i probabilistyczne. Do tych pierwszych zaliczyć można m.in. test Lucasa–Lehmera,[11] (przy użyciu tego testu znaleziono największe liczby pierwsze, test dotyczy badania pierwszości tzw. liczb Mersenne'a),[12] czy niektóre testy oparte na krzywych eliptycznych. Testy probabilistyczne, choć nie pozwalają na zdecydowanie z pewnością, czy dana liczba jest pierwsza mają tę przewagę, że zwykle są dużo szybsze od testów deterministycznych. Liczby, którym udaje się przejść pozytywnie test probabilistyczny, ale mimo to okazują się być jednak liczbami złożonymi znane są w kontekście liczb „pseudopierwszych". Istnieje wiele różnych rodzajów takich liczb, z których bodaj najbardziej znane to liczby pseudopierwsze Fermata, które mimo iż pozostają liczbami złożonymi to spełniają założenia Małego Twierdzenia Fermata, o którym opowiemy dalej. Przy okazji testów probabilistycznych wypada wspomnieć o dwóch testach: teście Rabina-Millera, który jest wyjątkowo efektywnym testem probabilistycznym oraz o tzw. teście AKS (od nazwisk twórców: Manindra Agrawala, Neeraja Kayala i Nitina Saxena, 2002), który to test deterministyczny sprawdza pierwszość zadanej liczby w czasie wielomianowym, słowem jego czas działania jest ograniczony za pomocą zależności wielomianowej od rozmiaru danych wejściowych. Do czasu pojawienia się tego testu nie było dowodu na to, iż test pierwszości zadanej liczby jest problemem rozwiązywalnym w czasie wielomianowym mimo, iż uważano że taka możliwość istnieje.

1.4 Kongruencje i ich własności, twierdzenie chińskie o resztach

Na pierwszej stronie swego dzieła *Disquisitiones Arithmeticae* Gauss wprowadza pojęcie „kongruencji", czyli jak to określać będziemy dalej „przystawania". Dzięki zastosowaniu tej notacji wiele własności i twierdzeń otrzymało prostszą postać, ale też znacznie ułatwiło to przeprowadzanie niektórych operacji matematycznych.

Definicja 1.4.1 (relacja przystawania modulo)**.** Niech $m \in \mathbb{N}$. Mówimy, że liczby całkowite k, l **przystają modulo** m**,** gdy $m|(k-l)$.

Oznaczenie: $k \equiv l \pmod{m}$.

Liczbę m nazywa się **modułem kongruencji.**

Uwaga 1.4.2. Relacja przystawania modulo m jest relacją równoważności w zbiorze liczb całkowitych.

Klasę równoważności liczby $k \in \mathbb{Z}$ względem relacji przystawania modulo m oznaczamy przez $[k]_m$, zaś zbiór wszystkich klas równoważności w relacji przystawania modulo m oznaczamy przez $\mathbb{Z}_m$. W dalszym ciągu wykładu często będziemy pisać po prostu $\mathbb{Z}_m = \{0, \ldots, m-1\}$, mając na myśli za każdym razem klasę równoważności reprezentowaną przez daną liczbę. Jest to poprawne, gdyż z algorytmu dzielenia z resztą wiemy, że liczby $0, \ldots, m-1$ wyczerpują wszystkie klasy równoważności (por. też 1.6.2).

Zauważmy, że relacja przystawania modulo jest zgodna z działaniami dodawania i mnożenia, co umożliwi w dalszej części wykładu wprowadzenie poprawnych działań w zbiorze $\mathbb{Z}_m$ – dokładniej, prawdziwe są następujące własności, których dowód pozostawiamy jako ćwiczenie.

Własność 1.4.3 (podstawowe własności kongruencji)**.** *Niech $m \in \mathbb{N}$ oraz $k, l, k', l' \in \mathbb{Z}$ będą takie, że $k \equiv k' \pmod{m}$ i $l \equiv l' \pmod{m}$. Wtedy:*

(1) $k \pm l \equiv k' \pm l' \pmod{m}$,

(2) $kl \equiv k'l' \pmod{m}$.

Z powyższej własności otrzymujemy natychmiastowy wniosek.

Wniosek 1.4.4. *Jeśli f jest wielomianem o współczynnikach całkowitych*[13] *oraz mamy dane takie $a, b \in \mathbb{Z}, m \in \mathbb{N}$, że $a \equiv b \pmod{m}$, to $f(a) \equiv f(b) \pmod{m}$.*

Dowód. Zapiszmy f w postaci: $f(x) = \sum_{i=0}^{n} c_i x^i$, gdzie $c_i \in \mathbb{Z}$. Jeśli $a \equiv b \pmod{m}$, to dla każdego $i \in \{0, \ldots, n\}$ mamy, że

$$a^i \equiv b^i \pmod{m} \quad \text{oraz} \quad c_i a^i \equiv c_i b^i \pmod{m}.$$

Dodając te kongruencje stronami przy zastosowaniu 1.4.3 otrzymujemy żądaną własność. □

[11] Edouard Lucas: matematyk francuski 1842-1891, Derrick Henry Lehmer: matematyk amerykański, 1905–1991.

[12] Liczby Mersenne'a: liczby postaci $2^p - 1$, gdzie p jest liczbą pierwszą, nazwane tak na cześć matematyka francuskiego Marina Mersenne'a, autora pierwszej tablicy liczb pierwszych tego typu (niestety zawierającą błędy) – Marin Mersenne: matematyk, filozof i teolog francuski, (1588–1648).

[13] Bazujemy tu na wiedzy Czytelnika wyniesionej ze szkoły, formalne pojęcie wielomianu zostanie określone w kolejnej części wykładu.

Kolejny zestaw własności relacji podzielności i kongruencji znajdzie zastosowanie wielokrotnie w dalszych rozważaniach, w tym przy rozwiązywaniu układów równań kongruencyjnych. Własności te łatwo wynikają z zastosowania zasadniczego twierdzenia arytmetyki 1.3.5 lub tożsamości Bézouta 1.2.4.

Własność 1.4.5 (własności kongruencji)**.**

(1) Jeśli $k, l \in \mathbb{Z}$, $m \in \mathbb{Z}^\star$ są takie, że $m|kl$ oraz m i k są względnie pierwsze, to $m|l$.

(2) Jeśli $a, m \in \mathbb{N}$, $k, l \in \mathbb{Z}$, to $ak \equiv al \pmod{am} \iff k \equiv l \pmod{m}$.

(3) Jeśli $m \in \mathbb{N}$, $a, k, l \in \mathbb{Z}$ są takie, że $\mathrm{NWD}(a, m) = d$ i $ak \equiv al \pmod{m}$, to $k \equiv l \pmod{\frac{m}{d}}$.

(4) Jeśli $a_1, \ldots, a_r \in \mathbb{Z}$ oraz liczba $k \in \mathbb{Z}$ jest względnie pierwsza z a_i dla $i = 1, \ldots, r$, to k jest względnie pierwsza z iloczynem $a_1 \cdot \ldots \cdot a_r$.

(5) Jeśli liczby $m_1, \ldots, m_r \in \mathbb{Z}^\star$ są parami względnie pierwsze oraz $k \in \mathbb{Z}$ jest taka, że $m_i|k$ dla każdego $i = 1, \ldots, r$, to $m_1 \cdot \ldots \cdot m_r|k$.

Dowód. Dla dowodu (1) wystarczy zauważyć, że wobec względnej pierwszości m i k istnieją takie $s, t \in \mathbb{Z}$ dla których zachodzi równość: $sm + tk = 1$ – mnożąc tę równość obustronnie przez l i wykorzystując założenie $m|kl$ otrzymujemy tezę. Dowód (2) sprowadza się do zapisania definicji obu kongruencji i skorzystania z faktu, że $a \neq 0$, zaś (3) otrzymujemy natychmiast z (1), gdy zauważymy, że założenie oznacza $\frac{m}{d} | \frac{a}{d}(k-1)$ zaś $\frac{m}{d}$ i $\frac{a}{d}$ są względnie pierwsze.

Dowód (4) można przeprowadzić nie wprost: gdyby liczba k miała wspólny z $a_1 \cdot \ldots \cdot a_r$ dzielnik większy od 1, to istniałby dla nich wspólny dzielnik będący liczbą pierwszą, co w połączeniu z (2) prowadziłoby do sprzeczności. Dowód własności (5), indukcyjny względem r, pozostawiamy Czytelnikowi. □

Przejdziemy teraz do rozważania równań oraz układów równań kongruencyjnych. Łatwo, rozpisując wprost definicję przystawania modulo sprawdzić, że równanie postaci $ax \equiv b \pmod{m}$ posiada rozwiązanie całkowite wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, m)|b$. Rozwiniemy nieco tę obserwację w poniższej własności.

Własność 1.4.6 (rozwiązanie kongruencji liniowej)**.** *Niech $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ i połóżmy $d = \mathrm{NWD}(a, m)$. Kongruencja $ax \equiv b \pmod{m}$ ma rozwiązanie całkowite wtedy i tylko wtedy, gdy $d|b$. Dodatkowo, jeśli $d|b$, to kongruencja $ax \equiv b \pmod{m}$ ma dokładnie d niekongruentnych rozwiązań całkowitych $x_i = x_0 + \frac{m}{d}i, i = 0, 1, \ldots, d-1$, gdzie x_0 jest dowolnie wybranym, ustalonym rozwiązaniem.*

Dowód. Zauważmy, że istnienie rozwiązania naszej kongruencji jest równoważne temu, że istnieje $x \in \mathbb{Z}$ takie, że $m|ax - b$ co z kolei jest równoważne stwierdzeniu, iż istnieje $y \in \mathbb{Z}$ takie, że $ax - b = my$ czyli $ax - my = b$. Równanie to ma rozwiązanie wtedy i tylko wtedy, gdy $d|b$, co jest konsekwencją twierdzenia 1.2.10.

Jeśli teraz para (x_0, y_0) jest szczególnym rozwiązaniem równania $ax - b = my$, to korzystając ponownie z twierdzenia 1.2.10 otrzymujemy, że każde inne rozwiązanie spełnia warunki

$$x \equiv x_0 \left(\mathrm{mod}\ \frac{m}{d}\right), \quad y \equiv y_0 \left(\mathrm{mod}\ \frac{m}{d}\right).$$

Zauważmy, że liczby

$$x_0, \quad x_0 + \frac{m}{d}, \ \ldots, \ x_0 + \frac{(d-1)m}{d}$$

są niekongruentne modulo m. Istotnie, jeśli $x_0 + \frac{im}{d} \equiv x_0 + \frac{jm}{d} \pmod{m}$ dla pewnych $i, j \in \{0, \ldots, d-1\}$, to $i \equiv j \pmod{d}$, co oznacza, że $i = j$ i dostajemy sprzeczność. W konsekwencji każda z liczb $x_0 + \frac{im}{d}$ dla $i \in \mathbb{N}$ przystaje do jednej z liczb $x_0 + \frac{im}{d}$ dla $i \in \{0, \ldots, d-1\}$, co kończy dowód naszego twierdzenia. □

W zastosowaniach często istnieje konieczność rozwiązywania układów kongruencji liniowych postaci

$$u_1 x \equiv v_1 \pmod{m_1}, \ u_2 x \equiv v_2 \pmod{m_1}, \ \ldots, \ u_n x \equiv v_n \pmod{m_n},$$

gdzie $u_i, v_i \in \mathbb{Z}, m_i \in \mathbb{N}$ dla $i = 1, \ldots, n$, są ustalone, zaś x jest poszukiwaną liczbą. Jest jasne, że warunkiem koniecznym istnienia rozwiązania jest istnienie rozwiązania każdej z kongruencji wchodzącej w skład układu. Jest to równoważne koniunkcji warunków $\mathrm{NWD}(u_i, m_i)|v_i$ dla $i = 1, 2, \ldots, n$. Oznacza to, że bez straty dla ogólności możemy założyć, że nasz układ ma postać

$$x \equiv a_1 \pmod{m_1}, \ x \equiv a_2 \pmod{m_2}, \ \ldots, \ x \equiv a_n \pmod{m_n}.$$

Możemy sformułować następujące ogólne, kluczowe twierdzenie.

Twierdzenie 1.4.7 (chińskie o resztach, TCR, wersja ogólna)**.** *Dla ustalonych układów liczb* $m_1, \ldots, m_n \in \mathbb{N}$ *oraz* $a_1, \ldots, a_n \in \mathbb{Z}$ *układ kongruencji*

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2},\ \ldots,\ x \equiv a_n \pmod{m_n}$$

ma rozwiązanie całkowite x *wtedy i tylko wtedy gdy dla dowolnych* $i, j \in \{1, \ldots, n\}, i \neq j$*, spełniony jest warunek* $\mathrm{NWD}(m_i, m_j) | (a_i - a_j)$.

Ponadto, jeśli rozwiązanie powyższego układu kongruencji istnieje, to jest ono jedyne modulo $\mathrm{NWW}(m_1, \ldots, m_n)$.

Dowód. Na początek wykażemy, że sformułowany warunek jest konieczny. Zakładamy zatem, że istnieje takie x_0, które jest rozwiązaniem naszego wyjściowego układu kongruencji. Niech $i, j \in \{1, \ldots, n\}, i \neq j$, i rozważmy kongruencje

$$x_0 \equiv a_i \pmod{m_i}, \quad x_0 \equiv a_j \pmod{m_j}.$$

Z pierwszej kongruencji dostajemy, że $x_0 = a_i + m_i y$ dla pewnego $y_0 \in \mathbb{Z}$. Wstawiając wyznaczoną wartość x_0 do drugiej kongruencji otrzymujemy kongruencję

$$m_i y_0 \equiv a_j - a_i \pmod{m_j}.$$

Kongruencja ta ma rozwiązanie wtedy i tylko wtedy, gdy $\mathrm{NWD}(m_i, m_j) | (a_i - a_j)$. Jeśli ten warunek jest spełniony, to y_0 jest wyznaczony jednoznacznie modulo $m_j / \mathrm{NWD}(m_i, m_j)$, zaś x_0 jest wyznaczony jednoznacznie modulo

$$m_i m_j / \mathrm{NWD}(m_i, m_j) = \mathrm{NWW}(m_i, m_j).$$

Ponieważ własność ta musi zachodzić dla dowolnych $i, j \in \{1, \ldots, n\}, i \neq j$, więc otrzymujemy konieczność naszego warunku.

Wykażemy teraz, że warunek $\mathrm{NWD}(m_i, m_j) | (a_i - a_j)$ dla $i, j \in \{1, \ldots, n\}, i \neq j$, jest również wystarczający. Bez straty ogólności możemy założyć, że $\mathrm{NWD}(m_i, m_j) > 1$ dla dowolnych $i, j \in \{1, \ldots, n\}$.

Rozważmy dwie pierwsze kongruencje naszego układu, tj.

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}$$

i przypuśćmy, że

$$x \equiv a \pmod{\mathrm{NWW}(m_1, m_2)}$$

jest rozwiązaniem. Naszym celem jest wykazanie, że dla $i = 3, \ldots, n$ spełniony jest warunek

$$\mathrm{NWD}(m_i, \mathrm{NWW}(m_1, m_2)) | (a_i - a).$$

Dla wygody obliczeń wprowadźmy oznaczenie $d_i := \mathrm{NWD}(m_i, \mathrm{NWW}(m_1, m_2))$. Niech $p \in \mathbb{P}$ będzie liczbą pierwszą dzielącą d_i, zaś α będzie takie, że $p^\alpha | d_i$. Ponadto przez β_j oznaczmy wykładnik liczby pierwszej p w rozkładzie liczby m_j na czynniki pierwsze dla $j = 1, \ldots, i$. Wiemy, że wykładnik p w rozkładzie $\mathrm{NWW}(m_1, m_2)$ wynosi $\max\{\beta_1, \beta_2\}$. W konsekwencji dostajemy, że

$$\alpha = \min\{\beta_i, \max\{\beta_1, \beta_2\}\} = \max\{\min\{\beta_1, \beta_i\}, \min\{\beta_2, \beta_i\}\}.$$

Z założenia widzimy, że

$$p^{\min\{\beta_1, \beta_i\}} | (a_1 - a_i), \quad p^{\min\{\beta_2, \beta_i\}} | (a_2 - a_i).$$

Ponieważ $p^{\beta_k} | (a_k - a)$ oraz $a_k - a_i = (a_k - a) + (a - a_i)$ dla $k = 1, 2$, otrzymujemy

$$p^{\min\{\beta_1, \beta_i\}} | (a_i - a), \quad p^{\min\{\beta_2, \beta_i\}} | (a_i - a),$$

i w konsekwencji $p^\alpha | (a_i - a)$. Ponieważ p^α było dowolną potęgą liczby pierwszej dzielącej d_i, więc musi być

$$d_i = \mathrm{NWD}(m_i, \mathrm{NWW}(m_1, m_2)) | (a_i - a).$$

Zauważmy teraz, że nasze rozumowanie pokazuje, biorąc $i = 1$ lub $i = 2$, że układ dwóch pierwszych kongruencji ma rozwiązanie dokładnie wtedy, gdy spełnione jest nasze założenie. Daje to tezę dla $n = 2$. Innymi słowy, przy założeniu $\mathrm{NWD}(m_1, m_2) | a_1 - a_2$, układ kongruencji

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}$$

jest równoważny kongruencji

$$x \equiv a \,(\mathrm{mod}\ \mathrm{NWW}(m_1, m_2)).$$

i posiada rozwiązanie. Rzecz jasna, rozwiązanie jest wyznaczone jednoznacznie modulo $\mathrm{NWW}(m_1, m_2)$. Dodając kongruencję $x \equiv a_3 \,(\mathrm{mod}\, m_3)$ i powtarzając rozumowanie otrzymamy rozwiązanie układu kongruencji $x \equiv a_i \,(\mathrm{mod}\, m_i), i = 1, 2, 3$, które jest jednoznaczne modulo

$$\mathrm{NWW}(m_3, \mathrm{NWW}(m_1, m_2)) = \mathrm{NWW}(m_1, m_2, m_3).$$

Kontynuując w ten sposób, po $n-1$ krokach, otrzymamy tezę naszego twierdzenia. □

Powyższe twierdzenie daje nam warunek konieczny i wystarczający istnienia rozwiązania układu kongruencji liniowych. Warto jednak zanotować i udowodnić inną metodą szczególną wersję twierdzenia 1.4.7, gdy moduły $m_1, \ldots, m_n$ są parami względnie pierwsze. Dowód (niezależny od twierdzenia ogólnego) przeprowadzony poniżej wart jest uwagi, gdyż daje, w połączeniu z rozszerzonym algorytmem Euklidesa, możliwość algorytmicznego rozwiązywania układów spełniających założenia szczególnej wersji TCR.

Twierdzenie 1.4.8 (chińskie o resztach, TCR, wersja szczególna)**.** *Niech $m_1, \ldots, m_n \in \mathbb{N}$ będą układem liczb parami względnie pierwszych, $a_1, \ldots, a_n \in \mathbb{Z}$. Wtedy:*

(1) istnieje $x \in \mathbb{Z}$ takie, że $x \equiv a_i \,(\mathrm{mod}\, m_i)$ dla każdego $i = 1, \ldots, n$.

(2) jeśli x_1, x_2 spełniają (1), to $x_1 \equiv x_2 \,(\mathrm{mod}\, M)$, gdzie $M = m_1 \cdot \ldots \cdot m_n$.

Dowód. By wykazać (1) podamy konstrukcję rozwiązania x. Niech $s_i := \frac{M}{m_i}$. Wtedy s_i jest iloczynem liczb m_j dla $j \neq i$ wobec tego jest iloczynem liczb względnie pierwszych z m_i. Z 1.4.5(4) wynika, że również liczby m_i i s_i są względnie pierwsze. Wobec tego istnieją $u_1, \ldots, u_n, v_1, \ldots, v_n \in \mathbb{Z}$ takie, że

$$u_i m_i + v_i s_i = 1 \quad \text{dla} \quad i = 1, \ldots, r.$$

Określmy teraz $x := a_1(v_1 s_1) + \ldots + a_n(v_n s_n)$. Wykażemy, że tak dobrane x spełnia kongruencję $x \equiv a_i \,(\mathrm{mod}\, m_i)$ dla $i = 1, \ldots, n$.

Ustalmy $i_0 \in \{1, \ldots, n\}$. Wtedy

$$x - a_{i_0} = a_1(v_1 s_1) + \ldots + a_{i_0}(v_{i_0} s_{i_0} - 1) + \ldots + a_n(v_n s_n).$$

Mamy jednak $m_{i_0} | u_{i_0} m_{i_0} = x - v_{i_0} s_{i_0}$. Ponadto s_i dla $i \neq i_0$ są podzielne przez m_{i_0} czyli $x \equiv a_{i_0} (\mathrm{mod}\, m_{i_0})$, czego oczekiwaliśmy.

Niech teraz x' spełnia również tę kongruencję, to oznacza, że $x' - x$ jest podzielne przez każde m_i. Wobec tego z 1.4.5(5) wynika, że $x' - x$ jest podzielne przez iloczyn $m_1 \cdot \ldots \cdot m_n$ i mamy tezę. □

Jak wspomnieliśmy, zaletą powyższego dowodu jest jego algorytmiczny charakter, gdyż każdy układ kongruencji rozważanej postaci o modułach względnie pierwszych może być rozwiązany w przedstawiony sposób. Jednakże, mankamentem tej metody jest liczba i wielkość obliczeń, które trzeba przeprowadzić by otrzymać poszukiwane rozwiązanie. Dlatego też w przypadku małych układów stosuje się metodę eliminacji kongruencji, podobną do metody Gaussa eliminacji zmiennych, którą wykorzystuje się przy rozwiązywaniu układów równań liniowych. By podać przykład zastosowania tej metody rozważmy układ kongruencji

$$\begin{cases} x \equiv 2 \,(\mathrm{mod}\, 3) \\ x \equiv 3 \,(\mathrm{mod}\, 5) \\ x \equiv 1 \,(\mathrm{mod}\, 7) \end{cases}.$$

Z pierwszej kongruencji dostajemy, że $x = 3a + 2$ dla pewnego $a \in \mathbb{Z}$. Wstawiając tak wyznaczoną wartość do drugiej kongruencji otrzymujemy $3a + 2 \equiv 3 \,(\mathrm{mod}\, 5)$ lub równoważnie $3a \equiv 1 \,(\mathrm{mod}\, 5)$. Po przemnożeniu stronami przez 2 dostajemy, że $a \equiv 2 \,(\mathrm{mod}\, 5)$, co implikuje, że $a = 5b + 2$ i $x = 3(5b + 2) + 2 = 15b + 8$ dla pewnego $b \in \mathbb{Z}$. Pozostaje nam zatem kongruencja $15b + 8 \equiv 1 \,(\mathrm{mod}\, 7)$ lub równoważnie, po redukcji modulo 7, $b \equiv 0 \,(\mathrm{mod}\, 7)$. Ostatecznie $b = 7c$ i tym samym $x = 105b + 8$, co oznacza, że najmniejszym dodatnim rozwiązaniem naszego układu jest $x = 8$.

Przedstawione podejście może być zastosowane również do układów kongruencji, których moduły nie są parami względnie pierwsze. Jeśli rozważany układ ma rozwiązanie (co oznacza, że warunek konieczny i wystarczający przedstawiony w sformułowaniu twierdzenia 1.4.7 zachodzi), to znajdziemy je eliminując kongruencje jedna po drugiej.

Alternatywna metoda polega na sprowadzeniu rozważanego układu do sytuacji, gdy moduły są parami względnie pierwsze. Przykładowo, rozważmy układ kongruencji

$$\begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 9 \pmod{10} \\ x \equiv 14 \pmod{15} \end{cases}$$

Układ ten jest równoważny następującym

$$\begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 9 \pmod 2 \\ x \equiv 9 \pmod 5 \\ x \equiv 14 \pmod 3 \\ x \equiv 14 \pmod 5 \end{cases} \iff \begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 4 \pmod 5 \\ x \equiv 2 \pmod 3 \end{cases}.$$

Moduły ostatniego układu są parami względnie pierwsze i oczywiście cały układ ma rozwiązanie (co może być również potwierdzone przy zastosowaniu twierdzenia 1.4.7).

1.5 Funkcja Eulera, jej własności i zastosowania

W tym podrozdziale zapoznamy się z najważniejszą dla dalszych zastosowań (w szczególności w teorii grup oraz w wykorzystaniu dalej m.in. w teorii ciał i teorii Galois) funkcją arytmetyczną[14]. Funkcję tę można definiować na różne sposoby, ale postawimy tu standardową definicję teorioliczbową.

Definicja 1.5.1 (funkcja Eulera)**.** Niech $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ będzie funkcją przypisującą liczbie n liczbę liczb $k \in \{1, \dots n\}$ względnie pierwszych z n, tzn.

$$\varphi(n) = \#\{k \in \{1, \dots, n\} : \ \mathrm{NWD}(k, n) = 1\}.$$

Funkcję φ nazywamy **funkcją Eulera**.

Własność 1.5.2 (podstawowe własności funkcji Eulera)**.** *Funkcja φ ma następujące własności:*

(1) $\varphi(1) = 1$, $(\mathrm{NWD}(1, 1) = 1)$.

(2) Niech p – liczba pierwsza. Wtedy: $\varphi(p) = p - 1 = p(1 - \frac{1}{p})$.

(3) Niech p – liczba pierwsza, $k \in \mathbb{N}$. Wtedy $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - \frac{1}{p})$, *gdyż mamy p^{k-1} liczb całkowitych takich, że $1 \leqslant l < p^k$, które są podzielne przez p, a to jedyne interesujące nas liczby, które nie są względnie pierwsze z p.*

Przypomnijmy, że funkcję arytmetyczną $f : \mathbb{N} \longrightarrow \mathbb{C}$ nazywamy multiplikatywną wtedy i tylko wtedy, gdy dla dowolnych względnie pierwszych $m, n \in \mathbb{N}$ spełniona jest równość $f(mn) = f(m)f(n)$. Udowodnimy teraz, że funkcja φ Eulera jest multiplikatywna.

Twierdzenie 1.5.3 (multiplikatywność funkcji Eulera)**.** *Dla dowolnych względnie pierwszych liczb $m, n \in \mathbb{N}$ zachodzi równość $\varphi(mn) = \varphi(m)\varphi(n)$.*

Dowód. Niech

$$I := \{k \in \{1, \dots, m\} : \ \mathrm{NWD}(k, m) = 1\}, \quad J := \{l \in \{1, \dots, n\} : \ \mathrm{NWD}(l, n) = 1\}$$

oraz

$$A := \{s \in \{1, \dots, m \cdot n\} : \ \mathrm{NWD}(s, m \cdot n) = 1\}.$$

Wtedy oczywiście $\#(I \times J) = \varphi(m)\varphi(n)$, zaś $\#(A) = \varphi(mn)$. Skonstruujemy bijekcję między zbiorami $I \times J$ i A.

[14] Funkcja o dziedzinie $\mathbb{N}$ i wartościach zespolonych.

Zgodnie z twierdzeniem chińskim o resztach 1.4.8, dla dowolnej pary liczb $(k,l) \in I \times J$ istnieje dokładnie jedna liczba $z_{k,l} \in \{1,\ldots,mn\}$ spełniająca warunki

$$\begin{cases} z_{k,l} \equiv k \pmod m \\ z_{k,l} \equiv l \pmod n \end{cases}$$

(jedyność wynika z żądania, aby $z_{k,l} \in \{1,\ldots,mn\}$). Liczba ta jest względnie pierwsza z liczbą m (bo k była) oraz z liczbą n (bo l była) stąd jest względnie pierwsza z mn. Mamy więc dobrze określone odwzorowanie:

$$\Phi : I \times J \ni (k,l) \longrightarrow z_{k,l} \in A.$$

Wykażemy, że Φ jest injekcją. Niech bowiem $z_{k,l} = z_{k',l'}$ i na przykład $1 \leqslant k < k' \leqslant m$. Wtedy $m|(z_{k,l} - k)$ i $m|(z_{k,l} - k')$, skąd $m|(k' - k)$, co prowadzi do sprzeczności.

By dokończyć dowód wykażemy, że Φ jest surjekcją. Jeśli $z \in A$, to $z = \Phi(k,l)$ gdzie $k := z \pmod m$ oraz $l := z \pmod n$. Łatwo sprawdzić, że $(k,l) \in I \times J$. Wobec tego $\varphi(m)\varphi(n) = \#(I)\cdot\#(J) = \#(I\times J) = \#(A) = \varphi(mn)$ i dostajemy tezę. □

Wniosek 1.5.4. *Jeśli $n \in \mathbb{N}$, to $\varphi(n) = n\prod_{p|n}(1-1/p)$, gdzie iloczyn bierzemy po liczbach pierwszych dzielących n.*

Dowód. Jeśli $n = p_1^{k_1}\cdot\ldots\cdot p_r^{k_r}$, gdzie $p_1,\ldots,p_r$ to parami różne liczby pierwsze oraz $k_1,\ldots,k_r > 0$, to

$$\varphi(n) = \varphi(p_1^{k_1})\cdot\ldots\cdot\varphi(p_r^{k_r}) = p_1^{k_1}\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot p_r^{k_r}\left(1-\frac{1}{p_r}\right) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right).$$

□

Udowodnimy teraz własność funkcji Eulera, która zostanie wykorzystana w ostatniej części wykładu przy badaniu własności grupy multiplikatywnej ciała skończonego.

Własność 1.5.5. *Dla każdego $n \in \mathbb{N}$ prawdziwa jest równość $\sum_{d|n}\varphi(d) = n$, gdzie sumujemy po wszystkich dodatnich dzielnikach n.*

Dowód. Zauważmy, że jeśli $k \in \{1,\ldots,n\}$, to $\mathrm{NWD}(n,k) = n/d$ dla pewnego dzielnika d liczby n. Jeżeli teraz:

$$n_d := \#\{k \in \mathbb{N} :\ k < n, \mathrm{NWD}(n,k) = n/d\},$$

to $n = \sum_{d|n} n_d$. Niech teraz liczba $k \in \{1,\ldots,n\}$ będzie taka, że $\mathrm{NWD}(n,k) = n/d = l$. Wtedy $k = lm$ dla pewnego $m < d$ oraz z równości $\mathrm{NWD}(n,k) = l$ otrzymujemy $\mathrm{NWD}(m,d) = l$. Oznacza to, że czyli liczby $k \in \{1,\ldots,n\}$ spełniające warunek $\mathrm{NWD}(n,k) = l$ są postaci lm, gdzie $m \in \{1,\ldots,d\}$ oraz $\mathrm{NWD}(m,d) = 1$. Otrzymujemy stąd równość $n_d = \varphi(d)$. Łącząc oba te fakty otrzymujemy tezę. □

1.6 Małe twierdzenie Fermata, twierdzenie Eulera oraz twierdzenie Wilsona

W tym podrozdziale przedstawimy trzy podstawowe twierdzenia elementarnej teorii liczb: małe twierdzenie Fermata, twierdzenie Eulera i twierdzenie Wilsona. Zaczniemy od sformułowania tzw. „Małego Twierdzenia Fermata", które z praktycznych względów wyprowadzimy jednak z ogólniejszego twierdzenia Eulera.

Twierdzenie 1.6.1 (Małe twierdzenie Fermata (MTF))**.** *Niech $p \in \mathbb{P}$ i $k \in \mathbb{Z}$.*

(1) Jeśli $\mathrm{NWD}(k,p) = 1$*, to* $k^{p-1} \equiv 1 \pmod p$.

(2) Jeśli $\mathrm{NWD}(k,p) = p$*, to* $k^p \equiv k \pmod p$.

Małe Twierdzenie Fermata sformułowane zostało w korespondencji z innym znanym siedemnastowiecznym matematykiem francuskim: Bernardem Frénicle de Bessy. Korespondencja tych dwóch uczonych była inspiracją do wielu zaskakujących odkryć, by jako przykład podać choćby nietypową własność liczby 1729, która jest najmniejszą liczbą naturalną, jaką można przedstawić na dwa różne sposoby w postaci sumy dwóch sześcianów. W swoim

liście do de Bessy'ego z roku 1640 Fermat formułuje niżej omówione twierdzenie, z charakterystycznym dla siebie komentarzem: „de quoi je vous envoierois la démonstration, si je n'appreéhendois d'être trop long", czyli w wolnym tłumaczeniu: „której to własności dowód bym Ci przesłał, gdyby nie był on tak długi". Komentarz ten na szczęście, w przeciwieństwie do analogicznego dotyczącego Wielkiego Twierdzenia Fermata, nie znalazł potwierdzenia. Około 100 lat później, Euler w pracy z roku 1736 zatytułowanej *Theorematum Quorundam ad Numeros Primos Spectantium Demonstratio* przedstawił dowód MTF (warto jednak wspomnieć, że później okazało się, że mniej więcej w tym samym czasie, niezależnie twierdzenie to udowodnił też Leibniz, o czym Euler nie miał jednak możliwości wiedzieć). Dziś istnieje niezliczona ilość dowodów twierdzenia MTF, w których wykorzystuje się narzędzia z bardzo różnorodnych dziedzin matematyki.

W tej chwili wykorzystamy fakt, że dziś możemy na niego patrzeć jak na wniosek z ogólniejszego twierdzenia Eulera. Zanim sformułujemy to twierdzenie będzie nam potrzeba jeszcze jedna definicja.

Definicja 1.6.2 (układ reszt)**.** Niech $m \in \mathbb{N}$ będzie ustalone. Układem reszt modulo m nazywamy dowolny m elementowy zbiór $U \subset \mathbb{Z}$ o tej własności, że dla dowolnego $i \in \{0, \ldots, m-1\}$ istnieje dokładnie jeden element $u \in U$, że $i \equiv u \pmod{m}$.

Przykładowo, zbiór $\{-2, 0, 1, 7\}$ jest układem reszt modulo 4.

Definicja 1.6.3 (zredukowany układ reszt)**.** Niech $m \in \mathbb{N}$ będzie ustalone. Zredukowanym układem reszt modulo m nazywamy dowolny $\varphi(m)$ elementowy zbiór $U \subset \mathbb{Z}$ o tej własności, że dla dowolnego $i \in \{1, \ldots, m\}$, $\mathrm{NWD}(i, m) = 1$, istnieje dokładnie jeden element $u \in U$, że $i \equiv u \pmod{m}$.

Przykładowo, zbiór $\{-3, -2, 1, 9\}$ jest zredukowanym układem reszt modulo 5.

Jesteśmy gotowi by sformułować i udowodnić następujące twierdzenie.

Twierdzenie 1.6.4 (Twierdzenie Eulera)**.** *Jeśli* $m \in \mathbb{N}$, $k \in \mathbb{Z}$ *oraz* $\mathrm{NWD}(k, m) = 1$, *to* $k^{\varphi(m)} \equiv 1 \pmod{m}$.

Dowód. Niech $U_m := \{a_1, \ldots, a_{\varphi(m)}\}$ będzie zredukowanym układem reszt modulo m. Zauważmy, że zbiór $kU_m = \{ka_1, \ldots, ka_{\phi(m)}\}$ również jest zredukowanym układem reszt modulo m, co jest konsekwencją względnej pierwszości liczb k i m. Oznacza to, że zachodzą związki

$$\prod_{i=1}^{\varphi(m)} a_i \equiv \prod_{i=1}^{\varphi(m)} (ka_i) = k^{\varphi(m)} \prod_{i=1}^{\varphi(m)} a_i \pmod{m}.$$

Ponieważ $\mathrm{NWD}\left(m, \prod_{i=1}^{\varphi(m)} a_i\right) = 1$ (por. 1.4.5(4)), więc możemy podzielić skrajne strony powyższej kongruencji przez $\prod_{i=1}^{\varphi(m)} a_i$ otrzymując w efekcie

$$k^{\varphi(m)} \equiv 1 \pmod{m}.$$

Na koniec zauważmy, że jeśli $m = p$ jest liczbą pierwszą jak w sformułowaniu twierdzenia Fermata, to dostajemy dokładnie tezę tego twierdzenia, gdyż $\varphi(p) = p - 1$. □

Nasze wstępne rozważania teorio-liczbowe zakończymy następującym twierdzeniem, sformułowanym przez Johna Wilsona[15] (wg *Meditationes Algebraicae* opublikowanego przez mentora Johna Wilsona Edwarda Waringa w 1770 roku mimo, iż żaden z nich nie potrafił wówczas udowodnić prezentowanej własności – dowód zamieszczony został dopiero w trzeciej edycji tekstu, faktycznie twierdzenie znane było znacznie wcześniej), zaś udowodnionym przez Lagrange'a w traktacie z tego samego roku.

Twierdzenie 1.6.5 (twierdzenie Wilsona)**.** *Liczba* $n \in \mathbb{N}$ *jest pierwsza wtedy i tylko wtedy, gdy* $(n-1)! \equiv -1 \pmod{n}$.

Dowód. Jeśli $n = 2$ lub $n = 3$, to teza zachodzi. Załóżmy zatem, że $n \geqslant 4$. Jeśli n jest liczbą złożoną, to jej wszystkie dzielniki znajdują się w zbiorze $A = \{1, 2, \ldots, n-1\}$. Rzecz jasna $\mathrm{NWD}((n-1)!, n) > 1$, co oznacza, że kongruencja $(n-1)! \equiv -1 \pmod{n}$ jest niemożliwa. Jeśli n jest liczbą pierwszą, to żadna z liczb $i \in A$ nie jest dzielnikiem n. Oznacza to, że $\mathrm{NWD}(i, n) = 1$ dla $i \in A$. W konsekwencji, dla dowolnego $i \in A$ istnieje dokładnie jedna liczba $a_i \in A$, dla której $ia_i \equiv 1 \pmod{n}$ (por. 1.4.6). Ponadto $i = a_i$ wtedy i tylko wtedy, gdy $i = 1$ lub $i = n - 1$ (bo

[15] John Wilson: matematyk angielski, 1741–1793, najbardziej znany właśnie ze sformułowania omawianego twierdzenia.

n jest liczbą pierwszą). Oznacza to, że pomijając liczby $i = 1$ oraz $i = n - 1$, zbiór $\{2, \ldots, n-2\}$ można ustawić w pary różnych elementów o iloczynie równym 1, co prowadzi nas do kongruencji

$$2 \cdot 3 \cdot \ldots \cdot (n-2) \equiv 1 \pmod{n}.$$

Mnożąc powyższą kongruencję stronami przez $n - 1$ otrzymujemy

$$(n-1)! \equiv n - 1 \equiv -1 \pmod{n},$$

co daje drugą część tezy i kończy dowód. □

1.7 Zadania

1. Obliczyć NWD(112, 341), NWD(331, 214), NWD(75, 14) i wyznaczyć liczbę kroków w algorytmie Euklidesa konieczną do obliczenia wskazanych liczb.

2. Dla przedstawionych poniżej par liczb a, b znaleźć $d = (a, b)$, a następnie znaleźć liczby całkowite x, y takie, że $ax + by = d$, gdzie:

   (a) $a = 32,\ b = 20$,
   (b) $a = 55,\ b = 14$,
   (c) $a = 35,\ b = 24$,
   (d) $a = 101,\ b = 19$.

3. Scharakteryzować wszystkie całkowite rozwiązania liniowych równań diofantycznych:

   (a) $127x + 13y = 1$,
   (b) $288x + 158y = 2$,
   (c) $119x - 28y = 7$,
   (d) $10x - 45y = 15$.

4. Udowodnić, że dla każdej liczby naturalnej $n \geqslant 1$ mamy $(n^2 + n + 1, n^4 + 1) = 1$.

5. Udowodnić, że $\mathrm{NWD}(a^m - 1, a^n - 1) = a^{\mathrm{NWD}(m,n)} - 1$, gdzie $a \in \mathbb{N}$.

6. Niech $a \in 2\mathbb{N}_+$. Dowieść, że $\mathrm{NWD}(a^{2^m} + 1, a^{2^n} + 1) = 1$ dla $m \neq n$. Wykorzystać ten fakt do dowodu, że istnieje nieskończenie wiele liczb pierwszych.

7. Dowieść, że istnieją dowolnie długie ciągi kolejnych liczb naturalnych, których wyrazy są liczbami złożonymi.

8. Rozwiązać (lub pokazać, że nie jest to możliwe) następujące układy kongruencji:

   (a) $\begin{cases} x \equiv 11 \pmod{14} \\ x \equiv 13 \pmod{20} \\ x \equiv 8 \pmod{11} \end{cases}$,

   (b) $\begin{cases} 2x \equiv 1 \pmod{11} \\ 6x \equiv 2 \pmod{5} \\ 3x \equiv 4 \pmod{7} \end{cases}$,

   (c) $\begin{cases} x \equiv 1 \pmod{10} \\ x \equiv 3 \pmod{12} \\ x \equiv 6 \pmod{15} \end{cases}$.

9. Znaleźć niekongruentne rozwiązania kongruencji liniowych:

   (a) $5x \equiv 7 \pmod{8}$,
   (b) $15x \equiv 40 \pmod{25}$,

(c) $13x \equiv 14 \pmod{15}$.

10. Obliczyć:
$$4^{14} \pmod{15}, \quad 7^{1200} \pmod{15}, \quad 25^{2550} \pmod{18}.$$

11. Dowieść, że jeśli n jest liczbą złożoną, to istnieje dzielnik d liczby n taki, że $1 < d \leqslant \sqrt{n}$.

12. Które z poniższych zdań jest prawdziwe (uzasadnić swoją odpowiedź)?

(a) Jeśli $\mathrm{NWD}(a, b) = 1$ i $\mathrm{NWD}(b, c) = 1$, to $\mathrm{NWD}(a, c) = 1$.

(b) Jeśli $\mathrm{NWD}(a, b) = 2$ i $\mathrm{NWD}(b, c) = 2$, to $\mathrm{NWD}(a, c) = 2$.

(c) Jeśli $\mathrm{NWD}(a, b) = d$, to $\mathrm{NWD}(a + b, a - b) = d$.

(d) $\mathrm{NWD}(a, a - b) = 1$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, b) = 1$.

13. Wykazać, że jeśli p, q są dwoma kolejnymi nieparzystymi liczbami pierwszymi, to liczba $p + q$ ma co najmniej trzy dzielniki pierwsze (liczone z krotnościami).

14. Wykazać, że jeśli dla $n \in \mathbb{N}_+$ i $p \in \mathbb{P}$ spełniona jest nierówność $\frac{n+1}{2} < p \leqslant n$, to
$$p \Big| \binom{n}{\frac{n+1}{2}}.$$

15. Scharakteryzować naturalne rozwiązania kongruencji
$$\prod_{i=1}^{n} i \equiv 0 \pmod{\sum_{i=1}^{n} i}.$$

Rozdział 2

Działania i ich własności

Zanim zaczniemy omawiać podstawowe struktury algebraiczne wprowadzimy pojęcie działania oraz uporządkujemy własności działań, jakie możemy określić na wzór znanych działań liczbowych.

Definicja 2.0.1 (działanie)**.** Niech X będzie zbiorem niepustym, zaś $X \times X := \{(x, y) : \ x \in X, y \in X\}$ iloczynem kartezjańskim tego zbioru przez siebie. Każde odwzorowanie przypisujące parze elementów z X (czyli elementowi z $X \times X$) element z X:

$$\star : X \times X \ni (x, y) \mapsto x \star y \in X,$$

nazywamy **działaniem na zbiorze** X. ([1])

Przykład 2.0.2.

(1) Odwzorowanie $\mathbb{Q}\times\mathbb{Q} \ni (x, y) \mapsto x \cdot y \in \mathbb{Q}$ jest działaniem na zbiorze liczb wymiernych (iloczyn liczb wymiernych jest liczbą wymierną).

(2) Odwzorowanie $\mathbb{N} \times \mathbb{N} \ni (x, y) \mapsto x - y \in \mathbb{Z}$ NIE jest działaniem na zbiorze $\mathbb{N}$ gdyż może parze liczb naturalnych przypisać liczbę ujemną.

Definicja 2.0.3 (rodzaje działań)**.** Niech $\star : X \times X \ni (x, y) \longrightarrow x \star y \in X$ będzie działaniem na zbiorze X.

(1) Działanie $\star$ nazywamy **łącznym**, gdy $\forall\ x, y, z \in X : \ (x \star y) \star z = x \star (y \star z)$.

(2) Działanie $\star$ nazywamy **przemiennym,** gdy $\forall\ x, y \in X : \ x \star y = y \star x$.

(3) Element $e \in X$ nazywamy **elementem neutralnym** działania $\star$, gdy $\forall\ x \in X : \ x \star e = e \star x = x$. ([2])

(4) Jeśli dla działania $\star$ istnieje element neutralny e, to dla dowolnego $x \in X$ element $\overline{x}$ nazywamy **elementem symetrycznym (elementem odwrotnym)** do elementu x względem działania $\star$, jeśli $x \star \overline{x} = \overline{x} \star x = e$. ([3])

(5) Jeśli na zbiorze X zadane są dwa działania: $\star$ oraz $\bullet$, to działanie $\bullet$ nazywamy **rozdzielnym względem działania** $\star$, gdy:

$$\forall\ x, y, z \in X : \ (x \star y) \bullet z = (x \bullet z) \star (y \bullet z) \ \text{ i } \ z \bullet (x \star y) = (z \bullet x) \star (z \bullet y).$$

2.1 Podstawowe przykłady działań

I. Kanoniczne przykłady liczbowe

(1) Działania dodawania wprowadzone na zbiorach $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.

(2) Działania mnożenia wprowadzone na zbiorach $\mathbb{Q}^\star$, $\mathbb{R}^\star$, $\mathbb{C}^\star$.[4]

[1] Czasem fakt, że para punktów z X przechodzi na punkt z X nazywa się wewnętrznością działania.

[2] Uwaga: element neutralny nie zawsze musi istnieć, np. w $\mathbb{N}$ nie istnieje element neutralny dodawania.

[3] Uwaga: element symetryczny może dla pewnych elementów istnieć, dla innych nie np. w zbiorze $\mathbb{Z}$ z działaniem mnożenia dla 1 element symetryczny istnieje, ale nie istnieje np. dla 2.

[4] Wskazane działania można oczywiście wprowadzać także na innych zbiorach liczbowych (np. mnożenie możemy określić na zbiorze liczb całkowitych) – prezentujemy tu jednak umownie „kanonicznie" rozumiane działania, które posiadają we wskazanych zbiorach szereg podstawowych własności.

II. Działania w zbiorach macierzy

Bardzo ważnym typem działania jest działanie mnożenia na odpowiednio dobranych zbiorach macierzy. Najczęściej pracować będziemy z macierzami o wartościach liczbowych (tzn. całkowitych, wymiernych, rzeczywistych lub zespolonych), ale rozważać będziemy też macierze o współczynnikach pochodzących np. z pierścieni reszt modulo liczba naturalna $n \geqslant 2$.

Zbiór wszystkim macierzy kwadratowych wymiaru n nad pewnym zbiorem liczbowym A będziemy oznaczać przez $M_n(A)$. Na zbiorze tym rozważać będziemy domyślnie działanie dodawania macierzy.

Zbiór wszystkich macierzy nieosobliwych[5] wymiaru n nad pewnym zbiorem liczbowym A oznaczać będziemy $GL_n(A)$. W zbiorze tym rozważać będziemy domyślnie działanie mnożenia macierzy.

III. Zbiory odwzorowań i działania na nich

Definicja 2.1.1 (permutacje zbioru)**.** Jeśli X jest zbiorem niepustym, zaś $f : X \longrightarrow X$ jest bijekcją zbioru X na samego siebie, to odwzorowanie takie będziemy nazywać **permutacją** zbioru X.

Zbiór wszystkich permutacji zbioru X będziemy oznaczać przez $S(X)$.

Szczególnym przypadkiem permutacji są permutacje zbioru skończonego.

Definicja 2.1.2 (permutacje)**.** Rozważmy zbiór n-elementowy: $\{1, 2, \ldots, n\}$. Każdą bijekcję tego zbioru na siebie będziemy nazywać **permutacją zbioru** $\{1, \ldots, n\}$ i zwyczajowo oznaczać będziemy takie odwzorowania przez litery greckie, np. σ. ([6])

Każde z takich odwzorowań zapisywać będziemy dalej także w poniższej, wygodnej w praktyce formie:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix},$$

gdzie oznaczenie to mówi, że nasze odwzorowanie σ przeprowadza 1 na $\sigma(1)$, 2 na $\sigma(2)$ itd. aż do n na $\sigma(n)$.

Zbiór permutacji zbioru X będziemy rozważać domyślnie z działaniem **składania** tzn. $g \star f := g \circ f$. Często, dla uproszczenia, zamiast mówić „składanie permutacji", będziemy stosować nazewnictwo „mnożenie permutacji" i zamiast pisać $\sigma \circ \tau$, napiszemy $\sigma \cdot \tau$ lub po prostu $\sigma\tau$.

Zbiór wszystkich permutacji zbioru $\{1, \ldots, n\}$ będziemy dalej oznaczać przez S_n.

2.1.0.1 Tabela działania na zbiorze

Częstym sposobem zapisu działania na zbiorze skończonym jest tabela tego działania – tak zwana tabliczka Cayleya.[7]

Ułóżmy dla przykładu tabelę działania w zbiorze permutacji trzyelementowych.

Tabela działania składania/mnożenia permutacji 3 elementowych $S_3 = \{\sigma_1, \sigma_2, \ldots, \sigma_6\}$, gdzie $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, ma postać:

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_5	σ_6	σ_3	σ_4
σ_3	σ_3	σ_6	σ_1	σ_5	σ_4	σ_2
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_4	σ_2	σ_3	σ_6	σ_1
σ_6	σ_6	σ_3	σ_4	σ_2	σ_1	σ_5

[5] Pamiętamy, że macierz nieosobliwa to macierz o wyznaczniku różnym od zera.

[6] Taka notacja przyjęła się za klasycznym podręcznikiem H.Wielandta, *Finite Permutation Groups*, Academic Press, New York, 1964.

[7] Arthur Cayley: matematyk i prawnik angielski (1821–1895) znany m.in. z prac na temat teorii grup. Pochodzi od niego w szczególności dowód faktu, że każda grupa (zbiór z działaniem łącznym, dla którego istnieje element neutralny i każdy z elementów posiada symetryczny, 3.1.2) może być traktowana jako „część" (formalnie: podgrupa 3.1.11) pewnej grupy permutacji (por. 3.2.13).

IV. Kongruencje i działania modulo

Na zbiorze $\mathbb{Z}_m$ (por. 1.4.2) będziemy wprowadzać dwa działania: dodawania i mnożenia.

Definicja 2.1.3.

(1) Dla $[k]_m, [l]_m \in \mathbb{Z}_m$ definiujemy: $[k]_m + [l]_m := [k+l]_m$;

(2) Dla $[k_m], [l]_m \in \mathbb{Z}_m$ definiujemy: $[k]_m \cdot [l]_m := [k \cdot l]_m$.

Gdy nie będzie to prowadziło do nieporozumień, poruszając się w $\mathbb{Z}_m$ będziemy pisać po prostu: $k+l$ i $k \cdot l$ rozumiejąc przez ów zapis odpowiednie działania modulo wykonywane na odpowiednich klasach. Zauważmy, że wprowadzone działania są poprawnie określone na podstawie 1.4.3.

Zobaczmy wspomniane operacje na przykładzie działania mnożenia w $\mathbb{Z}_5$:

$[3]_5 = [8]_5$, $[2]_5 = [12]_5$ – gdy wymnożymy mamy: $[3]_5 \cdot [2]_5 = [6]_5 = [1]_5$ i analogicznie $[8]_5 \cdot [12]_5 = [96]_5 = [1]_5$.

($\star$) Tabela działania mnożenia modulo 5 w $\mathbb{Z}_5^\star = \{1, 2, 3, 4\}$

$\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

2.2 Zadania

1. Sprawdzić, czy wprowadzone operacja w zbiorze X jest działaniem. Jeśli tak, to zbadać jego własności (przemienność, łączność, istnienie elementu neutralnego, istnienie elementu odwrotnego do każdego elementu zbioru):

   (a) $X = \mathbb{R}$ oraz $a \circ b = \frac{1}{2}a + b$ dla $a, b \in \mathbb{R}$;

   (b) $X = \mathbb{R}$ oraz $a \circ b = \max\{a, b\}$ dla $a, b \in \mathbb{R}$;

   (c) $X = \mathbb{Z}$ oraz $a \circ b = a + b - ab$ dla $a, b \in \mathbb{Z}$;

   (d) X – zbiór izometrii płaszczyzny z działaniem składania izometrii płaszczyzny;

   (e) X – zbiór obrotów płaszczyzny z działaniem składania obrotów płaszczyzny;

   (f) $X = \mathbb{Z}$ oraz $a \triangle b = \begin{cases} 0, & \text{gdy } a+b \text{ jest liczbą parzystą,} \\ 1, & \text{gdy } a+b \text{ jest liczbą nieparzystą,} \end{cases}$ gdzie $a, b \in \mathbb{Z}$;

   (g) $X = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}, \text{ gdzie } x \in \mathbb{Z} \right\}$ z działaniem mnożenia macierzy;

   (h) $X = \{(a + b\sqrt{2} + c\sqrt{3}) : (a, b, c) \in \mathbb{Z}^3\}$ z operacją dodawania (mnożenia) elementów;

   (i) $X = \{(a + b\sqrt{6} + c\sqrt{10} + d\sqrt{10}) : (a, b, c, d) \in \mathbb{Q}^4\}$ z operacją dodawania (mnożenia) elementów;

   (j) W poniższych podpunktach przyjmujemy $X = \{f : \mathbb{R} \longrightarrow (0, +\infty)\}$. Wykonać zadanie dla odpowiedniego zbioru i wskazanego działania wykonywanego na funkcjach:

      i. X z operacją dodawania (mnożenia);

      ii. zbiór $Y := \{f \in X : f(0) > f(1)\}$ z operacją dodawania (mnożenia);

      iii. zbiór $Y := \{f \in X : f(0) = 1\}$ z operacją dodawania (mnożenia);

      iv. zbiór $Y := \{f \in X : f$ jest funkcją parzystą$\}$ z operacją dodawania (mnożenia);

      v. zbiór $Y := \{f \in X : f$ jest funkcją nieparzystą$\}$ z operacją dodawania (mnożenia).

Rozdział 3

Podstawy teorii grup

Korzeni teorii grup należy się doszukiwać bardzo głęboko w rozwoju relacji między pojęciami klasycznej algebry, arytmetyki i geometrii – do powstania podstaw pojęcia grupy doprowadziły w dużej mierze próby znalezienia wspólnego opisu własności teorioliczbowych i geometrycznych. Te dwa elementy, wspierane bodźcem poszukiwania rozwiązań równań wyższych stopni, zostały w końcu sprowadzone do wspólnej płaszczyzny i utworzono zręby m.in. języka teorii grup. Postęp czyniony w badaniach geometrii nieeuklidesowych, dalej prace Gaussa, Eulera, Lagrange'a[1] i wielu innych nad rozwiązalnością równań stopnia co najmniej 5 legły u podstaw badań Galois[2] i Abela[3]. Od czasu tych dwóch matematyków całe pokolenia następców podejmowały idee przez nich zapoczątkowane rozwijając teorię grup i ciał – by wspomnieć Dedekinda[4], Kroneckera[5], czy Jordana[6]. To oni wzbogacili wprowadzane wcześniej pojęcia i stosowali już teorię grup w mniej lub bardziej znanej nam dziś formie. Konkretny wkład większości z nich poznamy w dalszym ciągu wykładu. W przeciągu wieków pojęcie grupy przeszło długą ewolucję zanim nabrało współczesnego kształtu, a i dziś możliwe są dwa różne podejścia do charakteryzacji struktury grupowej. Oprzemy się na aksjomatycznym pojęciu grupy.[7]

3.1 Podstawowe definicje i przykłady

Pojęcie grupy

Zanim wprowadzimy pojęcie grupy zacznijmy od prostej obserwacji.

Uwaga 3.1.1. Rozważmy działanie $\star$ na zbiorze X, które jest działaniem łącznym i posiada element neutralny. Wtedy:

(1) element neutralny jest wyznaczony jednoznacznie,

(2) jeśli dla elementu $x \in X$ istnieje element symetryczny, to jest on jedyny.

Dowód. (1) Wystarczy zauważyć, że jeśli $e \in X$ oraz $\tilde{e} \in X$ są elementami neutralnymi dla działania $\star$, to $\tilde{e} = \tilde{e} \star e = e$.

(2) Jeśli $\bar{x} \in X$ oraz $\tilde{x} \in X$ są elementami symetrycznymi dla elementu $x \in G$, to

$$\tilde{x} = \tilde{x} \star e = \tilde{x} \star (x \star \bar{x}) = (\tilde{x} \star x) \star \bar{x} = e \star \bar{x} = \bar{x}.$$

□

[1] Joseph Louis Lagrange: matematyk i astronom włoskiego pochodzenia, pracujący głównie we Francji, (1736–1813).

[2] Evariste Galois: matematyk francuski, „Mozart matematyki", zginął mając zaledwie 21 lat, (1811–1832) pozostawiając po sobie ogromny wkład w rozwój teorii grup i nowoczesnej teorii równań algebraicznych.

[3] Niels Henrik Abel: matematyk norweski (1802–1829).

[4] Julius Wilhelm Richard Dedekind: matematyk niemiecki, (1831–1916).

[5] Leopold Kronecker: matematyk niemiecki (1823–1891).

[6] Marie Ennemond Camille Jordan: matematyk francuski, (1838–1922).

[7] Pojęcie grupy, jeszcze nienazwane, wystąpiło po raz pierwszy u Lagrange'a (grupa permutacji n elementów). W swoim *Disquisitiones* Gauss wykorzystuje grupę addytywną i multiplikatywną reszt modulo m, bada też grupy klas form kwadratowych. Dość często autorstwo terminu „grupa" przypisuje się Galois, który użył w jednym ze swoich rękopisów określenia „groupe", ale tę samą nazwę zastosował do tego, co dziś określamy jako warstwy grupy względem podgrupy, miał więc chyba bardziej na myśli po prostu „zbiór" niż to co my rozumiemy jako grupę, czyli zbiór z działaniem o konkretnych własnościach. Z pewnością formalnym twórcą pojęcia grupy abstrakcyjnej jest Arthur Cayley, który zdefiniował je w 1854 roku w swoim pierwszym artykule o teorii grup opublikowanym w Philosophical Magazine. Do tego czasu zajmowano się jedynie grupami permutacji n elementów. Dalej należy obecną formę pojęcia grupy wiązać z pracami Kroneckera, Burnside'a, von Dycka i H.M. Webera.

Definicja 3.1.2 (grupa)**.** Niech G będzie zbiorem niepustym, zaś

$$\star : G \times G \ni (x, y) \longrightarrow x \star y \in G$$

działaniem (2.0.1) na G dla którego:

(1) zachodzi łączność,

(2) istnieje element neutralny $e \in G$,

(3) każdy element $x \in G$ posiada element symetryczny $\overline{x} \in G$.

Wtedy parę $(G, \star)$ nazywamy **grupą z działaniem** $\star$. Jeśli nie będzie to prowadziło do nieporozumień, będziemy często pisali po prostu grupa G zamiast grupa $(G, \star)$. W domyśle jednak grupa jest zawsze zbiorem wraz z działaniem[8].

Jeśli dodatkowo działanie $\star$ jest przemienne, to grupę nazywamy **przemienną** lub **abelową**.

Uwaga 3.1.3.
(1) Jeśli od określonego na G działania wymagamy jedynie łączności, to parę $(G, \star)$ nazywamy **półgrupą**.

(2) Jeśli $(G, \star)$ jest półgrupą i dodatkowo zakładamy, że istnieje w G element neutralny działania $\star$, to $(G, \star)$ nazywamy **monoidem**.

Półgrupy i monoidy, choć to struktury znacznie uboższe od grup znajdują wiele konkretnych, praktycznych zastosowań, by wymienić choćby teorię języków formalnych czy genetykę (por. np. [11]).

Definicja 3.1.4 (rząd grupy)**.** O grupie G mówimy, że jest skończona, gdy zbiór G jest skończony. Wówczas liczbę elementów G, czyli $\#G$ nazywamy **rzędem grupy** G i oznaczamy $|G|$.
Jeśli zbiór G jest nieskończony, to mówimy, że G jest grupą o **rzędzie nieskończonym** (lub **grupą nieskończoną**) i piszemy $|G| = \infty$.

Przykład 3.1.5.
(1) Dla grup: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ mamy: element neutralny $e = 0$, element symetryczny = liczba przeciwna do danej; są to nieskończone grupy abelowe.

(2) Dla grup: $(\mathbb{Q}^\star, \cdot)$, $(\mathbb{R}^\star, \cdot)$, $(\mathbb{C}^\star, \cdot)$ mamy: element neutralny $e = 1$, element symetryczny = odwrotność danej liczby; są to nieskończone grupy abelowe.

(3) Grupy reszt modulo:

$(\mathbb{Z}_n, +_n)$, gdzie $[k]_n +_n [l]_n := [k + l]_n$, jest to skończona grupa abelowa rzędu n;

$(\mathbb{Z}_n^\star, \cdot_n)$, gdzie $[k]_n \cdot_n [l]_n := [k \cdot l]_n$, jest to skończona grupa (abelowa) rzędu $(n-1)$ wtedy i tylko wtedy, gdy $n \in \mathbb{P}$ – fakt ten proponujemy sprawdzić w ramach ćwiczenia.

(4) $(U(\mathbb{Z}_n), \cdot_n)$, gdzie $U(\mathbb{Z}_n) := \{k \in \mathbb{Z}_n : \text{ NWD}(k, n) = 1\}$ – grupa reszt modulo n liczb względnie pierwszych z n; jest to skończona grupa abelowa rzędu $\varphi(n)$ (por. 1.5.1).

(5) Grupy macierzy z działaniem dodawania macierzy: $(\mathrm{M}_n(G), +)$ – grupa macierzy kwadratowych wymiaru n o współczynnikach z G, gdzie G oznacza zazwyczaj grupy addytywne $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ lub $\mathbb{C}$.

Jeśli $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ lub $\mathbb{Z}_p$ dla $p \in \mathbb{P}$, to $(\mathrm{GL}_n(F), \cdot)$ oznacza grupę nieosobliwych macierzy kwadratowych wymiaru n o współczynnikach z F, z działaniem mnożenia macierzy o współczynnikach z F. W ten sposób budujemy ważne przykłady grup nieprzemiennych (w tym w zależności od mocy zbioru podkładowego zwykle nieskończonych).

(6) Grupy symetryczne (ogólne grupy permutacji).

Działanie składania wprowadza na zbiorze $S(X)$, gdzie X – zbiór niepusty, strukturę grupy. Grupa $(S(X), \circ)$ bywa nazywana grupą symetryczną.

Dla $X := \{1, \ldots, n\}$ grupę $(S_n, \circ)$ nazywamy **grupą permutacji** n-elementowych. Rząd tej grupy to $n!$. Łatwo wykazać, że grupa ta jest grupą nieprzemienną wtedy i tylko wtedy, gdy liczba elementów w zbiorze X jest większa niż 2.

[8] Pamiętajmy, że na jednym zbiorze możemy wprowadzić często kilka różnych działań, które zadadzą na nim strukturę grupy.

Ponownie, w zależności od mocy zbiory podkładowego, mamy na ogół do czynienia z grupami nieprzemiennymi: skończonymi lub nieskończonymi.

(7) Grupa diedralna (dihedral group[9]) – grupa symetrii wielokąta foremnego z działaniem składania. Można spotkać się z dwoma notacjami dla tej grupy: D_n oraz D_{2n}, gdzie ta ostatnia związana jest z liczbą elementów grupy symetrii n-kąta foremnego (grupa taka złożona jest z n odbić i n-obrotów, w tym obrotu o 360 stopni traktowanego jako identyczność).

Do tej pory wprowadzaliśmy podstawowe definicje dotyczące pojęcia grupy i dla podkreślenia abstrakcyjnego charakteru tego pojęcia oznaczaliśmy działanie w grupie przez $\star$. Jednak zwykle w rozważaniach stosuje się bardziej swobodną terminologię: używa się klasycznie dwóch notacji: **multiplikatywnej** i **addytywnej**.

	Działanie	Element neutralny	Element symetryczny
Nazwa	mnożenie	jedynka grupy	element odwrotny
Oznaczenie	$x \cdot y$ lub xy	1_G lub 1	x^{-1}

Tablica 3.1: Notacja multiplikatywna.

	Działanie	Element neutralny	Element symetryczny
Nazwa	dodawanie	zero grupy	element przeciwny
Oznaczenie	$x + y$	0_G lub 0	$-x$

Tablica 3.2: Notacja addytywna.

Czasami w podręcznikach notacja addytywna stosowana jest w przypadku, gdy grupa jest abelowa. W skrypcie w dalszym ciągu teorii grup będziemy standardowo stosować notację multiplikatywną oraz skrótowo operować wyrażeniem „grupa G" zamiast „grupa $(G, \star)$", a także znakiem mnożenia $\cdot$ (często w ogóle pomijanym), zamiast $\star$. Nie należy jednak zapominać o tym, że grupa to zawsze zbiór **z działaniem** (co podkreślaliśmy wcześniej), a na jednym zbiorze można wprowadzać różne rodzaje działań, które zadają istotnie różne z punktu widzenia teorii grup struktury (por. 3.2.7).

Zauważmy, że według definicji działania możemy je „wykonywać" tylko na dwóch elementach – wiemy jaki element jest przypisany parze elementów. Łatwo jednak wprowadzić rekurencyjnie możliwość mnożenia skończenie wielu elementów tak, by zachować istotne własności.

Definicja 3.1.6 (iloczyn standardowy)**.** Niech G będzie grupą oraz $a_1, \ldots, a_n \in G$. Wtedy określamy **iloczyn elementów** $\prod_{i=1}^{n} a_i = a_1 \cdot \ldots \cdot a_n$ następująco:

$$\prod_{i=1}^{n} a_i = a_1 \cdot \ldots \cdot a_n := \begin{cases} a_1, & \text{dla } n = 1 \\ \left(\prod_{i=1}^{n-1} a_i\right) a_n, & \text{dla } n > 1. \end{cases}$$

Zobaczymy teraz, że takie uogólnienie ma pożądane cechy.

Własność 3.1.7 (podstawowe własności działania w grupie)**.** *Niech G będzie grupą oraz niech $a_1, \ldots, a_n \in G$. Wtedy:*

(1) zachodzi uogólnione prawo łączności, tzn. $(a_1 \cdot \ldots \cdot a_k)(a_{k+1} \cdot \ldots \cdot a_n) = a_1 \cdot \ldots \cdot a_n$ dla dowolnego $0 < k < n$.

(2) zachodzi wzór $(a_1 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1}$.

(3) jeśli dodatkowo grupa G jest przemienna, to zachodzi uogólnione prawo przemienności, tzn. $a_{\sigma(1)} \cdot \ldots \cdot a_{\sigma(n)} = a_1 \cdot \ldots \cdot a_n$ dla dowolnej permutacji $\sigma \in S_n$.

Dowód. Dowody wszystkich podpunktów przeprowadzamy indukcyjnie względem n.

[9] Dihedral group – określenie to oznacza dokładnie „grupę dwuścianu".

(1) Gdy $n = 1$ lub $n = 2$, to teza jest oczywista, zaś jeśli $n > 2$, to w oparciu o łączność działania w grupie zauważmy, że

$$\begin{aligned}(a_1 \cdot \ldots \cdot a_k)(a_{k+1} \cdot \ldots \cdot a_n) &= (a_1 \cdot \ldots \cdot a_k)\big((a_{k+1} \cdot \ldots \cdot a_{n-1})a_n\big)\\ &= \big((a_1 \cdot \ldots \cdot a_k)(a_{k+1} \cdot \ldots \cdot a_{n-1})\big)a_n\\ &= (a_1 \cdot \ldots \cdot a_{n-1})a_n\\ &= a_1 \cdot \ldots \cdot a_n.\end{aligned}$$

(2) W oczywisty sposób zaczynamy od $n = 2$. Wówczas zauważamy, że $(a_1a_2)(a_2^{-1}a_1^{-1}) = 1$, czyli z jedyności elementu odwrotnego mamy tezę.

Jeśli $n > 2$ oraz teza jest prawdziwa dla $(n-1)$ elementów, to

$$(a_1 \cdot \ldots \cdot a_n)^{-1} = a_n^{-1}(a_1 \cdot \ldots \cdot a_{n-1})^{-1} = a_n^{-1} \cdot \ldots \cdot a_1^{-1}.$$

(3) Dla $n = 2$ teza to nic innego jak przemienność działania w grupie.

Niech więc $n > 2$ oraz niech $1 \leqslant j \leqslant n$ będzie takie, że $\sigma(j) = n$. Możemy założyć, że $1 < j < n$ (z sytuacją $j = 1$ lub $j = n$ radzimy sobie prosto, stosując założenie indukcyjne bezpośrednio do pozostałych elementów i ewentualnie wykorzystując dodatkowo przemienność grupy). Mamy teraz

$$\begin{aligned}a_{\sigma(1)} \cdot \ldots \cdot a_{\sigma(n)} &= (a_{\sigma(1)} \cdot \ldots \cdot a_{\sigma(j-1)})a_n(a_{\sigma(j+1)} \cdot \ldots \cdot a_{\sigma(n)})\\ &= (a_{\sigma(1)} \cdot \ldots \cdot a_{\sigma(j-1)}a_{\sigma(j+1)} \cdot \ldots \cdot a_{\sigma(n)})a_n\\ &= (a_{\varrho(1)} \cdot \ldots \cdot a_{\varrho(n-1)})a_n\\ &= (a_1 \cdot \ldots \cdot a_{n-1})a_n\\ &= a_1 \cdot \ldots \cdot a_n,\end{aligned}$$

gdzie permutacja $\varrho \in S_{n-1}$ dana jest wzorem

$$\varrho(k) = \begin{cases}\sigma(k), & \text{gdy } \ 1 \leqslant k \leqslant j-1,\\ \sigma(k+1), & \text{gdy } \ j \leqslant k \leqslant n-1.\end{cases}$$

„Opisowo" możemy streścić powyższe rozumowanie następująco: szukamy miejsca, w którym jest a_n a następnie korzystając z łączności i przemienności grupy (bierzemy jako jeden element a_n a jako drugi iloczyn tych, które stoją „za nim") przesuwamy go na koniec. Do pierwszej części, która jest permutacją $(n-1)$-elementową stosujemy założenie indukcyjne. □

Zauważmy dodatkowo prostą, a jednocześnie bardzo użyteczną własność, która wynika wprost z łączności i istnienia elementu odwrotnego do dowolnego elementu grupy.

Własność 3.1.8 (prawo skracania)**.** *Jeśli a, b, c są elementami grupy G, to z faktu, że $ab = ac$ lub $ba = ca$ wynika, że $b = c$.*

Warto tu przypomnieć fakt, o którym pisaliśmy już w notce historycznej przy okazji definicji wprowadzonej przez Webera. Mianowicie, można wykazać (co pozostawiamy jako ćwiczenie), że prawo skracania jest równoważne istnieniu elementu odwrotnego w przypadku gdy zbiór G jest skończony. Warto jednocześnie poszukać przykładu takiego monoidu nieskończonego (por. 3.1.3) nie będącego grupą, w którym zachodzi prawo skracania.

Odnotujmy teraz dla porządku formalną definicję potęgi całkowitej elementu w grupie.

Definicja 3.1.9 (potęgowanie)**.** Gdy G jest grupą, $a \in G$ oraz $k \in \mathbb{Z}$, to określamy

$$a^k := \begin{cases}\prod\limits_{i=1}^{k} a, & \text{gdy } \ k > 0,\\ 1, & \text{gdy } \ k = 0,\\ (a^{-1})^{-k}, & \text{gdy } \ k < 0.\end{cases}$$

Inaczej ostatnią równość możemy zapisać $a^{-k} = (a^{-1})^k$ dla $k > 0$. Zauważmy, że w półgrupie możliwe jest potęgowanie z wykładnikiem > 0, natomiast w monoidzie określone są potęgi o wykładniku $\geqslant 0$.

Bezpośrednio z 3.1.7 i definicji potęgi wynikają podstawowe własności operacji potęgowania.

Własność 3.1.10 (własności potęgowania)**.** *Jeśli G jest grupą, $a \in G$ oraz $k, l \in \mathbb{Z}$, to $a^k a^l = a^{k+l}$ oraz $(a^k)^l = a^{kl}$.*

Podgrupy

Jak w przypadku każdego typu struktury matematycznej tak i w przypadku grup naturalnie wprowadzamy pojęcie podstruktury. Wobec faktu, że definicja ta odnosi się do podstawowego określenia struktury wrócimy wyjątkowo dla jej postawienia do notacji ogólnej.

Definicja 3.1.11 (podgrupa)**.** Jeśli $(G, \star)$ jest grupą, to podzbiór $H \subset G$ nazywamy **podgrupą** grupy G, gdy:

(1) $H \neq \varnothing$,

(2) zawężenie $\star|_{H\times H}$ przyjmuje wartości w H (czyli jest to działanie na H),

(3) $(H, \star|_{H\times H})$ ma strukturę grupy.

Działanie $\star$ po zawężeniu do $H \times H$ nazywamy **działaniem indukowanym**. Inaczej mówiąc H, jest podgrupą G, jeśli jest grupą z działaniem indukowanym z G. Piszemy wtedy $H < G$.

Poniższa własność obejmuje najczęściej wykorzystywane równoważne określenia pojęcia podgrupy.

Własność 3.1.12 (warunki równoważne na podgrupę)**.** *Gdy G jest grupą oraz $H \subseteq G$, to następujące warunki są równoważne:*

(1) H jest podgrupą G,

(2) $H \neq \varnothing$ oraz spełnione są dwa warunki:

(i) dla dowolnych x, $y \in H$ zachodzi $xy \in H$,

(ii) dla dowolnego $x \in H$ zachodzi $x^{-1} \in H$.

(3) $H \neq \varnothing$ oraz spełniony jest warunek:

(i) dla dowolnych x, $y \in H$ zachodzi $xy^{-1} \in H$.

Dowód. Zauważmy, że oczywiście jeśli H jest podgrupą, to spełnione są warunki z (2), zaś jeśli spełnione są warunki z (2), to zachodzi także warunek z (3), gdyż jeśli x, $y \in H$, to na podstawie (2)(ii) mamy $y^{-1} \in H$ a z (2)(i) mamy $xy^{-1} \in H$.

Niech teraz spełniony będzie warunek (3). Zauważmy najpierw, że skoro $H \neq \emptyset$ to istnieje $x \in H$, więc zgodnie z warunkiem (3) mamy, że $1_G \in x \cdot x^{-1} \in H$. Jeśli teraz $z \in H$ jest dowolnym elementem, to biorąc $x := 1_G \in H$, $y := z \in H$ dostaniemy, że $z^{-1} = 1_G z^{-1} \in H$.

Ostatecznie niech a, $b \in H$. Wiemy już, że wtedy też $b^{-1} \in H$, biorąc więc $x := a$, $y = b^{-1}$ i stosując warunek (3) mamy, że $ab = xy^{-1} \in H$. Ponieważ łączność działania zachodzi dla każdych elementów w G, więc i dla każdych elementów podzbioru G (jakim jest H), wykazaliśmy, że H jest podgrupą G. □

Poniższa uwaga, której dowód pozostawiamy jako ćwiczenie mówi, że sytuacja jeszcze bardziej się upraszcza, gdy mamy do czynienia z podzbiorem skończonym.

Uwaga 3.1.13. Gdy H jest skończonym i niepustym podzbiorem grupy G, to wystarczy wykazać, że działanie w grupie G zawężone do $H \times H$ przyjmuje wartości w H, aby podzbiór H stanowił podgrupę G.

Uwaga ta oczywiście nie jest prawdziwa w przypadku nieskończonego podzbioru, co można łatwo zauważyć rozważając np. $H = \mathbb{N}$ w grupie $(\mathbb{Z}, +)$.

Przykład 3.1.14. (1) $(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$.

(2) $(\mathbb{Q}^*, \cdot\,) < (\mathbb{R}^*, \cdot\,) < (\mathbb{C}^*, \cdot\,)$.

(3) Dla $n \in \mathbb{N}$ określamy $U_n(\mathbb{C}) = \{z \in \mathbb{C} : z^n = 1\}$. Wtedy $(U_n(\mathbb{C}), \cdot\,) < (\mathbb{C}^*, \cdot\,)$.

(4) Jeśli G jest grupą, to podzbiór

$$C(G) := \{x \in G : xa = ax \text{ dla wszystkich } a \in G\}^{(10)}$$

nazywamy **centrum** grupy G. Łatwo sprawdzić, że centrum $C(G)$ jest podgrupą w G i jest to podgrupa abelowa.

[10] Zdarza się, że w podręcznikach **centrum grupy** jest oznaczane przez $Z(G)$ – pochodzi to od notacji z wersji niemieckiej.

Własność 3.1.15 (charakteryzacja podgrup w $\mathbb{Z}$)**.** *Niepusty podzbiór H zbioru liczb całkowitych $\mathbb{Z}$ jest podgrupą grupy $(\mathbb{Z},+)$ wtedy i tylko wtedy, gdy $H=n\mathbb{Z}$ dla pewnego $n\in\mathbb{N}_0$.*

Dowód. Sprawdzenie, że każdy podzbiór postaci $n\mathbb{Z}$ jest podgrupą pozostawiamy jako proste ćwiczenie. Udowodnimy, że każda podgrupa ma taką postać. Jeśli $H=\{0\}$, to wystarczy przyjąć $n=0$. Załóżmy więc, że $H\neq\{0\}$ i przyjmijmy (korzystając z zasady minimum)

$$n=\min\{k\in\mathbb{N}:\ k\in H\}.$$

Zauważmy, że nasze określenie ma sens, gdyż zbiór którego minimum bierzemy jest niepusty (H jest podgrupą, więc jeśli zawiera jakąś liczbę, to zawiera także liczbę do niej przeciwną). Ponieważ $n\in H$, więc $n\mathbb{Z}\subseteq H$. Jeśli zaś $k\in H$, to możemy podzielić k przez n z resztą (por. 1.1.4) otrzymując takie $(q,r)\in\mathbb{Z}\times\mathbb{Z}$, że $k=qn+r$ oraz $0\leqslant r<n$. Oczywiście $r=k-qn\in H$, co wobec minimalności n daje $r=0$. W takich razie $k=qn\in n\mathbb{Z}$ oraz $H\subseteq n\mathbb{Z}$. □

Uwaga 3.1.16.
(1) Każda grupa G posiada zawsze dwie (czasem równe) podgrupy: całą grupę G oraz podgrupę **trywialną** $\{1_G\}$ złożoną tylko z elementu neutralnego. Podgrupę G nazywamy podgrupą **niewłaściwą** grupy G. Każdą podgrupę $H<G$ różną od G nazywamy podgrupą **właściwą**.

(2) Jeśli G jest grupą, $K<H$ oraz $H<G$, to wtedy $K<G$.

(3) Jeśli G jest grupą, $\{H_i\}_{i\in I}$ jest niepustą rodziną podgrup G, to przecięcie

$$\bigcap_{i\in I}H_i:=\{x\in G:\ x\in H_i,\forall\ i\in I\}$$

również jest podgrupą G.

(4) Suma mnogościowa podgrup nie musi być podgrupą. Przykładowo $H_1=2\mathbb{Z}$ oraz $H_2=3\mathbb{Z}$ są podgrupami $\mathbb{Z}$, jednak $H_1\cup H_2$ nie jest podgrupą $\mathbb{Z}$, bo $5=2+3\notin H_1\cup H_2$.

Jako proste ćwiczenie proponujemy wykazanie faktu, że dla dwóch podgrup H i K grupy G zachodzi równoważność: $H\cup K$ jest podgrupą G wtedy i tylko wtedy, gdy $H\subset K$ lub $K\subset H$.

3.2 Homomorfizmy grup

Jednym z najskuteczniejszych narzędzi badania własności danej grupy jest porównywanie jej z innymi znanymi już wcześniej grupami. Aby móc to wykonać trzeba wiedzieć kiedy dwie grupy posiadają dokładnie takie same struktury — służyć nam do tego będą tak zwane homomorfizmy grup. Podobnie jak w przypadku definicji podgrupy, dla postawienia definicji homomorfizmu użyjemy ogólnej notacji, rozróżniając tym samym rodzaje działań w obu porównywanych grupach. Dalej jednak tak w grupie wyjściowej jak i docelowej stosować będziemy tę samą notację multiplikatywną.

Definicja 3.2.1 (homomorfizm grup)**.** Jeśli $(G,\star)$ oraz $(\widetilde{G},\bullet)$ są grupami, to odwzorowanie $f\colon G\to\widetilde{G}$ nazywamy homomorfizmem grupy G w grupę $\widetilde{G}$, gdy

$$\forall\ x,y\in G:\qquad f(x\star y)=f(x)\bullet f(y).$$

Zbiór wszystkich homomorfizmów grupy G w grupę $\widetilde{G}$ oznaczamy $\mathrm{Hom}(G,\widetilde{G})$.

Przykład 3.2.2. Rozważmy odwzorowanie następujące: $f:\mathbb{R}\ni x\longmapsto 3^x\in\mathbb{R}^+$. Zauważmy, że ponieważ w $\mathbb{R}$ mamy działanie dodawania, a w $\mathbb{R}^+$ mnożenia, więc nasze odwzorowanie jest homomorfizmem, gdyż:

$$f(x+y)=3^{x+y}=3^x3^y=f(x)\cdot f(y).$$

To odwzorowanie pozwala nam „zamienić" dodawanie na mnożenie. Odwrotna transformacja może zostać przeprowadzona za pomocą logarytmu – są to ważne odwzorowania z punktu widzenia zastosowań. Są takie sytuacje, gdy mnożenie (lub odp. dodawanie) jest znacznie łatwiejsze do wykonania niż dodawanie (odp. mnożenie), warto więc wówczas wykorzystać taką zamianę, gdyż z punktu widzenia teorii grup, dzięki powyższemu homomorfizmowi (*de facto* izomorfizmowi – por. niżej) grupy $(\mathbb{R},+)$ i $(\mathbb{R}^+,\cdot)$ są nierozróżnialne.

Wyróżniamy następujące rodzaje homomorfizmów:

$$\begin{aligned} \text{monomorfizm} &= \text{homomorfizm injektywny},\\ \text{epimorfizm} &= \text{homomorfizm surjektywny},\\ \text{izomorfizm} &= \text{homomorfizm bijektywny},\\ \text{endomorfizm} &= \text{homomorfizm z grupy w nią samą},\\ \text{automorfizm} &= \text{endomorfizm bijektywny}. \end{aligned}$$

Zbiór izomorfizmów grupy G w $\widetilde{G}$ oznaczamy $\mathrm{Iso}(G,\widetilde{G})$. Zbiór endomorfizmów grupy G oznaczamy $\mathrm{End}(G)$, natomiast zbiór automorfizmów grupy G zapisujemy jako $\mathrm{Aut}(G)$.

Przykład 3.2.3. Przyjrzyjmy się przykładom:

(1) $f:\mathbb{R}^\star \ni x \mapsto x^2 \in \mathbb{R}^+$ jest epimorfizmem, ale nie jest injekcją.

(2) $g:\mathbb{R} \ni x \mapsto 2^x \in \mathbb{R}^\star$ jest monomorfizmem, ale nie jest surjekcją.

(3) $h:\mathbb{R} \ni x \mapsto 3^x \in \mathbb{R}^+$ jest izomorfizmem grup.

Uwaga 3.2.4. Jeśli $f\colon G \to G'$ oraz $g : G' \to G''$ są homomorfizmami grup, to również $g \circ f\colon G \to G''$ jest homomorfizmem grup. Ponadto, jeśli f jest bijekcją, to f^{-1} także jest homomorfizmem grup.

Dowód. Pierwsza część tezy jest łatwym ćwiczeniem z zakresu składania funkcji. Dla dowodu części drugiej niech $x', y' \in G'$. Wówczas istnieją jedyne takie elementy $x, y \in G$, że $x' = f(x)$ i $y' = f(y)$. Wobec tego

$$f^{-1}(x'y') = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(x')f^{-1}(y').$$ □

Zauważmy, że powyższa uwaga mówi, że homomorfizmy są dość szczególnymi odwzorowaniami – jeśli tylko bowiem homomorfizm jest odwracalny, to odwzorowanie odwrotne jest także morfizmem w swojej klasie. Nie zawsze morfizmy z klas rozważanych w matematyce zachowują się w ten sposób: na przykład w topologii łatwo wskazać bijekcję, która jest odwzorowaniem ciągłym, ale odwrotne odwzorowanie już nie jest ciągłe.

Definicja 3.2.5 (grupy izomorficzne)**.** Grupy $G, \widetilde{G}$ nazywamy **izomorficznymi**, jeśli istnieje izomorfizm grupy G na grupę $\widetilde{G}$. Fakt, że grupy $G, \widetilde{G}$ są izomorficzne oznaczamy $G \cong \widetilde{G}$.

Pojęcie grup izomorficznych jest niezwykle istotnym pojęciem dla badania ich własności. Grupy izomorficzne bowiem, z punktu widzenia własności algebraicznych są nie do rozróżnienia na poziomie struktury grupowej.

Przykład 3.2.6. (1) Jeśli H jest podgrupą grupy G, to zanurzenie $\imath\colon H \ni x \mapsto x \in G$ jest monomorfizmem.

(2) Zbiór $\mathrm{Aut}(G)$ automorfizmów grupy G z działaniem składania ma strukturę grupy, ponadto każde odwzorowanie postaci

$$\varphi_a\colon G \ni x \mapsto axa^{-1} \in G,$$

gdzie $a \in G$ jest automorfizmem grupy G. Odwzorowania takie nazywamy **automorfizmami wewnętrznymi** grupy G. Zbiór $\mathrm{Inn}(G)$ automorfizmów wewnętrznych grupy G jest podgrupą w $\mathrm{Aut}(G)$.

Uwaga 3.2.7. Rozważmy następujący zbiór $\mathbb{Z}_2 \times \mathbb{Z}_2 := \{(0,0),(0,1),(1,0),(1,1)\}$ – na tym zbiorze wprowadzamy działanie dodawania modulo 2 „po współrzędnych" tzn. np. $(1,1)+(1,0) = (0,1)$ itd. Łatwo ułożyć tabelę takiego działania i zobaczyć, że mamy do czynienia z grupą.

Zauważmy, że grupa ta ma 4 elementy, podobnie jak grupa $\mathbb{Z}_4$ – wobec tego łatwo wypisać odwzorowanie, które będzie bijekcją między tymi zbiorami – te zbiory są równoliczne. Jednak jak się okazuje żadna z wypisanych bijekcji nie będzie homomorfizmem, o czym przekonamy się dalej (por. 3.3.11). Fakt ten bierze się stąd, że każdy element $\mathbb{Z}_4$ jest potęgą (w sensie dodawania!) elementu 1. Natomiast w $\mathbb{Z}_2 \times \mathbb{Z}_2$ nie istnieje odpowiednik elementu o takiej własności. Jeśli potęgujemy np. $(1,1)$ to dostaniemy: $(1,1)$ i $(0,0)$ – żadnego innego elementu. Podobnie jest z pozostałymi, nie ma więc jednego elementu którego potęgą byłyby wszystkie inne.

Własność 3.2.8 (podstawowe własności homomorfizmów grup)**.** *Niech $f\colon G \to \widetilde{G}$ będzie homomorfizmem grup. Wtedy zachodzą następujące własności:*

(1) $f(1_G) = 1_{\widetilde{G}}$,

(2) jeśli $x \in G$, to $f(x^{-1}) = [f(x)]^{-1}$,

(3) jeśli $H < G$, to $f(H) < \widetilde{G}$,

(4) jeśli $\widetilde{H} < \widetilde{G}$, to $f^{-1}(\widetilde{H}) < G$.

Dowód.
(1) Zauważmy, że $f(1_G)f(1_G) = f(1_G \cdot 1_G) = f(1_G)$, stąd na przykład z prawa skracania mamy $f(1_G) = 1_{\widetilde{G}}$.

(2) Jeśli $x \in G$, to mamy $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_G) = 1_{\widetilde{G}}$, zatem z jedyności elementu odwrotnego mamy $[f(x)]^{-1} = f(x^{-1})$.

(3) Skorzystamy z własności 3.1.12. Wobec niepustości H mamy $f(H) \neq \emptyset$. Jeśli teraz $a, b \in f(H)$, to istnieją takie $x, y \in H$, że $a = f(x)$ oraz $b = f(y)$. Otrzymujemy zatem, że

$$ab^{-1} = f(x)[f(y)]^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H),$$

gdyż $xy^{-1} \in H$.

(4) Dowód przeprowadzimy analogicznie jak w przypadku obrazu. Zauważmy, że $f^{-1}(\widetilde{H})$ jest zbiorem niepustym, gdyż na podstawie (1) należy do niego 1_G. Niech teraz $x, y \in f^{-1}(\widetilde{H})$ co oznacza zgodnie z definicją, że $f(x)$, $f(y) \in \widetilde{H}$, skoro zaś $\widetilde{H}$ jest podgrupą to wiemy, że $f(x)[f(y)]^{-1} \in \widetilde{H}$. Zgodnie z punktem (2) mamy jednak $f(x)[f(y)]^{-1} = f(xy^{-1})$ skąd $xy^{-1} \in f^{-1}(\widetilde{H})$, co kończy dowód. □

Określimy teraz dla porządku dwa podstawowe, znane z teorii mnogości obiekty, które odgrywać będą rolę w dalszych rozważaniach.

Definicja 3.2.9 (jądro i obraz homomorfizmu)**.** Jeśli $f\colon G \to \widetilde{G}$ jest homomorfizmem grup, to **obrazem** f nazywamy zbiór

$$\operatorname{Im} f := f(G) = \{y \in \widetilde{G} : \exists\, x \in G : f(x) = y\},$$

zaś **jądrem** f nazywamy zbiór

$$\operatorname{Ker} f := f^{-1}(1_{\widetilde{G}}) = \{x \in G : f(x) = 1_{\widetilde{G}}\}.$$

Wprost z 3.2.8 wynika poniższy wniosek.

Wniosek 3.2.10 (własności jądra i obrazu)**.** *Jeśli $G, \widetilde{G}$ są grupami, zaś $f\colon G \to \widetilde{G}$ jest homomorfizmem grup, to wtedy* $\operatorname{Ker} f < G$ *oraz* $\operatorname{Im} f < \widetilde{G}$.

Kolejna własność jest dobrym narzędziem badania injektywności homomorfizmów grup.

Własność 3.2.11 (charakteryzacja monomorfizmu)**.** *Niech $f\colon G \to \widetilde{G}$ będzie homomorfizmem grup. Wtedy:*

(1) f jest monomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker} f = \{1_G\}$,

(2) f jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{Im} f = \widetilde{G}$.

Dowód. Dowodu wymaga jedynie punkt (1). Przypuśćmy najpierw, że f jest injekcją oraz, że $x \in \operatorname{Ker} f$. Wtedy $1_{\widetilde{G}} = f(x) = f(1_G)$, czyli $x = 1_G$. Wobec tego $\operatorname{Ker} f \subseteq \{1_G\}$ – jednak $1_G \in \operatorname{Ker} f$, więc mamy równość. Załóżmy teraz równość $\operatorname{Ker} f = \{1_G\}$. Jeśli $x, y \in G$ są takie, że $f(x) = f(y)$, to $1_{\widetilde{G}} = f(x)[f(y)]^{-1} = f(xy^{-1})$, czyli $xy^{-1} \in \operatorname{Ker} f$, zatem $xy^{-1} = 1_G$, czyli $x = y$. □

Przykład 3.2.12. Odwzorowanie $\mathrm{GL}_2(\mathbb{R}) \ni A \mapsto \det A \in \mathbb{R}^*$ jest homomorfizmem grup. Jego jądro oznaczamy przez $\mathrm{SL}_2(\mathbb{R})$ i nazywamy specjalną grupą liniową.

Bardzo ważnym twierdzeniem w teorii grup jest twierdzenie, które mówi, że każda grupa może być traktowana w pewnym sensie jak grupa permutacji elementów swojego zbioru.

Twierdzenie 3.2.13 (Cayley)**.** *Każda grupa jest izomorficzna z podgrupą swojej grupy symetrycznej (por. 2.1.1).*

Dowód. Jeśli G jest grupą i a jej ustalonym elementem, to rozważmy odwzorowanie

$$\psi_a \colon G \ni x \mapsto ax \in G.$$

Zauważmy, że jest to odwzorowanie bijektywne, gdyż odwzorowaniem odwrotnym jest $\psi_{a^{-1}}$. Możemy zatem określić

$$\Psi \colon G \ni a \mapsto \psi_a \in S(G).$$

Wystarczy teraz udowodnić, że jest to monomorfizm grup. Istotnie, jeśli $a, b \in G$, to dla dowolnego $x \in G$ mamy

$$\begin{aligned}\Psi(ab)(x) &= \psi_{ab}(x) = (ab)x = a(bx) = \psi_a(bx)\\ &= \psi_a(\psi_b(x)) = (\psi_a \circ \psi_b)(x) = (\Psi(a) \circ \Psi(b))(x),\end{aligned}$$

skąd otrzymujemy równość $\Psi(ab) = \Psi(a) \circ \Psi(b)$. Jeśli teraz $\Psi(a) = \mathrm{id}_G$, to

$$a = a \cdot 1_G = \psi_a(1_G) = \Psi(a)(1_G) = 1_G,$$

czyli Ψ rzeczywiście jest monomorfizmem. Oznacza, to że Ψ jest izomorfizmem pomiędzy G i $\Psi(G)$. Ponieważ $\Psi(G)$ jest podgrupą $S(G)$ (por.3.2.8 (3)), więc możemy G z punktu widzenia teorii grup utożsamiać z podgrupą $S(G)$. □

3.3 Generatory grup

Podgrupy generowane przez zbiór

Przyjrzyjmy się bliżej wzorcowemu przykładowi, czyli grupie $(\mathbb{Z}, +)$. Zauważmy, że każdy element tego zbioru można otrzymać dodając do siebie stosowną liczbę elementów 1 lub -1. W sytuacji takiej powiemy, że element 1 generuje grupę $\mathbb{Z}$.

Rozważmy teraz zbiór liczb naturalnych parzystych. Jest to podzbiór $\mathbb{Z}$, który nie tworzy jednak podgrupy. Aby dostać podgrupę musimy „dorzucić" ujemne liczby parzyste. W ten sposób otrzymamy $2\mathbb{Z}$ — najmniejszą podgrupę $\mathbb{Z}$, która zawiera $2\mathbb{N}$. Jest to tak zwana podgrupa generowana przez zbiór $2\mathbb{N}$. W tym rozdziale przyjrzymy się pojęciu podgrupy generowanej przez zadany zbiór, czyli najmniejszej podgrupie zadanej grupy, która ten zbiór zawiera.

Definicja 3.3.1 (podgrupa generowana przez zbiór, generatory)**.** Jeśli G jest grupą, zaś $S \subseteq G$, to zbiór

$$\langle S \rangle := \bigcap_{H<G, S\subseteq H} H$$

nazywamy **podgrupą generowaną** przez zbiór S([11]). Jeśli zachodzi $\langle S \rangle = G$, to elementy zbioru S nazywamy **generatorami** grupy G. Gdy $S = \{a_1, \ldots, a_n\}$ piszemy po prostu $\langle S \rangle = \langle a_1, \ldots, a_n \rangle$.

Zauważmy, że jeśli $S = \emptyset$, to $\langle S \rangle = \{1_G\}$. Jeśli $S \neq \emptyset$, to postawiona definicja zdaje się być mało praktyczna. Interesować nas będzie dalej jak przedstawić elementy grupy generowanej przez pewien niepusty zbiór tak, by łatwiej było takie podgrupy wyznaczać.

Własność 3.3.2 (postać elementów w grupie generowanej)**.** *Jeśli G jest grupą, $\varnothing \neq S \subseteq G$, to*

$$\langle S \rangle = \{s_1^{k_1} \cdot \ldots \cdot s_n^{k_n} : s_1, \ldots, s_n \in S,\ k_1, \ldots, k_n \in \mathbb{Z},\ n \in \mathbb{N}\}.$$

Dowód. Oznaczmy przez $H = \{s_1^{k_1} \cdot \ldots \cdot s_n^{k_n},\ n \in \mathbb{N}, k_i \in \mathbb{Z}, s_i \in S\}$.

Oczywiście $S \subset H$, łatwo też wykazać, że jest to podgrupa korzystając z 3.1.12. Jest to bowiem zbiór niepusty (zawiera niepusty zbiór S), zaś biorąc dwa elementy H postaci: $x = s_1^{k_1} \cdot \ldots \cdot s_n^{k_n}$, $y = r_1^{l_1} \cdot \ldots \cdot r_p^{l_p}$ otrzymujemy: $xy^{-1} = s_1^{k_1} \cdot \ldots \cdot s_n^{k_n} \cdot r_p^{-l_p} \cdot \ldots \cdot r_1^{-l_1}$ czyli element z H, bo $-l_1, \ldots, -l_p \in \mathbb{Z}$.

Wobec tego zachodzi zawieranie $\langle S \rangle \subset H$ (skoro $\langle S \rangle$ to przecięcie wszystkich podgrup zawierających S).

Ponieważ jednocześnie każda podgrupa G, która zawiera S musi zawierać też H (dzięki wewnętrzności działania oraz przynależności elementu odwrotnego), więc $\langle S \rangle = H$. □

[11] Dzięki uwadze 3.1.16(3) wiemy, że istotnie jest to podgrupa.

Wniosek 3.3.3 (podgrupa generowana przez jeden element)**.** *Jeśli G jest grupą oraz $a \in G$, to wtedy $\langle a\rangle = \{a^k : k \in \mathbb{Z}\}$.*

Przykład 3.3.4.
(1) Zbiór generatorów na ogół nie jest jedyny — na przykład dla grupy $(\mathbb{Z}, +)$ otrzymujemy $\mathbb{Z} = \langle 1\rangle = \langle -1\rangle$. Dodatkowo zawsze jest $\langle G\rangle = G$.

(2) W grupie $(\mathbb{Z}, +)$ podgrupą generowaną przez $A = \{6, 15\}$ jest $\langle A\rangle = \{6k + 15l : k, l \in \mathbb{Z}\}$ i łatwo pokazać, że jest to $3\mathbb{Z}$, czyli podgrupa generowana przez największy wspólny dzielnik liczb 6 i 15.

(3) Grupa $(\mathbb{Q}, +)$ jest przykładem grupy, która nie posiada skończonego układu generatorów. Ale za to można wykazać, że każda skończenie generowana podgrupa grupy $\mathbb{Q}$ da się wygenerować za pomocą jednego generatora.

(4) Grupa $(\mathbb{Q}^*, \cdot\,)$ jest generowana przez zbiór liczb pierwszych i -1 i nietrudno sprawdzić, że jest to minimalny (w sensie inkluzji) układ jej generatorów.

(5) Mieliśmy już przykład dwóch grup równolicznych, które nie były izomorficzne (por. 3.2.7) – grupy te nie miały jednak tej samej minimalnej liczby generatorów. Niestety okazuje się, że dwie grupy tego samego rzędu o takiej samej minimalnej liczbie generatorów też nie muszą być izomorficzne. Opiszemy je niżej. Niech

$$a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}, \qquad c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Rozważmy teraz dwie grupy:

$$Q = \langle a, b\rangle \subseteq \mathrm{GL}_2(\mathbb{C}),$$
$$H = \langle a, c\rangle \subseteq \mathrm{GL}_2(\mathbb{C}).$$

Obie te grupy są ośmioelementowe, nie dadzą się wygenerować przez jeden element i nie są izomorficzne. Grupa Q nazywana jest grupą kwaternionów, gdyż jest izomorficzna z ośmioelementową podgrupą multiplikatywną $\{\pm 1, \pm i, \pm j, \pm k\}$ rzeczywistej algebry kwaternionów $\mathbb{H}$.[12]

3.3.1 Rząd elementu w grupie, grupy cykliczne

Definicja 3.3.5 (rząd elementu)**.** Jeśli G jest grupą, to **rzędem elementu** $a \in G$ nazywamy rząd grupy $\langle a\rangle$. Rząd elementu a oznaczamy przez $|a|$.

Uwaga 3.3.6. (1) Jeśli G jest grupą i $a \in G$, to $|a| \leqslant |G|$. Ponadto $|a| = 1$ wtedy i tylko wtedy, gdy $a = 1$ (w podgrupie generowanej przez element $a \neq 1_G$, muszą się znaleźć co najmniej dwa elementy: 1_G oraz a).

(2) W grupie $(\mathbb{Z}, +)$ każdy niezerowy element ma rząd nieskończony, ale nie każdy taki element generuje całą grupę $\mathbb{Z}$.

Będziemy chcieli teraz udowodnić twierdzenie, które w praktyce ułatwi obliczanie rzędów elementów, dla których rząd ten jest skończony. Twierdzenie poprzedzimy pomocniczym lematem.

Lemat 3.3.7. *Niech G będzie grupą, niech $a \in G$ oraz $H_n(a) = \{1, a, \ldots, a^{n-1}\}$ dla $n \in \mathbb{N}$. Wtedy:*

(1) jeśli $a^n = 1$, to $H_n(a) \leqslant G$ oraz $|a| \leqslant n$,

(2) jeśli $|a| = n$, to $|H_n(a)| = n$ oraz $\langle a\rangle = H_n(a)$.

Dowód. (1) Wprost z definicji mamy, że $1 \in H_n(a)$, czyli $H_n(a) \neq \emptyset$. Jeśli teraz $x, y \in H_n(a)$, to istnieją takie $0 \leqslant p, q < n$, że $x = a^p$ oraz $y = a^q$. Zapisując $p - q = kn + r$, gdzie $0 \leqslant r < n$ otrzymujemy

$$xy^{-1} = a^p a^{-q} = a^{p-q} = a^{kn+r} = (a^n)^k a^r = a^r \in H_n(a),$$

czyli $H_n(a) < G$. Jednocześnie $a \in H_n(a)$, stąd $\langle a\rangle \subseteq H_n(a)$, więc $|a| \leqslant |H_n(a)| \leqslant n$.

(2) Wykażemy, że jeśli $|H_n(a)| < n$, to $|a| < n$. Istotnie, jeśli $|H_n(a)| < n$, to oznacza to, że istnieją takie $0 \leqslant p < q < n$, że $a^p = a^q$, czyli $a^r = 1$, gdzie $0 < r = q - p < n$. Na podstawie (1) mamy więc $|a| \leqslant r < n$. Teraz, jeśli $|a| = n$, to $H_n(a) \subseteq \langle a\rangle$ i oba te zbiory są skończone i mają tę samą liczbę elementów, skąd ich równość. □

[12] Jest to jedna z dwóch nieprzemiennych grup rzędu 8 – drugą jest grupa izometrii kwadratu. Charakterystyczną cechą tej grupy jest fakt, że wszystkie jej podgrupy są normalne, mimo jej nieprzemienności.

Twierdzenie 3.3.8 (wzór praktyczny na rząd elementu)**.** *Jeśli G jest grupą, $a \in G$ oraz $|a| < \infty$, to $|a| = \min\{n \in \mathbb{N} : a^n = 1\}$ oraz $\langle a \rangle = \{1_G, a, a^2, \ldots, a^{n-1}\}$.*

Dowód. Zauważmy, że dzięki założeniu $|a| < \infty$ zbiór względem którego bierzemy minimum jest niepusty. Istotnie, gdyby nie istniała liczba naturalna n dla której $a^n = 1$, to mielibyśmy dla dowolnych $k, l \in \mathbb{N}$ nierówność $a^{k-l} \neq 1$, czyli $a^k \neq a^l$. Tym samym $\langle a \rangle$ byłaby nieskończona.

Oznaczmy zatem

$$n_0 = \min\{n \in \mathbb{N} : a^n = 1\}, \qquad m_0 = |a|.$$

Chcemy wykazać, że $m_0 = n_0$. Po pierwsze $a^{n_0} = 1$, więc na podstawie lematu 3.3.7 jest $m_0 \leqslant n_0$. Ponadto $\langle a \rangle = H_{m_0}(a) = \{1, \ldots, a^{m_0-1}\}$, więc istnieje takie $0 \leqslant p < m_0$, że $a^{m_0} = a^p$ i wtedy $a^{m_0-p} = 1$. Korzystając znów z lematu 3.3.7 mamy $m_0 \leqslant m_0 - p$, a tym samym $p = 0$ i $a^{m_0} = 1$. Z minimalności liczby n_0 otrzymujemy $n_0 \leqslant m_0$.

Postać podgrupy generowanej przez a wynika wprost z lematu 3.3.7. □

Wniosek 3.3.9 (porównanie potęg elementów)**.** *Niech G będzie grupą, $a \in G$ spełnia $|a| = n$ oraz niech $k, l \in \mathbb{Z}$. Zachodzą następujące własności:*

(1) $a^k = 1$ wtedy i tylko wtedy, gdy $n \mid k$.

(2) $a^k = a^l$ wtedy i tylko wtedy, gdy $k \equiv l \pmod{n}$.

Dowód.
(1) Oczywiście, jeśli $n \mid k$, to mamy $a^k = 1$. Niech więc $a^k = 1$. Podzielmy k z resztą przez n, wtedy $k = qn + r$, gdzie $0 \leqslant r < n$. Wobec tego

$$1 = a^k = a^{qn+r} = (a^n)^q a^r = a^r,$$

czyli $r = 0$ i $n \mid k$.

(2) Jest to bezpośredni wniosek z (1), gdyż warunek $a^k = a^l$ jest równoważny warunkowi $a^{k-l} = 1$. □

Przyjrzyjmy się jak na prostym przykładzie pracuje twierdzenie 3.3.8. Rozważmy grupę $(\mathbb{Z}_8, +)$ oraz element $2 \in \mathbb{Z}_8$. Jeśli chcemy wygenerować podgrupę $\langle 2 \rangle$ w naszej grupie, to musimy zgodnie z udowodnionymi własnościami „potęgować" element 2 aż otrzymamy element neutralny grupy, czyli $\langle 2 \rangle = \{0, 2, 4, 6\}$. Jest to element rzędu 4, tzn. $|2| = 4$ w $\mathbb{Z}_8$.

Grupy cykliczne

Szczególnie ciekawą, a jednocześnie dość łatwą w analizie klasą grup, są tzw. grupy cykliczne, czyli takie, które generowane są przez jeden element. Inaczej mówiąc, każdy element takiej grupy jest uzyskiwany jako potęga jednego ustalonego elementu. Tak jest, jak łatwo widać, dla grup $(\mathbb{Z}, +)$ i $(\mathbb{Z}_n, +)$, gdzie 1 generuje w każdym przypadku całą grupę.

Definicja 3.3.10 (grupa cykliczna)**.** Grupę G nazywamy **cykliczną**, jeśli jest ona generowana przez jeden element, tzn. istnieje takie $a \in G$, że $G = \langle a \rangle$.

Omówimy teraz najprostsze własności grup cyklicznych.

Własność 3.3.11 (podstawowe własności grup cyklicznych)**.** *Niech $f \colon G \to \widetilde{G}$ będzie homomorfizmem grupy cyklicznej G o generatorze $a \in G$ w grupę $\widetilde{G}$ oraz niech H będzie podgrupą grupy G. Wtedy zachodzą następujące własności:*

(1) G jest grupą abelową,

(2) $\operatorname{Im} f$ jest grupą cykliczną,

(3) H jest grupą cykliczną.

Dowód.
(1) Jeśli $x, y \in G$, to istnieją takie $k, l \in \mathbb{Z}$, że $x = a^k$ oraz $y = a^l$. Mamy:

$$xy = a^k a^l = a^{k+l} = a^{l+k} = a^l a^k = yx.$$

(2) Udowodnimy, że $f(G) = \langle f(a)\rangle$. Jeśli bowiem $y \in f(G)$, to $y = f(a^k)$ dla pewnego $k \in \mathbb{Z}$. Jednak korzystając m.in. z 3.2.8(1) i (2) oraz definicji homomorfizmu mamy $f(a^k) = [f(a)]^k$, tym samym $y \in \langle f(a)\rangle$, czyli $f(G) \subseteq \langle f(a)\rangle$. Zawieranie w drugą stronę jest oczywiste.

(3) Jeśli $H = \{1\} = \langle 1\rangle$, to mamy tezę. Załóżmy więc, że H nie jest trywialna i określmy

$$s = \min\{n \in \mathbb{N} : a^n \in H\}.$$

Wykażemy, że $H = \langle a^s\rangle$. Jeżeli $x \in H$, to dzięki cykliczności G wiemy, że $x = a^k$ dla pewnego $k \in \mathbb{Z}$. Jeśli $k = qs+r$, gdzie $0 \leqslant r < s$, to

$$x = a^k = a^{qs+r} = (a^s)^q a^r,$$

stąd $a^r = x(a^s)^{-q} \in H$, czyli z minimalności s musi być $r = 0$. Ostatecznie $x = (a^s)^q \in \langle a^s\rangle$, czyli $H \subseteq \langle a^s\rangle$. Inkluzja w drugą stronę jest oczywista. □

Zauważmy, że wykazaliśmy po drodze także następujący

Wniosek 3.3.12. *Jeśli $f : G \longrightarrow \widetilde{G}$ jest izomorfizmem grup, to a jest generatorem G wtedy i tylko wtedy, gdy $f(a)$ jest generatorem $\widetilde{G}$.*

Dowód własności dotyczącej podgrupy grupy cyklicznej można przeprowadzić inaczej, wykorzystując twierdzenie o klasyfikacji grup cyklicznych (udowodnimy je za chwilę, 3.3.13) i postać podgrup w $(\mathbb{Z}, +)$, którą znamy (por. 3.1.15). Jednak przedstawiony dowód ma tę zaletę, że pokazuje bezpośrednio jak znaleźć element generujący podgrupę w grupie cyklicznej.

Jak się okazuje grupy cykliczne można bardzo dokładnie opisać — oczywiście pamiętając o tym, że „opis" w sensie algebraicznym oznacza opis z dokładnością do izomorfizmu.

Twierdzenie 3.3.13 (klasyfikacja grup cyklicznych)**.** *Niech G będzie grupą cykliczną. Wtedy:*

(1) jeśli $|G| = \infty$, to wtedy $G \cong \mathbb{Z}$, gdzie izomorfizm wyraża się wzorem $\phi(k) = a^k$,

(2) jeśli $|G| = n$, to wtedy $G \cong \mathbb{Z}_n$, gdzie izomorfizm wyraża się wzorem $\phi_n([k]) = a^k$.

Dowód. Niech $a \in G$ będzie generatorem grupy G.

(1) Określmy

$$\phi\colon \mathbb{Z} \ni k \mapsto a^k \in G.$$

Wprost z określenia i z postaci elementów w grupie generowanej przez a (wniosek 3.3.3) wynika, że jest to epimorfizm. Jeśli zaś dla pewnego $k \in \mathbb{Z}$ jest $\phi(k) = 1_G$, to $a^k = 1$, czyli również $a^{-k} = 1$. Gdyby $k \neq 0$, to byłoby $l = |k| > 0$ i $a^l = 1$, zatem z lematu 3.3.7 wynika $|G| = |a| \leqslant l$, co stoi w sprzeczności z założeniem nieskończoności grupy. Ostatecznie $k = 0$, czyli jądro ϕ jest jednoelementowe i tym samym ϕ jest izomorfizmem (co jest konsekwencją własności 3.2.11).

(2) Niech $|G| = n$. Tym razem określmy odwzorowanie

$$\phi_n\colon \mathbb{Z}_n \ni [k]_n \mapsto a^k \in G.$$

Po pierwsze zauważmy, że takie określenie jest poprawne. Istotnie, zgodnie z wnioskiem 3.3.9(2) dostajemy, że $k \equiv l \pmod n$ wtedy i tylko wtedy, gdy $a^k = a^l$. Równoważność ta dowodzi nie tylko poprawnej określoności, ale też injektywności odwzorowania. W oczywisty sposób ϕ_n jest epimorfizmem co kończy dowód. □

Często, modelowa (jedyna z dokładnością do izomorfizmu) grupa cykliczna rzędu n oznaczana jest przez C_n, zaś nieskończona grupa cykliczna przez C_∞.

Jak dowiemy się dalej, jeśli mamy do czynienia z dowolną grupą, której rząd jest liczbą pierwszą p, to taka grupa musi już być cykliczna rzędu p. Tym samym, na podstawie poprzedniego twierdzenia jedyną (z dokładnością do izomorfizmu) grupą o zadanym rzędzie będącym liczbą pierwszą p jest grupa C_p.

Ciekawym problemem jest pytanie o to dla jakich jeszcze innych liczb n, oprócz liczb pierwszych, zachodzi taka własność, że jedyną grupą rzędu n jest grupa cykliczna C_n. Okazuje się, że liczby takie mają dość prostą charakteryzację (liczby takie nazywa się liczbami cyklicznymi i mają one też inną, teorioliczbową równoważną definicję).

Otóż zachodzi twierdzenie: *Grupa C_n jest jedyną grupą rzędu n wtedy i tylko wtedy, gdy* $\mathrm{NWD}(n, \varphi(n)) = 1$, *gdzie φ oznacza funkcję Eulera.*

Zauważmy, że na przykład dla $n = 4$ mamy $\varphi(4) = 2$, czyli zgodnie z tym twierdzeniem istnieją co najmniej dwie grupy rzędu 4. Można wykazać, że istnieją dokładnie dwie grupy rzędu cztery: C_4 oraz $C_2 \times C_2$, gdzie w tej drugiej rozważamy działanie „po współrzędnych".[13]

Dotychczasowe rozważania prowadzą też do wniosków mówiących o postaci generatorów dowolnej grupy cyklicznej.

Wniosek 3.3.14. *Niech G będzie grupą cykliczną o generatorze $a \in G$.*

(1) Jeśli $|G| = \infty$, to jedynymi generatorami grupy G są elementy a oraz a^{-1}.

(2) Jeśli $|G| = n$, to dla $k \in \mathbb{Z}$ jest $G = \langle a^k \rangle$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(n, k) = 1$.

(3) Jeśli $|G| = n$, to liczba generatorów grupy G jest równa $\varphi(n)$ 1.6.1

Dowód. Dla dowodu (1) zauważmy, że zgodnie z twierdzeniem klasyfikacyjnym mamy $G \cong \mathbb{Z}$, więc dzięki wnioskowi 3.3.12 tylko obrazy przez ϕ (3.3.13) elementów 1 i (-1) mogą generować G (gdyż tylko 1 i (-1) generują $\mathbb{Z}$). Obrazami tymi są oczywiście a oraz a^{-1}.

W przypadku gdy $|G| = n$, to jeśli a^k $(0 \leqslant k < n)$ jest generatorem, to $a = (a^k)^p = a^{kp}$ dla pewnego $p \in \mathbb{Z}$, zatem $a^{kp-1} = 1$, czyli z 3.3.9 $n \mid kp - 1$. Istnieje więc takie $q \in \mathbb{Z}$, że $pk + qn = 1$, czyli $\mathrm{NWD}(n, k) = 1$. Odwrotnie, jeśli $\mathrm{NWD}(n, k) = 1$, to z wniosku 1.2.5 wynika, że istnieją takie $p, q \in \mathbb{Z}$, że $pk + qn = 1$. Mamy w takim razie:

$$a = a^{pk+qn} = (a^k)^p (a^n)^q = (a^k)^q,$$

czyli za pomocą a^k jesteśmy w stanie otrzymać generator grupy G, więc również całą grupę. □

Jednym z przykładów grup cyklicznych ważnych z punktu widzenia dalszych zastosowań są grupy $U_n(\mathbb{C})$ – zespolonych pierwiastków n-tego stopnia z jedynki. Każda taka grupa jest grupą cykliczną. Generatory grupy $U_n(\mathbb{C})$ nazywamy **n-tymi pierwiastkami pierwotnymi z jedynki.** Z naszego twierdzenia wynika, że jeśli $\zeta \in U_n(\mathbb{C})$ jest pierwiastkiem pierwotnym z jedynki stopnia n, to element ζ^k jest pierwiastkiem pierwotnym z jedynki stopnia n wtedy i tylko wtedy, gdy $\mathrm{NWD}(n, k) = 1$.

Grupy cykliczne odgrywają ogromną rolę, na przykład w klasyfikacji grup skończonych. Są one bowiem „cegiełkami", z których zbudowane są na przykład wszystkie skończone grupy abelowe.

Twierdzenie o klasyfikacji takich grup wypowiemy w tej części bez dowodu – udowodnimy je w drugiej części skryptu (twierdzenie 9.4.5). Zanim jednak to zrobimy musimy wprowadzić pojęcie iloczynu/sumy prostej grup.

Definicja 3.3.15 (produkt grup)**. Iloczynem prostym** (**produktem**) niepustej rodziny grup $\{G_i\}_{i \in I}$ nazywamy zbiór $\prod\limits_{i \in I} G_i$ wraz z działaniem

$$(a_i)_{i \in I}(b_i)_{i \in I} := (a_i b_i)_{i \in I}, \qquad (a_i)_{i \in I}, (b_i)_{i \in I} \in \prod_{i \in I} G_i.$$

Definicja 3.3.16 (suma prosta grup)**. Sumą prostą** niepustej rodziny grup $\{G_i\}_{i \in I}$ nazywamy zbiór

$$\bigoplus_{i \in I} G_i := \left\{ (a_i)_{i \in I} \in \prod_{i \in I} G_i : a_i = 1 \text{ dla prawie wszystkich } i \in I \right\}$$

wraz z działaniem

$$(a_i)_{i \in I}(b_i)_{i \in I} := (a_i b_i)_{i \in I}, \qquad (a_i)_{i \in I}, (b_i)_{i \in I} \in \bigoplus_{i \in I} G_i.$$

Jeśli $I = \{1, \ldots, n\}$, to piszemy

$$\prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n \qquad \text{oraz} \qquad \bigoplus_{i=1}^{n} G_i = G_1 \oplus \cdots \oplus G_n.$$

Ponadto zauważmy, że $G_1 \times \cdots \times G_n = G_1 \oplus \cdots \oplus G_n$.

W oczywisty sposób wprowadzone wyżej działania wprowadzają na omawianych zbiorach strukturę grupy, co usprawiedliwia nazewnictwo. Mając taki zestaw informacji możemy pokusić się najpierw o klasyfikację grup niskich rzędów – też przeprowadzimy ją bez dowodu.

[13] Więcej o klasyfikacji ogólniejszej por. 3.3.18.

Uwaga 3.3.17.
(1) Jeśli $n_1, \ldots, n_r > 0$ oraz $n = n_1 \cdots n_r$, to $C_n \cong C_{n_1} \oplus \cdots \oplus C_{n_r}$ wtedy i tylko wtedy, gdy liczby $n_1, \ldots, n_r$ są parami względnie pierwsze.

(2) Jeśli $n = p_1^{k_1} \cdots p_r^{k_r}$ jest rozkładem liczby naturalnej n na iloczyn liczb pierwszych $p_1, \ldots, p_r \in \mathbb{P}$ parami różnych, to

$$C_n \cong C_{p_1^{k_1}} \oplus \cdots \oplus C_{p_r^{k_r}}.$$

Uwaga 3.3.18 (klasyfikacja grup rzędu $\leqslant 10$)**.** Jeśli G jest grupą rzędu $\leqslant 10$, to jest ona izomorficzna (jest w klasie izomorfizmu) jednej z poniższych grup.

Rząd grupy	Klasy izomorfizmu
1	0 (grupa jednoelementowa)
2	C_2
3	C_3
4	$C_2 \oplus C_2$ (pierwsza grupa niecykliczna), C_4
5	C_5
6	$C_2 \oplus C_3$, S_3 (pierwsza grupa nieprzemienna)
7	C_7
8	$C_2 \oplus C_2 \oplus C_2$, $C_2 \oplus C_4$, C_8, D_4, Q (grupa kwaternionów)
9	$C_3 \oplus C_3$, C_9
10	$C_2 \oplus C_5$, D_5

Tablica 3.3: Klasyfikacja grup rzędu $\leqslant 10$.

Przypadek gdy rząd jest liczbą pierwszą omówimy niebawem. Pozostałym warto przyjrzeć się w ramach ćwiczeń. Nieprzypadkowo gdy $n = 4$ lub $n = 9$ dostajemy dokładnie dwie grupy. Rezultat ten można uogólnić: *Jeśli $p \in \mathbb{P}$, to jedynymi grupami rzędu p^2 są $C_p \oplus C_p$ oraz C_{p^2}. W szczególności grupa rzędu p^2 jest abelowa.*

Twierdzenie 3.3.19 (Klasyfikacja skończonych grup abelowych)**.** *(Por. twierdzenie 9.4.5) Jeśli G jest skończoną grupą abelową, to istnieją takie $p_1, \ldots, p_r \in \mathbb{P}$ oraz $k_1, \ldots, k_r > 0$, że $G \cong C_{p_1^{k_1}} \oplus \cdots \oplus C_{p_r^{k_r}}$.*

Inaczej mówiąc każda skończona grupa abelowa jest sumą prostą grup cyklicznych. Jak się okazuje własność taka dotyczy również grup abelowych skończenie generowanych.

Twierdzenie 3.3.20 (Klasyfikacja skończenie generowanych grup abelowych)**.** *Każda skończenie generowana grupa abelowa jest izomorficzna z grupą postaci $C_{d_1} \oplus \cdots \oplus C_{d_r} \oplus C_\infty^d$, gdzie liczby $d_1, \ldots, d_r > 1$ spełniają dodatkowo $d_i \mid d_{i+1}$ dla $i = 1, \ldots, r-1$ oraz $d \geqslant 0$.*

3.4 Grupa ilorazowa

Warstwy grupy względem jej podgrup

Podstawowym przykładem grupy, który wykorzystujemy do ilustracji wielu pojęć jest grupa $(\mathbb{Z}, +)$. Zastanówmy się w jaki sposób, ustalając $n \in \mathbb{N}$ utworzyliśmy z tej grupy grupę reszt modulo n. Wprowadziliśmy na $\mathbb{Z}$ relację, która łączyła dwie liczby k i l dokładnie wtedy, gdy liczba $(k - l)$ była elementem podgrupy $n\mathbb{Z}$. Relacja tak wprowadzona okazywała się być relacją równoważności i mogliśmy rozważać klasy abstrakcji. Spróbujemy teraz taki sposób tworzenia nowej struktury uogólnić na sytuację dowolnej grupy G i jej podgrupy H. Zaczniemy od określenia na zbiorze G relacji zależnych od H – jako, że G w przeciwieństwie do $\mathbb{Z}$ nie musi być przemienna rozważymy dwie relacje, na bazie których przy dodatkowych założeniach utworzymy nową strukturę: **grupę ilorazową**.

Gdy G jest grupą, zaś H jej podgrupą, to na zbiorze G określamy relacje

$$a_H \mathcal{R} b :\iff a^{-1}b \in H,$$

$$a \mathcal{R}_H b :\iff ab^{-1} \in H.$$

Własność 3.4.1 (relacje modulo podgrupa)**.** *Niech G będzie grupą, $H < G$ oraz $a \in G$. Wtedy:*

(1) relacje ${}_H\mathcal{R}$ oraz $\mathcal{R}_H$ są relacjami równoważności, tzn. są zwrotne, symetryczne i przechodnie,

(2) klasami równoważności elementu a (czyli zbiorami elementów, które są z nim w relacji) względem relacji ${}_H\mathcal{R}$ oraz $\mathcal{R}_H$ są zbiory

$$[a]_{{}_H\mathcal{R}} = aH = \{ah : h \in H\},$$
$$[a]_{\mathcal{R}_H} = Ha = \{ha : h \in H\},$$

odpowiednio.

(3) $aH = H = Ha$ wtedy i tylko wtedy, gdy $a \in H$.

Dowód. (1) Zwrotność wynika z faktu, że $1 \in H$, zaś symetryczność z tego, że jeśli $x \in H$, to również $x^{-1} \in H$. Przechodniość jest zapewniona przez fakt, że jeśli $x, y \in H$, to $xy \in H$.

(2) Zauważmy, że $a\,{}_H\mathcal{R}\,b$ wtedy i tylko wtedy, gdy istnieje takie $h \in H$, że $a^{-1}b = h$, a to ma miejsce tylko wtedy, gdy $b = ah \in aH$. Podobnie postępujemy dla relacji $\mathcal{R}_H$.

(3) Jeśli $aH = H = Ha$, to oczywiście $a = a \cdot 1 \in aH = H$. Gdy zaś $a \in H$, to oznacza, że $1^{-1} \cdot a = a \cdot 1^{-1} \in H$, więc a jest w obu relacjach z 1, co oznacza równość warstw $aH = 1H = H$ i $Ha = H1 = H$. □

Definicja 3.4.2 (relacje równoważności względem podgrupy, warstwy)**.** Jeśli G jest grupą, zaś H jej podgrupą, to relacje równoważności ${}_H\mathcal{R}$ oraz $\mathcal{R}_H$ nazywamy odpowiednio **lewostronną i prawostronną relacją równoważności grupy G względem podgrupy H**. Klasę równoważności elementu grupy G względem tych relacji nazywamy odpowiednio **warstwą** lewostronną i prawostronną tego elementu względem podgrupy H.

Wróćmy do przykładu grupy $(\mathbb{Z}, +)$. Weźmy dowolną podgrupę H w tej grupie — wiemy, że jest ona postaci $H = n\mathbb{Z}$ dla pewnego $n \in \mathbb{N}$. Wówczas $k\,\mathcal{R}_H\,l$ wtedy i tylko wtedy, gdy $k - l \in n\mathbb{Z}$, a to ma miejsce dokładnie wtedy, gdy $k \equiv l \pmod{n}$. Stąd zbiór warstw, który otrzymujemy w ten sposób, to, tak jak chcieliśmy, zbiór reszt modulo n.

Własność 3.4.3 (podstawowe własności warstw)**.** *Niech H będzie podgrupą grupy G oraz niech $a, b \in H$. Wtedy:*

(1) $\bigcup_{a \in G} aH = G = \bigcup_{a \in G} Ha$.

(2) Dla dowolnych $a, b, \in G$: $aH = bH$ albo $aH \cap bH = \varnothing$, podobnie dla warstw prawostronnych.

(3) Każda warstwa lewostronna (prawostronna) względem podgrupy H jest równoliczna z podgrupą H.

(4) Zbiór $(G/H)_l := \{aH : a \in G\}$ jest równoliczny ze zbiorem $(G/H)_r := \{Ha : a \in G\}$.

Dowód. Zauważmy, że (1) oraz (2) wynikają z faktu, że warstwy są klasami abstrakcji względem pewnej relacji równoważności na zbiorze G. Dowód (3) oraz (4) przeprowadzimy dla warstw lewostronnych (analogicznie przebiega on dla warstw prawostronnych).

By dowieść (3), skonstruujemy bijekcję między warstwą elementu $a \in G$ a podgrupą H. Niech

$$\varphi\colon H \ni x \mapsto ax \in aH.$$

Jest jasne, że odwzorowanie to jest surjekcją. Jest ono również injekcją, bo gdy $ax = ay$, to mnożąc przez a^{-1} z lewej strony otrzymujemy $x = y$. Wobec tego oba zbiory są równoliczne.

(4) Skonstruujemy znów bijekcję między oboma zbiorami warstw

$$\Phi\colon (G/H)_l \ni aH \mapsto Ha^{-1} \in (G/H)_r.$$

Najpierw sprawdzimy poprawną określoność i zarazem injektywność naszego odwzorowania:

$$aH = bH \iff a^{-1}b \in H \iff b^{-1}a \in H \iff Hb^{-1} = Ha^{-1}.$$

Ponadto $Ha = \Phi(a^{-1}H)$, co zapewnia surjektywność naszego odwzorowania. Wobec tego oba zbiory są równoliczne. □

Powyższe twierdzenie pozwala nam wprowadzić jedną z ważniejszych definicji w teorii grup, definicje indeksu podgrupy w grupie oraz udowodnić bazowe twierdzenie tej teorii.

Definicja 3.4.4 (indeks podgrupy w grupie)**. Indeksem** grupy G względem jej podgrupy H (indeksem podgrupy H w grupie G) nazywamy liczbę warstw lewostronnych (prawostronnych) grupy G względem podgrupy H jeśli jest ich skończenie wiele; w przeciwnym wypadku mówimy, że indeks jest nieskończony. Innymi słowy

$$[G : H] := |(G/H)_l| = |(G/H)_r|.$$

Z określenia indeksu $[G : H]$ wynika, że $[G : H] \neq 0$.

Twierdzenie 3.4.5 (Lagrange)**.** *Jeśli H jest podgrupą grupy G, to $|G| = [G : H]|H|$.*[14]

Dowód. W dowodzie będziemy powoływać się na własności 3.4.3. Zauważmy najpierw, że jeśli H jest nieskończoną podgrupą G, to również G jest zbiorem nieskończonym, więc zarówno lewa jak i prawa strona są nieskończone i teza zachodzi niezależnie od tego jaki jest indeks podgrupy H w G.

Załóżmy teraz, że $|H| < \infty$. Dla dowodu rozważać będziemy warstwy lewostronne grupy G względem podgrupy H, czyli zbiory postaci aH. Jako, że warstwy to klasy abstrakcji, to $G = \bigcup_{a\in G} aH$ oraz warstwy dwóch różnych elementów są albo rozłączne albo się pokrywają, wobec tego stosując pewnik wyboru możemy założyć, iż z każdej warstwy wybieramy jeden element i przedstawiamy G jako sumę rozłącznych warstw tzn. $G = \bigcup_{a\in S} aH$, gdzie S oznacza zbiór pojedynczych reprezentantów wszystkich warstw. Jeśli warstw jest nieskończenie wiele, to grupa G jest nieskończona i ponownie zachodzi równość z tezy.

Jeśli indeks jest skończony, to $\#S = [G : H]$. Wiemy, że każda warstwa jest równoliczna z H, czyli w ten sposób $|G| = \#\bigcup_{a\in S} aH = \sum_{a\in S} \#(aH) = \sum_{a\in S} |H| = [G : H]|H|$ co chcieliśmy dowieść. □

Wniosek 3.4.6 (wnioski z twierdzenia Lagrange'a)**.** *Niech G będzie grupą skończoną rzędu n, $H < G$ oraz niech $a \in G$. Wtedy:*

(1) $|H| \mid |G|$ oraz $|a| \mid |G|$.

(2) Jeśli $n \in \mathbb{P}$, to $G \cong C_n$.

Dowód.
(1) Jest to bezpośrednia konsekwencja twierdzenia Lagrange'a.

(2) Jeśli $n \in \mathbb{P}$, to istnieje w G element różny od neutralnego, powiedzmy a. Wtedy jego rząd jest dzielnikiem $|G| = n$ i jest różny od 1, skąd $|a| = n$ i $\langle a\rangle = G$. Jest więc G grupą cykliczna rzędu n, czyli jak wiemy z twierdzenia klasyfikacyjnego 3.3.13 jest $G \cong C_n$. □

Twierdzenie Lagrange'a bywa też komentowane jako prosty wniosek z szerszej własności jaką przytoczymy poniżej.

Twierdzenie 3.4.7 (prawo wieży dla grup)**.** *Niech G będzie grupą, zaś H, K podgrupami G takimi, że $K \subset H \subset G$. Wówczas zachodzi wzór:*

$$[G : K] = [G : H][H : K]$$

gdzie równość tę należy rozumieć tak, że w przypadku gdy jedna ze stron jest nieskończona to nieskończona jest też druga strona.

Dowód. Niech $(a_i)_{i\in I}$ będzie układem reprezentantów warstw prawostronnych grupy G względem podgrupy H, gdzie każda warstwa jest reprezentowana jedynie raz, zaś $(b_j)_{j\in J}$ analogicznie układem reprezentantów warstw prawostronnych grupy H względem podgrupy K. Zauważmy, że

$$G = \bigcup_{i\in I} Ha_i, \qquad \#I = [G : H] \tag{$\star$}$$

$$H = \bigcup_{j\in J} Kb_j, \qquad \#J = [H : K]. \tag{$\star\star$}$$

Zauważmy teraz, że $G = \bigcup_{(i,j)\in I\times J} Kb_ja_i$. Istotnie, wystarczy skomentować zawieranie grupy G w prawej stronie równości. Niech więc $g \in G$, wtedy z $(\star)$ istnieje takie $i \in I$ takie, że $g \in Ha_i$ czyli istnieje $h \in H$ takie, że $g = ha_i$. Na podstawie $(\star\star)$ istnieje $j \in J$ takie, że $h \in Kb_j$ skąd $g = ha_i \in Kb_ja_i$.

[14] Przyjmujemy: $\infty \cdot \infty = \infty$.

Jeśli teraz udowodnimy, że $Kb_{j_1}a_{i_1}$, $Kb_{j_2}a_{i_2}$ są rozłączne o ile tylko $(i_1, j_1) \neq (i_2, j_2)$, to będziemy wiedzieć, że $\bigcup_{(i,j)\in I\times J} Kb_ja_i$ to rozbicie na rozłączne klasy abstrakcji G względem K. Z równości tej widać w szczególności, iż zbiór tych klas jest nieskończony wtedy i tylko wtedy, gdy co najmniej jeden ze zbiorów indeksów I, J jest nieskończony. Otrzymamy wówczas równość

$$[G : K] = \#(I \times J) = \#I \cdot \#J = [G : H][H : K]$$

czego oczekujemy.

Przypuśćmy więc, że $Kb_{j_1}a_{i_1} = Kb_{j_2}a_{i_2}$ – wtedy oczywiście $HKb_{j_1}a_{i_1} = HKb_{j_2}a_{i_2}$. Ponieważ jednak $K \subset H$ więc $b_{j_1}, b_{j_2} \in H$, więc $HKb_{j_s} = H$ dla $s = 1, 2$. Tym samym $Ha_{i_1} = Ha_{a_2}$ i z wyboru a_{i_s} mamy, że $a_{i_1} = a_{i_2}$. W konsekwencji $Kb_{j_1} = Kb_{j_2}$ i dostajemy $j_1 = j_2$. □

Jako bezpośredni wniosek z naszego twierdzenia możemy ponownie wywnioskować twierdzenie Lagrange'a, podstawiając za $K = \{1_G\}$.

3.4.1 Podgrupy normalne

Zauważmy, że w poprzedniej części udowodniliśmy, że liczba warstw lewo- i prawostronnych grupy G względem jej podgrupy H jest taka sama ale nie oznacza to wcale, że te warstwy muszą być takie same! Rozważmy grupę S_3 i jej podgrupę $H = \{\mathrm{id}, (1, 2)\}$. Podgrupa H ma 2 elementy, wobec tego z twierdzenia Lagrange'a wiemy, że warstwy będą 3 i każda z nich będzie dwuelementowa. Bardzo łatwo jednak sprawdzić, wyznaczając te warstwy bezpośrednio, że lewostronne są różne od prawostronnych.

Taka sytuacja prowadzi nas do postawienia definicji kolejnego ważnego pojęcia w teorii grup: podgrupy normalnej.

Definicja 3.4.8 (podgrupa normalna)**.** Podgrupę H grupy G nazywamy **normalną**, jeśli zachodzi równość warstw prawo i lewostronnych tzn. $\forall\ a \in G :\ aH = Ha$. Piszemy wtedy $H \lhd G$.

Nie zawsze możliwym jest bezpośrednie wyznaczenie wszystkich warstw – poniższa własność dostarczy nam wygodnego sposobu sprawdzania, czy dana podgrupa jest normalna.

Własność 3.4.9 (warunek równoważny na normalność)**.** *Niech G będzie grupą oraz $H < G$. Wówczas H jest normalna w G wtedy i tylko wtedy, gdy $\forall\ a \in G\ \forall\ h \in H :\ aha^{-1} \in H$.*

Dowód. Załóżmy najpierw, że H jest podgrupą normalną G i ustalmy dowolne $a \in G$ oraz $h \in H$. Wtedy element ah należy do zbioru aH, o którym z normalności wiemy, że spełnia warunek $aH = Ha$ czyli istnieje $h' \in H$ takie, że $ah = h'a$. Stąd $aha^{-1} = h' \in H$, więc nasz warunek jest spełniony.

Załóżmy teraz, że warunek który proponujemy jest spełniony. Chcemy pokazać, że $aH = Ha$. Niech więc $ah \in aH$. Zgodnie z naszym warunkiem wiemy, że $aha^{-1} \in H$, więc istnieje takie $h' \in H$, że $aha^{-1} = h'$ skąd $ah = h'a \in Ha$ więc mamy zawieranie $aH \subset Ha$.

Niech teraz $ha \in Ha$. Zwróćmy uwagę, że nasz warunek ma „duży kwantyfikator" czyli dla dowolnego elementu z grupy G zachodzi $bHb^{-1} \subset H$. Jako element b przyjmijmy więc a^{-1} i dostaniemy, że $a^{-1}ha \in H$ skąd więc $a^{-1}ha = h'$ dla pewnego $h' \in H$ i $ha = ah' \in aH$ więc mamy zawieranie w drugą stronę. □

Uwaga 3.4.10 (podstawowe własności pojęcia normalności)**.** Niech $K \subseteq H$ będą podgrupami grupy G. Zachodzą następujące własności:

(1) $\{1_G\} \lhd G$ oraz $G \lhd G$,

(2) jeśli $K \lhd G$, to $K \lhd H$,[15]

(3) każda podgrupa grupy abelowej jest jej podgrupą normalną,

(4) jeżeli $[G : H] = 2$, to H jest podgrupą normalną, co wynika z faktu, że jedną z warstw (zarówno lewo- jak i prawostronnych) jest warstwa elementu neutralnego równa H, drugą z konieczności tworzyć muszą wszystkie pozostałe elementy,

[15] Nie oznacza to, że normalność jest pojęciem przechodnim; można rozważyć na przykład w grupie S_4 podgrupę $K := \langle(1\ 2)(3\ 4)\rangle$ normalną w $H := \{(1\ 2)(3\ 4), (1\ 3)(4\ 2), (2\ 3)(4\ 1), \mathrm{id}\}$, która jest normalna w S_4 podczas gdy K nie jest normalna w S_4. Zastosowany został zapis cykliczny permutacji por. 3.6.1).

(5) grupa kwaternionów (por. przykład 3.3.4 (5)) jest nieabelowa ale każda jej podgrupa jest normalna.

Własność 3.4.11 (homomorfizmy a normalność). *Niech $f\colon G \to \widetilde{G}$ będzie homomorfizmem grup, niech $H, H_i \lhd G$ dla $i \in I$ oraz niech $\widetilde{H} \lhd \widetilde{G}$. Wtedy:*

(1) $\bigcap_{i\in I} H_i \lhd G$,

(2) $f(H) \lhd f(G)$([16]),

(3) $f^{-1}(\widetilde{H}) \lhd G$.

Dowód. Wystarczy w każdym przypadku zastosować na przykład warunek z 3.4.9 i wykorzystać własności znane z wcześniejszej teorii dla podgrup. □

3.4.2 Konstrukcja grupy ilorazowej

Niech G będzie dowolną grupą, zaś H jej podgrupą normalną. Wprowadzimy teraz zapowiadaną wcześniej strukturę grupy na zbiorze wszystkich warstw grupy G względem podgrupy H.

Niech G/H oznacza zbiór wszystkich warstw lewostronnych (prawostronnych) grupy G względem podgrupy H. Innymi słowy:

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

Na zbiorze tym zadajemy następujące działanie

$$(aH)(bH) := (ab)H, \qquad a, b \in G.$$

Twierdzenie 3.4.12 (twierdzenie o konstrukcji grupy ilorazowej). *Niech H będzie podgrupą normalną grupy G. Wtedy:*

(1) działanie zadane powyżej jest poprawnie określone,

(2) zbiór G/H z wprowadzonym wyżej działaniem ma strukturę grupy,

(3) odwzorowanie $\pi_H\colon G \ni a \mapsto aH \in G/H$ jest epimorfizmem grup, ponadto mamy $\operatorname{Ker}\pi_H = H$.

Dowód.
(1) Niech $aH = a_1H$, $bH = b_1H$. Pytamy się czy wtedy $(ab)H = (a_1b_1)H$. Skoro $aH = a_1H$, to $a^{-1}a_1 \in H$, zaś skoro $bH = b_1H$ to $b^{-1}b_1 \in H$. Policzmy teraz $(ab)^{-1}(a_1b_1) = b^{-1}a^{-1}a_1b_1 \in b^{-1}Hb_1 = b^{-1}b_1H = H$, gdzie w przedostatniej równości wykorzystaliśmy normalność H, zaś w ostatniej skorzystaliśmy z faktu, że $b^{-1}b_1 \in H$. Z naszego rozumowania wynika, że określone działanie jest poprawnie zdefiniowane.

(2) Łączność działania w G/H wynika z łączności działania w G. Widać też od razu, że warstwa $1H = H$ jest elementem neutralnym określonego działania. Ponadto, skoro $(aH)(a^{-1}H) = (aa^{-1})H = H$, to $(aH)^{-1} = a^{-1}H$.

(3) Fakt, że π_H jest homomorfizmem grup wynika bezpośrednio z określenia działania w grupie G/H. Ponieważ każdy element grupy G/H jest postaci aH dla pewnego $a \in G$, więc jest to oczywiście surjekcja. Jeśli $a \in G$, to $\pi_H(a) = 1_{G/H}$ wtedy i tylko wtedy, gdy $aH = H$, zaś równość ta ma miejsce dokładnie wtedy, gdy $a \in H$ (3.4.1(3)), skąd wynika teza o jądrze. □

Definicja 3.4.13 (grupa ilorazowa). Jeśli G jest grupą, zaś H jej podgrupą normalną, to zbiór $G/H = \{aH :\ a \in G\}$ z działaniem $(aH)(bH) := (ab)H$ nazywamy **grupą ilorazową** grupy G przez podgrupę H. Odwzorowanie $\pi_H : G \ni a \longrightarrow aH \in G/H$ nazywamy odwzorowaniem (rzutowaniem) kanonicznym (naturalnym) grupy G na grupę G/H.

Zauważmy, że zgodnie z naszymi wcześniejszymi uwagami grupa ilorazowa jaka powstanie po podzieleniu $G = \mathbb{Z}$ przez $H = n\mathbb{Z}$ (wobec abelowości G oczywiście H jest normalna), to nic innego jak $(\mathbb{Z}_n, +_n)$. Proste przeliczenie pokazuje, że odwzorowanie:

$$\psi : \mathbb{Z}/n\mathbb{Z} \ni k + n\mathbb{Z} \mapsto [k]_n \in \mathbb{Z}_n$$

jest izomorfizmem grup.

W języku grupy ilorazowej możemy wyrazić jeszcze jeden przydatny warunek równoważny na to, aby podgrupa była normalna.

[16] Niekoniecznie w $\widetilde{G}$ – wystarczy rozważyć zanurzenie w G dowolnej podgrupy H, która nie jest normalna w G.

Własność 3.4.14 (warunek na normalność w języku homomorfizmu)**.** *Podgrupa H grupy G jest jej podgrupą normalną wtedy i tylko wtedy, gdy istnieje grupa $\widetilde{G}$ oraz taki homomorfizm grup $f\colon G \to \widetilde{G}$, że $H = \operatorname{Ker} f$.*

Dowód. Jeśli H jest podgrupą normalną grupy G, to zgodnie z twierdzeniem 3.4.12 wystarczy przyjąć $\widetilde{G} = G/H$ oraz $f = \pi_H$. Odwrotnie, jądro homomorfizmu jest zawsze podgrupą normalną będąc przeciwobrazem podgrupy normalnej, jaką jest podgrupa trywialna. □

3.5 Twierdzenia o homomorfizmach grup

Twierdzenie 3.5.1 (twierdzenie o przenoszeniu podgrup)**.** *Jeśli $f\colon G \to \widetilde{G}$ jest epimorfizmem grup, $\mathcal{G}$ jest rodziną podgrup w G zawierających $\operatorname{Ker} f$, zaś $\widetilde{\mathcal{G}}$ jest rodziną wszystkich podgrup w $\widetilde{G}$, to odwzorowania*

$$\Phi\colon \mathcal{G} \ni H \mapsto f(H) \in \widetilde{\mathcal{G}},$$

$$\Psi\colon \widetilde{\mathcal{G}} \ni \widetilde{H} \mapsto f^{-1}(\widetilde{H}) \in \mathcal{G}$$

są wzajemnie odwrotnymi bijekcjami. Bijekcje te zachowują również podgrupy normalne.

Dowód. Zauważmy najpierw, że powyższe odwzorowania są poprawnie określone, również w przypadku podgrup normalnych, wobec faktu, że f jest epimorfizmem, więc jak wiemy obraz podgrupy normalnej jest podgrupą normalną. Dzięki surjektywności f mamy też $f(f^{-1}(A)) = A$ dla dowolnego $A \subseteq G$, w szczególności jest $\Phi \circ \Psi = \mathrm{id}_{\widetilde{\mathcal{G}}}$. Wiemy również, że dla dowolnego $A \subseteq G$ jest $A \subseteq f^{-1}(f(A))$, zatem jeśli $\operatorname{Ker} f \subseteq H < G$, to pozostaje wykazać, że $f^{-1}(f(H)) \subseteq H$. Istotnie, jeśli $x \in f^{-1}(f(H))$, to $f(x) \in f(H)$, zatem istnieje takie $h \in H$, że $f(x) = f(h)$, czyli $h^{-1}x \in \operatorname{Ker} f$. Ostatecznie jest więc $x \in h \operatorname{Ker} f \subseteq hH = H$, czyli $\Psi \circ \Phi = \mathrm{id}_{\mathcal{G}}$ oraz Φ i Ψ są wzajemnie odwrotnymi bijekcjami. □

Dobrą ilustracją zastosowania twierdzenia 3.5.1 jest wyznaczenie postaci podgrup w grupach reszt modulo n. Rozważamy epimorfizm

$$f\colon \mathbb{Z} \ni k \mapsto [k]_n \in \mathbb{Z}_n.$$

By wyznaczyć podgrupy w $\mathbb{Z}_n$ wystarczy wyznaczyć podgrupy w $\mathbb{Z}$, zawierające jądro odwzorowania, czyli podgrupę $n\mathbb{Z}$ (podgrupy te są charakteryzowane przez podzielniki naturalne n) i przenieść je za pomocą f. Dla przykładu z twierdzenia tego otrzymujemy, że wszystkie podgrupy w grupie $(\mathbb{Z}_8, +)$, to $\{0\}$, $\{0, 4\}$, $\{0, 2, 4, 6\}$ i cała grupa.

Twierdzenie 3.5.2 (Podstawowe twierdzenie o izomorfizmie)**.** *Jeśli $f\colon G \to \widetilde{G}$ jest homomorfizmem grup, to wtedy $G/\operatorname{Ker} f \cong \operatorname{Im} f$.*

Dowód. Zauważmy najpierw, że sformułowanie w tezie ma sens tzn. istnieje grupa ilorazowa $G/\operatorname{Ker} f$ – istotnie, $\operatorname{Ker} f = f^{-1}(\{1_{\widetilde{G}}})$ czyli jako przeciwobraz podgrupy normalnej jądro jest podgrupą normalną (oczywiście, łatwo to sprawdzić także w oparciu o warunek równoważny 3.4.9).

Izomorfizm skonstruujemy bezpośrednio. Rozważmy odwzorowanie:

$$F : G/\operatorname{Ker} f \ni a \operatorname{Ker} f \longmapsto f(a) \in \operatorname{Im} f.$$

Sprawdzimy, że jest ono poprawnie określonym izomorfizmem (z oczywistych względów jest to surjekcja).

Zauważmy, że mamy następujący ciąg równoważności:

$$\begin{aligned} a \operatorname{Ker} f = b \operatorname{Ker} f &\iff b^{-1}a \in \operatorname{Ker} f \iff f(b^{-1}a) = 1_{\widetilde{G}} \iff [f(b)]^{-1} f(a) = 1_{\widetilde{G}} \\ &\iff f(b) = f(a) \iff F(b \operatorname{Ker} f) = F(a \operatorname{Ker} f). \end{aligned}$$

Wynikanie od strony lewej do prawej dowodzi poprawnej określoności odwzorowania, zaś od prawej do lewej jego injektywności.

Sprawdźmy jeszcze, że F jest homomorfizmem:

$$F[(a \operatorname{Ker} f) \cdot (b \operatorname{Ker} f)] = F((ab) \operatorname{Ker} f) = f(ab) = f(a)f(b) = F(a \operatorname{Ker} f) F(b \operatorname{Ker} f).$$

□

3.6 Grupy permutacji S_n

Będziemy rozważać grupy permutacji zbioru $\{1,\dots,n\}$ dla $n \in \mathbb{N}$. Grupa ta zasługuje na szczególną uwagę z co najmniej kilku powodów: wobec swojej historycznej roli w rozwoju teorii grup, wobec twierdzenia Cayleya (3.2.13), które w pewien sposób wiąże dowolną grupę z pewną grupą permutacji i wreszcie wobec jej kluczowego znaczenia w powiązaniu teorii grup z rozwiązywaniem równań wielomianowych, o czym powiemy w drugiej części skryptu. Tutaj zbierzemy jedynie podstawowe, przydatne dalej, informacje o tej grupie.

Elementy zbioru S_n będziemy oznaczać na dwa sposoby: albo jako odwzorowania

$$\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\}$$

albo symbolem

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}.$$

Oczywiście, jak wiemy zbiór S_n z działaniem składania (mnożenia) permutacji tworzy grupę (nieprzemienną dla $n > 2$).

Definicja 3.6.1 (cykl k-elementowy, transpozycja)**.** Jeśli $\{a_1,\dots,a_k\} \subseteq \{1,\dots,n\}$ jest zbiorem k-elementowym, gdzie $1 < k \leqslant n$, to permutację $\varrho \in S_n$ określoną wzorem

$$\varrho(a_1) = a_2,\ \dots,\ \varrho(a_{k-1}) = a_k,\ \varrho(a_k) = a_1, \qquad \varrho(j) = j, \qquad j \notin \{a_1,\dots,a_k\}$$

nazywamy **cyklem k-elementowym** i zapisujemy $\varrho = (a_1\ a_2\ \dots\ a_k)$. Liczbę k nazywamy długością cyklu ϱ. Permutację identycznościową traktujemy jako cykl długości 1. Cykl dwuelementowy nazywamy **transpozycją.**

Przykładem cyklu jest permutacja $\left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 3&7&5&4&2&6&1 \end{smallmatrix}\right) = (1\ 3\ 5\ 2\ 7)$, natomiast permutacja $\left(\begin{smallmatrix} 1&2&3&4&5&6&7 \\ 3&5&7&6&2&4&1 \end{smallmatrix}\right)$ nie jest cyklem.

Definicja 3.6.2 (cykle rozłączne)**.** Cykle $\sigma = (a_1\ \dots\ a_k) \in S_n$ oraz $\varrho = (b_1\ \dots\ b_l) \in S_n$ nazywamy **rozłącznymi**, jeśli $\{a_1,\dots,a_k\} \cap \{b_1,\dots,b_l\} = \varnothing$.

Przykładowo, cykle $(1\ 2\ 3\ 4)$ oraz $(5\ 6)$ są rozłączne, natomiast cykle $(1\ 3)$ oraz $(3\ 5\ 4)$ rozłączne nie są. Zauważmy ponadto, że $(1\ 2\ 3\ 4)(5\ 6) = \left(\begin{smallmatrix} 1&2&3&4&5&6 \\ 2&3&4&1&6&5 \end{smallmatrix}\right) = (5\ 6)(1\ 2\ 3\ 4)$ natomiast $(1\ 3)(3\ 5\ 4) = (1\ 3\ 5\ 4) \neq (1\ 5\ 4\ 3) = (3\ 5\ 4)(1\ 3)$.[17]

Obserwacja 3.6.3 (przemienność cykli rozłącznych)**.** *Cykle rozłączne są przemienne.*

Dowód. Niech $\sigma = (a_1\ \dots\ a_k) \in S_n$ oraz $\varrho = (b_1\ \dots\ b_l) \in S_n$ będą cyklami rozłącznymi. Wybierzmy $1 \leqslant i \leqslant n$. Jeśli $i \notin \{a_1,\dots,a_k\} \cup \{b_1,\dots,b_l\}$, to $\sigma(i) = \varrho(i) = i$, zatem $(\sigma\circ\varrho)(i) = i = (\varrho\circ\sigma)(i)$. Jeśli zaś $i \in \{a_1,\dots,a_k\}$, to $i \notin \{b_1,\dots,b_l\}$. W szczególności $\sigma(i) \in \{a_1,\dots,a_k\}$ oraz $(\sigma\circ\varrho)(i) = \sigma(i) = (\varrho\circ\sigma)(i)$. Podobnie, gdy $i \in \{b_1,\dots,b_l\}$, to mamy $(\sigma\circ\varrho)(i) = \varrho(i) = (\varrho\circ\sigma)(i)$. Łącznie jest więc $\sigma\circ\varrho = \varrho\circ\sigma$. □

Twierdzenie 3.6.4 (rozkład permutacji na cykle)**.** *Każda permutacja ma jednoznaczny rozkład na cykle rozłączne.*

Dowód. Niech $\sigma \in S_n$. Istnienie rozkładu permutacji σ na cykle rozłączne wykażemy indukcyjnie względem n. Dla $n = 1, 2$ jest to oczywiste. Przypuśćmy więc, że $n > 2$ oraz, że każda permutacja zbioru o co najwyżej $(n-1)$-elementach jest cyklem lub iloczynem cykli rozłącznych. Możemy założyć, że $\sigma \neq \mathrm{id}$. Wobec tego istnieje takie $a \in \{1,\dots,n\}$, że $\sigma(a) \neq a$. Oznaczmy $a_1 = a$, $a_2 = \sigma(a_1)$, itd. Wtedy $a_1 \neq a_2$. Ponieważ zbiór $\{1,\dots,n\}$ jest skończony, to istnieje j, dla którego istnieje takie i, że $1 \leqslant i < j \leqslant n$ oraz $a_i = a_j$. Wybierzmy minimalną liczbę o tej własności i oznaczmy ją przez j_0. Niech teraz $1 \leqslant i_0 < j_0 \leqslant n$ spełnia $a_{j_0} = a_{i_0}$. Jeśli wykażemy, że $i_0 = 1$, to otrzymamy pierwszy cykl. Przypuśćmy więc, że $i_0 > 1$, wtedy jednak $\sigma(a_{j_0-1}) = a_{j_0} = a_{i_0} = \sigma(a_{i_0-1})$, czyli dzięki injektywności σ jest $a_{j_0-1} = a_{i_0-1}$ i mamy sprzeczność z minimalnością j_0. Wobec tego $i_0 = 1$, czyli permutację σ możemy zapisać następująco

$$\sigma = \begin{pmatrix} a_1 & \cdots & a_{j_0-1} \\ a_2 & \cdots & a_1 \end{pmatrix} \circ \varrho, \qquad \varrho = \begin{pmatrix} b_{j_0} & \cdots & b_n \\ \sigma(b_{j_0}) & \cdots & \sigma(b_n) \end{pmatrix},$$

gdzie $\{b_{j_0},\dots,b_n\} = \{1,\dots,n\} \setminus \{a_1,\dots,a_{j_0-1}\}$. Korzystając z założenia indukcyjnego otrzymujemy dalszy rozkład na cykle rozłączne permutacji ϱ, a tym samym rozkład na cykle rozłączne permutacji σ. Niech teraz

$$\sigma = \sigma_1 \circ \cdots \circ \sigma_s = \varrho_1 \circ \cdots \circ \varrho_r$$

[17] Zwykle w takim zapisie pomijamy znak składania $\circ$ pomiędzy permutacjami.

będą rozkładami permutacji σ na cykle rozłączne. Jeśli $\sigma_1 = (a_1\ \ldots\ a_k)$, to a_1 występuje w dokładnie jednym z cykli ϱ_i dla $i = 1, \ldots, r$. Możemy założyć, że a_1 występuje w cyklu $\varrho_1 = (b_1\ \ldots\ b_l)$ oraz, że $a_1 = b_1$ (możemy cyklicznie przestawić elementy $b_1, \ldots, b_l$ tak, aby a_1 znalazł się jako pierwszy w zapisie). Mamy $a_2 = \sigma(a_1) = \sigma(b_1) = b_2$, itd. Musi więc być $k = l$ oraz $\sigma_1 = \varrho_1$, zatem

$$\sigma_2 \circ \cdots \circ \sigma_s = \varrho_2 \circ \cdots \circ \varrho_r.$$

Teraz zwykła indukcja kończy dowód. □

Rozważmy permutację $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 1 & 7 & 8 & 6 & 11 & 2 & 4 & 9 & 10 & 5 \end{smallmatrix}\right) \in S_{11}$. Łatwo sprawdzić, że otrzymujemy rozkład na cykle rozłączne postaci $\sigma = (1\ 3\ 7\ 2)(4\ 8)(5\ 6\ 11)$.

Wniosek 3.6.5 (rozkład permutacji na transpozycje)**.** *Niech $n > 1$ oraz $\sigma \in S_n$.*

(1) Każda permutacja n-elementowa jest iloczynem transpozycji [18]*.*

(2) Jeśli w jednym z rozkładów na transpozycje permutacji σ występuje parzysta (nieparzysta) liczba transpozycji, to jest tak również w dowolnym innym rozkładzie na transpozycje tej permutacji.

Dowód.
(1) Dla identyczności mamy np. $\mathrm{id} = (i\ j)(i\ j)$, gdzie $i \neq j$. Dalej wystarczy ograniczyć się do cykli długości $1 < r \leqslant n$ i zauważyć, że $(a_1\ \ldots\ a_r) = (a_1\ a_r)(a_1\ a_{r-1}) \cdot \ldots \cdot (a_1\ a_2)$.

(2) Dla dowolnej permutacji σ określmy liczbę zwaną jej wyróżnikiem następująco:

$$\Delta(\sigma) := \prod_{1 \leqslant i < j \leqslant n} \big(\sigma(j) - \sigma(i)\big).$$

Oczywiście, jeśli $\tau \in S_n$ jest transpozycją, to $\Delta(\sigma \circ \tau) = -\Delta(\sigma)$. Niech teraz

$$\sigma = \sigma_1 \circ \ldots \circ \sigma_s = \tau_1 \circ \ldots \circ \tau_r,$$

gdzie $\sigma_1, \ldots, \sigma_s \in S_n$ oraz $\tau_1, \ldots, \tau_r \in S_n$ są transpozycjami. Mamy więc:

$$\Delta(\sigma) = (-1)^s \Delta(\mathrm{id}) = (-1)^r \Delta(\mathrm{id}).$$

Ponieważ $\Delta(\mathrm{id}) \neq 0$, to $(-1)^s = (-1)^r$, czyli r oraz s są tej samej parzystości. □

Definicja 3.6.6 (znak permutacji)**.** Permutację $\sigma \in S_n$ $(n > 1)$ nazywamy **parzystą (nieparzystą)**, jeśli w jej rozkładzie na transpozycje liczba transpozycji jest parzysta (nieparzysta). Jeśli liczba transpozycji występujących w pewnym rozkładzie permutacji σ jest równa s, to liczbę $\mathrm{sgn}(\sigma) = (-1)^s$ nazywamy znakiem permutacji σ. Gdy $n = 1$, to przyjmujemy, że jedyna permutacja identycznościowa jest permutacją parzystą.

Dzięki wnioskowi 3.6.5 wiemy, że znak permutacji z definicji 3.6.6 jest poprawnie określony. Ponadto, dla $n > 1$ odwzorowanie

$$\mathrm{sgn}\colon S_n \ni \sigma \mapsto \mathrm{sgn}(\sigma) \in \{-1, 1\}$$

jest epimorfizmem o jądrze A_n — będącym zbiorem wszystkich permutacji parzystych.

Definicja 3.6.7 (grupa alternująca)**.** Grupę A_n złożoną ze wszystkich n-elementowych permutacji parzystych nazywamy **grupą alternującą** stopnia n.

Obserwacja 3.6.8 (własności A_n)**.** *A_n jest podgrupą normalną w S_n. Ponadto $|A_n| = n!/2$ dla $n > 1$.*[19]

Dowód. Fakt, że $A_n \lhd S_n$ wynika stąd, że A_n jest jądrem wyżej określonego homomorfizmu. Jeśli $n > 1$, to na podstawie podstawowego twierdzenia o izomorfizmie (3.5.2) mamy $S_n/A_n \cong \{-1, 1\} \cong C_2$, skąd wynika równość $[S_n : A_n] = |S_n/A_n| = 2$ i z twierdzenia Lagrange'a (3.4.5) mamy $|A_n| = |S_n|/2 = n!/2$. □

Fakt, który wykażemy poniżej, choć ciekawy sam w sobie jest przygotowaniem do powiązania możliwości odzyskania pierwiastków wielomianów za pomocą operacji na ich współczynnikach z własnościami grup wyznaczonych przez rozważane wielomiany. Wykażemy, że dla $n \geqslant 5$ grupa A_n nie ma istotnych podgrup normalnych – to czyni pośrednio wyjątkowymi równania wielomianowe dla stopni większych od 4.

[18] Transpozycje te jednak nie muszą być rozłączne.
[19] Liczność zbioru permutacji parzystych można oczywiście prosto wykazać na bazie własności kombinatorycznych.

Definicja 3.6.9 (grupa prosta)**.** Grupę nie zawierającą nietrywialnej, właściwej podgrupy normalnej nazywamy **prostą**.

Twierdzenie 3.6.10 („prostota A_n")**.** *Grupa A_n jest prosta dla $n \geqslant 5$.*

Dowód. Niech $\{\mathrm{id}\} \neq H \lhd A_n$ oraz ustalmy $\sigma \in H \setminus \{\mathrm{id}\}$. Dowód przedstawimy w dwóch krokach.

Krok 1. Wykażemy, że H zawiera iloczyn pewnych dwóch transpozycji rozłącznych. Rozłóżmy σ na iloczyn cykli rozłącznych. Mamy wtedy cztery możliwości:

(1) w rozkładzie σ nie występuje cykl o długości mniejszej niż 4,

(2) w rozkładzie σ występują co najmniej dwa cykle i jeden z nich jest długości 3 ,

(3) σ jest cyklem długości 3,

(4) σ jest iloczynem parzystej liczby rozłącznych transpozycji.

W każdym z przypadków dobierzemy pewną permutację $\tau \in A_n$ tak, aby z dokładnością do ewentualnej zmiany numeracji elementów wszystkie sytuacje przedstawiała tabela:

Przypadek	$\sigma \in H$	$\tau \in A_n$	$\sigma\tau\sigma^{-1}\tau^{-1} \in H$
(1)	$(1\ 2\ 3\ 4\ \ldots)\bar{\sigma}$	$(1\ 2\ 3)$	$(1\ 4\ 2)$
(2)	$(1\ 2\ 3)(4\ 5\ \ldots)\bar{\sigma}$	$(1\ 2\ 4)$	$(1\ 4\ 3\ 5\ 2)$
(3)	$(1\ 2\ 3)$	$(1\ 2\ 4)$	$(1\ 2)(3\ 4)$
(4)	$(1\ 2)(3\ 4)\bar{\sigma}$	$(1\ 2\ 3)$	$(1\ 3)(2\ 4)$

Jak widać do H zawsze należy iloczyn dwóch rozłącznych transpozycji. W przypadku (3) i (4) jest to oczywiste, przypadek (1) sprowadza się do (3) (skoro otrzymaliśmy cykl długości 3), zaś przypadek (2) sprowadza się do (1), zatem również do (3).

Krok 2. Korzystając z kroku 1 ustalmy $\sigma = (1\ 2)(3\ 4) \in H$. Wykażemy, że iloczyn dowolnych dwóch transpozycji należy do H, co będzie oznaczało, że $H = A_n$. Rozważmy najpierw iloczyn dwóch transpozycji rozłącznych $(i\ j)(k\ l)$. Niech

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ i & j & k & l & \tau(5) & \cdots & \tau(n) \end{pmatrix}.$$

Wówczas $\tau \in A_n$ lub $\pi = \tau(1\ 2) \in A_n$, zatem $\tau\sigma\tau^{-1} \in H$ lub $\pi\sigma\pi^{-1} = \tau\sigma\tau^{-1} \in H$. Tak czy inaczej $\varrho = \tau\sigma\tau^{-1} \in H$ oraz $\varrho = \tau\sigma\tau^{-1} = (i\ j)(k\ l)$. Gdy natomiast mamy do czynienia z permutacją $(i\ j)(i\ k)$, gdzie $j \neq k$, to istnieją takie $l, m \in \{1, \ldots, n\} \setminus \{i, j, k\}$, że $l \neq m$ oraz mamy $(i\ j)(i\ k) = [(i\ j)(l\ m)][(l\ m)(i\ k)] \in H$. □

Wniosek 3.6.11. *Dla dowolnego $n > 1$ grupa A_n jest jedyną podgrupą indeksu 2 w S_n.*

Dowód. Dla $n < 5$ własność można sprawdzić bezpośrednim rachunkiem, ograniczymy się więc do komentarza dla $n \geqslant 5$. Niech $H \leqslant S_n$ będzie podgrupą indeksu 2. Wiemy, że $H \lhd S_n$, zatem $H \cap A_n \lhd A_n$. Skoro A_n jest grupą prostą, to $H \cap A_n = A_n$ lub $H \cap A_n = \{\mathrm{id}\}$. Gdyby zachodziła druga możliwość, to podgrupa H zawierałaby tylko jedną permutację parzystą i co najmniej 59 permutacji nieparzystych. Wybierzmy dwie różne permutacje $\sigma, \tau \in H \setminus \{\mathrm{id}\}$. Zauważmy, że permutacje σ^2 oraz $\sigma\tau$ są parzyste i leżą w H, zatem $\sigma^2 = 1 = \sigma\tau$, więc $\sigma = \tau$, sprzeczność. Musi zachodzić zatem $H \cap A_n = A_n$, czyli $A_n \subseteq H$. Równość rzędów obu podgrup gwarantuje, że $H = A_n$. □

3.7 Zadania

1. Niech $X = \{f : \mathbb{R} \to (0, +\infty)\}$ z działaniem mnożenia funkcji. Sprawdzić, że X jest grupą. Czy $Y \subset X$ jest podgrupą X, gdzie Y jest dana poniżej?
   (a) $Y = \{f \in X : f(0) > f(1)\}$;
   (b) $Y = \{f \in X : f(0) = 1\}$;
   (c) $Y := \{f \in X : f$ jest funkcją parzystą$\}$;
   (d) $Y := \{f \in X : f$ jest funkcją nieparzystą$\}$.
2. Sprawdzić, że zbiór $\mu_\infty = \{z \in \mathbb{C} : \ \exists n \in \mathbb{N} : \ z^n = 1\} = \bigcup_{n\in\mathbb{N}} \mu_n$ pierwiastków zespolonych z liczby 1 dowolnych stopni jest grupą względem mnożenia liczb.

3. Udowodnić, że dla dowolnych grup $(G, \circ)$, $(G', \bullet)$ iloczyn kartezjański $G \times G'$ jest grupą względem działania $\cdot$ określonego wzorem
$$(a, a') \cdot (b, b') = (a \circ a', b \bullet b').$$

4. Niech $a \in \mathbb{R}_+$. Udowodnić, że przedział $[0, a)$ tworzy grupę abelową względem działania $\oplus$ określonego wzorem
$$x \oplus y = \begin{cases} x + y & \text{jeśli } x + y < a, \\ x + y - a & \text{jeśli } x + y \geqslant a. \end{cases}$$

5. Niech $(G, \cdot)$ będzie grupą i niech funkcja $f : G \longrightarrow A$ będzie bijekcją. Wykazać, że jeśli działanie $\oplus$ w zbiorze A jest określone wzorem $a_1 \oplus a_2 = f(f^{-1}(a_1) \cdot f^{-1}(a_2))$, to para $(A, \oplus)$ jest grupą.

6. Korzystając z poprzedniego zadania wykazać, że w zbiorze $\mathbb{N}$ można określić takie działanie, względem którego $\mathbb{N}$ jest grupą.

7. Niech H_1, H_2 będą podgrupami grupy abelowej G. Dowieść, że zbiór
$$H_1 + H_2 := \{h_1 + h_2 : \ h_1 \in H_1, \ h_2 \in H_2\}$$
jest podgrupą grupy G oraz że podgrupa ta jest najmniejsza w sensie inkluzji podgrupą grupy G zawierającą każdą z podgrup H_1 i H_2.

8. Sprawdzić, czy dana funkcja ϕ jest homomorfizmem grup. Jeśli tak, to wyznaczyć jądro i obraz tego homomorfizmu.
   (a) $\phi : \mathbb{Z} \to \mathbb{Z}, \ \phi(a) = na$, gdzie $n \in \mathbb{N}$;
   (b) $\phi : \mathbb{C}^* \to \mathbb{C}^*, \ \phi(z) = |z|$;
   (c) $\phi : \mathbb{C} \to \mathbb{R}, \ \phi(z) = |z|$;
   (d) $\phi : \mathbb{R}^* \to \mathbb{R}^*, \ \phi(a) = a^2$;
   (e) $\phi : \mathbb{R}^* \to \mathbb{R}^*, \ \phi(a) = \sqrt[3]{a}$;
   (f) $\phi : \mathbb{C}^* \to \mathbb{C}^*, \ \phi(z) = z^m$, gdzie $n \in \mathbb{N}$;
   (g) $\phi : \mathbb{R}^+ \to \mathbb{R}, \ \phi(a) = \log a$;
   (h) $\phi : \mathbb{Z} \to \mathbb{Z}_n, \ \phi(a) = a \pmod n$;
   (i) $\phi : \mu_n \to \mu_n, \ \phi(z) = z^k$, gdzie $k \in \mathbb{N}$ i $k|n$ oraz $\mu_n = \{z \in \mathbb{C} : \ z^n = 1\}$ (z działaniem mnożenia);
   (j) $\phi : M_2(\mathbb{R}) \to M_2(\mathbb{R}), \ \phi(A) = A^T$;
   (k) $\phi : M_2(\mathbb{R}) \to \mathbb{R}, \ \phi(A) = \det(A)$.

9. Udowodnić, że grupy $\mathbb{R}$ i $\mathbb{R}^*$ nie są izomorficzne.

10. Niech
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 4 & 3 & 1 \end{pmatrix} \qquad \text{i} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$$
Obliczyć
$$\sigma\tau, \tau\sigma, \tau^{-1}\sigma^{-1}.$$
Rozłożyć permutacje σ i τ na iloczyn cykli i iloczyn transpozycji sąsiednich elementów, wyznaczyć ich znak i rząd.

11. Dla każdego elementu $a \in G$ wyznaczyć podgrupę generowaną przez a i określić rząd elementu a, gdzie:
   (a) $G = \mathbb{Z}_8$,
   (b) $G = \mathbb{Z}_2 \times \mathbb{Z}_5$,
   (c) $G = (\{a \in \{1, \ldots, 14\} : \ (a, 14) = 1\}, \cdot_{14})$.

12. Podać liczbę elementów rzędu 2, 3, 4, 5, 6 w grupie G, gdzie:

(a) $\mathbb{Z}_{12}$,

(b) $\mathbb{Z}_2 \times \mathbb{Z}_8$,

(c) $\mathbb{Z}_5 \times \mathbb{Z}_{15}$,

(d) $\mathbb{Z} \times \mathbb{Z}_{30}$,

(e) $\mathbb{Z} \times \mathbb{Z}_{11}^*$.

13. Niech G będzie grupą. Udowodnić, że dla dowolnych $a, b \in G$ zachodzi $|ab| = |ba|$.

14. Udowodnić, że żadna z poniższych grup nie jest cykliczna:

(a) $\mathbb{Z} \times \mathbb{Z}_n$, gdzie $n \in \mathbb{N}_{\geqslant 2}$,

(b) $\mathbb{Z} \times \mathbb{C}$,

(c) $\mathbb{Z}_2 \times \mathbb{Z}_n$, gdzie $n \in \mathbb{N}_{\geqslant 2}$,

(d) $\mathbb{Z}_n \times \mathbb{Z}_n$, gdzie $n \in \mathbb{N}_{\geqslant 2}$.

15. W grupie S_3 wygenerować podgrupę przez $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, sprawdzić jej normalność oraz wyliczyć indeks.

16. Rozważmy grupę $(\mathbb{C}^\star, \cdot)$ oraz jej podgrupę $H = \mathbb{R}^+$. Odpowiedzieć na pytanie jaki podzbiór płaszczyzny tworzy warstwa ustalonej liczby $z \in \mathbb{C}^\star$ względem podgrupy H.

17. Wykazać, że dla każdego $n \in \mathbb{N}_+$ istnieje grupa G, która jest generowana przez dokładnie n-elementów.

18. Sprawdzić, że zbiór $H = \{bi : \ b \in \mathbb{R}\}$ jest podgrupą normalną grupy $\mathbb{C}$. Opisać warstwy elementów $z \in \mathbb{C}$ względem tej podgrupy, a następnie wykazać, że $\mathbb{C}/H \cong \mathbb{R}$.

19. Sprawdzić, że zbiór $H = \{(x, y, z) \in \mathbb{R}^3 : \ x + y = x - z = 0\}$ jest podgrupą normalną grupy $\mathbb{R}^3$. Opisać warstwy elementów $(x, y, z) \in \mathbb{R}^3$ względem tej podgrupy, a następnie wykazać, że $\mathbb{R}^3/H \cong \mathbb{R}$.

20. Sprawdzić, że zbiór $H = \{(x, y) \in \mathbb{R}^2 : \ x = 2y\}$ jest podgrupą normalną grupy $\mathbb{R}^3$. Opisać warstwy elementów $(x, y, z) \in \mathbb{R}^3$ względem tej podgrupy, a następnie wykazać, że $\mathbb{R}^2/H \cong \mathbb{R}^2$.

21. Wykazać, że w grupie kwaternionów wszystkie podgrupy są normalne choć grupa nie jest abelowa.

22. Niech $\mathbb{R}^\infty = \{\{a_i\}_{i=1}^\infty : \ a_i \in \mathbb{R}, \ i = 1, 2, \ldots\}$, $H = \{\{a_i\}_{i=1}^\infty : \ a_1 = a_2 = 0\}$. Dowieść, że $\mathbb{R}^\infty/H \cong \mathbb{R}^\infty$.

23. Wykazać, że jeśli $f : G \longrightarrow G'$ jest homomorfizmem grup to jądro tego homomorfizmu jest normalną podgrupą G.

24. Rozstrzygnąć dla jakich $n \in \mathbb{N}_{\geqslant 2}$, podgrupa $H_n = \{\sigma \in S_n : \ \sigma(2) = 2\}$ jest normalna w S_n.

Rozdział 4

Podstawy teorii pierścieni

4.1 Podstawowe definicje i przykłady

Do tej pory strukturę algebraiczną zadawaliśmy na zbiorze za pomocą jednego działania. Teraz, podobnie jak to w sposób naturalny pojawia się w przypadkach podzbiorów liczbowych, będziemy operować dwoma działaniami zadając tym samym (przy odpowiednich własnościach działań) strukturę pierścienia. Najbardziej „intuicyjnym" przykładem jest tu ponownie znany nam zbiór liczb całkowitych, na którym mamy dwa naturalne działania: dodawania i mnożenia. Jest to „bazowy" dla nas przykład pierścienia.

Definicja 4.1.1 (pierścień)**.** Jeśli P jest zbiorem niepustym, na którym zadano dwa działania oznaczane odpowiednio $+$ oraz $\cdot$ (nazywane dodawaniem i mnożeniem) o następujących własnościach:

(1) $(P,+)$ jest grupą abelową z elementem neutralnym oznaczanym przez $0_P =: 0$,

(2) $(P,\cdot)$ jest półgrupą (łączność mnożenia),

(3) $a(b+c) = ab+ac$ oraz $(b+c)a = ba+ca$ dla dowolnych $a,b,c \in P$ (rozdzielność mnożenia względem dodawania),

to trójkę $(P,+,\cdot)$ (w skrócie, jeśli nie prowadzi to do nieporozumień: P) nazywamy wówczas **pierścieniem**. Dodatkowo, jeśli:

(4) istnieje takie $1 := 1_P \in P$, że $a \cdot 1 = a = 1 \cdot a$ dla dowolnego $a \in P$ (element neutralny mnożenia), to mówimy o pierścieniu z jedynką,

(5) $ab = ba$ dla dowolnych $a,b \in P$ (przemienność mnożenia), to mówimy o pierścieniu przemiennym.

Jeśli zachodzą warunki (1)–(5), to mówimy o **pierścieniu przemiennym z jedynką**.

Podzbiór R pierścienia $(P,+,\cdot)$ nazywamy jego **podpierścieniem**, gdy $(R,+|_{R\times R},\cdot|_{R\times R})$ jest pierścieniem. Jeśli P ma jedynkę 1_P, to dodatkowo wymagamy aby $1_P \in R$.

Własność 4.1.2 (podstawowe własności elementów pierścienia)**.** *Niech P będzie pierścieniem oraz niech a, b, $a_1,\ldots,a_n$, $b_1,\ldots,b_m \in P$. Wtedy zachodzą własności:*

(1) $a \cdot 0 = 0 = 0 \cdot a$

(2) $(-a)b = -ab = a(-b)$ *oraz* $(-a)(-b) = ab$.

(3) $(ka)b = k(ab) = a(kb)$, $k(a+b) = ka+kb$ *oraz* $k(la) = (kl)a = l(ka)$ *dla* $k,l \in \mathbb{Z}$.

(4) $\big(\sum_{i=1}^{n} a_i\big)\big(\sum_{j=1}^{m} b_j\big) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$.

Dowód. Dla przykładu udowodnimy (1) oraz część (2). Jako, że pozostałe dowody przebiegają analogicznie pozostawimy je Czytelnikowi w formie ćwiczenia.

Dla dowodu pierwszej równości z (1), zauważmy, że $a\cdot 0 = a\cdot(0+0) = (a\cdot 0)+(a\cdot 0)$ na podstawie rozdzielności mnożenia względem dodawania. Z równości $a\cdot 0 = (a\cdot 0)+(a\cdot 0)$ widzimy, że $a\cdot 0$ jest elementem neutralnym dodawania, skąd $a\cdot 0 = 0$.

Dla dowodu pierwszej z równości w (2), zauważamy, że na podstawie rozdzielności i (1) mamy związek $(-a)b + (ab) = [(-a)+a]b = 0\cdot b = 0$, czyli element $(-a)b$ jest elementem przeciwnym do ab. □

Wprost z aksjomatyki pierścienia łatwo wykazać, że w szczególnym przypadku dwóch przemiennych elementów zachodzi znany z własności liczbowych wzór, którego dowód pozostawiamy także w formie ćwiczenia. Podkreślmy tu, że ogólnie nie możemy zapisać w pierścieniu równości $(a+b)^2 = a^2 + 2ab + b^2$. Istotnie, bez założenie przemienności działania mnożenia w P, możemy tylko napisać, że $(a+b)^2 = a^2 + ab + ba + b^2$. Zanotujmy następującą

Uwaga 4.1.3 (dwumian Newtona)**.** Jeśli P jest pierścieniem oraz $a, b \in P$ są ze sobą przemienne, to dla dowolnego $n \in \mathbb{N}$ zachodzi równość $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.

Zestawimy teraz definicje wyróżnionych elementów zadanego pierścienia, z którymi będziemy mieli do czynienia w dalszej części wykładu.

Mówiąc dalej „pierścień" mamy na myśli pierścień przemienny z $1 \neq 0$.

Definicja 4.1.4 (dzielnik zera, element odwracalny)**.** Jeśli P jest pierścieniem, to element $a \in P^\star$ nazywamy **dzielnikiem zera**, gdy istnieje taki element $b \in P^\star$, że $ab = 0$. Zbiór dzielników zera pierścienia P oznaczamy $\mathrm{D}(P)$.

Element $u \in P$ nazywamy **odwracalnym (jednością)**, jeśli istnieje taki element $v \in P$, że $uv = 1$. Zbiór elementów odwracalnych pierścienia P oznaczamy przez $\mathrm{U}(P)$.

Ogólnie, w pierścieniach nieprzemiennych można wprowadzić pojęcie lewostronnych (prawostronnych) dzielników zera i elementów odwracalnych. My, z racji rozważania jedynie pierścieni przemiennych, będziemy operować nieco uproszczoną wersją dzielników zera i elementów odwracalnych.

Przykład 4.1.5.
(1) Dla pierścienia $(\mathbb{Z}, +, \cdot)$ mamy $\mathrm{D}(\mathbb{Z}) = \emptyset$ oraz $\mathrm{U}(\mathbb{Z}) = \{-1, 1\}$.

(2) Dla pierścienia $(\mathbb{Z}_6, +, \cdot)$ mamy $\mathrm{D}(\mathbb{Z}_6) = \{2, 3, 4\}$ oraz $\mathrm{U}(\mathbb{Z}_6) = \{1, 5\}$.

Definicja 4.1.6 (pierścień całkowity, ciało)**.** Mówimy, że pierścień P jest **całkowity** (jest **dziedziną**), jeśli P nie posiada dzielników zera. Inaczej, pierścień jest całkowity, gdy zachodzi w nim implikacja: $a, b \in P$, $a \cdot b = 0 \implies a = 0$ lub $b = 0$.

Pierścień, w którym każdy niezerowy element jest odwracalny nazywamy **ciałem**.

Przykład 4.1.7. Najprostszym przykładem pierścienia całkowitego jest pierścień liczb całkowitych $\mathbb{Z}$. Jest to także przykład pierścienia całkowitego, który nie jest ciałem.

Definicja 4.1.8 (homomorfizm pierścieni)**.** Jeśli P oraz R są pierścieniami, to odwzorowanie $f\colon P \to R$ nazywamy **homomorfizmem pierścieni**, gdy

$$f(x+y) = f(x) + f(y), \qquad f(xy) = f(x)f(y) \qquad \text{dla dowolnych } \ x, y \in P$$

oraz zachodzi $f(1_P) = 1_R$.[1]

Stosujemy tu analogiczną jak w teorii grup terminologię dotyczącą monomorfizmu, epimorfizmu, endomorfizmu czy izomorfizmu.

Własność 4.1.9 (element odwracalne a dzielniki zera)**.** *Niech P będzie pierścieniem z $1 \neq 0$. Wtedy zachodzą następujące własności:*

(1) Element odwracalny nie może być dzielnikiem zera, tzn. $\mathrm{U}(P) \cap \mathrm{D}(P) = \varnothing$.

(2) Każde ciało jest pierścieniem całkowitym.

(3) Zbiór $\mathrm{U}(P)$ *tworzy grupę z działaniem mnożenia.*

Dowód. Uzasadnimy pierwsze dwie własności, ostatnią zostawiamy jako ćwiczenie.

(1) Jeśli $a \in P$ byłby jednocześnie elementem odwracalnym i dzielnikiem zera, to byłby to element niezerowy dla którego istniałyby dwa elementy: $b \in P^\star$, $c \in P$ takie, że $ab = 0$ oraz $ac = 1$. Mnożąc pierwsze z równań obustronnie przez c dostalibyśmy $cab = c \cdot 0 = 0$. Korzystając z przemienności mnożenia mamy $acb = 0$, a ponieważ $ac = 1$, to dostajemy, że $b = 0$ co jest sprzeczne z założeniem.

(2) Skoro w ciele każdy element niezerowy jest odwracalny, to zgodnie z (1) żaden niezerowy element nie może być dzielnikiem zera, czyli pierścień jest całkowity. □

[1] Zauważmy, że w przypadku homomorfizmów grup własność „przenoszenia elementu neutralnego" wynikała bezpośrednio z definicji homomorfizmu: było to efektem istnienia elementu odwrotnego do dowolnego elementu w grupie, oczywiście homomorfizm pierścieni przenosi element neutralny dodawania ale nie musi przenosić elementu neutralnego mnożenia, stąd dodatkowe założenie.

4.2 Pojęcie ideału i operacje na ideałach

Wprowadzimy teraz pojęcie, które odgrywa w teorii pierścieni podobną rolę jak podgrupy normalne w teorii grup. W szczególności to właśnie za pomocą tego typu podzbiorów będziemy konstruować pierścienie ilorazowe.

Definicja 4.2.1 (ideał)**.** Podzbiór $I \subseteq P$ pierścienia P nazywamy **ideałem** w P, jeśli:

(1) $(I, +)$ jest podgrupą $(P, +)$,

(2) dla dowolnych $a \in I$, $r \in P$ zachodzi $a \cdot r \in I$ (tzw. warunek pochłaniania)

Jeśli I jest ideałem w P, to piszemy $I \lhd P$. Ideał I nazywamy **właściwym**, jeśli $I \neq P$, zaś **nietrywialnym** gdy $I \neq \{0\}$.

Podobnie jak w przypadku dzielników zera i jedności, można też mówić o ideałach lewostronnych (prawostronnych).

Analogicznie jak w przypadku grup, przecięcie dowolnej liczby ideałów jest ideałem (suma mnogościowa ideałów nie musi być ideałem, wszak nie musi być podgrupą grupy addytywnej pierścienia). Własność ta prowadzi do określenia (znów analogicznie jak w grupach) pojęcia ideału generowanego przez zbiór.

Definicja 4.2.2 (ideał generowany przez zbiór)**.** Jeśli A jest podzbiorem pierścienia P, to przecięcie wszystkich ideałów pierścienia P zawierających podzbiór A nazywamy **ideałem generowanym przez zbiór** A, innymi słowy

$$(A) := \bigcap_{I \lhd P : A \subseteq I} I.$$

W szczególności, jeśli $A = \{a_1, \ldots, a_n\}$, to piszemy $(A) = (a_1, \ldots, a_n)$.

Definicja 4.2.3 (pierścień (dziedzina) ideałów głównych)**.** Jeśli P jest pierścieniem, to mówimy, że ideał $I \lhd P$ jest **główny**, jeśli istnieje taki element $a \in P$, że $I = (a)$. Mówimy, że P jest **pierścieniem ideałów głównych**, jeśli każdy ideał w P jest główny. **Dziedziną ideałów głównych** nazywamy pierścień ideałów głównych, który dodatkowo jest całkowity.

Przykład 4.2.4. Pierścień $\mathbb{Z}$ jest dziedziną ideałów głównych. Z jednej strony wiemy, że jest on całkowity, a z drugiej strony wiemy, że wszystkie podgrupy są postaci $n\mathbb{Z}$, które to zbiory tworzą ideały generowane przez odpowiednie $n \in \mathbb{N}$ (por. własność poniżej), czyli są ideałami głównymi.

Własność 4.2.5 (własności ideałów)**.** *Niech P będzie pierścieniem, $a_1, \ldots, a_n \in P$ oraz $I \lhd P$. Wtedy zachodzą następujące własności:*

(1) $(a_1, \ldots, a_n) = Pa_1 + \ldots + Pa_n = \{r_1a_1 + \ldots + r_na_n,\ r_i \in P\}$,

(2) jeśli $I \cap \mathrm{U}(P) \neq \varnothing$, *to wtedy* $I = P$,

(3) P jest ciałem wtedy i tylko wtedy, gdy jedynymi ideałami w P są (0) oraz P.

Dowód.
(1) Niech $J = Pa_1 + \ldots + Pa_n$. Najpierw wykażemy, że J jest ideałem co będzie oznaczało, że $(a_1, \ldots, a_n) \subseteq J$. Fakt, że $(J, +)$ jest podgrupą $(P, +)$ jest natychmiastowy. Istotnie, jeśli $b, c \in J$, to

$$b = b_1a_1 + \cdots + b_na_n, \qquad c = c_1a_1 + \ldots + c_na_n$$

dla pewnych $b_i, c_i \in P$ $(1 \leqslant i \leqslant n)$. Stąd wniosek, że

$$b - c = (b_1 - c_1)a_1 + \ldots + (b_n - c_n)a_n \in J.$$

Podobnie, gdy $a \in P$, to

$$ab = (ab_1)a_1 + \ldots + (ab_n)a_n \in J.$$

Zawieranie w drugą stronę wynika z definicji ideału. Skoro $a_1, \ldots, a_n \in (a_1, \ldots, a_n)$, to każda ich kombinacja z J też musi należeć do $(a_1, \ldots, a_n)$.

(2) Gdy $u \in I \cap \mathrm{U}(P)$ oraz $v \in P$ spełnia $uv = 1$, to dla $a \in P$ jest $a = auv \in I$, mamy więc $P \subset I$, skąd równość.

(3) Załóżmy najpierw, że P jest ciałem i wybierzmy niezerowy ideał I w P. Skoro I jest niezerowy, to $I \cap \mathrm{U}(P) \neq \varnothing$, czyli z (2) mamy $I = P$, co kończy dowód tej implikacji.

Załóżmy teraz, że w P nie ma innych ideałów poza trywialnym i całym P i rozważmy element niezerowy $a \in P$. Wobec $(a) \neq (0)$ mamy $(a) = P$, czyli istnieje takie $b \in P$, że $ab = 1$, a zatem jest to element odwracalny. Kończy to dowód faktu, że P jest ciałem. □

Zauważmy, że podpierścień właściwy nie musi być ideałem, na przykład $\mathbb{Z}$ jest podpierścieniem $\mathbb{Q}$, nie jest to jednak ideał, gdyż $\mathbb{Q}$ jako ciało nie zawiera nietrywialnych ideałów właściwych.

Twierdzenie 4.2.6 (działania na ideałach)**.** *Niech I, J będą ideałami w pierścieniu P. Wtedy zachodzą własności:*

(1) Zbiory

$$I + J = \{a + b : a \in I,\, b \in J\},$$

$$IJ = \Big\{ \sum_{i=1}^{n} a_i b_i : a_1, \ldots, a_n \in I,\, b_1, \ldots, b_n \in J,\, n \in \mathbb{N} \Big\}$$

są ideałami w P,

(2) $IJ \subseteq I \cap J \subseteq I + J$,

(3) jeśli $\mathcal{I}$ jest łańcuchem ideałów w pierścieniu P (w sensie inkluzji), to wtedy $I = \bigcup \mathcal{I}$ jest ideałem w P.

Dowód. Własność (1) pozostawiamy do przeliczenia wprost z definicji. Dla uzasadnienia własności (2) wystarczy zauważyć, że $IJ \subseteq I \subseteq I + J$ oraz $IJ \subseteq J \subseteq I + J$, zatem $IJ \subseteq I \cap J \subseteq I + J$.

Wreszcie, dla dowodu (3), zauważmy, że jeśli $a, b \in I$ oraz $c \in P$, to istnieją takie $I_1, I_2 \in \mathcal{I}$, że $a \in I_1$ oraz $b \in I_2$. Niech na przykład $I_1 \subseteq I_2$. Wtedy $a - b \in I_2 \subseteq I$ oraz $ac \in I_1 \subseteq I$, co kończy dowód. □

4.2.1 Pierścień ilorazowy

Jeśli I jest ideałem pierścienia P, to wówczas $(I, +)$ jest podgrupą grupy abelowej $(P, +)$, czyli podgrupą normalną. Możemy wobec tego rozważać grupę ilorazową $(P/I, +)$ z działaniem: $(a + I) + (b + I) = (a + b) + I$. Przypomnijmy, że w notacji addytywnej elementy P/I mają postać $a + I$, gdzie $a \in P$ oraz

$$a + I = b + I \iff a - b \in I, \qquad a + I = I = 0_{P/I} \iff a \in I.$$

Możemy jednak na tym zbiorze wprowadzić też mnożenie: $(a + I) \cdot (b + I) := (ab) + I$, gdzie mnożenie ab to działanie mnożenia w P. By to działanie miało sens, musimy sprawdzić, że nie zależy ono od wyboru reprezentantów.

Własność 4.2.7 (poprawność definicji pierścienia ilorazowego)**.** *Niech I będzie ideałem pierścienia P. Wtedy zachodzą własności:*

(1) działania wprowadzone wyżej na P/I są poprawnie określone,

(2) zbiór P/I z działaniami $(a+I)+(b+I) = (a+b)+I$ oraz $(a+I)(b+I) = ab+I$ dla $a, b \in P$ tworzy strukturę pierścienia,

(3) odwzorowanie $\pi\colon P \ni a \mapsto a + I \in P/I$ jest epimorfizmem pierścieni.

Dowód. Dla dowodu (1) niech $a, b, a', b' \in P$ spełniają $a + I = a' + I$ oraz $b + I = b' + I$, to $a - a' \in I$ oraz $b - b' \in I$. Wtedy $ab - a'b' = a(b - b') + (a - a')b' \in I$ co oznacza, że $ab + I = a'b' + I$ czyli $(a + I)(b + I) = (a' + I)(b' + I)$, więc istotnie jest to poprawnie określone działanie. Pozostałe dwa punkty wynikają wprost z własności działań w P, określenia działań w P/I i definicji odwzorowania π. □

Definicja 4.2.8 (pierścień ilorazowy)**.** Jeśli I jest ideałem w pierścieniu P, to zbiór P/I z działaniami

$$(a + I) + (b + I) := (a + b) + I, \qquad (a + I)(b + I) := ab + I, \qquad a, b \in P$$

nazywamy **pierścieniem ilorazowym** pierścienia P względem ideału I.

4.2.2 Twierdzenie chińskie o resztach dla ideałów

Na koniec podstawowych rozważań o ideałach sformułujemy nieco zaskakującą własność, która jak zobaczymy stanowi uogólnienie twierdzenia chińskiego o resztach jakie poznaliśmy w ramach podstaw teorii liczb (por. 1.4.8). Zaczniemy od krótkiego lematu.

Lemat 4.2.9. *Niech P będzie pierścieniem, I, $I_1, \ldots, I_n$ ideałami w P takimi, że $I + I_i = P$ dla $i = 1, \ldots, n$. Wtedy $I + I_1 \cdot \ldots \cdot I_n = I + I_1 \cap \ldots \cap I_n = P$.*

Dowód. Wiemy, że $I_1 \cdot \ldots \cdot I_n \subset I_1 \cap \ldots \cap I_n$, więc wystarczy wykazać, że $I + I_1 \cdot \ldots \cdot I_n = P$. Dowód przeprowadzimy indukcyjnie względem n — liczby ideałów. Dla $n = 1$ teza wynika wprost z założenia. Dla $n = 2$ istnieją elementy $a_i \in I$ oraz $b_i \in I_i$ takie, że $a_1 + b_i = 1$ dla $i = 1, 2$. Mamy więc:

$$1 = (a_1 + b_1)(a_2 + b_2) = (a_1a_2 + a_1b_2 + b_1a_2) + b_1b_2 \in I + I_1I_2$$

zatem $I + I_1I_2 = P$.

Dla $n > 2$ zakładamy prawdziwość tezy dla $(n-1)$ ideałów. Z założenia indukcyjnego mamy więc $I + I_1 \cdot \ldots \cdot I_{n-1} = P$ oraz $I + I_n = P$. Stąd zaś wykorzystując tezę dla $n = 2$ mamy $I + I_1 \cdot (I_2 \cdot \ldots \cdot I_{n-1}) = P$. □

Dla sformułowania poniższego twierdzenia, przyjmujemy notację $a \equiv b \pmod{I}$ wtedy i tylko wtedy, gdy $b - a \in I$, czyli $a + I = b + I$.

Twierdzenie 4.2.10 (twierdzenie chińskie o resztach dla ideałów)**.** *Niech P – pierścień, $I_1, \ldots, I_n$ – ideały w P takie, że $I_i + I_j = P$ dla $i \neq j$ oraz $a_1, \ldots, a_n \in P$. Wtedy istnieje takie element $a \in P$, że*

$$a \equiv a_i \pmod{I_i} \qquad \forall\ i = 1, \ldots, n \tag{$\star$}$$

oraz jeśli dodatkowo element b także spełnia warunek $(\star)$, to $a \equiv b \pmod{I_1 \cap \ldots \cap I_n}$.

Dowód. Zauważmy, że druga część tezy jest natychmiastowa, bo jeśli $a \equiv a_i \pmod{I}$ oraz $b \equiv a_i \pmod{I}$, to $a \equiv b \pmod{I}$ dla $i = 1, \ldots, n$. Stąd $a \equiv b \pmod{I_1 \cap \ldots \cap I_n}$.

Dla dowodu części pierwszej najpierw zastosujemy lemat by uzyskać, że:

$$I_i + \bigcap_{j \neq i} I_j = P, \qquad i = 1, \ldots, n.$$

Oznacza to, że istnieją $b_i \in I_i$ oraz $c_i \in \bigcap_{j \neq i} I_j$ takie, że $a_i = b_i + c_i$, dla $i = 1, \ldots, n$. Niech $a := c_1 + \ldots + c_n$. Wtedy:

$$a - a_i = c_i - a_i + \sum_{j \neq i} c_j = -b_i + \sum_{j \neq i} c_j \in I_i, \qquad i = 1, \ldots, n,$$

czyli $a \equiv a_i \pmod{I_i}$ dla $i = 1, \ldots, n$. □

Biorąc $P := \mathbb{Z}$, $I_i = (m_i)$, gdzie liczby $m_1, \ldots, m_r$ są parami względnie pierwsze dostajemy klasyczne twierdzenie chińskie z teorii liczb.

4.3 Twierdzenia o homomorfizmach pierścieni

W tym rozdziale sformułujemy dwa podstawowe twierdzenia teorii pierścieni, które są bezpośrednimi odpowiednikami udowodnionych w 3.5 dla grup. Zaczniemy od prostej obserwacji.

Obserwacja 4.3.1. *Niech $f : P \to R$ będzie homomorfizmem pierścieni. Wtedy:*

(1) $\operatorname{Ker} f$ *jest ideałem w P,*

(2) $\operatorname{Im} f$ *jest podpierścieniem w R.*[2]

[2] $\operatorname{Im} f$ może nie być ideałem w R.

Twierdzenie 4.3.2 (twierdzenie o przenoszeniu ideałów przez homomorfizm)**.** *Niech P, R – pierścienie, $f : P \to R$ – epimorfizm pierścieni. Wtedy odwzorowanie*

$$\Phi : \{I : I \text{ ideał w } P,\ \operatorname{Ker} f \subset I\} \ni I \longmapsto f(I) \in \{J : J \text{ ideał w } R\}$$

jest bijekcją.

Dowód. Podobnie jak w dowodzie twierdzenia o przenoszeniu podgrup (por. 3.5.1) zauważamy, że odwzorowanie odwrotne do Φ to $\widetilde{\Phi}(J) = f^{-1}(J)$. Wystarczy jedynie sprawdzić, że przeciwobraz ideału jest ideałem, co jest prostym ćwiczeniem. □

Twierdzenie 4.3.3 (twierdzenie o izomorfizmie dla pierścieni)**.** *Niech $f\colon P \to R$ będzie homomorfizmem pierścieni. Wtedy $P/\operatorname{Ker} f \cong \operatorname{Im} f$, czyli pierścienie te są izomorficzne.*

Dowód. Ponieważ $(P, +)$ jest grupą, zaś jądro jej podgrupą normalną, więc wiemy z teorii grup iż odwzorowanie: $F : P/\operatorname{Ker} f \ni a + \operatorname{Ker} f \mapsto f(a) \in \operatorname{Im} f$ zadaje izomorfizm grup (por. 3.5.2). Wystarczy sprawdzić, że jest to też homomorfizm pierścieni. Mamy następujący ciąg równości

$$F((a + \operatorname{Ker} f) \cdot (b + \operatorname{Ker} f)) = F(ab + \operatorname{Ker} f) = f(ab) = f(a)f(b) = F(a + \operatorname{Ker} f)F(b + \operatorname{Ker} f),$$

co kończy dowód, jeśli tylko zauważymy, że $F(1_{P/\operatorname{Ker} f}) = F(1_P + \operatorname{Ker} f) = f(1_P) = 1_R$. □

4.4 Szczególne rodzaje ideałów

4.4.1 Ideały pierwsze

Definicja 4.4.1 (ideał pierwszy)**.** Jeśli P jest pierścieniem, to ideał $I \neq P$ nazywamy **ideałem pierwszym**, gdy dla dowolnych takich $a, b \in P$, że $ab \in I$ wynika, że $a \in I$ lub $b \in I$.

Łatwo, wprost z definicji wykazać, że ideały pierwsze w pierścieniu $\mathbb{Z}$, to ideały generowane przez liczby pierwsze oraz ideał zerowy.

Własność 4.4.2 (charakteryzacja pierwszości w języku ilorazowego)**.** *Jeśli P jest pierścieniem, zaś I – ideał w P, $I \neq P$, to I jest pierwszy wtedy i tylko wtedy, gdy pierścień P/I jest całkowity.*

Dowód. Załóżmy najpierw, że I jest ideałem pierwszym i weźmy takie elementy $a+I$, $b+I$ z pierścienia ilorazowego, że $(a + I)(b + I) = 0_{P/I}$. Wtedy $ab + I = 0_{P/I}$ co oznacza, że $ab \in I$. Z pierwszości ideału mamy więc, że $a \in I$ lub $b \in I$, skąd $a + I = 0$ lub $b + I = 0$ i mamy całkowitość pierścienia P/I.

Odwrotnie, załóżmy że P/I całkowity i weźmy a, $b \in P$ takie, że $ab \in I$. Wtedy $(a + I)(b + I) = ab + I = 0_{P/I}$ skąd z całkowitości P/I mamy $a + I = 0$ lub $b + I = 0$ czyli $a \in I$ lub $b \in I$, czyli I jest ideałem pierwszym. □

4.4.2 Ideały maksymalne

Definicja 4.4.3 (ideał maksymalny)**.** Jeśli P jest pierścieniem, to ideał $\mathfrak{m} \neq P$ nazywamy **ideałem maksymalnym**, gdy dla dowolnego ideału $I \lhd P$ z zawierania $\mathfrak{m} \subseteq I$, wynika, że $I = \mathfrak{m}$ lub $I = P$.

Przykładowo ideał (n) w $\mathbb{Z}$ jest maksymalny wtedy i tylko wtedy, gdy $|n|$ jest liczbą pierwszą, ale w przeciwieństwie do własności pierwszości ideał zerowy nie jest ideałem maksymalnym w $\mathbb{Z}$.

Własność 4.4.4 (charakteryzacja maksymalności w języku pierścienia ilorazowego)**.** *Jeśli P jest pierścieniem, zaś $\mathfrak{m}$ jest ideałem właściwym w P, to ideał $\mathfrak{m}$ jest maksymalny wtedy i tylko wtedy, gdy $P/\mathfrak{m}$ jest ciałem.*

Dowód. Przypomnijmy, że rzutowanie kanoniczne $\pi\colon P \to P/\mathfrak{m}$ jest epimorfizmem pierścieni i wiemy, że każdy ideał $\overline{J}$ w pierścieniu $P/\mathfrak{m}$ jest obrazem przez to rzutowanie pewnego takiego ideału J w P, że $\mathfrak{m} \subseteq J$ (por. 4.3.2). Jeśli więc $\mathfrak{m}$ jest ideałem maksymalnym, to jedynymi takimi ideałami I, że $\mathfrak{m} \subseteq I$ są $\mathfrak{m}$ oraz cały pierścień P. Ich obrazy przez odwzorowanie π to jedyne ideały w $P/\mathfrak{m}$. Oczywiście $\pi(P) = P/\mathfrak{m}$, zaś $\pi(\mathfrak{m}) = \mathfrak{m}/\mathfrak{m} = \{a+\mathfrak{m},\ a \in \mathfrak{m}\} = 0_{P/\mathfrak{m}}$. Wobec tego $P/\mathfrak{m}$ jest ciałem na podstawie własności 4.2.5.

Jeśli teraz $P/\mathfrak{m}$ jest ciałem, to $P/\mathfrak{m}$ nie posiada nietrywialnych ideałów właściwych. Weźmy taki ideał I pierścienia P, że $\mathfrak{m} \subseteq I$. Wtedy $\pi(I) = I/\mathfrak{m} = \{a + \mathfrak{m},\ a \in I\}$ jest ideałem w $P/\mathfrak{m}$, zatem $I/\mathfrak{m} = (0)$ lub $I/\mathfrak{m} = P/\mathfrak{m}$. W pierwszym przypadku widzimy, że jeśli $a \in I$, to $a + \mathfrak{m} = 0 + \mathfrak{m}$, czyli $a \in \mathfrak{m}$, co oznacza, że $I = \mathfrak{m}$. W drugim przypadku, w szczególności $1 + \mathfrak{m} \in I/\mathfrak{m}$, czyli istnieje takie $a \in I$, że $1 + \mathfrak{m} = a + \mathfrak{m}$. Stąd $1 - a = s$ dla pewnego $s \in \mathfrak{m}$. Mamy jednak $\mathfrak{m} \subset I$, więc $1 - a \in I$, skąd $1 \in I$, a tym samym $I = P$. □

Własność 4.4.5 (własności ideału maksymalnego)**.** *Niech P będzie pierścieniem. Wtedy zachodzą własności:*

(1) każdy ideał właściwy w P zawiera się w pewnym ideale maksymalnym,

(2) każdy ideał maksymalny w P jest ideałem pierwszym.

Dowód.
(1) Ustalmy ideał $I \neq P$ i rozważmy rodzinę $\{J \lhd P : I \subseteq J \neq P\}$. Jest ona niepusta i uporządkowana częściowo przez inkluzję. Ponadto dowolny łańcuch $\mathcal{I}$ w tej rodzinie posiada w niej majorantę $S = \bigcup \mathcal{I}$ (por. 4.2.6(3)). Zauważmy, że ta suma nie może być całym pierścieniem bo należała by do niej jedynka, co by oznaczało, że 1 należałaby do któregoś z ideałów z łańcucha. Wtedy jednak taki ideał musi być całym pierścieniem. Dzięki lematowi Kuratowskiego-Zorna istnieje w tej rodzinie element maksymalny i ideał ten spełnia tezę.

(2) Jeśli ideał $\mathfrak{m}$ jest maksymalny, to $P/\mathfrak{m}$ jest ciałem, w szczególności $P/\mathfrak{m}$ jest pierścieniem całkowitym i własność 4.4.2 kończy dowód. □

Przykład 4.4.6.
(1) W pierścieniu $\mathbb{Z}$ ideały pierwsze to (0) oraz (p), gdzie p jest liczbą pierwszą. Ideały maksymalne są zaś postaci (p) dla liczby pierwszej p.

(2) W pierścieniu wielomianów $\mathbb{Z}[x]$[3] ideał (x) jest ideałem pierwszym, nie jest to jednak ideał maksymalny (bo $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ jest pierścieniem całkowitym lecz nie ciałem).

4.5 Pierścień wielomianów

4.5.1 Wielomiany jednej zmiennej

Niech P będzie ustalonym pierścieniem. Określmy zbiór

$$R := \{(a_0, a_1, \ldots) \in P^{\mathbb{N}_0} : \ \exists\, i_0 \in \mathbb{N}_0 : \ \forall\, i \geqslant i_0 : \ a_i = 0\}.$$

Na zbiorze R wprowadzamy następujące działania:

$$(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots)$$
$$(a_0, a_1, \ldots)(b_0, b_1, \ldots) = (c_0, c_1, \ldots), \quad \text{gdzie} \quad c_k = \sum_{i+j=k} a_i b_j, \quad \text{dla} \quad k \in \mathbb{N}_0.$$

Bezpośrednie przeliczenie prowadzi do następującej własności.

Własność 4.5.1. *(1) Działania określone powyżej wprowadzają na R strukturę pierścienia.*

(2) Odwzorowanie $i : P \ni a \mapsto (a, 0, 0, \ldots) \in R$ jest injektywnym homomorfizmem pierścieni.

Definicja 4.5.2 (zmienna nad pierścieniem)**.** Element $(0_P, 1_P, 0_P, 0_P \ldots)$ wprowadzonego powyżej pierścienia R oznaczamy przez X i nazywamy **zmienną** nad pierścieniem P.

Definicja 4.5.3 (pierścień wielomianów)**.** Pierścień R z określonymi powyżej działaniami nazywamy **pierścieniem wielomianów** nad pierścieniem P jednej zmiennej X i oznaczamy $P[X]$.

Elementy tego pierścienia nazywamy **wielomianami jednej zmiennej** nad pierścieniem P.

Definicja 4.5.4 (stopień wielomianu)**.** Dla dowolnego elementu $f = (a_0, a_1, \ldots) \in P[X] \setminus \{0\}$ określamy

$$\deg(f) := \max\{n \in \mathbb{N}_0 : \ a_n \neq 0\}.$$

Liczbę tę nazywamy **stopniem** wielomianu f. Dla wielomianu zerowego przyjmujemy stopień równy $-\infty$.

Zauważmy, że dzięki 4.5.1 wyjściowy pierścień P można traktować jako podpierścień pierścienia $P[X]$. Zgodnie z określeniem mnożenia w pierścieniu $P[X]$ i określeniem zmiennej X, mamy następującą własność.

[3] Z formalną definicją pierścienia wielomianów zapoznamy się niebawem.

Własność 4.5.5 (przedstawienie wielomianu)**.** *Dowolny niezerowy wielomian $f \in P[X]$ posiada jednoznaczne przedstawienie w postaci:*

$$f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0, \qquad (\star)$$

gdzie $a_i \in P$ oraz $a_n \neq 0$ dla $n = \deg(f)$.

Definicja 4.5.6 (współczynniki wielomianu)**.** Elementy a_i z powyższego przedstawienia wielomianu nazywamy **współczynnikami wielomianu** f,

element a_0 nazywamy współczynnikiem wolnym f,

element a_n, gdzie $n = \deg(f)$, nazywamy współczynnikiem wiodącym f.

Wielomian którego współczynnik wiodący jest równy 1 nazywamy wielomianem **unitarnym** lub inaczej **monicznym**.

Następna własność powie nam co dzieje się ze stopniem wielomianów, gdy wykonujemy na nich podstawowe operacje.

Własność 4.5.7 (własności stopnia)**.** *Niech P – pierścień, $f, g \in P[X]$. Wtedy*

(1) $\deg(f+g) \leqslant \max\{\deg(f), \deg(g)\}$,

(2) $\deg(f \cdot g) \leqslant \deg(f) + \deg(g)$.[4]

Jeśli dodatkowo oba wielomiany są niezerowe i współczynnik wiodący któregoś z wielomianów nie jest dzielnikiem zera w pierścieniu P, to zachodzi wzór:

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

Dowód. Niech $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, $g = b_m X^m + a_{m-1}X^{m-1} + \ldots + b_1 X + b_0$, gdzie $n = \deg(f)$ i $m = \deg(g)$. Oznacza to, że $a_n \neq 0$ i $b_m \neq 0$.

Nierówność dla sumy wynika wprost z definicji i widać od razu, że nie można jej zastąpić równością. By nierówność była ostra, wystarczy wziąć dowolny niezerowy wielomian f i położyć $g = -f$.

Również w przypadku iloczynu widać na podstawie jego definicji, że najwyższym współczynnikiem wiodącym jaki możemy uzyskać jest współczynnik indeksowany przez $n+m$. Współczynnik z tym wskaźnikiem jest równy $a_n b_m$. Jeśli więc któryś z tych współczynników nie jest dzielnikiem zera, to wobec niezerowości obu też $a_n b_m \neq 0$ i wówczas $\deg(f \cdot g) = \deg(f) + \deg(g)$. □

Wniosek 4.5.8 (stopień w pierścieniu całkowitym)**.** *Jeśli P jest pierścieniem całkowitym, $f, g \in P[X]$. to* $\deg(f \cdot g) = \deg(f) + \deg(g)$.

Przykład 4.5.9. Niech $P = \mathbb{Z}_6$ oraz $f(X) = 2X + 1 \in \mathbb{Z}_6[X]$ i $g(X) = 3X \in \mathbb{Z}_6[X]$. Wtedy $\deg(f) = 1 = \deg(g)$, ale $(fg)(X) = 3X$ i wobec tego $\deg(fg) = 1 < 2 = \deg(f) + \deg(g)$.

Własność 4.5.10. *Jeśli P jest pierścieniem całkowitym, to także pierścień $P[X]$ jest pierścieniem całkowitym.*

Dowód. Niech $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, $g(X) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_1 x + b_0$ będą wielomianami niezerowymi z $P[X]$ takimi, że $fg = 0$. Przyjmujemy, że $\deg(f) = n$ i $\deg(g) = m$.

Skoro $fg = 0$, to również $a_n b_m = 0$. Jednakże, pierścień P jest całkowity, wobec tego oznacza to, że $a_n = 0$ lub $b_m = 0$, czyli $\deg(f) < n$ lub $\deg(g) < m$, co prowadzi do sprzeczności. □

Twierdzenie 4.5.11 (algorytm dzielenia z resztą dla wielomianów)**.** *Jeśli P jest pierścieniem, $f \in P[X]$ oraz $g \in P[X]$ jest wielomianem o odwracalnym współczynniku wiodącym, to istnieje dokładnie jedna para $q, r \in P[X]$ dla której $f = qg + r$ oraz $\deg r < \deg g$.*

Dowód. Niech $f = \sum_{i=0}^{n} a_i X^i$ oraz $g = \sum_{j=0}^{m} b_j X^j$, gdzie b_m jest odwracalny. Jednoznaczność jest natychmiastowa, gdyż jeśli $f = qg + r = q'g + r'$, gdzie $\deg r < \deg g$ oraz $\deg r' < \deg g$, to

$$\deg g + \deg(q - q') = \deg(g(q - q')) = \deg(r - r') < \deg g. \ (^5)$$

Stąd $\deg(q - q') < 0$, czyli $q = q'$ i w konsekwencji $r = r'$.

[4] Przyjmujemy konwencję: $-\infty + n = -\infty$ oraz $-\infty + (-\infty) = -\infty$.

[5] Tu wykorzystujemy fakt, że b_m nie jest dzielnikiem zera.

Udowodnimy teraz istnienie odpowiedniej pary.

Rozważmy najpierw, nieco trywialny, przypadek gdy $n < m$. Wówczas wystarczy przyjąć $q = 0$ oraz $r = f$. Wtedy $g = 0 \cdot g + f$ oraz $\deg r = n < m = \deg g$, więc teza jest spełniona.

Gdy zaś $n \geqslant m$, to dowód przeprowadzimy indukcyjnie względem n.

Jeśli $n = 0$, to również $m = 0$ i wystarczy przyjąć $q = a_0 b_0^{-1}$ oraz $r = 0$. Jeśli zaś $n > 0$, to zauważmy, że wielomian $f - a_n b_m^{-1} X^{n-m} g$ jest stopnia $< n$. Z założenia indukcyjnego istnieją takie wielomiany $q_1, r_1 \in P[X]$, że $f - a_n b_m^{-1} X^{n-m} = q_1 g + r_1$ oraz $\deg r_1 < \deg g$. Wystarczy teraz przyjąć $q = q_1 + a_n b_m^{-1} X^{n-m}$ oraz $r = r_1$, by otrzymać odpowiednie przedstawienie dla f. Zauważmy, że dzięki założeniu $n \geqslant m$, mamy, że $n - m \in \mathbb{N}_0$, więc mamy istotnie do czynienia z wielomianem. □

Dzielenie z resztą w pierścieniu wielomianów nie zawsze jest wykonalne. Na przykład w pierścieniu $\mathbb{Z}[X]$ nie da się podzielić z resztą X przez $2X$.

Uwaga 4.5.12. Jeśli K jest ciałem, to w $K[X]$ zawsze możemy wykonać algorytm dzielenia z resztą o ile oczywiście dzielimy przez wielomian niezerowy.

4.6 Pierścienie euklidesowe

Definicja 4.6.1 (pierścień (dziedzina) Euklidesa)**.** Jeśli P jest pierścieniem, zaś $\varphi\colon P^\star \to \mathbb{N}$ taką funkcją, że dla każdych $a \in P$ i $b \in P^\star$ istnieją takie $q, r \in P$, że:

(1) $a = bq + r$,

(2) jeśli $r \neq 0$, to $\varphi(r) < \varphi(b)$,

to wówczas parę (P, φ) nazywamy **pierścieniem Euklidesa** lub **euklidesowym**. Jeśli P jest dodatkowo pierścieniem całkowitym, to mówimy, że (P, φ) jest **dziedziną Euklidesa**. Funkcja φ nazywana jest czasem „algorytmem Euklidesa" w pierścieniu P.

Warto zaznaczyć, że nasza definicja nakłada niewiele założeń na funkcję φ. Często w definicji pierścienia euklidesowego pojawiają się dodatkowe założenia o funkcji φ (na przykład jej multiplikatywność). Okazuje się, że w zależności od tego jakie dodatkowe własności narzucamy na funkcję φ, możemy otrzymywać różne charakteryzacje pierścieni euklidesowych.

Przykład 4.6.2.
(1) Jeśli przyjmiemy $\varphi(k) = |k|$ dla $k \in \mathbb{Z}$, to $(\mathbb{Z}, \varphi)$ będzie dziedziną Euklidesa. W tym przypadku, dla dowolnej pary liczb całkowitych, otrzymujemy dokładnie dwie reszty spełniające warunki z definicji (o ile jedna liczba nie dzieli drugiej). Pierścienie takie nazywane są pierścieniami z podwójną resztą. Jak się okazuje jedynym (z dokładnością do izomorfizmu) pierścieniem euklidesowym z podwójną resztą jest wspomniany pierścień $(\mathbb{Z}, |\ |)$.

(2) Każde ciało K jest dziedziną Euklidesa z funkcją φ określoną wzorem

$$\varphi(a) = 1.$$

(3) Pierścień liczb całkowitych Gaussa $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ jest dziedziną Euklidesa z funkcją φ określoną wzorem

$$\varphi(a + bi) = a^2 + b^2, \qquad a + bi \in \mathbb{Z}[i].$$

(4) Niech K będzie ciałem, wtedy pierścień $K[X]$ z funkcją $\varphi(f) := \deg(f)$ jest dziedziną Euklidesa. Okazuje się, że pierścień euklidesowy (P, φ) z jednoznaczną resztą (o ile nie jest ciałem) jest izomorficzny właśnie z pierścieniem $K[X]$, gdzie $K = \mathrm{U}(P) \cup \{0\}$.

Udowodnimy teraz jedną ważną własność pierścieni Euklidesa, dotyczącą ideałów w takich pierścieniach.

Twierdzenie 4.6.3 (ideały w pierścieniu euklidesowym)**.** *Każdy pierścień Euklidesa jest pierścieniem ideałów głównych.*

Dowód. Jeżeli (P, φ) jest pierścieniem Euklidesa, zaś I jest ideałem niezerowym w P, to zbiór $\varphi(I \setminus \{0\})$ jest niepusty, czyli posiada element najmniejszy. Niech więc $b \in I \setminus \{0\}$ będzie takie, że

$$\varphi(b) = \min\{\varphi(a) : a \in I \setminus \{0\}\}.$$

Weźmy teraz $a \in I$. Istnieją wtedy takie $q, r \in P$, że

$$a = bq + r, \qquad \varphi(r) < \varphi(b).$$

Ponadto $r = a - bq \in I$. Gdyby r było elementem niezerowym, to byłby to element należący do $I \setminus \{0\}$ o wartości $\varphi(r) < \varphi(b)$. Z założenia $\varphi(b)$ jest wartością minimalną spośród obrazów elementów z $I \setminus \{0\}$ – sprzeczność z założeniem. Musi więc być $r = 0$ i stąd $a = bq \in (b)$, co oznacza, że $I = (b)$. □

4.7 Specjalne elementy w pierścieniach

Można śmiało powiedzieć, że ten rozdział stanowi uogólnienie własności jakie poznaliśmy w podstawach teorii liczb dla operacji na liczbach całkowitych. Przeniesiemy pojęcia takie jak największy wspólny dzielnik, najmniejsza wspólna wielokrotność, jednoznaczność rozkładu na elementy nierozkładalne (odpowiedniki liczb pierwszych) w pierścieniach. Pamiętajmy, że w przeciwieństwie do sytuacji w $\mathbb{Z}$ do której jesteśmy przyzwyczajeni, w strukturze pierścienia nie mamy naturalnego porządku, trudno więc mówić o elementach „największych", czy też „najmniejszych" – te pojęcia zostaną zastąpione odpowiednimi własnościami podzielności.

Definicja 4.7.1 (relacja podzielności i stowarzyszenia)**.** Jeśli P jest pierścieniem oraz $a, b \in P$, to mówimy, że **element** b **dzieli** a w P, jeśli istnieje taki element $c \in P$, że $a = bc$. Piszemy wtedy $b \mid a$. Elementy $a, b \in P^\star$ nazywamy **stowarzyszonymi**, jeśli $a \mid b$ oraz $b \mid a$. Piszemy wtedy $a \sim b$.

Wprost z definicji otrzymamy zestaw niżej wymienionych własności.

Uwaga 4.7.2 (podstawowe własności stowarzyszenia)**.** Niech P będzie pierścieniem. Wtedy zachodzą następujące własności:

(1) relacja stowarzyszenia w $P^\star$ jest zwrotna, symetryczna i przechodnia,

(2) $\forall\, a \in P^\star :\ a \sim 1 \iff a \in \mathrm{U}(P)$,

(3) w pierścieniu całkowitym mamy dla $a,\, b \neq 0$: $a \sim b \iff b = au$ dla pewnego $u \in \mathrm{U}(P)$.

Z banalnych przykładów przytoczmy dwa: liczby -2 i 2 są stowarzyszone w $\mathbb{Z}$, zaś wielomiany $2x + 2$ i $x + 1$ w $\mathbb{Q}[x]$.

4.7.1 Elementy nierozkładalne

Definicja 4.7.3 (element nierozkładalny/rozkładalny)**.** Jeśli P jest pierścieniem, to element $a \in P^\star \setminus \mathrm{U}(P)$ nazywamy **nierozkładalnym**, gdy dla dowolnych $b, c \in P$ z faktu $a = bc$ wynika $b \in \mathrm{U}(P)$ lub $c \in \mathrm{U}(P)$.

Element $a \in P^\star \setminus \mathrm{U}(P)$ nazywamy **rozkładalnym**, jeśli istnieją takie elementy nieodwracalne b, c, że $a = bc$.

Przykład 4.7.4.
(1) W pierścieniu $\mathbb{Z}$ każda liczba pierwsza p (podobnie $-p$) jest elementem nierozkładalnym. Są to jedyne elementy nierozkładalne w tym pierścieniu.

(2) W pierścieniu wielomianów jednej zmiennej $K[X]$ każdy wielomian postaci $X - a$ jest nierozkładalnym elementem tego pierścienia.

Uwaga 4.7.5. Jeśli w pierścieniu P element $a \in P$ jest nierozkładalny, zaś $u \in P$ jest odwracalny, to element au też jest elementem nierozkładalnym pierścienia P.

Dowód. Element au jest niezerowy gdyż inaczej mnożąc przez u^{-1} dostaniemy $a = 0$. Jest to też element nieodwracalny, w przeciwnym wypadku a byłby odwracalny. Niech teraz $au = bc$, wtedy $a = (bu^{-1})c$. Z nierozkładalności elementu a wynika, że bu^{-1} lub c jest odwracalny. Jeśli więc c nie jest odwracalny, to musi istnieć takie $d \in P$, że $bu^{-1}d = 1$, czyli b jest elementem odwracalnym. □

Własność 4.7.6 (pierwszość ideału a nierozkładalność generatora)**.** *Niech P będzie pierścieniem całkowitym oraz niech $a \in P^\star$. Jeśli ideał (a) jest pierwszy, to element a jest nierozkładalny.*

Dowód. Skoro ideał (a) jest pierwszy, to element a jest nieodwracalny (inaczej (a) byłby całym pierścieniem). Ponadto, jeśli $a = bc$, gdzie $b, c \in P$, to $bc \in (a)$, stąd $b \in (a)$ lub $c \in (a)$. Załóżmy, że $b \in (a)$. Istnieje wtedy takie $u \in P$, że $b = au$, a stąd $b = bcu$ i dzięki $b \neq 0$ oraz całkowitości P mamy $cu = 1$, czyli c jest elementem odwracalnym. Analogiczne postępowanie, gdy $c \in (a)$, prowadzi do wniosku, że b jest odwracalny. □

Przykład 4.7.7.
(1) Gdy pierścień nie jest całkowity, to może się zdarzyć, że ideał główny jest pierwszy, a mimo to jego generator jest rozkładalny, np. (2) w $\mathbb{Z}_6$ jest ideałem pierwszym ale $2 = 2 \cdot 4$, gdzie 2 i 4 są nieodwracalne.

(2) Implikacja odwrotna w obserwacji 4.7.6 nie musi być prawdziwa, tzn. ideał generowany przez element nierozkładalny nie musi być pierwszy. Dla przykładu rozważmy pierścień $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Element $1 + \sqrt{-5}$ jest nierozkładalny, ale ideał przez niego generowany zawiera 6 nie zawierając ani 2 ani 3.

Przyjrzyjmy się teraz jak się ma sprawa w szczególnym typie pierścieni jakim są dziedziny ideałów głównych.

Twierdzenie 4.7.8 (własności ideałów w DIG)**.** *Jeśli P jest dziedziną ideałów głównych oraz $a \in P^\star$, to ideał (a) jest maksymalny wtedy i tylko wtedy, gdy jest pierwszy, a to zachodzi dokładnie wtedy, gdy element a jest nierozkładalny.*

Dowód. Oczywiście wystarczy wykazać, że jeśli a jest elementem nierozkładalnym, to ideał (a) jest maksymalny. Niech więc ideał $I \subseteq P$ spełnia warunek $(a) \subseteq I$. Ponieważ każdy ideał w P jest główny, to istnieje takie $b \in P$, że $I = (b)$. Wobec tego $a = bc$ dla pewnego $c \in P$. Dzięki nierozkładalności a, jeden z elementów b lub c jest odwracalny. Jeśli b jest odwracalny, to $I = P$, jeśli zaś c jest odwracalny, to $b = ac^{-1}$ oraz $I = (a)$. □

Zauważmy, że wobec tego wszystkie elementy w danym pierścieniu możemy podzielić na cztery grupy: zero, elementy odwracalne, elementy nierozkładalne i elementy rozkładalne.

4.7.2 Elementy pierwsze

Definicja 4.7.9 (element pierwszy)**.** Niech P będzie pierścieniem. Element $p \in P^\star \setminus U(P)$ nazywamy **elementem pierwszym** jeśli zachodzi implikacja:

$$\forall\, a, b \in P :\ p|ab \implies p|a \ \text{ lub } \ p|b.$$

Własność 4.7.10. *Niech P będzie pierścieniem. Wtedy zachodzą następujące własności:*

(1) jeśli p jest elementem pierwszym, który dzieli iloczyn elementów z P: $a_1 \cdot \ldots \cdot a_n$, to istnieje takie $i \in \{1, \ldots, n\}$, że $p|a_i$,

(2) element $a \in P^\star \setminus U(P)$ jest elementem pierwszym wtedy i tylko wtedy, gdy (a) jest ideałem pierwszym,

(3) w pierścieniu całkowitym każdy element pierwszy jest elementem nierozkładalnym, nie są to jednak pojęcia równoważne.

Dowód. Pierwsze dwa punkty wynikają bezpośrednio z definicji odpowiednich obiektów oraz zastosowania indukcji matematycznej. Uzasadnimy więc punkt (3). Niech $p = ab$, wówczas z pierwszości wynika, że $p|a$ lub $p|b$, jeśli więc na przykład $p|a$, to $a = pc$ dla pewnego $c \in P$ i $p(1 - bc) = 0$. Korzystając z całkowitości P otrzymujemy, że $1 = bc$ czyli b jest elementem odwracalnym w P, skąd nierozkładalność p. Przykład na brak implikacji odwrotnej w ogólnej sytuacji zobaczymy poniżej. □

Przykład 4.7.11. Rozważmy pierścień $P = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5} :\ a, b \in \mathbb{Z}\}$ oraz element $1 + i\sqrt{5} \in P$. Jest to element nierozkładalny, czego uzasadnienie pozostawiamy jako ćwiczenie, ale nie jest on elementem pierwszym w tym pierścieniu, gdyż $1 + i\sqrt{5}|6$ ale nie dzieli ani 3 ani 2.

Podsumujmy informację o związkach między pierwszością a nierozkładalnością w pierścieniu całkowitym na podstawie 4.7.10 i 4.7.8.

Twierdzenie 4.7.12. *Niech P będzie pierścieniem całkowitym oraz $a \in P^\star \setminus U(P)$. Wtedy zachodzą własności:*

(1) a – pierwszy $\implies$ a – nierozkładalny

(2) jeśli dodatkowo P jest dziedziną ideałów głównych, to zachodzi równoważność:

$$a \text{ – pierwszy} \iff a \text{ – nierozkładalny.}$$

4.7.3 Największy wspólny dzielnik i najmniejsza wspólna wielokrotność

Definicja 4.7.13 (największy wspólny dzielnik)**.** Niech P będzie pierścieniem oraz $a_1, \ldots, a_n \in P$, gdzie przynajmniej jeden z tych elementów jest niezerowy. Element $d \in P$ nazywamy **największym wspólnym dzielnikiem** elementów $a_1, \ldots, a_n$, gdy:

(1) $d \mid a_i$ dla $i = 1, \ldots, n$ (d jest wspólnym dzielnikiem elementów $a_1, \ldots, a_n$),

(2) jeśli $d' \in P$ spełnia $d' \mid a_i$ dla $i = 1, \ldots, n$, to $d' \mid d$.

Zbiór największych wspólnych dzielników dla $a_1, \ldots, a_n$ oznaczamy przez $\mathrm{NWD}(a_1, \ldots, a_n)$.

Definicja 4.7.14 (najmniejsza wspólna wielokrotność)**.** Niech P będzie pierścieniem oraz $a_1, \ldots, a_n \in P$. Element $m \in P$ nazywamy **najmniejszą wspólną wielokrotnością** elementów $a_1, \ldots, a_n$, gdy:

(1) $a_i \mid m$ dla $i = 1, \ldots, n$ (m jest wspólną wielokrotnością elementów $a_1, \ldots, a_n$),

(2) jeśli $m' \in P$ spełnia $a_i \mid m'$ dla $i = 1, \ldots, n$, to $m \mid m'$.

Zbiór najmniejszych wspólnych wielokrotności dla $a_1, \ldots, a_n$ oznaczamy przez $\mathrm{NWW}(a_1, \ldots, a_n)$.

Zauważmy, że największy wspólny dzielnik oraz najmniejsza wspólna wielokrotność nie są jedyne – są wyznaczone jednoznacznie z dokładnością do relacji stowarzyszenia: np. $\mathrm{NWD}(12, 30) = \{-6, 6\}$ oraz $\mathrm{NWW}(12, 18) = \{-36, 36\}$. W obu przypadkach są to więc zbiory, a nie elementy. Często jednak piszemy np. $\mathrm{NWD}(12, 30) = 6$ co oznacza, że 6 reprezentuje zbiór największych wspólnych dzielników, z których wszystkie są ze sobą stowarzyszone.

Definicja 4.7.15 (elementy względnie pierwsze)**.** Elementy $a_1, \ldots, a_n$ pierścienia P nazywamy **względnie pierwszymi**, jeśli $1 \in \mathrm{NWD}(a_1, \ldots, a_n)$.

Największy wspólny dzielnik jest szczególnie przydatny w wyznaczaniu generatorów ideałów głównych.

Twierdzenie 4.7.16 (generatory w pierścieniu całkowitym)**.** *Niech P będzie pierścieniem całkowitym oraz niech $a_1, \ldots, a_n \in P$ będą takie, że ideał $(a_1, \ldots, a_n)$ jest główny. Wtedy:*

(1) element $d \in \mathrm{NWD}(a_1, \ldots, a_n)$ wtedy i tylko wtedy, gdy $(a_1, \ldots, a_n) = (d)$,

(2) element $m \in \mathrm{NWW}(a_1, \ldots, a_n)$ wtedy i tylko wtedy, gdy $(a_1) \cap \ldots \cap (a_n) = (m)$.

Dowód.
(1) Jeśli $d \in \mathrm{NWD}(a_1, \ldots, a_n)$, to d dzieli każde a_i czyli dla każdego i mamy, że $a_i \in (d)$ skąd oczywiście $(a_1, \ldots, a_n) \subseteq (d)$. Ponieważ ideał $(a_1, \ldots, a_n)$ jest główny, więc istnieje takie $b \in P$, że $(a_1, \ldots, a_n) = (b)$. Wobec tego każde a_i należy do (b), więc b dzieli elementy $a_1, \ldots, a_n$. Skoro d jest największym wspólnym dzielnikiem, to $b \mid d$, czyli $(d) \subseteq (b)$ i otrzymujemy żądaną równość. Odwrotnie, niech teraz $d \in P$ będzie takie, że $(a_1, \ldots, a_n) = (d)$. Wtedy oczywiście $d \mid a_i$ dla $i = 1, \ldots, n$. Ponadto, gdy $d' \in P$ również dzieli elementy $a_1, \ldots, a_n$, to $(d) = (a_1, \ldots, a_n) \subseteq (d')$, czyli $d' \mid d$, a stąd $d \in \mathrm{NWD}(a_1, \ldots, a_n)$.

(2) Załóżmy, że $(a_1) \cap \ldots \cap (a_n) = (m)$ dla pewnego $m \in P$. Wtedy oczywiście $a_i \mid m$ dla $i = 1, \ldots, n$. Jeśli $m' \in P$ oraz $a_i \mid m'$ dla $i = 1, \ldots, n$, to $m' \in (a_1) \cap \cdots \cap (a_n) = (m)$, czyli $m \mid m'$, stąd zaś $m \in \mathrm{NWW}(a_1, \ldots, a_n)$. Odwrotnie, jeśli $m \in \mathrm{NWW}(a_1, \ldots, a_n)$, to mamy $m \in (a_1) \cap \ldots \cap (a_n)$, czyli $(m) \subseteq (a_1) \cap \cdots \cap (a_n)$. Gdy zaś $a \in (a_1) \cap \ldots \cap (a_n)$, to $a_i \mid a$ dla $i = 1, \ldots, n$, a stąd $m \mid a$, czyli $a \in (m)$, co daje $(a_1) \cap \ldots \cap (a_n) \subseteq (m)$. □

Zbierzemy poniżej zestaw własności największego wspólnego dzielnika w pierścieniach – polecamy ich udowodnienie jako dobre ćwiczenia na zapoznanie się z tym pojęciem.

Własność 4.7.17. *Niech P będzie pierścieniem całkowity, $a, b, c, a_1, \ldots, a_n \in P$. Wtedy, jeśli odpowiednie elementy poniżej istnieją, tzn. rozważane zbiory* NWD *są niepuste, to zachodzą związki:*

(1) jeśli $d \in \mathrm{NWD}(a_1, \ldots, a_n)$ i $a_i = db_i$ dla $i \in \{1, \ldots, n\}$, to elementy $b_1, \ldots, b_n$ są względnie pierwsze,

(2) jeśli $a|b$, to $\mathrm{NWD}(a, b) = a$,

(3) $\mathrm{NWD}(ac, bc) = \mathrm{NWD}(a, b)c$,

(4) $\mathrm{NWD}(\mathrm{NWD}(a, b), c) = \mathrm{NWD}(a, \mathrm{NWD}(b, c))$,

(5) jeśli $\mathrm{NWD}(a, b) = 1, \mathrm{NWD}(a, c) = 1$, to $\mathrm{NWD}(a, bc) = 1$.

4.8 O nierozkładalności wielomianów

4.8.1 Pierwiastki wielomianów

Definicja 4.8.1 (pierwiastek wielomianu)**.** Niech P będzie pierścieniem, $c \in P$ oraz $f = a_0+a_1X+\ldots+a_nX^n \in P[X]$. **Wartością wielomianu** f na elemencie c nazywamy element $f(c)$ pierścienia P określony następująco:

$$f(c) := a_0 + a_1c + \ldots + a_nc^n.$$

O elemencie c mówimy, że jest **pierwiastkiem** wielomianu f, gdy $f(c) = 0 = 0_P$.

Twierdzenie 4.8.2 (twierdzenie Bézouta)**.** *Jeśli $f \in P[X]$, $c \in P$, to $f(c) = 0$ wtedy i tylko wtedy, gdy $X - c|f$.*

Dowód. Zauważmy, że jeśli $X - c|f$, to $f = (X - c)g$ dla pewnego $g \in P[X]$, czyli licząc wartości po obu stronach dostajemy $f(c) = (c - c)g(c) = 0$.

Niech teraz $f(c) = 0$. Ponieważ współczynnik wiodący wielomianu $X - c$ jest odwracalny, więc możemy przez ten wielomian dzielić z resztą. Z algorytmu dzielenia z resztą dla wielomianów (4.5.11) istnieją więc takie $g, r \in P[X]$, że $f = g(X - c) + r$ gdzie stopień r jest mniejszy od 1. Wstawmy teraz do obu stron c: $f(c) = r$ skąd mamy $f = g(X - c) + f(c)$. Ale z założenia $f(c) = 0$, czyli $(X - c)|f$. □

4.8.2 Nierozkładalność wielomianów niskich stopni nad ciałem

Własność 4.8.3 (nierozkładalność nad ciałem)**.** *Niech K będzie ciałem oraz $f \in K[X]$. Wtedy zachodzą własności:*

(1) jeśli f jest wielomianem stopnia 1, to f ma pierwiastek w K,

(2) jeśli f jest wielomianem stopnia 1, to f jest nierozkładalny w $K[X]$,

(3) jeśli f jest wielomianem stopnia 2 lub 3 to f jest nierozkładalny w $K[X]$ wtedy i tylko wtedy, gdy f nie ma pierwiastków w K.

Dowód. (1) Skoro f ma stopień 1, to $f = aX + b \in K[X]$ gdzie $a \neq 0$. Wobec tego element $-b \cdot a^{-1} \in K$ jest jego pierwiastkiem.

(2) Element f, jako wielomian stopnia 1 jest niezerowy i nieodwracalny. Niech więc $f = gh$, gdzie g, $h \in K[X]$. Ponieważ $K[X]$ to pierścień całkowity, więc $1 = \deg(g \cdot h) = \deg(g)+\deg(h)$, skąd np. g jest wielomianem stopnia zero, czyli stałą niezerową, a więc elementem odwracalnym w K, gdyż K jest ciałem. Wobec tego f jest nierozkładalny.

(3) Jeśli f jest wielomianem stopnia 2, to z powodów jak w (2) może się rozłożyć jedynie na iloczyn wielomianów stopnia 1. Jeśli f jest wielomianem stopnia 3, to może się rozłożyć na iloczyn wielomianów, z których przynajmniej jeden jest stopnia 1. Jeśli więc f jest rozkładalny, to jednym z czynników jest wielomian stopnia 1, który na mocy (1) ma pierwiastek w K. Jeśli zaś f ma pierwiastek $c \in K$, to z twierdzenia Bézouta $f = (X - c)g$, gdzie $X - c$, g-nieodwracalne w $K[X]$, czyli f rozkładalny. □

Zanim powiemy coś więcej o metodach badania nierozkładalności wielomianów w ogólniejszej sytuacji, wprowadzimy odpowiednik konstrukcji ciała liczb wymiernych na bazie liczb całkowitych. Celem jest możliwość zanurzenia danego pierścienia w ciało, w którym można będzie odwracać elementy.

4.8.3 Ciało ułamków

Jeżeli P jest pierścieniem całkowitym, to na zbiorze $P \times P^\star$ definiujemy relację

$$(a, s) \sim (a', s') : \iff as' - a's = 0.$$

Własność 4.8.4. *Wprowadzona powyżej relacja jest równoważnością na zbiorze $P \times P^\star$.*

Dowód. Zwrotność jest oczywista. Istotnie, jeśli $(a, s) \in P \times P^\star$, to $as - as = 0$, zatem $(a, s) \sim (a, s)$. Symetria wynika z faktu, że jeśli $(a, s) \sim (a', s')$, to $as' - a's = 0$ i stąd $a's - as' = 0$, czyli $(a', s') \sim (a, s)$. Dla uzasadnienia przechodniości załóżmy teraz, że $(a, s) \sim (a', s')$ oraz $(a', s') \sim (a'', s'')$. Wobec tego mamy $as' - a's = 0$ oraz $a's'' - a''s' = 0$. Mnożąc pierwsze z równań przez s'' a drugie przez s i dodając stronami dostaniemy, że $s'(as'' - a''s) = 0$. Skoro $s' \neq 0$ i pierścień jest całkowity, to musi być $as'' - a''s = 0$ i w konsekwencji $(a, s) \sim (a'', s'')$. □

Klasę równoważności pary $(a,s) \in P \times P^\star$ względem relacji $\sim$ będziemy oznaczać przez $a/s = \frac{a}{s}$, zaś zbiór ilorazowy $(P \times P^\star)/\sim$ przez $K(P)$.

Na zbiorze $K(P)$ wprowadzimy działania dodawania i mnożenia wzorując się na znanym sposobie dodawania i mnożenia ułamków w $\mathbb{Q}$. Mianowicie:

$$a/s + a'/s' := (as' + a's)/ss', \qquad (a/s)(a'/s') := aa'/ss', \qquad \text{dla} \quad a/s, a'/s' \in K(P).$$

Własność 4.8.5. *Zdefiniowane powyżej działania są poprawnie określone i zbiór $K(P)$ z tak wprowadzonym dodawaniem i mnożeniem ma strukturę ciała. Ponadto odwzorowanie $i\colon P \ni a \mapsto a/1 \in K(P)$ jest monomorfizmem pierścieni.*

Dowód. Po pierwsze musimy wykazać, że wartości działań nie zależą od wyboru reprezentantów. Wykażemy ten fakt dla dodawania. Niech $a/s = a'/s'$ oraz $b/t = b'/t'$. Oznacza to, że

$$as' - a's = 0, \qquad bt' - b't = 0.$$

Mamy teraz, że

$$(at + bs)s't' - (a't' + b's')st = tt'(as' - a's) + ss'(bt' - b't) = 0.$$

Dla mnożenia mamy zaś

$$(ab)s't' - (a'b')st = (at' - a't)bs' + (bs' - b's)a't = 0.$$

Chcąc pokazać, że $K(P)$ z tak wprowadzonymi działaniami jest ciałem, wystarczy wykonać odpowiednie obliczenia korzystając z przemienności i łączności w P. Łatwo również sprawdzić, że $0/1$ jest zerem, zaś $1/1$ jedynką pierścienia $K(P)$. Zauważmy jeszcze, że $1/1 \neq 0/1$, bo inaczej byłoby $1 = (1\cdot 1 - 0\cdot 1) = 0$ wbrew założeniu że $1 \neq 0$. Elementem odwrotnym do każdego elementu postaci $\frac{a}{s}$, gdzie $a \neq 0$, jest element $\frac{s}{a}$. Zauważmy też, że dla dowolnego $s \in P^\star$ jest $s/s = 1/1$ oraz $0/s = 0/1$. Na koniec jeśli $a, b \in P$, to

$$i(a+b) = (a+b)/1 = a/1 + b/1 = i(a) + i(b),$$

$$i(ab) = ab/1 = (a/1)(b/1) = i(a)i(b).$$

Skoro jest to więc homomorfizm, to wiadomo, że będzie on injektywny dokładnie wtedy, gdy jego jądro składa się tylko z zera (por. 3.2.11). Ale jeśli $\frac{a}{1} = \frac{0}{1}$, to wprost z definicji mamy $a = 0$, co kończy dowód. □

Definicja 4.8.6 (ciało ułamków)**.** Jeśli P jest pierścieniem całkowitym z $1 \neq 0$, to ciało $K(P)$ nazywamy **ciałem ułamków** pierścienia P.

Przykład 4.8.7.
(1) Gdy $P = \mathbb{Z}$, to przeprowadzenie konstrukcji ciała ułamków prowadzi do ciała $\mathbb{Q}$.

(2) Jak wiemy, pierścień $K[X]$ jest całkowity jeśli K jest ciałem. Ciało ułamków tego pierścienia oznaczamy $K(X)$ i nazywamy ciałem funkcji wymiernych zmiennej X nad ciałem K.

4.8.4 Pierścienie faktorialne

Definicja 4.8.8 (rozkład skończony i rozkład jednoznaczny)**.** Mówimy, że element niezerowy a pierścienia całkowitego P ma **rozkład skończony**, jeśli

(1) a jest nierozkładalny lub można go zapisać jako skończony iloczyn elementów nierozkładalnych.

Mówimy, że element niezerowy a posiada **rozkład jednoznaczny**, jeśli posiada on rozkład skończony oraz spełniony jest warunek:

(2) z równości $a = p_1 \dots p_k$, $a = q_1 \dots q_l$, gdzie $p_i, q_j, i = 1, \dots, k, j = 1, \dots, l$ to elementy nierozkładalne wynika, że $k = l$ i istnieje taka permutacja $\sigma \in S_k$, że $p_i \sim q_{\sigma(i)}$.

Twierdzenie 4.8.9. *Niech P będzie pierścieniem całkowitym, w którym każdy element nieodwracalny posiada rozkład skończony.*

Wtedy następujące warunki są równoważne:

(1) każdy element nieodwracalny w P posiada rozkład jednoznaczny w P,

(2) dla każdych dwóch elementów $a, b \in P^\star$ zbiór $\mathrm{NWW}(a,b)$ *jest niepusty,*

(3) dla każdych dwóch elementów $a, b \in P^\star$ zbiór $\mathrm{NWD}(a,b)$ *jest niepusty,*

(4) każdy element nierozkładalny w P jest elementem pierwszym w P.

Dowód. Udowodnimy kolejno odpowiednie implikacje.

(1) $\Longrightarrow$ (2) Niech a, $b \in P$. Wtedy zgodnie z istnieniem skończonego rozkładu możemy je zapisać jako:

$$a = \prod_{i=1}^{n} p_i^{\alpha_i}, \quad b = \prod_{j=1}^{m} p_j^{\beta_i},$$

gdzie p_k – elementy nierozkładalne. Zauważmy, że poprzez dobranie indeksów, dla których α_i lub β_j są zerami, możemy przyjąć, że $n = m$. Wtedy łatwo sprawdzić, że zachodzi $c := \prod_{k=1}^{n} p_k^{\gamma_k} \in \mathrm{NWW}(a,b)$, gdzie $\gamma_k := \max\{\alpha_k, \beta_k\}$.

(2) $\Longrightarrow$ (3)

Niech $c \in \mathrm{NWW}(a,b)$ i zauważmy, że element ab jest wspólną wielokrotnością elementów a, b, skąd z definicji NWW wiemy, że $c|ab$, czyli istnieje $d \in P$ dla którego $ab = cd$. Wykażemy, że $d \in \mathrm{NWD}(a,b)$.

Zauważmy najpierw, że $d|a$ i $d|b$. Istotnie, wiadomo, że $a|c$, skąd istnieje takie $a_1 \in P$, że $c = a_1 a$, czyli $ab = a_1 ad$. Tym samym $a(b - a_1 d) = 0$, co wobec niezerowości a i całkowitości pierścienia dowodzi, że $b = a_1 d$, czyli $d|b$. Analogicznie dowodzimy drugą podzielność.

Załóżmy teraz, że $\widetilde{d} \in P^\star$ jest wspólnym podzielnikiem a i b, czyli istnieją takie $\widetilde{a}, \widetilde{b} \in P^\star$, że $a = \widetilde{d}\widetilde{a}$, $b = \widetilde{d}\widetilde{b}$. Zauważmy najpierw, że $\widetilde{c} := \widetilde{d}\widetilde{a}\widetilde{b}$ jest wspólną wielokrotnością a i b jako, że $\widetilde{d}\widetilde{a}\widetilde{b} = \widetilde{b}a = \widetilde{a}b$, tym samym $\widetilde{c} = c\alpha$ dla pewnego $\alpha \in P^\star$.

Ostatecznie więc otrzymamy $\widetilde{d}\widetilde{a}\widetilde{d}\widetilde{b} = ab = cd$, skąd $c\alpha\widetilde{d} = cd$ i ponownie korzystając z niezerowości c i całkowitości P otrzymamy, że $\widetilde{d}|d$, więc d jest największym wspólnym dzielnikiem wyjściowych elementów.

(3) $\Longrightarrow$ (4)

Niech $p|ab$ będzie elementem nierozkładalnym. Gdyby element p nie dzielił ani a ani b, to oznaczałoby, że $\mathrm{NWD}(p,a) = 1$ i $\mathrm{NWD}(p,b) = 1$, a wobec tego $\mathrm{NWD}(p,ab) = 1$ i jednocześnie $\mathrm{NWD}(p,ab) = p$, więc otrzymana sprzeczność dowodzi implikacji.

(4) $\Longrightarrow$ (1)

Niech $a \in P \setminus U(P)$ i niech $a = p_1 \cdot \ldots \cdot p_s = q_1 \cdot \ldots \cdot q_r$ gdzie p_i – elementy nierozkładalne, czyli pierwsze.

Ponieważ p_1 jest elementem pierwszym wobec tego musi dzielić któryś z elementów q_j (na przykład q_1), a ponieważ q_1 jest nierozkładalny więc oznacza to, że $p_1 = uq_1$ gdzie u jest elementem odwracalnym. Stąd $q_1(q_2 \cdot \ldots \cdot q_r - up_2 \cdot \ldots \cdot p_s) = 0$ a ponieważ $q_1 \neq 0$ otrzymujemy $q_2 \cdot \ldots \cdot q_r = up_2 \cdot \ldots \cdot p_s$.

Powtarzając analogiczne rozumowanie skończenie wiele razy otrzymamy tezę. □

Definicja 4.8.10 (pierścień faktorialny)**.** Pierścień całkowity nazywamy **pierścieniem faktorialnym** lub **dziedziną z jednoznacznością rozkładu**, jeśli każdy element nieodwracalny tego pierścienia posiada rozkład jednoznaczny.

Twierdzenie 4.8.11. *Każda dziedzina ideałów głównych jest pierścieniem faktorialnym.*

Dowód. Zgodnie z poprzednim twierdzeniem oraz własnością 4.7.12 wystarczy wykazać, że każdy niezerowy element nieodwracalny w P można przedstawić jako iloczyn skończenie wielu elementów nierozkładalnych.

Przypuśćmy więc, że istnieje taki element, który tego rozkładu nie ma i rozważmy niepusty zbiór S złożony ze wszystkich niezerowych, nieodwracalnych elementów pierścienia P, których nie można przedstawić jako skończonego iloczynu elementów nierozkładalnych.

Niech $\{I_s\}_{s \in S}$ będzie rodziną ideałów, gdzie $I_s = (s)$. Jest to rodzina niepusta musi mieć więc element maksymalny[6].

[6]Korzystamy z Lematu Kuratowskiego–Zorna, zauważając wcześniej, że każdy łańcuch ideałów (względem inkluzji) ma majorantę będą sumą ideałów z łańcucha.

Niech to będzie I_{s_0}. Element s_0 jest na pewno rozkładalny, bo należy do S. Wobec tego istnieją a, b – nieodwracalne w P takie, że $s_0 = ab$. Stąd $(s_0) \subset (a)$ i $(s_0) \subset (b)$ i są to istotne zawierania. Z maksymalności ideału (s_0) wynika, że $a \notin S$ i $b \notin S$, więc można je przedstawić jako skończone iloczyny elementów nierozkładalnych. Wobec tego można tak przedstawić element s_0 – sprzeczność.

Oznacza to, że rodzina S jest rodziną pustą, co daje nam żądaną własność. □

Powyższe twierdzenie pozwala nam uporządkować dotychczas omawiane klasy pierścieni w ciąg zawierań, który warto odnotować.

Uwaga 4.8.12.
(1) Zachodzą następujące zawierania:

$$\{\text{Dziedziny Euklidesa}\} \subset \{\text{Dziedziny ideałów głównych}\} \subset \{\text{Pierścienie faktorialne}\},$$

(2) Wszystkie powyższe zawierania są istotne. Wśród przykładów pierścieni ideałów głównych, które nie są euklidesowe wymienić można $\mathbb{Z}[i\sqrt{19}]$, zaś pierścień faktorialny, który nie jest pierścieniem ideałów głównych to na przykład $\mathbb{Z}[X]$.

4.9 Badanie nierozkładalności wielomianów w $P[X]$, gdzie P – faktorialny

Definicja 4.9.1 (wielomian pierwotny)**.** Jeśli P jest pierścieniem faktorialnym oraz $f \in P[X]$, to f nazywamy **pierwotnym**, gdy jego współczynniki są względnie pierwsze.

Wprost z definicji wynika ważna uwaga.

Uwaga 4.9.2. Jeśli wielomian $f \in P[X]$ jest nierozkładalny, to musi być pierwotny.

Własność 4.9.3 (lemat Gaussa $P[X]$)**.** *Jeśli P jest pierścieniem faktorialnym, to iloczyn wielomianów pierwotnych w $P[X]$ jest wielomianem pierwotnym w $P[X]$.*

Dowód. Przypuśćmy, że mamy dwa wielomiany $f = a_0 + a_1X + \ldots + a_nX^n \in P[X]$, $g = b_0 + b_1X + \ldots + b_mX^m \in \mathbb{Z}[X]$ pierwotne, których iloczyn $f \cdot g = c_0 + c_1X + \ldots + c_{m+n}X^{m+n}$ nie jest pierwotny.

Wtedy istnieje element nierozkładalny (a wobec faktorialności P jest to element pierwszy) p, który dzieli wszystkie c_i. Skoro jednak f i g są pierwotne, to zbiory $A = \{i = 0, \ldots, n : \ p \nmid a_i\}$, $B = \{j = 0, \ldots, m : \ p \nmid b_j\}$ są niepuste i możemy poprawnie określić ich minima: $r = \min A$, $s := \min B$. Jeśli teraz policzymy współczynnik c_{r+s} to występują w nim wyrazy postaci a_ib_j gdzie $i + j = r + s$. Jeśli $i < r$ to a_i dzieli się przez p, czyli a_ib_j też, a gdy $i > r$, to $j < s$ czyli b_j dzieli się przez p, a tym samym też a_ib_j. W takim razie przez p musi się dzielić też wyraz a_rb_s. Ale p jest elementem pierwszym, więc musi dzielić a_r lub b_s co prowadzi do sprzeczności. □

Własność 4.9.4 (przedstawienie wielomianu w $P[X]$)**.** *Niech P będzie pierścieniem faktorialnym oraz $f \in P[X]$ wielomian stopnia co najmniej 1. Wtedy:*

(1) istnieje taki elementy $c \in P$ oraz wielomian pierwotny $f^\star \in P[X]$, że $f = cf^\star$,

(2) jeśli $f = cf^\star = c_1f_1^\star$ gdzie $c, c_1 \in P$ i wielomiany $f^\star, f_1^\star \in P[X]$ są pierwotne, to $c \sim c_1$ w P oraz $f^\star \sim f_1^\star$ w $P[X]$.

Dowód.
(1) Jeśli $f = a_0 + a_1X + \ldots + a_nX^n$, to $f = cf^\star$, gdzie $c \in \mathrm{NWD}(a_0, \ldots, a_n)$ oraz $f^\star = b_0 + b_1X + \ldots + b_nX^n$, gdzie $b_i = \frac{a_i}{c}$ dla $i = 0, 1, \ldots, n$.

(2) Jeśli teraz mielibyśmy inny rozkład tzn. $f = cf^\star = c_1f_1^\star$, gdzie c, $f^\star$ są jak w dowodzie punktu (1), to ponieważ c_1 musi dzielić wszystkie współczynniki f, zaś c to NWD tych współczynników, to wiadomo, że $c_1|c$, czyli $c = dc_1$ dla pewnego $d \in P$. Stąd $c_1df^\star = c_1f^\star$, czyli $c_1(df^\star - f_1^\star) = 0$. Ponieważ $c_1 \neq 0$ i jesteśmy w pierścieniu całkowitym, to mamy, że $df^\star = f_1^\star$. Oznacza to jednak, że d dzieli wszystkie współczynniki $f_1^\star$, które są względnie pierwsze, skąd $d \sim 1$, czyli $f^\star \sim f_1^\star$ i $c \sim c_1$. □

Własność 4.9.5 (rozkład w $P[X]$ i w $K(P)[X]$)**.** *Jeśli P jest pierścieniem faktorialnym, $f \in P[X]$ oraz istnieją takie g_1, $g_2 \in K(P)[X]$, że $f = g_1g_2$ i $\deg(g_i) > 0$ dla $i = 1, 2$, to istnieją $f_i \in P[X]$ takie, że $deg(f_i) > 0$ i $f = f_1f_2$.*

Dowód. Zauważmy najpierw, że dowolny wielomian $h \in K(P)[X]$ ma postać:

$$h = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \ldots + \frac{a_n}{b_n}X^n,$$

gdzie $a_i \in P$, $b_i \in P^\star$. Mnożąc obie strony na przykład przez jeden z elementów zbioru $\mathrm{NWW}(b_0, \ldots, b_n)$ otrzymamy, że istnieje $c \in P$ takie, że $ch \in P[X]$. Korzystając z rozkładu na stałą i wielomian pierwotny możemy więc powiedzieć, że dla dowolnego $h \in K(P)[X]$ istnieją: c, $d \in P$ oraz wielomian $h^\star \in P[X]$ – pierwotny takie, że $ch = dh^\star$ oraz stopień h jest taki sam jak stopień $h^\star$.

Niech więc teraz $f \in P[X]$ i $f = g_1g_2$ jak w założeniach, gdzie $g_i \in K(P)[X]$. Dla wielomianów g_i istnieją więc $c_i, d_i \in P$ oraz $g_i^\star \in P[X]$ takich samych (dodatnich) stopni jak odpowiednie g_i, że $c_ig_i = d_ig_i^\star$ oraz istnieje $d \in P$ i $f^\star \in P[X]$ – pierwotny taki, że $f = df^\star$.

Wobec tego $c_1c_2df^\star = c_1c_2f = (c_1g_1)(c_2g_2) = (d_1d_2)g_1^\star g_2^\star$. Z lematu Gaussa wnioskujemy, że $g_1^\star g_2^\star$ jest wielomianem pierwotnym, czyli z jednoznaczności zapisu mamy: $c_1c_2d \sim d_1d_2$ oraz $f^\star \sim g_1^\star g_2^\star$. Oznacza to, że istnieje takie $u = 1$ lub $u = -1$, że $f = df^\star = dug_1^\star g_2^\star$. Wystarczy więc przyjąć $f_1 := dug_1^\star \in P[X]$ i $f_2 := g_2^\star \in P[X]$ by otrzymać tezę. □

Twierdzenie 4.9.6 (kryterium Eisensteina)**.** *Niech P będzie pierścieniem faktorialnym, $f = a_0 + a_1X + \ldots + a_nX^n \in P[X]$ oraz załóżmy, że istnieje taki element nierozkładalny $p \in P$, że $p|a_i$ dla $i = 0, \ldots, n-1$, $p \nmid a_n$ oraz $p^2 \nmid a_0$.*

Wtedy f jest nierozkładalny w $K(P)[X]$, zaś jeśli dodatkowo f jest pierwotny, to jest nierozkładalny w $P[X]$.

Dowód. Dla dowodu nie wprost przypuśćmy, że $a_0 + a_1X + \ldots + a_nX^n = f = g_1g_2$ w pierścieniu $K(P)[X]$ i oba wielomiany g_i są nieodwracalne w $K(P)[X]$. W szczególności ich stopień jest co najmniej 1. Z przygotowań wiemy, że istnieją takie wielomiany dodatniego stopnia f_1, $f_2 \in P[X]$, że $f = f_1f_2$.

Niech

$$f_1 = b_0 + b_1X + \ldots + b_rX^r, \qquad f_2 = c_0 + c_1X + \ldots + c_sX^s.$$

Ponieważ $p \nmid a_n = b_rc_s$, to $p \nmid b_r$ oraz $p \nmid c_s$. Z drugiej strony $p \mid a_0 = b_0c_0$ oraz $p^2 \nmid b_0c_0$, zatem p dzieli tylko b_0 lub tylko c_0. Możemy założyć, że $p \mid b_0$ oraz $p \nmid c_0$. Jeśli przyjmiemy

$$k = \min\{i \in \{0, \ldots, r\} : p \nmid b_i\},$$

to $p \mid b_i$ dla $i < k$. Oczywiście $1 \leqslant k \leqslant r < n$ i stąd $p \mid a_k$. Skoro tak, to również

$$p \mid a_k - (b_0c_{k-1} + \ldots + b_{k-1}c_1) = b_kc_0.$$

Otrzymujemy sprzeczność, gdyż $p \nmid b_k$ oraz $p \nmid c_0$.

Oczywiście, jeśli f jest pierwotny, to jego rozkład nie może być rozkładem w $P[X]$. Istotnie, taki rozkład musiałby być rozkładem na wielomiany niższych stopni, co dawałoby rozkład f na czynniki nieodwracalne także w $K(P)[X]$, więc jeśli f spełnia założenia twierdzenia i jest pierwotny, to jest nierozkładalny także w $P[X]$. □

Przykład 4.9.7. Kryterium Eisensteina można stosować nawet w sytuacjach pozornie nie dopuszczających takiej możliwości. Dla zbadania nierozkładalności wielomianu

$$f = 1 + X + \ldots + X^{p-1} \in \mathbb{Z}[X],\ ^{7}$$

gdzie p jest liczbą pierwszą. Warto zauważyć, że jego nierozkładalność jest równoważna nierozkładalności wielomianu $g(X) = f(X+1)$, a następnie przedstawić f w postaci $f = (X^p - 1)/(X - 1)$. Wtedy

$$g(X) = \frac{(X+1)^p - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1} = X^{p-1} + pX^{p-2} + \cdots + p.$$

Pozostaje zauważyć, że $p \mid \binom{p}{i}$ dla $0 < i < p$ i ponadto $p \nmid 1$ oraz $p^2 \nmid p$.

[7] Oczywiście, z zasadniczego twierdzenia arytmetyki $\mathbb{Z}$ jest pierścieniem faktorialnym.

4.10 Dziedziczenie faktorialności na pierścień wielomianów

Udowodnimy teraz podstawowe twierdzenie, które pozwoli nam na przeniesienie własności rozkładu na pierścień wielomianów.

Twierdzenie 4.10.1 (Gauss)**.** *Jeśli P jest pierścieniem faktorialnym, to pierścień $P[X]$ też jest pierścieniem faktorialnym.*

Dowód. (I) Istnienie rozkładu. Przedstawmy wielomian $f \in P[X]$ zgodnie z 4.9.4 jako $f = c(f)f^\star$, gdzie $c(f) \in P$ i $f^\star$ wielomian pierwotny. Na podstawie tego zapisu wystarczy rozważyć dwa przypadki:

(1) $f \in P$, czyli f jest wielomianem stałym.

(2) f – wielomian pierwotny.

(1) Ponieważ, jak łatwo sprawdzić, elementy pierścienia P, które są nierozkładalne w P, są również nierozkładalne w $P[X]$, więc istnienie rozkładu wynika w tym przypadku z faktorialności pierścienia P.

(2) Postępujemy indukcyjnie względem $n = \deg(f)$.

($\bullet$) $\deg(f) = 1$. Wielomian stopnia jeden może się rozłożyć jedynie na stałą i wielomian stopnia 1, ale ponieważ f jest pierwotny, to jego współczynniki są względnie pierwsze i jest to wielomian nierozkładalny.

($\bullet$) Zakładamy, że umiemy rozłożyć wielomiany stopnia $\leqslant n-1$.

Jeśli f jest nierozkładalny, to mamy tezę. Załóżmy więc, że istnieją f_1, f_2 nieodwracalne takie, że $f = f_1 f_2$. Jednak f jest pierwotny, stąd $\deg(f_1) < n$ i $\deg(f_2) < n$ (inaczej pewien nierozkładalny element z P dzieliłby wszystkie współczynniki f) oraz f_1 i f_2 są pierwotne. Korzystając z założenia indukcyjnego dostajemy poszukiwany rozkład.

(II) Jednoznaczność rozkładu.

Niech $f = p_1 \cdot \ldots \cdot p_k g_1 \cdot \ldots \cdot g_l = q_1 \cdot \ldots \cdot q_r h_1 \cdot \ldots \cdot h_n$, gdzie wszystkie czynniki po prawej stronie są nierozkładalne oraz:

$\deg(p_i) = \deg(q_j) = 0$ dla dowolnych $i \in \{1, \ldots, k\}$, $j \in \{1, \ldots, r\}$, gdzie $\deg(g_i) > 0$ oraz $\deg(h_j) > 0$ dla dowolnych $i \in \{1, \ldots, l\}$, $j \in \{1, \ldots, n\}$.

Wykażemy, że $k = r$ i $l = n$ oraz po ewentualnym przenumerowaniu $p_i \sim q_i$ i $g_j \sim h_j$.

Wielomiany g_i, h_j są nierozkładalne, więc są pierwotne. Wobec tego, na podstawie lematu Gaussa, oba iloczyny $g_1 \cdot \ldots \cdot g_l$ i $h_1 \cdot \ldots \cdot h_n$ są też wielomianami pierwotnymi.

Korzystając znów z jednoznaczności przedstawienia wielomianu jako iloczynu stałej i wielomianu pierwotnego dostajemy, że $p_1 \cdot \ldots \cdot p_k \sim q_1 \cdot \ldots \cdot q_r$ oraz $g_1 \cdot \ldots \cdot g_l \sim h_1 \cdot \ldots \cdot h_n$. Istnieją wobec tego takie elementy odwracalne $u \in P$, $v \in P$, że $(up_1) \cdot \ldots \cdot p_k \sim q_1 \cdot \ldots \cdot q_r$ oraz $(vg_1) \cdot \ldots \cdot g_l \sim h_1 \cdot \ldots \cdot h_n$. Z całkowitości pierścienia otrzymujemy też $uv = 1$.

Z jednoznaczności rozkładu w P mamy $k = r$ i z dokładnością do przenumerowania: $p_1 \sim up_1 \sim q_1, \ldots, p_k \sim q_k$.

Elementy $vg_1, g_2 \ldots, g_l$ oraz $h_1, \ldots, h_n$ są pierwotne i nierozkładalne w $P[X]$, więc są również nierozkładalne w $K(P)[X]$. Ponieważ $K(P)$ jest ciałem, więc $K(P)[X]$ jest pierścieniem ideałów głównych, czyli faktorialnym (por. 4.8.11). Wobec tego $l = n$ i z dokładnością do przenumerowania indeksów mamy, że $g_1 \sim vg_1 \sim h_1, \ldots, g_l \sim h_l$ w $K(P)[X]$. Oznacza to, że rozważane elementy są stowarzyszone w $P[X]$ i dostajemy tezę. □

4.11 Zadania

1. (a) Sprawdzić, czy zbiór $P = \mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$ ze zwykłymi działaniami dodawania i mnożenia liczb rzeczywistych tworzy pierścień, czy jest to pierścień całkowity oraz czy jest to ciało.
   (b) Na analogiczne pytania odpowiedzieć dla zbioru P i działań:
   $$(a + b\sqrt{2}) + (c + d\sqrt{2}) := (a + b) + (c + d)\sqrt{2}, \ (a + b\sqrt{2})(c + d\sqrt{2} = (ac + 2bd) + (ad + bd)\sqrt{2}.$$

2. Sprawdzić, czy zbiór funkcji parzystych określonych na $\mathbb{R}$ z działaniami dodawaniami mnożenia funkcji jest pierścieniem.

3. Sprawdzić, że $\mathbb{Z}[i] = \{a + bi, \ a, b \in \mathbb{Z}\}$ jest pierścieniem z działaniami dodawania i mnożenia liczb zespolonych. Wyznaczyć zbiór elementów odwracalnych tego pierścienia i zbiór jego dzielników zera.

4. Niech d będzie ustaloną liczbą całkowitą, która nie jest kwadratem żadnej liczby całkowitej. Sprawdzić, że $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d},\ a, b \in \mathbb{Z}\}$ jest pierścieniem z działaniami dodawania i mnożenia liczb zespolonych. Ustalić jak wygląda $U(\mathbb{Z}[\sqrt{d}])$ w zależności od d oraz jak wygląda $D(\mathbb{Z}[\sqrt{d}])$.

5. Udowodnić, że w pierścieniu $\mathbb{Z}_m$ (z działaniami dodawania i mnożenia modulo m) zachodzą następujące równoważności:

$$(a) \qquad k \in U(\mathbb{Z}_m) \iff \mathrm{NWD}(k, m) = 1$$
$$(b) \qquad k \in D(\mathbb{Z}_m) \iff k \neq 0 \mod m \text{ oraz } \mathrm{NWD}(k, m) > 1.$$

6. Wyznaczyć dzielniki zera i elementy odwracalne w pierścieniach $\mathbb{Z}_6 \times \mathbb{Z}$, $\mathbb{Z}_3 \times \mathbb{Z}_8$, $\mathbb{Z}_6 \times \mathbb{Z}_{10}$.

7. Wyznaczyć postać dzielników zera oraz elementów odwracalnych w pierścieniach: $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{R} \times \mathbb{Z}$ oraz $\mathbb{Z} \times \mathbb{Z}[i]$.

8. Odpowiedzieć na pytanie, czy w pierścieniu funkcji rzeczywistych na przedziale $[0, 1]$ (z działaniami dodawania i mnożenia funkcji) istnieją dzielniki zera.

9. Sprawdzić, że zbiór $P = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix},\ a, b \in P \right\}$ z działaniami dodawania i mnożenia macierzy tworzy pierścień oraz zbadać, czy są w nim dzielniki zera.

10. Wyznaczyć wszystkie dzielniki zera i elementy odwracalne w pierścieniu $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{k}{2^n},\ k \in \mathbb{Z},\ n \in \mathbb{N}_0 \right\}$.

11. Wyznaczyć grupę jedności pierścienia $\mathbb{Z}[\sqrt{-d}] = \{a + b\sqrt{-d} :\ a, b \in \mathbb{Z}\}$, gdzie $d \in \mathbb{N}_+$.

12. Udowodnić, że pierścienie $\mathbb{Z}[\sqrt{2}]$ i $\mathbb{Z}[\sqrt{5}]$ nie są izomorficzne.

13. Udowodnić, że $\mathbb{R}^\infty$ jest izomorficzny z każdym z następujących pierścieni: $\mathbb{R} \times \mathbb{R}^\infty$, $\mathbb{R}^2 \times \mathbb{R}^\infty$, $\mathbb{R}^\infty \times \mathbb{R}^\infty$.

14. Udowodnić, że jeśli $\phi : A \to B$ jest homomorfizmem pierścieni, to $\operatorname{Ker} \phi$ jest ideałem w A.

15. Udowodnić, że jeśli $\phi : A \to B$ jest epimorfizmem pierścieni oraz I jest ideałem w A, to zbiór $\phi(I)$ jest ideałem pierścienia B. Pokazać, że założenie epimorficzności ϕ jest istotne.

16. Niech R będzie pierścieniem i $I,\ J$ ideałami w R. Dowieść, że zbiór

$$I : J := \{a \in R :\ \forall b \in J :\ ab \in I\}.$$

17. Wykazać, że zbiór ideałów pierwszych w pierścieniu $\mathbb{Z}[X]$ jest nieskończony.

18. Udowodnić, że jeśli $\phi :\ A \to B$ jest homomorfizmem pierścieni i J jest ideałem w B, to zbiór $\phi^{-1}(J)$ jest ideałem w A.

19. Wykazać, że ideał $(5, X)$ pierścienia $\mathbb{Z}[X]$ nie jest główny.

20. Sprawdzić, czy zbiór tych funkcji $f \in C([0, 1])$, które spełniają podany warunek, jest ideałem pierścienia $C([0, 1])$:

    (a) $f(0) \in \mathbb{Q}$,
    (b) $f(0) = f(1)$,
    (c) $\forall x \in [0, \frac{1}{2}] :\ f(x) = 0$.

21. Udowodnić, że jeśli R jest pierścieniem, to dla dowolnych $a,\ b \in R$ zachodzi równość $(aR)(bR) = (ab)R$.

22. Niech p będzie ideałem pierwszym w pierścieniu R i niech I_1, I_2 będą ideałami w R takimi, że $I_1 \cap I_2 \subset p$. Wykazać, że $I_1 \subset p$ lub $I_2 \subset p$.

23. Niech $R = \mathbb{R}[x]$. Wykazać, że następujące zbiory są ideałami w R:

    (a) $A_1 := \{f \in R :\ f(0) = 0\}$,

(b) $A_2 := \{f \in R : \ f(a) = 0\}$, gdzie $a \in \mathbb{R}$ jest ustalone.

(c) $A_3 := \{f \in R : \ f(0) = f(1) = 0\}$.

24. Znaleźć generatory dla każdego z ideałów z poprzedniego zadania i odpowiedzieć na pytanie z jakim pierścieniem izomorficzny jest iloraz R/A_i.

Rozdział 5

Elementy teorii ciał

5.1 Rozszerzenia ciał

5.1.1 Stopień rozszerzenia, wieża rozszerzeń

Definicja 5.1.1 (rozszerzenie ciał, ciało proste)**.** Jeśli $K \subset L$, L jest ciałem, zaś K jest ciałem z działaniami indukowanymi z L, to mówimy, że K **jest podciałem** ciała L, zaś L nazywamy **rozszerzeniem ciała** K. Omawiane rozszerzenie ciał oznaczamy L/K. [1] Jeśli dla rozszerzenia L/K jest $K \neq L$, to K nazywamy **podciałem właściwym** ciała L. Ciało, które nie posiada podciał właściwych nazywamy **ciałem prostym**.

Definicja 5.1.2 (K-homomorfizm ciał)**.** Jeśli $\sigma\colon L_1 \to L_2$ jest homomorfizmem ciał L_1, L_2 [2] będących rozszerzeniem ciała K, to σ nazywamy K-homomorfizmem, gdy $\sigma|_K = \mathrm{id}_K$.

Przykład 5.1.3. Przyjrzyjmy się najpierw prostym przykładom.

(1) Łatwo zauważyć z definicji, że ciałami prostymi są na przykład $\mathbb{Q}$ oraz $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą. Jak dowiemy się za chwilę są to jedyne możliwe ciała proste.

(2) Zbadajmy jak wyglądają $\mathbb{R}$-homomorfizmy ciała $\mathbb{C}$. Niech więc $\sigma : \mathbb{C} \longrightarrow \mathbb{C}$ będzie takim $\mathbb{R}$-homomorfizmem. Wtedy $\sigma(a+bi) = \sigma(a)+\sigma(b)\sigma(i) = a+b\sigma(i)$ dla dowolnej liczby $a+bi \in \mathbb{C}$. Jak widać każdy $\mathbb{R}$-homomorfizm ciała $\mathbb{C}$ jest wyznaczony jednoznacznie przez swoją wartość na i. Jednocześnie $-1 = \sigma(-1) = \sigma(i^2) = \sigma(i)^2$, czyli $\sigma(i) = \pm i$. Wobec tego jedynymi $\mathbb{R}$-homomorfizmami ciała $\mathbb{C}$ są identyczność oraz sprzężenie.

Zauważmy, że jeśli ciało L jest rozszerzeniem ciała K, to na ciało L można patrzeć jak na przestrzeń wektorową nad ciałem K. Prowadzi nas to do kolejnej definicji.

Definicja 5.1.4 (stopień rozszerzenia ciał)**.** Jeśli ciało L jest rozszerzeniem ciała K, to **stopniem rozszerzenia** L/K nazywamy wymiar L jako przestrzeni wektorowej nad K i oznaczamy

$$[L : K] := \dim_K L.$$

Mówimy, że rozszerzenie L/K jest **skończone**, jeśli $[L : K] < \infty$. W przeciwnym wypadku rozszerzenie L/K nazywamy nieskończonym i piszemy wtedy $[L : K] = \infty$.

Przykład 5.1.5. Rozszerzenie $\mathbb{C}/\mathbb{R}$ jest rozszerzeniem skończonym (stopnia 2), natomiast rozszerzenia $\mathbb{R}/\mathbb{Q}$, $\mathbb{C}/\mathbb{Q}$ oraz $K(X)/K$ są nieskończone.

Twierdzenie 5.1.6 (prawo wieży)**.** *Dla dowolnych rozszerzeń ciał: M/L oraz L/K zachodzi równość* $[M : K] = [M : L][L : K]$.

Dowód. Jeśli $[M : K] < \infty$, to oczywiście $[M : L] < \infty$. Jednocześnie L jest podprzestrzenią wektorową M nad K, czyli musi też być $[L : K] < \infty$. Odwrotnie, jeśli $[M : L]$ lub $[L : K]$ są nieskończone, to również stopień rozszerzenia $[M : K]$ jest w oczywisty sposób nieskończony.

[1] Nie należy tego oznaczenia mylić ze strukturą ilorazową! Oznaczenie to mówi tylko, że K jest podciałem L, zaś inne funkcjonujące w literaturze oznaczenia to: $K \subset L$, $K \leqslant L$.

[2] Homomorfizm ciał L_1, L_2, to dokładnie homomorfizm pierścieni L_1, L_2.

Załóżmy więc teraz, że $r = [M : L] < \infty$ oraz $s = [L : K] < \infty$ i wybierzmy bazy: $\{m_1, \ldots, m_r\}$ przestrzeni M nad L oraz $\{l_1, \ldots, l_s\}$ przestrzeni L nad K. Jeśli $m \in M$, to istnieją takie $\lambda_1, \ldots, \lambda_r \in L$, że

$$m = \lambda_1 m_1 + \ldots + \lambda_r m_r.$$

Każdy element λ_i może zostać zapisany jako

$$\lambda_i = \kappa_{i1} l_1 + \ldots + \kappa_{is} l_s, \qquad \text{dla pewnych} \qquad \kappa_{i1}, \ldots, \kappa_{is} \in K, \qquad i = 1, \ldots, r.$$

W konsekwencji otrzymujemy równość

$$m = \sum_{i=1}^{r} \lambda_i m_i = \sum_{i=1}^{r} \Big(\sum_{j=1}^{s} \kappa_{ij} l_j \Big) m_i = \sum_{i=1}^{r} \sum_{j=1}^{s} \kappa_{ij} (m_i l_j).$$

Wobec tego elementy $m_i l_j$ ($1 \leqslant i \leqslant r$ oraz $1 \leqslant j \leqslant s$) generują M nad K.

Sprawdzimy dalej, czy są one liniowo niezależne. Przypuśćmy więc, że

$$\sum_{i=1}^{r} \sum_{j=1}^{s} \alpha_{ij} (m_i l_j) = 0, \qquad \alpha_{ij} \in K \ (1 \leqslant i \leqslant r, \ 1 \leqslant j \leqslant s). \tag{$\star$}$$

Przegrupowując elementy w ($\star$) i korzystając z liniowej niezależności $m_1, \ldots, m_r$ nad L dostajemy

$$\sum_{i=1}^{r} \Big(\sum_{j=1}^{s} \alpha_{ij} l_j \Big) m_i = 0, \quad \text{zatem} \quad \sum_{j=1}^{s} \alpha_{ij} l_j = 0 \text{ dla } i = 1, \ldots, r. \tag{$\star\star$}$$

Pozostaje skorzystać z liniowej niezależności $l_1, \ldots, l_s$ nad K aby z ($\star\star$) otrzymać $\alpha_{ij} = 0$ dla wszystkich $1 \leqslant i \leqslant r$ oraz $1 \leqslant j \leqslant s$, co oznacza, że układ $\{m_i l_j : i = 1, \ldots, r, \ j = 1, \ldots, s\}$ jest bazą M nad K. Wykazaliśmy więc, że $[M : K] < \infty$ oraz $[M : K] = [M : L][L : K]$. □

5.1.2 Podciało proste i charakterystyka ciała

Analogicznie jak w teorii pierścieni dowodzimy, że dla podzbioru $A \subset K$ ciała K, zbiór będący przecięciem wszystkich podciał ciała K zawierających A jest podciałem ciała K. Ciało to nazywamy ciałem generowanym przez zbiór A.

Uwaga 5.1.7. Zaobserwujmy kilka prostych własności.

(1) Jeśli L/K jest rozszerzeniem ciał, $|L| = n$ oraz $|K| = k$, to $k \mid n$ – dla tego wniosku wystarczy skorzystać z twierdzenia Lagrange'a (por. wnioski 3.4.6) dla grup $(L, +)$ oraz $(K, +)$.

(2) Każde ciało zawiera dokładnie jedno podciało proste. Rzeczywiście, jeśli K jest ciałem, zaś K_0 podciałem ciała K generowanym przez zbiór pusty (innymi słowy K_0 jest przecięciem wszystkich podciał ciała K), to K_0 jest ciałem prostym. By się o tym przekonać wystarczy zauważyć, że jeśli $F \subset K_0$ jest podciałem, to F jest również podciałem ciała K. Z konstrukcji K_0 mamy $K_0 \subset F$. Jest to również jedyne podciało proste ciała K, gdyż jeśli K' jest również podciałem prostym K, to $K_0 \subset K'$ i z faktu, że K' nie zawiera podciał właściwych wynika, że $K' = K_0$.

Definicja 5.1.8 (charakterystyka ciała)**.** Jeśli K jest ciałem oraz istnieje taka liczba naturalna n, że $n \cdot 1_K = 0_K$ [3], to **charakterystyką ciała** K nazywamy najmniejszą z liczb naturalnych[4] o tej własności. Jeśli takiej liczby nie ma, to mówimy, że K jest **ciałem charakterystyki zero**[5]. Charakterystykę ciała K oznaczamy $\operatorname{char} K$.

Przykład 5.1.9. Odnotujmy kilka ważnych przykładów.

(1) $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.

(2) Jeśli p jest liczbą pierwszą, to $\operatorname{char} \mathbb{Z}_p = p$.

(3) Jeśli K jest podciałem ciała L, to $\operatorname{char} K = \operatorname{char} L$.

[3] Wyrażenie $n \cdot 1$ rozumiemy tutaj jako sumę n jedynek.
[4] Pamiętajmy, że w skrypcie założono, że 0 NIE jest liczbą naturalną.
[5] Przyjmuje się czasem, że wówczas charakterystyka jest nieskończona.

Zauważymy teraz bezpośredni związek charakterystyki ciała z jego podciałem prostym.

Własność 5.1.10 (charakterystyka a ciało proste)**.** *Niech K będzie ciałem, zaś K_0 jego podciałem prostym. Wtedy zachodzą własności:*

(1) $\operatorname{char} K = 0$ *lub* $\operatorname{char} K$ *jest liczbą pierwszą,*

(2) jeśli $\operatorname{char} K = 0$*, to wtedy* $K_0 \cong \mathbb{Q}$*,*

(3) jeśli $\operatorname{char} K = p > 0$*, to wtedy* $K_0 \cong \mathbb{Z}_p$*.*

Dowód. W dowodzie wszędzie 1 oznacza 1_K.
(1) Niech $\operatorname{char} K = p > 0$ i przypuśćmy, że $p = nm$, gdzie n, m są liczbami naturalnymi mniejszymi od p. Wtedy na podstawie rozdzielności mnożenia względem dodawania w ciele K mamy

$$0 = p \cdot 1 = nm \cdot 1 = n \cdot (m \cdot 1) = (n \cdot 1)(m \cdot 1),$$

czyli jako, że ciało jest pierścieniem całkowitym (por. 4.1.9), to $n \cdot 1 = 0$ lub $m \cdot 1 = 0$ wbrew minimalności liczby p.

(2) Jeśli $\operatorname{char} K = 0$, to określmy

$$L = \left\{ \frac{k \cdot 1}{n \cdot 1} : k \in \mathbb{Z},\ n \in \mathbb{N} \right\}. \quad [6]$$

Jak łatwo sprawdzić jest to podciało ciała K izomorficzne z $\mathbb{Q}$, izomorfizmem jest

$$\mathbb{Q} \ni \frac{k}{n} \longrightarrow \frac{k \cdot 1}{n \cdot 1} \in L,$$

gdzie zerowość charakterystyki wykorzystujemy wykazując poprawną określoność i injektywność odwzorowania. Ponadto każde podciało ciała K zawiera jedynkę, musi więc zawierać L, czyli $L = K_0$.

(3) Jeśli $\operatorname{char} K = p > 0$, to określmy

$$L = \{0 \cdot 1, 1 \cdot 1, \ldots, (p-1) \cdot 1\}.$$

Zauważmy, że elementy zbioru L są różne między sobą. Przypuśćmy bowiem, że $n \cdot 1 = m \cdot 1$ dla pewnych $0 \leqslant n < m < p$. Wówczas $(m-n) \cdot 1 = 0$ oraz $0 < m - n < p$, co prowadzi do sprzeczności z założeniem o charakterystyce ciała K. Zauważmy dalej, że L jest podciałem ciała K. Istotnie, mamy bowiem

$$n \cdot 1 - k \cdot 1 = (n-k) \cdot 1 = l \cdot 1, \qquad l \equiv n - k \pmod{p}, \qquad 0 \leqslant l < p.$$

Jeśli zaś $n \neq 0$, to istnieje takie $0 < m < p$, że $nm \equiv 1 \pmod{p}$ (gdyż $\mathbb{Z}_p$ jest ciałem). W konsekwencji

$$\frac{k \cdot 1}{n \cdot 1} = \frac{nmk \cdot 1}{n \cdot 1} = \frac{mk \cdot 1}{1 \cdot 1} = mk \cdot 1. \quad [7]$$

Łatwo sprawdzić, że ciało L jest izomorficzne z $\mathbb{Z}_p$, izomorfizmem jest

$$\mathbb{Z}_p \ni n_p \longrightarrow n \cdot 1 \in L. \quad [8]$$

Ponadto każde podciało ciała K zawiera jedynkę, musi więc zawierać L, czyli $L = K_0$. □

Wniosek 5.1.11. *Niech K będzie ciałem p-elementowym, gdzie p jest liczbą pierwszą. Wówczas:*

(1) jedynymi ciałami prostymi są ciała $\mathbb{Q}$ oraz $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą,

(2) $K \cong \mathbb{Z}_p$*.*

Dowód. Zauważmy, że część pierwsza wynika bezpośrednio z naszego twierdzenia. Dla dowodu (2) odnotujmy najpierw, że jeśli ciało jest skończone, to musi mieć charakterystykę dodatnią. Niech więc $\operatorname{char} K = q > 0$. Wtedy K zawiera podciało proste K_0 izomorficzne z $\mathbb{Z}_q$. Zgodnie z uwagą 5.1.7 mamy $q \mid p$, czyli $p = q$ oraz $K = K_0 \cong \mathbb{Z}_p$. □

Twierdzenie 5.1.12 (o ciałach skończonych)**.** *Zachodzą następujące charakteryzacje ciał skończonych:*

[6] Stosujemy konwencję $1/a = a^{-1}$ dla $a \in K \setminus \{0\}$.
[7] Podobnie jak wcześniej należy wybrać odpowiednich reprezentantów wśród $\{0, 1, \ldots, p-1\}$.
[8] Podobnie jak w przypadku (1) tak i tutaj charakterystyka ponownie odgrywa rolę przy sprawdzaniu injektywności odwzorowania.

(1) każde ciało skończone ma p^n elementów dla pewnej liczby pierwszej p oraz pewnego $n \in \mathbb{N}$,

(2) dla dowolnej liczby pierwszej p i liczby naturalnej n istnieje ciało p^n elementowe (jest to tzw. ciało Galois, które zwyczajowo oznaczamy przez $\mathbb{F}_{p^n}$),

(3) jeśli dwa ciała skończone są równoliczne to są izomorficzne.

Dowód. W tym rozdziale udowodnimy jedynie (1). Dowód pozostałych części znajdziemy w kolejnych rozdziałach (por. wniosek 5.4.4). Dla dowodu (1) niech K będzie ciałem skończonym o k elementach. Wtedy wiemy, że ciało to ma dodatnią charakterystykę będącą pewną liczbą pierwszą p i tym samym zawiera podciało proste izomorficzne z $\mathbb{Z}_p$. Wobec tego K jest przestrzenią wektorową nad $\mathbb{Z}_p$ i tym samym posiada pewną skończoną bazę $v_1, \ldots, v_n$ nad $\mathbb{Z}_p$. Mamy więc: $K = \{\lambda_1 v_1 + \ldots + \lambda_n v_n, \lambda_i \in \mathbb{Z}_p\}$ i tym samym K ma p^n elementów, gdzie n to wymiar K nad ciałem prostym jako przestrzeni wektorowej. □

5.1.3 Rozszerzenia proste i skończenie generowane

Zaczniemy od prostego uogólnienia pierścienia wielomianów jednej zmiennej. Dla potrzeb tej części materiału wprowadzimy rekurencyjną definicję pierścienia wielomianów wielu zmiennych – tak określony pierścień jest jednak izomorficzny z powstałym dzięki bezpośredniej konstrukcji (por. rozdział 10.).

Definicja 5.1.13 (wielomiany n zmiennych nad pierścieniem)**.** Jeśli P jest pierścieniem, $n \in \mathbb{N}$ to rekurencyjnie określamy **pierścień wielomianów** n **zmiennych nad pierścieniem** P jako:

(1) $P[X_1] := P[X]$ – pierścień wielomianów jednej zmiennej, który określiliśmy wcześniej,

(2) $P[X_1, \ldots, X_n] := P[X_1, \ldots, X_{n-1}][X_n]$ – czyli pierścień wielomianów jednej zmiennej X_n nad pierścieniem wielomianów $(n-1)$-zmiennych.

Definicja 5.1.14 (rozszerzenie generowane przez elementy)**.** Jeśli L/K jest rozszerzeniem ciał oraz $u_1, \ldots, u_n \in L$, to przez $K[u_1, \ldots, u_n]$, odpowiednio $K(u_1, \ldots, u_n)$, oznaczamy podpierścień, odpowiednio podciało, ciała L generowane przez zbiór $K \cup \{u_1, \ldots, u_n\} \subseteq L$. Łatwo sprawdzić[9], że

$$K[u_1, \ldots, u_n] = \{f(u_1, \ldots, u_n) : f \in K[X_1, \ldots, X_n]\},$$

$$K(u_1, \ldots, u_n) = \left\{\frac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)} : f, g \in K[X_1, \ldots, X_n],\ g(u_1, \ldots, u_n) \neq 0\right\}.$$

Definicja 5.1.15 (rozszerzenie (proste) skończenie generowane)**.** Rozszerzenie ciał L/K nazywamy rozszerzeniem **skończenie generowanym**, jeśli istnieją takie $u_1, \ldots, u_n \in L$, że $L = K(u_1, \ldots, u_n)$. W przypadku, gdy $n = 1$, czyli $L = K(u)$ dla pewnego $u \in L$ rozszerzenie L/K nazywamy **prostym**. Element u nazywamy wtedy **elementem prymitywnym** tego rozszerzenia.

Uwaga 5.1.16. Jeśli ciało L jest rozszerzeniem ciała K oraz $u_1, \ldots, u_n \in L$, to zachodzą własności:

$$K[u_1, \ldots, u_n] = K[u_1, \ldots, u_{n-1}][u_n],$$

$$K(u_1, \ldots, u_n) = K(u_1, \ldots, u_{n-1})(u_n).$$

5.2 Rozszerzenia algebraiczne

Twierdzenie 5.2.1 (o wstępnej charakteryzacji rozszerzeń)**.** *Jeśli L/K jest rozszerzeniem ciał, $u \in L$ oraz*

$$F_u \colon K[X] \ni f \longrightarrow f(u) \in K[u],$$

to możliwe są dwa przypadki:

(1) $\operatorname{Ker} F_u = (0)$ *i wówczas* $K(u) \cong K(X)$ *oraz* $[K(u) : K] = \infty$

[9] Standardowo, sprawdzamy, że zbiory określone po prawych stronach równości mają strukturę odpowiednio pierścienia/ciała zawierającego wskazane elementy, a następnie stwierdzamy że ich elementy muszą znajdować się w dowolnym pierścieniu/ciele generowanym przez nie, na podstawie wewnętrzności podstawowych operacji.

(2) $\operatorname{Ker} F_u \neq (0)$ *i wówczas istnieje dokładnie jeden taki wielomian unitarny i nierozkładalny* $p_u \in K[X]$, *że* $\operatorname{Ker} F_u = (p_u)$. *Wtedy też* $K[X]/(p_u) \cong K(u)$ *oraz* $[K(u) : K] = \deg p_u < \infty$.

Dowód. Załóżmy dla dowodu (1), że $\operatorname{Ker} F_u = (0)$. Wtedy homomorfizm F_u jest izomorfizmem pierścieni, który w naturalny sposób indukuje izomorfizm ciał

$$F_u^*\colon K(X) \ni \frac{f}{g} \longrightarrow \frac{f(u)}{g(u)} \in K(u),$$

przy czym poprawna określoność tego odwzorowania oraz jego injektywność wynika z faktu, że $g(u) \neq 0$ wtedy i tylko wtedy, gdy $g \neq 0$, dzięki założeniu o trywialności jądra.

Rozszerzenie $K(X)/K$ jest nieskończone, gdyż elementy $1_K, X, X^2, \ldots$ są liniowo niezależne nad K. Oznacza to, że rozszerzenie $K(u)/K$ jest nieskończone.

Dla dowodu (2) rozważmy ideał $I := \operatorname{Ker} F_u \neq (0)$ i zauważmy, że z postaci $I = \{f \in K[X] : f(u) = 0\}$ łatwo wynika iż jest to ideał pierwszy, gdyż

$$fg \in I \iff (fg)(u) = 0 \iff^{10} f(u) = 0 \text{ lub } g(u) = 0 \iff f \in I \text{ lub } g \in I.$$

Wiemy, że $K[X]$ jest dziedziną ideałów głównych (por. przykład 4.6.2(4) oraz twierdzenie 4.6.3). Oznacza to, że I jest ideałem maksymalnym (por. twierdzenie 4.7.8). Innymi słowy istnieje taki wielomian nierozkładalny i unitarny (dzięki temu, że mnożenie przez stałą niezerową nie zmienia ideału) $p_u \in K[X]$, że $I = (p_u)$. W takiej sytuacji p_u jest wyznaczony jednoznacznie[11]. Skoro ideał I jest maksymalny, to $K[X]/I$ jest ciałem (por. własność 4.4.4). Z twierdzenia o izomorfizmie mamy, że $K[X]/I \cong K[u]$. Tym samym $K[u]$ jest ciałem, a że jednocześnie $K[u]$ to najmniejszy podpierścień L zawierający $K \cup \{u\}$, więc w konsekwencji mamy $K[u] = K(u)$.

Pozostaje wykazać, że $[K(u) : K] = \deg p_u$. Oznaczmy $n = \deg p_u$ i rozważmy element $f \in K[X]$. Stosując algorytm dzielenia z resztą otrzymujemy $f + I = r + I$ dla pewnego $r \in K[X]$, spełniającego warunek $\deg r < n$. Oznacza to, że elementy $K[X]/I$ są generowane nad K przez obrazy elementów $1_K, X, \ldots, X^{n-1}$ w $K[X]/I$. Elementy te tworzą bazę $K[X]/I$ nad K, gdyż są również liniowo niezależne. Istotnie, jeśli

$$\alpha_0(1 + I) + \alpha_1(X + I) + \ldots + \alpha_{n-1}(X^{n-1} + I) = 0, \qquad \alpha_0, \ldots, \alpha_{n-1} \in K,$$

to $\alpha_0 + \alpha_1 X + \ldots + \alpha_{n-1}X^{n-1} \in I$, czyli jest to wielomian podzielny przez p_u, a ponieważ jest stopnia $< n$, to podzielność ta, dzięki całkowitości rozważanych pierścieni, jest możliwa tylko wtedy, gdy $\alpha_0 = \alpha_1 = \ldots = \alpha_{n-1} = 0$. Skoro $\{1_K + I, X + I, \ldots, X^{n-1} + I\}$ tworzy bazę $K[X]/I$ nad K, to dzięki izomorfizmowi

$$K[X]/I \ni f + I \longrightarrow f(u) \in K(u)$$

otrzymujemy, że bazą $K(u)$ nad K jest zbiór $\{1_K, u, \ldots, u^{n-1}\}$. □

Przykład 5.2.2. Rozważmy rozszerzenie $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Wielomian $f = X^3 - 2 \in \mathbb{Q}[X]$ jest nierozkładalny (np. z kryterium Eisensteina), unitarny, stopnia 3 i taki, że $f(\sqrt[3]{2}) = 0$. Zgodnie z poprzednim twierdzeniem $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, zaś bazą $\mathbb{Q}(\sqrt[3]{2})$ nad $\mathbb{Q}$ jest zbiór $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$. W szczególności $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$.

Definicja 5.2.3 (element algebraiczny (przestępny))**.** Jeśli L/K jest rozszerzeniem ciał, to element $u \in L$ nazywamy **algebraicznym** nad K, jeśli istnieje taki niezerowy wielomian $f \in K[X]$, że $f(u) = 0$. Innymi słowy u jest algebraiczny nad K. Elementy nie będące algebraicznymi nad K nazywamy elementami **przestępnymi** nad K.

Uwaga 5.2.4.
(1) Każdy element z K jest algebraiczny nad K.

(2) Elementy z $\mathbb{C}$ algebraiczne nad $\mathbb{Q}$ nazywamy liczbami algebraicznymi, natomiast elementy z $\mathbb{C}$ przestępne nad $\mathbb{Q}$ nazywamy liczbami przestępnymi. Przykładowo liczby $\sqrt[n]{2}$ oraz i są algebraiczne, zaś liczby e oraz π są przestępne **uzupełnić odniesienie do bibliografii !**.

Skupimy się w tej części na dokładniejszej analizie pojęć charakteryzujących elementy algebraiczne.

[10] Korzystamy z całkowitości ciała L gdzie należy $(fg)(u)$.
[11] Jeśli $I = (f)$, to p_u oraz f są stowarzyszone, tzn. $f = vp_u$ dla pewnego $v \in K \setminus \{0\}$. Gdy dodatkowo wielomian f jest unitarny, to musi być $v = 1$, czyli $f = p_u$.

Definicja 5.2.5 (wielomian minimalny i stopień elementu algebraicznego)**.** Jeśli L/K jest rozszerzeniem ciał oraz element $u \in L$ jest algebraiczny nad K, to jedyny wielomian unitarny i nierozkładalny $p_u \in K[X]$, którego pierwiastkiem jest u nazywamy **wielomianem minimalnym elementu u nad K**. **Stopniem elementu u nad K** nazywamy liczbę $[K(u) : K] = \deg p_u$.

Definicja 5.2.6 (domknięcie/rozszerzenie algebraiczne)**.** Jeżeli L/K jest rozszerzeniem ciał, to zbiór

$$K_{\text{alg}}(L) := \{u \in L : \text{ element } u \text{ jest algebraiczny nad } K\}$$

nazywamy **domknięciem algebraicznym ciała K w ciele L**. Ponadto rozszerzenie L/K nazywamy **algebraicznym**, jeśli każdy element z L jest algebraiczny nad K, tzn. gdy $K_{\text{alg}}(L) = L$.

Spróbujemy teraz ustalić zależności między poznanymi do tej pory typami rozszerzeń: rozszerzeniami skończonymi, rozszerzeniami skończenie generowanymi i rozszerzeniami algebraicznymi. Bezpośrednio z twierdzenia 5.2.1 wynika prosta uwaga.

Uwaga 5.2.7. Jeśli u jest elementem algebraicznym nad K, to rozszerzenie $K(u)/K$ jest rozszerzeniem skończonym stopnia równego stopniowi elementu u nad K.

Twierdzenie 5.2.8 (o zależnościach między rozszerzeniami)**.** *Niech L/K będzie rozszerzeniem ciał.*

(1) Jeśli rozszerzenie L/K jest skończone, to jest algebraiczne i skończenie generowane.

(2) Jeśli rozszerzenie L/K jest skończenie generowane przez elementy algebraiczne nad K, to jest skończone.

Dowód. Dla dowodu (1) niech $[L : K] = n < \infty$. Jeśli $u \in L$, to elementy $1_K, u, \ldots, u^n$ są K-liniowo zależne. Istnieją więc takie $\alpha_0, \ldots, \alpha_n \in K$ nie wszystkie równe zeru, że $\alpha_n u^n + \cdots + \alpha_1 u + \alpha_0 = 0$, czyli u jest algebraiczny nad K. Jeśli teraz elementy $u_1, \ldots, u_n \in L$ tworzą bazę L nad K, to $L = K(u_1, \ldots, u_n)$.

Jeśli zaś teraz jak w (2) mamy $L = K(u_1, \ldots, u_n)$, gdzie $u_i \in L$ dla $i = 1, \ldots, n$, są algebraiczne nad K, to rozważmy kolejne rozszerzenia ciał

$$K \subseteq K(u_1) \subseteq K(u_1, u_2) \subseteq \cdots \subseteq K(u_1, \ldots, u_{n-1}) \subseteq K(u_1, \ldots, u_{n-1}, u_n).$$

Rozszerzenie $K(u_1, \ldots, u_{i-1}) \subseteq K(u_1, \ldots, u_{i-1}, u_i) = K(u_1, \ldots, u_{i-1})(u_i)$ jest rozszerzeniem o element algebraiczny dla $i = 1, \ldots, n$, wobec tego z uwagi 5.2.7 jest to rozszerzenie skończone, czyli z twierdzenia 5.1.6 rozszerzenie $K \subseteq K(u_1, \ldots, u_n)$ jest skończone. □

Twierdzenie 5.2.9. *Niech $K \subseteq L \subseteq M$ będzie rozszerzeniem ciał.*

(1) Jeśli rozszerzenia L/K oraz M/L są algebraiczne, to również rozszerzenie M/K jest algebraiczne.

(2) Zbiór $K_{\text{alg}}(L)$ jest podciałem ciała L.

Dowód. Dla dowodu (1) zauważmy najpierw, że jeśli $u \in M$, to istnieją takie $b_0, \ldots, b_n \in L$ nie wszystkie równe zeru, że spełnione jest równanie $b_n u^n + \ldots + b_1 u + b_0 = 0$, czyli u jest algebraiczny nad $K(b_0, \ldots, b_n) \subseteq L$. Wobec tego na podstawie twierdzenia 5.2.8 oba rozszerzenia

$$K \subseteq K(b_0, \ldots, b_n) \subseteq K(b_0, \ldots, b_n)(u) = K(b_0, \ldots, b_n, u)$$

są skończone, czyli również rozszerzenie $K \subseteq K(b_0, \ldots, b_n, u)$ jest skończone, zatem ponownie z twierdzenia 5.2.8 element u jest algebraiczny nad K.

Dowodząc w analogiczny sposób (2) rozważmy $u, v \in K_{\text{alg}}(L)$ i rozszerzenia $K \subseteq K(u) \subseteq K(u, v)$. Oba te rozszerzenia są skończone (znów twierdzenie 5.2.8). Oznacza to, że rozszerzenie $K \subseteq K(u, v)$ jest skończone, czyli algebraiczne, co oznacza, że także elementy $u \pm v, uv, u/v \in K(u, v)$ są algebraiczne nad K. □

5.3 Ciało rozkładu wielomianu

Zauważmy najpierw, że wielomian generalnie może mieć więcej pierwiastków niż jego stopień: np. $f = X^3$ w $\mathbb{Z}_8[X]$ ma 4 pierwiastki: $0, 2, 4, 6$, co wydaje się dość zaskakujące. Poniższa własność powie nam jednak, że nie może tak być, gdy pierścień współczynników jest całkowity, dlatego rozważane przez nas najczęściej wcześniej wielomiany o współczynnikach rzeczywistych takich niespodzianek nie kryją.

Definicja 5.3.1 (krotność pierwiastka)**.** Jeśli $c \in P$ jest pierwiastkiem wielomianu $f \in P[X]$, $k \in \mathbb{N}$, to mówimy, że c jest **pierwiastkiem k-krotnym** f, gdy $(X-c)^k$ dzieli f zaś $(X-c)^{k+1}$ nie dzieli f w $P[X]$ (oczywiście z twierdzenia Bézouta wiemy, że skoro c to pierwiastek wielomianu f, to na pewno $(X-c)$ dzieli f).

Własność 5.3.2 (liczba pierwiastków wielomianu)**.** *Jeśli $f \in P[X]$ gdzie P – całkowity, to liczba pierwiastków wielomianu f w pierścieniu P nie przekracza stopnia wielomianu.*

Dowód. Udowodnimy najpierw własność następującą: jeśli $c_1, \ldots, c_n$ to pierwiastki wielomianu $f \in P[X]$ gdzie P – całkowity, każdy z pierwiastków jest krotności odpowiednio k_i, to istnieje $g \in P[X]$ takie, że $f = (X-c_1)^{k_1} \cdot \ldots \cdot (X-c_n)^{k_n} \cdot g$ gdzie $g(c_i) \neq 0$ dla $i = 1, \ldots, n$.

Teza tej własności zachodzi wprost z definicji krotności pierwiastka dla $n = 1$, więc dalej prowadzimy dowód indukcyjny, zakładając jej prawdziwość przy liczbie różnych pierwiastków mniejszej niż $n > 1$. Skoro c_n to pierwiastek k_n-krotny f, to $f = (X-c_n)^{k_n} \cdot h$ dla pewnego $h \in P[X]$ i wielomian h nie może zerować się w c_n (ze względu na twierdzenie Bézouta, gdyż krotność tego pierwiastka to k_n). Z drugiej strony $f(c_i) = 0$ dla $i = 1, \ldots, n-1$ czyli ponieważ $c_i - c_n \neq 0$ dla $i = 1, \ldots, n-1$, to z całkowitości pierścienia c_i muszą być pierwiastkami h. Muszą one też być pierwiastkami odpowiednio k_i krotnymi, gdyż $(X-c_n)^{k_n}$ nie zeruje się na c_i, co kończy dowód dzięki indukcji.

Jeśli teraz dla wielomianu f stopnia m i jego pierwiastków $c_1, \ldots, c_n$, zastosujemy omawianą wyżej własność i zapiszemy $f = (X-c_1)^{k_1} \cdot \ldots \cdot (X-c_n)^{k_n} \cdot g$, to dzięki całkowitości pierścienia zachodzi równość $m = \deg f \geqslant c_1 + \ldots + c_r$. Oznacza to, że liczba pierwiastków nie może przekroczyć stopnia (tak naprawdę, nawet liczona z krotnościami). □

Odnotujmy w tym momencie niezwykle istotne twierdzenie dotyczące pierwiastków wielomianów w ciele liczb zespolonych. **Odnośnik do dowodu, dowód ????**

Twierdzenie 5.3.3 (Zasadnicze twierdzenie algebry)**.** *W ciele liczb zespolonych dowolny pierwiastek wielomianu $f \in \mathbb{C}[X]$ stopnia $n \in \mathbb{N}$, ma dokładnie n pierwiastków liczonych z krotnościami.*

Definicja 5.3.4 (liniowy rozkład wielomianu)**.** Wielomian $f \in K[X]$ nazywamy **liniowo rozkładalnym** nad rozszerzeniem L ciała K, jeśli istnieją takie $a \in K$ oraz $u_1, \ldots, u_n \in L$, że $f = a(X-u_1)\ldots(X-u_n)$.

Definicja 5.3.5 (ciało rozkładu wielomianu)**.** Jeśli K jest ciałem oraz $f \in K[X]$, to ciało L nazywamy **ciałem rozkładu wielomianu f nad K**, gdy:

(1) wielomian f rozkłada się całkowicie nad ciałem L,

(2) f nie rozkłada się całkowicie nad żadnym właściwym podciałem L zawierającym K.

Własność 5.3.6. *Jeśli L/K jest rozszerzeniem ciał oraz wielomian $f \in K[X]$ rozkłada się liniowo nad L, to istnieje dokładnie jedno takie podciało M ciała L, że $K \subseteq M \subseteq L$ oraz M jest ciałem rozkładu f nad K.*

Dowód. Zgodnie z założeniem w $L[X]$ możemy zapisać $f = a(X-u_1)\ldots(X-u_n)$ dla pewnych $a \in K$ oraz $u_1, \ldots, u_n \in L$. Wystarczy teraz przyjąć $M = K(u_1, \ldots, u_n)$. □

Twierdzenie 5.3.7 (twierdzenie o istnieniu pierwiastka)**.** *Jeśli $f \in K[X]$ gdzie K – ciało jest wielomianem stopnia co najmniej 1, to istnieje L rozszerzenie ciała K oraz $u \in L$ takie, że $f(u) = 0$.*

Dowód. Ponieważ K jest ciałem, więc $K[X]$ jest dziedziną ideałów głównych, a tym samym pierścieniem faktorialnym (por. twierdzenie 4.8.11) co oznacza, że istnieje rozkład f na czynniki nierozkładalne w $K[X]$. Niech $g \in K[X]$ będzie jednym czynników występujących w rozkładzie. Zauważmy, że wystarczy znaleźć takie rozszerzenie L ciała K, że to g ma w nim pierwiastek.

Zauważmy, że w naszej sytuacji ideał $I = (g)$ jest maksymalny w $K[X]$ (por. twierdzenie 4.7.8). W takim razie $L = K[X]/I$ jest ciałem oraz

$$\imath \colon K \ni a \mapsto a + I \in L$$

jest monomorfizmem ciał, czyli ciało K możemy utożsamiać z podciałem ciała L. Jeśli teraz rozważymy element $u = X + I$, to otrzymamy

$$f(u) = f(X) + I = I = 0_{K[X]/I} = 0_L,$$

gdyż $f \in I$. W takim razie u jest pierwiastkiem wyjściowego wielomianu w rozszerzeniu L. □

Twierdzenie 5.3.8 (twierdzenie o istnieniu ciała rozkładu)**.** *Dowolny wielomian jednej zmiennej nad ciałem posiada ciało rozkładu.*

Dowód. Niech K będzie ciałem i niech $f \in K[X]$. Zauważmy najpierw, że dzięki własności 5.3.6 wystarczy znaleźć ciało, nad którym f rozkłada się liniowo. Jeśli $\deg f \leqslant 1$, to ciałem rozkładu f jest K, niech zatem $\deg f > 1$ – zastosujemy dalej rozumowanie indukcyjne. Jeśli dla wielomianu stopnia $(n-1)$ istnieje ciało rozkładu, to weźmy wielomian $f \in K[X]$ stopnia $n > 1$ – z twierdzenia o istnieniu pierwiastka istnieje rozszerzenie L ciała K oraz $u \in L$ takie, że $f(u) = 0$. Dzięki twierdzeniu Bézouta możemy wtedy zapisać $f = (X-u)g$ dla pewnego $g \in L[X]$, przy czym stopień g jest mniejszy od n. Stosując do g założenie indukcyjne otrzymujemy M – rozszerzenie ciała L (tym samym rozszerzenie ciała K) takie, że $g = a(X-u_2)\cdot\ldots\cdot(X-u_n)$ w $M[X]$, co daje też odpowiedni rozkład f. □

Co ciekawe, ciało rozkładu wielomianu jest jednoznacznie wyznaczone. Sformułujemy to twierdzenie poniżej, ale jego dowód przedstawimy w drugiej części skryptu (por. twierdzenie 12.1.2).

Twierdzenie 5.3.9 (o jednoznaczności ciała rozkładu)**.** *Jeśli K jest ciałem, to każde dwa ciała rozkładu wielomianu $f \in K[x]$ są K-izomorficzne.*

5.4 Ciała skończone

Dzięki poznanym własnościom ciał rozkładu możemy teraz uzupełnić nasze wiadomości dotyczące ciał skończonych. Do tej pory dowiedzieliśmy się jedynie, że dla ustalonej liczy pierwszej p jedynym ciałem jest ciało $\mathbb{F}_p$. Pora na zbadanie sytuacji ogólnej. Wiemy już, że każde ciało skończone ma p^n elementów dla pewnej liczby pierwszej p i $n \in \mathbb{N}$ (por. twierdzenie 5.1.12). Wykażemy teraz, że dla dowolnej liczby pierwszej p oraz $n > 0$, istnieje ciało p^n-elementowe i jest ono jedyne. Zaczniemy od prostej własności.

Własność 5.4.1. *Jeśli K jest ciałem charakterystyki $p > 0$, to dla dowolnego $n \in N$ odwzorowanie*

$$F_n \colon K \ni a \longrightarrow a^{p^n} \in K$$

jest monomorfizmem ciał.

Dowód. Widać, że odwzorowanie F_n jest n-krotnym złożeniem odwzorowania F_1, możemy zatem ograniczyć uwagę do $F = F_1$. Jeśli teraz $a, b \in K$, to mamy $F(0) = 0$, $F(1) = 1$ oraz $F(ab) = (ab)^p = a^p b^p = F(a)F(b)$. Mamy również

$$F(a+b) = (a+b)^p = a^p + \sum_{0<i<p} \binom{p}{i} a^i b^{p-i} + b^p = a^p + b^p = F(a) + F(b),$$

gdyż $p \mid \binom{p}{i}$ dla $0 < i < p$, co oznacza, że F jest monomorfizmem ciał. □

Wniosek 5.4.2. *Jeśli K jest ciałem charakterystyki $p > 0$, to dla dowolnych $n, k \in \mathbb{N}$ i elementów $a_1, \ldots, a_k \in K$ zachodzi równość*

$$\left(\sum_{i=1}^{k} a_i\right)^{p^n} = \sum_{i=1}^{k} a_i^{p^n}.$$

Jeśli K jest ciałem charakterystyki $p > 0$, to odwzorowanie $F = F_1$ z własnśoci 5.4.1 jest nazywane monomorfizmem Frobeniusa ciała K. Jeśli ciało K jest skończone, to monomorfizm ten jest automorfizmem ([12]).

Twierdzenie 5.4.3. *Jeśli K jest ciałem skończonym charakterystyki $p > 0$, to K ma $q = p^n$ elementów wtedy i tylko wtedy, gdy jest ciałem rozkładu wielomianu $X^q - X$ nad podciałem prostym ciała K.*

[12] Jeśli $f \colon X \to X$ jest injekcją (surjekcją) oraz $|X| < \infty$, to wtedy f jest bijekcją.

Dowód. Jeśli ciało K ma q elementów, to zauważmy, że grupa $(K^\star, \cdot)$ jest $q-1$ elementowa. Wobec tego, jeśli $a \in K^*$, to $|a| \mid q-1$, czyli $a^{q-1} = 1$. Ogólnie, dla dowolnego $a \in K$ mamy więc $a^q = a$. Innymi słowy wszystkie elementy ciała K są pierwiastkami wielomianu $X^q - X$. Z drugiej strony, wielomian ten nie ma więcej niż q pierwiastków, co oznacza, że pierwiastki wielomianu $X^q - X$ to dokładnie elementy ciała K. Stąd wniosek, że wielomian ten rozkłada się liniowo nad K i oczywiście nie rozkłada się liniowo w żadnym mniejszym podciele ciała K. Wobec tego K jest ciałem rozkładu naszego wielomianu.

Odwrotnie, niech K będzie ciałem rozkładu wielomianu $f = X^q - X$ nad $\mathbb{F}_p$. Jeśli określimy $\sigma\colon K \to K$ wzorem $\sigma(a) = a^q$ dla $a \in K$, to z własności 5.4.1 wiemy, że σ jest monomorfizmem. Co więcej element $a \in K$ jest pierwiastkiem f wtedy i tylko wtedy, gdy $\sigma(a) = a$, co oznacza, że pierwiastki wielomianu f tworzą podciało ciała K. Ponieważ K jest ciałem rozkładu wielomianu f, to musi to być całe ciało K (inaczej f rozkładałby w podciele właściwym K). Inaczej mówiąc, K złożone jest z pierwiastków wielomianu f. Ponadto pierwiastki te są parami różne, bo $f' = qX^{q-1} - 1 = -1 \neq 0$ i stąd wniosek, że K ma q elementów. □

Dzięki twierdzeniu 5.3.9 możemy sformułować następujący wniosek charakteryzujący ciała skończone.

Wniosek 5.4.4. *Dla dowolnej liczby pierwszej p oraz $n > 0$ istnieje ciało p^n-elementowe $\mathbb{F}_{p^n}$ ([13]). Ponadto dwa ciała skończone są izomorficzne wtedy i tylko wtedy, gdy mają tyle samo elementów.*

Przykład 5.4.5. Rozważmy wielomiany X^3+X+1 oraz X^3+X^2+1 w $\mathbb{F}_2[x]$ oba są wielomianami nierozkładalnymi. Wobec tego $\mathbb{F}_2[X]/(X^3+X+1)$ i $\mathbb{F}_2[X]/(X^3+X^2+1)$ są ciałami 8-elementowymi. Zgodnie z wnioskiem 5.4.4 są to ciała izomorficzne.

Wniosek 5.4.6. *Dla dowolnego $r \in \mathbb{N}$ istnieje nierozkładalny wielomian $f \in \mathbb{F}[X]$ stopnia r.*

Dowód. Niech F będzie ciałem, które ma p^r elementów. Z twierdzenia 5.4.3 wynika, że F jest izomorficzne z ciałem $\mathbb{F}_p[X]/(f(X))$, gdzie $f \in \mathbb{F}_p[X]$ jest nierozkładalny. Ponieważ $\#\mathbb{F}_p[X]/(f(X))$ ma dokładnie p^r elementów, więc stopień f wynosi r. □

W świetle powyższej obserwacji pojawiają się dwa pytania: (i) jak szukać nierozkładalnego wielomianu f stopnia r; oraz (ii) jak dużo jest takich wielomianów?

Twierdzenie 5.4.7. *Wielomian $F = X^{p^n} - X$ jest iloczynem wszystkich wielomianów nierozkładalanych, których stopnie dzielą n.*

Dowód. Niech $f \in \mathbb{F}_p[X]$ będzi wielomianem nierozkładalnym stopnia n i rozważmy ciało $K = \mathbb{F}_p[\alpha]$, gdzie α jest jakimś pierwiastkiem wielomianu f. Wiemy, że ciało K jest izomorifczne z $\mathbb{F}_p[X]/(f(X))$. W szczególności $\#K = p^n$. Jeśli $g \in \mathbb{F}_p[X]$ jest taki, że $g(\alpha) = 0$, to z minimalności f wynika, że f dzieli wielomian g. Jednocześnie, z twierdzenia 5.4.3 wynika, że każdy element ciała K jest pierwiastkiem wielomianu F. W szczególności, wielomian F jest podzielny przez wielomian f. Zauważmy, że jeśli f jest takie, że $\deg f = d$ oraz $d|n$, to zachodzi analogiczna własność. Istotnie, skoro $d|n$, to $n = ed$ dla pewnego $e \in \mathbb{N}$ z faktu, że $f(\alpha) = 0$ oraz $\alpha^{p^d} = \alpha$ wynika, że $\alpha^{p^n} = \alpha$ i α jest pierwiastkiem wielomianu F.

By dokończyć dowód wystarczy pokazać, że nie istnieje wielomian nierozkładalanych $f \in \mathbb{F}_p[X]$ stopnia $> n$, który dzieli F. Dla dowodu nie wprost załóżmy, że taki wielomian istnieje. Dokładniej, $f \in \mathbb{F}_p[X]$ jest nierozkładalny, $\deg f = m > n$ oraz $f|F$. Niech $K = \mathbb{F}_p[X]/(f(X))$. Możemy napisać

$$K = \{q(\alpha) :\ q \in \mathbb{F}_p[X], \deg q \leqslant s-1\},$$

gdzie α jest pierwiastkiem wielomianu f. Jeśli $q(\alpha) = \sum_{i=0}^{s-1} a_i\alpha^i$ reprezentuje element ciała K, to w wniosku 5.4.2 otrzymujemy

$$q(\alpha)^{p^n} = \sum_{i=0}^{s-1} a_i^{p^n}\alpha^{ip^n} = \sum_{i=0}^{s-1} a_i\alpha^{ip^n}.$$

Z założenia $f|F$, więc $F(\alpha) = 0$, czyli $\alpha^{p^n} = \alpha$ i w konsekwencji $q(\alpha)^{pn} = q(\alpha^{pn}) = q(\alpha)$. Oznacza to, że każdy elment ciała K jest zerem wielomianu F i otrzymujemy, że wielomian F ma p^m różnych pierwiastków. Sprzeczność, bo $p^m > p^n = \deg F$. □

[13] Ciało to bywa też nazywane p^n-elementowym ciałem Galois i oznaczane $\mathbb{GF}(p^n)$.

Przykład 5.4.8. Można pokazać, że dla $n = 1, \ldots, 5$, rozkład w $\mathbb{F}_2[X]$ wielomianu $F_n = X^{2^n} - X$ na iloczyn wielomianów nierozkłalanych ma postać

$$\begin{aligned}
F_1 &= X(X+1),\\
F_2 &= X(X+1)\left(X^2+X+1\right),\\
F_3 &= X(X+1)\left(X^3+X+1\right)\left(X^3+X^2+1\right),\\
F_4 &= X(X+1)\left(X^2+X+1\right)\left(X^4+X+1\right)\left(X^4+X^3+1\right)\left(X^4+X^3+X^2+X+1\right),\\
F_5 &= X(X+1)\left(X^5+X^2+1\right)\left(X^5+X^3+1\right)\left(X^5+X^3+X^2+X+1\right)\\
&\quad \left(X^5+X^4+X^2+X+1\right)\left(X^5+X^4+X^3+X+1\right)\left(X^5+X^4+X^3+X^2+1\right)
\end{aligned}$$

Naszym celem jest wyznaczenie jawnego wzoru na liczbę wielomianów nierozkładalnych w $\mathbb{F}_p[X]$, które mają stopnień d. Dokładniej, oznaczmy

$$\mathrm{Ir}_p(d) = \#\{f \in \mathbb{F}_p[X] : \ f \ \text{ nierozkładalny stopnia } \ d\}.$$

Zanim otrzymamy wzór na $\mathrm{Ir}_p(d)$ będziemy potrzebować kilku pojęć i rezultatów dotyczących funkcji multiplikatywnych [2, Chapter 2].

Definicja 5.4.9 (Funkcja multiplikatywna)**.** Powiemy, że funkcja $h : \mathbb{N} \to \mathbb{C}$ jest multiplikatywną, gdy spełnia następujący warunek:

$$\forall a, b \in \mathbb{N} : \ \mathrm{NWD}(a,b) = 1 \implies h(ab) = h(a)h(b).$$

Definicja 5.4.10 (Funkcja Möbiusa)**.** Niech $n \in \mathbb{N}_+$ i napiszmy $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, gdzie $p_1, \ldots, p_k$ są różnymi liczbami pierwszymi. Funkcję $\mu(n)$ nazywamy funkcją μ Möbiusa i definiujemy jako

$$\mu(n) = \begin{cases} 1 & n = 1,\\ (-1)^k & \alpha_1 = \ldots = \alpha_k = 1,\\ 0 & \text{w przeciwnym przypadku.} \end{cases}$$

Funkcja Möbiusa jest funkcją multiplikatywną. Istotnie, jeśli $\mathrm{NWD}(m,n) = 1$ i $\mu(mn) = 0$, to istnieje $p \in \mathbb{P}$, że $p^2 | n$ lub $p^2 | m$. Stąd $\mu(m)\mu(n) = 0$. Jeśli teraz $m = p_1 \cdot \ldots \cdot p_i, n = q_1 \cdot \ldots \cdot q_j$ i stąd

$$\mu(mn) = (-1)^{i+j} = (-1)^i \cdot (-1)^j = \mu(m)\mu(n).$$

Lemat 5.4.11. *Niech $I(m) = \lfloor \frac{1}{m} \rfloor$. Dla $n \in \mathbb{N}_+$ prawdziwa jest równość*

$$\sum_{d|n} \mu(d) = I(n).$$

Dowód. Teza zachodzi dla $n = 1$. Skoro $n > 1$, to możemy napisać $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$. Jeśli $d|n$ i d jest podzielne przez kwadrat liczby pierwszej, to oczywiście $\mu(d) = 0$. Możemy zatem napisać

$$\begin{aligned}
\sum_{d|n} \mu(d) &= 1 + \sum_{i=1}^{k} \mu(p_i) + \sum_{1 \leqslant i_1 < i_2 \leqslant k} \mu(p_{i_1} p_{i_2}) + \ldots + \mu(p_1 \cdot \ldots \cdot p_k)\\
&= \sum_{i=0}^{k} \binom{k}{i} (-1)^i = (1-1)^k = 0.
\end{aligned}$$

□

Definicja 5.4.12 (Splot Dirichleta)**.** Niech $h_1, h_2 : \mathbb{N} \to \mathbb{C}$. Funkcję $h : \mathbb{N}_+ \to \mathbb{C}$ zdefiniowaną jako

$$h(n) = \sum_{d|n} h_1(d) h_2\left(\frac{n}{d}\right)$$

nazywamy splotem Dirichleta funkcji h_1, h_2 i oznaczamy przez $h = h_1 * h_2$.

Zauważmy również, że dla splotu funkcji h_1, h_2 możemy alternatywnie napisać

$$(h_1 * h_2)(n) = \sum_{ab=n} h_1(a)h_2(b).$$

Splot Dirichleta jest ciekawym i użytecznym przykładem działania w zbiorze funkcji arytmetycznych $\mathcal{A} := \{h : h : \mathbb{N} \to \mathbb{C}\}$.

Twierdzenie 5.4.13. *Splot Dirichleta jest działaniem w zbiorze $\mathcal{A}$. Splot Dirichleta jest łączny i przemienny, zaś elementem neutralnym względem splotu Dirichleta jest funkcja I.*

Dowód. Pierwsza część tezy jest oczywista. Mamy również, że

$$(h_1 * h_2)(n) = \sum_{ab=n} h_1(a)h_2(b) = \sum_{ab=n} h_2(a)h_1(b) = (h_2 * h_1)(n),$$

co oznacza, że $*$ jest działaniem przemiennym.

Niech $h_1, h_2, h_3 \in \mathcal{A}$. By dowieść łączności zauważmy, że prawdziwa jest równość

$$\begin{aligned}(h_1 * (h_2 * h_3))(n) &= \sum_{ab=n} h_1(a)(h_2 * h_3)(b) \\ &= \sum_{ab=n} h_1(a) \sum_{cd=b} h_2(c)h_3(d) = \sum_{acd=n} h_1(a)h_2(c)h_3(d).\end{aligned}$$

Rozpisując $((h_1 * h_2) * h_3)(n)$ w analogiczny sposób dostajemy równość $h_1 * (h_2 * h_3) = (h_1 * h_2) * h_3$.

W końcu, mamy, że

$$(h * I)(n) = \sum_{d|n} h(d)I\left(\frac{n}{d}\right) = \sum_{d|n} h(d)\left\lfloor \frac{d}{n} \right\rfloor = h(n)$$

i dostajemy tezę. □

Twierdzenie 5.4.14. *Jeśli h_1, h_2 są funkcjami multiplikatywnymi, to $h_1 * h_2$ również jest funkcją multiplikatywną.*

Dowód. Niech $h = h_1 * h_2$ i $m, n \in \mathbb{N}_+$ spełniają warunek $\mathrm{NWD}(m, n) = 1$. Wówczas

$$h(mn) = \sum_{c|mn} h_1(c)h_2\left(\frac{mn}{c}\right).$$

Skoro $\mathrm{NWD}(m, n) = 1$ i $c|mn$, więc $c = ab$ dla pewnych $a, b \in \mathbb{N}_+$ spełniających warunki: $\mathrm{NWD}(a, b) = 1, a|m, b|n$ oraz $\mathrm{NWD}\left(\frac{m}{a}, \frac{n}{b}\right) = 1$. Stąd

$$\begin{aligned}h(mn) &= \sum_{c|mn} h_1(c)h_2\left(\frac{mn}{c}\right) = \sum_{a|m,b|n} h_1(ab)h_2\left(\frac{mn}{ab}\right) \\ &= \sum_{a|m,b|n} h_1(a)h_1(b)h_2\left(\frac{m}{a}\right)h_2\left(\frac{n}{b}\right) \\ &= \left(\sum_{a|m} h_1(a)h_2\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} h_1(b)h_2\left(\frac{n}{b}\right)\right) = h(m)h(n).\end{aligned}$$

□

Zauważmy, że jeśli $u(n) = 1$, to $\mu * u = I$. Ta prosta obserwacja, która jest konsekwencją lematu 5.4.11 umożliwia nam wykazanie następującego.

Twierdzenie 5.4.15 (Formuła inwersyjna Möbiusa)**.** *Niech $h_1, h_2 \in \mathcal{A}$. Wówczas*

$$h_1(n) = \sum_{d|n} h_2(d) \iff h_2(n) = \sum_{d|n} h_1(d)\mu\left(\frac{n}{d}\right).$$

Dowód. ($\Longrightarrow$) Mnożąc (w sensie splotu Dirichleta) równość $h_1 = h_2 * u$ z prawej strony przez μ otrzymujemy

$$h_1 * \mu = (h_2 * u) * \mu = h_2 * (u * \mu) = h_2 * I = h_2$$

i dostajemy tezę. Analogicznie, z równości $h_2 = h_1 * \mu$, po przemnożeniu z prawej strony przez u oraz skorzystaniu z łączności splotu Dirichleta, dostajemy $u * h_2 = h_1$. □

Jesteśmy gotowi by udowodnić następujące.

Twierdzenie 5.4.16. *Dla dowolnego $n \in \mathbb{N}$ zachodzi równość*

$$\mathrm{Ir}_p(n) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d.$$

Dowód. Z twierdzenia 5.4.7 wynika, że

$$\sum_{d|n} \mathrm{Ir}_p(d) d = p^n.$$

Równoważnie $(\mathrm{Ir}_p * N)(n) = p^n$, gdzie $N(n) = n$. Stosując teraz formułę inwersyjną Möbiusa otrzymujemy równość $n \,\mathrm{Ir}_p(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) p^d$ i dzieląc przez n dostajemy tezę. □

Zilustrujmy nasz rezultat pokazując liczbę wielomianów nierozkładalnych wielomianów monicznych stopnia n dla $p = 2, 3, 5$ oraz $n = 1, \ldots, 10$.

n	1	2	3	4	5	6	7	8	9	10
$p = 2$	2	1	2	3	6	9	18	30	56	99
p^n	2	4	8	16	32	64	128	256	512	1024
$p = 3$	3	3	8	18	48	116	312	810	2184	5880
p^n	3	9	27	81	243	729	2187	6561	19683	59049
$p = 5$	5	10	40	150	624	2580	11160	48750	217000	976248
p^n	5	25	125	625	3125	15625	78125	390625	1953125	9765625
$p = 7$	7	21	112	588	3360	19544	117648	720300	4483696	28245840
p^n	7	49	343	2401	16807	117649	823543	5764801	40353607	282475249

Tabela. Liczba $\mathrm{Ir}_p(n)$ monicznych wielomianów nierozkładlanych stopnia n versus liczba wielomianów stopnia n w $\mathbb{F}_p[X]$, dla $p = 2, 3, 5, 7$ oraz $n \leqslant 10$.

5.5 Zadania

1. Zbadać, które z poniższych zbiorów ze standardowymi działaniami dodawania i mnożenia są ciałami:
   (a) $A = \{a + b\sqrt{2} : \ a, b \in \mathbb{Q}\}$,
   (b) $A = \{a + b\sqrt{2} + c\sqrt{3} : \ a, b, c \in \mathbb{Q}\}$,
   (c) $A = \{a + b2^{1/n} : \ a, b \in \mathbb{Q}\}, n \geqslant 3$,
   (d) $A = \mathbb{Z}[X]/(X^2 + 1)$,
   (e) $A = \mathbb{Q}[X, Y]/(X, Y)$.
2. Wyznaczyć element odwrotny do $x \in K$, gdzie
   (a) $x = 1 + \sqrt{3}$, $K = \mathbb{Q}(\sqrt{3})$,
   (b) $x = 1 + 3^{1/3} + 3^{2/3}$, $K = \mathbb{Q}(3^{1/3})$,
   (c) $x = 1 + i$, $K = \mathbb{Q}(i, \sqrt{2})$.
   (d) $x = 1 + \sqrt{2} + \sqrt{3}$, $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
3. Wypisać tabelkę działania w ciele $\mathbb{F}_2(\alpha)$, gdzie $f(\alpha) = 0$ oraz:
   (a) $f = X^2 + X + 1$,
   (b) $f = X^3 + X + 1$.
4. Niech $a, b \in \mathbb{Z}$ i załóżmy, że a, b nie są kwadratami. Pokazać, że $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}(\sqrt{b})$ wtedy i tylko wtedy, gdy ab jest kwadratem w $\mathbb{Q}$.
5. Podać przykład ciał skończonych K_1, K_2, K_3, K_4, które mają 4, 8, 9, 16 elementów, odpowiednio.
6. Wyznaczyć wielomiany minimalne (nad $\mathbb{Q}$) dla $1 + \sqrt{2}$, $1 + \sqrt{2} + \sqrt{3}$, $i + \sqrt{2}$, $3^{1/3} + 1$, $i - \sqrt{-2}$.

7. Znaleźć te elementy $a \in \mathbb{Z}_5$, dla których pierścień ilorazowy $\mathbb{Z}_5[X]/(X^3 + 2X^2 + aX + 3)$ jest ciałem.

8. Udowodnić, że pierścień $P = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$ z działaniami dodawania i mnożenia macierzy jest ciałem izomorficznym z $\mathbb{C}$.

9. Niech d będzie liczbą bezkwadratową. Wykazać, że

$$R = \left\{ \begin{pmatrix} a & b \\ db & a \end{pmatrix} : \ a, b \in \mathbb{R} \right\}$$

z działaniami mnożenia i dodawania macierzy, jest pierścieniem izomorficznym z ciałem $\mathbb{Z}[\sqrt{d}]$.

10. Znaleźć stopień rozszerzenia ciał L/K.

    (a) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}$,
    (b) $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, $K = \mathbb{Q}(\sqrt{2})$.

11. Niech $K_1 < K_2 < K_3 < K_4$ będą parami różnymi ciałami, dla których $[K_3 : K_1] = 6$ oraz $[K_4 : K_2] = 15$. Wyznaczyć $[K_2 : K_1]$, $[K_3 : K_2]$ oraz $[K_4 : K_3]$.

12. Niech $L = \mathbb{Q}(i, \sqrt{p})$, gdzie $p \in \mathbb{P}$. Wyznaczyć bazę oraz stopień rozszerznia L/K_i, gdzie $K_1 = \mathbb{Q}$, $K_2 = \mathbb{Q}(i)$, $K_3 = \mathbb{Q}(\sqrt{p})$, $K_4 = \mathbb{Q}(i + \sqrt{p})$.

13. Pokazać, że jedynymi podciałami ciała $\mathbb{Q}(\sqrt{p})$, gdzie $p \in \mathbb{N}$ nie jest kwadartem, są $\mathbb{Q}, \mathbb{Q}(\sqrt{p})$.

14. Wyznaczyć ciał rozkładu wielomianu $f \in \mathbb{Q}[X]$ nad ciałem L, gdzie:

    (a) $f = X^4 + 1$, $L = \mathbb{Q}$;
    (b) $f = X^4 + 1$, $L = \mathbb{Q}(i)$;
    (c) $f = X^4 + 4$, $L = \mathbb{Q}$;
    (d) $f = X^4 + 4$, $L = \mathbb{Q}(\sqrt{2})$;
    (e) $f = X^6 + X^3 + 1$, $L = \mathbb{Q}$;
    (f) $f = X^6 + X^3 + 1$, $L = \mathbb{Q}(i\sqrt{3})$.

Rozdział 6

Twierdzenie o istnieniu pierwiastków prymitywnych w $\mathbb{Z}_m^*$

6.1 Podstawowe własności rzędu

Definicja 6.1.1 (rząd elementu modulo m)**.** Niech $m \in \mathbb{N}_{\geqslant 2}, a \in \mathbb{Z}$ i załóżmy, że $\mathrm{NWD}(a,m) = 1$. Liczbę

$$\mathrm{ord}_m(a) := \min\{k \in \mathbb{N} : \ a^k \equiv 1 \ (\mathrm{mod}\ m)\}$$

nazywamy **rzędem** a **modulo** m**.**

Uwaga 6.1.2. Z twierdzenia Eulera (por. 1.6.4) wiemy, że przy powyższych założeniach dotyczących m i a, spełniona jest kongruencja $a^{\varphi(m)} \equiv 1 \ (\mathrm{mod}\ m)$. Oznacza to, że rząd elementu a modulo m jest poprawnie określony (bierzemy minimum po zbiorze niepustym) oraz zachodzi nierówność $\mathrm{ord}_m(a) \leqslant \varphi(m)$. Warto też zauważyć, że rząd elementu a modulo m jest dokładnie rzędem a jako elementu w grupie $U(\mathbb{Z}_m)$ (por. 3.1.5 (4)).

Przykład 6.1.3. Niech $m = 14$. Mamy $\{a \in \{1,\dots,14\} : (a,12) = 1\} = \{1,3,5,9,11,13\}$. Bezpośrednie sprawdzenie pokazuje, że:

$$\mathrm{ord}_{14}(1) = 1, \quad \mathrm{ord}_{14}(3) = \mathrm{ord}_{14}(5) = 6, \quad \mathrm{ord}_{14}(9) = \mathrm{ord}_{14}(11) = 3, \quad \mathrm{ord}_{14}(13) = 2.$$

Twierdzenie 6.1.4 (własności rzędu)**.** *Niech* $m \in \mathbb{N}_{\geqslant 2}$*,* $a,b,k,k_1,k_2 \in \mathbb{Z}$*, gdzie* $\mathrm{NWD}(ab,m) = 1$*. Wówczas:*

(1) jeśli $a^k \equiv 1 \ (\mathrm{mod}\ m)$*, to* $\mathrm{ord}_m(a) | k$ *– w szczególności* $\mathrm{ord}_m(a) | \varphi(m)$*,*

(2) jeśli $a^{k_1} \equiv a^{k_2} \ (\mathrm{mod}\ m)$*, to* $k_1 \equiv k_2 \ (\mathrm{mod}\ \mathrm{ord}_m(a))$*,*

(3) jeśli $\mathrm{NWD}(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$*, to* $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a)\,\mathrm{ord}_m(b)$*,*

(4) $\mathrm{ord}_m(a^k) = \mathrm{ord}_m(a)/(k, \mathrm{ord}_m(a))$*.*

Dowód. (1) Niech $t = \mathrm{ord}_m(a)$. Z twierdzenia o dzieleniu z resztą wiemy, że istnieją liczby $q,r \in \mathbb{N}_0$ spełniające warunki: $k = qt + r$ i $r < t$. Z założenia o k mamy

$$1 \equiv a^k \equiv a^{qt+r} \equiv (a^t)^q a^r \equiv a^r \ (\mathrm{mod}\ m).$$

Ponieważ $r < t$, więc z minimalności t mamy $r = 0$ i tym samym $k = qt$, co oznacza, że $t|k$. Biorąc w szczególności $k = \varphi(m)$, na podstawie 1.6.4, dostajemy pierwszą część tezy.

(2) Mnożąc kongruencję $a^{k_1} \equiv a^{k_2} \ (\mathrm{mod}\ m)$ stronami przez $(a^{-1})^{k_2}$ (gdzie a^{-1} oznacza odwrotność a modulo m, czyli jedyne rozwiązanie kongruencji liniowej $ax \equiv 1 \ (\mathrm{mod}\ m)$), otrzymujemy że $a^{k_1-k_2} \equiv 1 \ (\mathrm{mod}\ m)$ i punkt (1) daje tezę.

Zauważmy w tym momencie, że pierwsze dwa punkty wynikają też niezależnie od naszego dowodu z własności 3.3.9 zastosowanych do grupy $U(\mathbb{Z}_m)$.

(3) Niech $t_1 = \mathrm{ord}_m(a), t_2 = \mathrm{ord}_m(b)$ oraz połóżmy $t = \mathrm{ord}_m(ab)$. Zauważmy, że $t_1 | t \cdot t_2$. Istotnie

$$a^{t\cdot t_2} \equiv a^{t\cdot t_2}(b^{t_2})^t \equiv a^{t\cdot t_2} b^{t\cdot t_2} \equiv (ab)^{t\cdot t_2} \equiv ((ab)^t)^{t_2} \equiv 1 \ (\mathrm{mod}\ m).$$

W analogiczny sposób dowodzimy, że $t_2|t\cdot t_1$. Ponieważ $\mathrm{NWD}(t_1,t_2)=1$, więc z uzyskanych podzielności wnioskujemy, że $t_1|t$ oraz $t_2|t$, co oznacza że $t_1t_2|t$. Z drugiej strony mamy

$$(ab)^{t_1t_2}\equiv (a^{t_1})^{t_2}(b^{t_2})^{t_1}\equiv 1 \pmod m.$$

Oznacza to, że $t|t_1t_2$. W konsekwencji naszych rozważań dostajemy $t=t_1t_2$, co było do wykazania.

(4) Niech $h=\mathrm{ord}_m(a)$, $t=\mathrm{ord}_m(a^k)$ i $d=\mathrm{NWD}(k,h)$ – wtedy $a^{tk}\equiv 1 \pmod m$ co implikuje, że $h|tk$. Niech teraz $h_1=h/d$ i $k_1=k/d$. Z określenia h_1,k_1 wynika, że $\mathrm{NWD}(h_1,k_1)=1$. Ponieważ $h|tk$, więc $h_1d|tk_1d$. Stąd $h_1|tk_1$ i dostajemy, że $h_1|t$. Z drugiej strony mamy, że

$$(a^k)^{h_1}\equiv a^{kh_1}\equiv a^{k_1dh_1}=(a^{dh_1})^{k_1}\equiv 1 \pmod m.$$

Oznacza to, że $t|h_1$ i w konsekwencji $t=h_1=h/d=\mathrm{ord}_m(a)/\mathrm{NWD}(k,\mathrm{ord}_m(a))$. □

Definicja 6.1.5 (pierwiastek prymitywny)**.** Niech $m\in\mathbb{N}_{\geqslant 2}$. Liczbę $a\in\mathbb{Z}$ nazywamy **pierwiastkiem prymitywnym modulo** m (inaczej: dla m), gdy $\mathrm{ord}_m(a)=\varphi(m)$.

Jako natychmiastowy wniosek z twierdzenia 6.1.4 otrzymujemy następujący:

Wniosek 6.1.6. *Niech g będzie pierwiastkiem prymitywnym dla m i $k\in\mathbb{N}$. Wówczas g^k jest pierwiastkiem prymitywnym dla m wtedy i tylko wtedy, gdy $(k,\varphi(m))=1$.*

Dowód. Ponieważ g jest pierwiastkiem prymitywnym modulo m, więc $\mathrm{ord}_m(g)=\varphi(m)$. Z twierdzenia 6.1.4 (4) dostajemy, że

$$\mathrm{ord}_m(g^k)=\frac{\varphi(m)}{\mathrm{NWD}(k,\varphi(m))},\quad \text{czyli}\quad \mathrm{ord}_m(g^k)=\varphi(m)\iff \mathrm{NWD}(k,\varphi(m))=1,$$

co kończy dowód. □

Wniosek 6.1.7. *Jeśli $m\in\mathbb{N}_{\geqslant 2}$ ma pierwiastek prymitywny, to ma ich dokładnie $\varphi(\varphi(m))$.*

Dowód. Niech g będzie pierwiastkiem prymitywnym dla m. Z definicji oznacza to, że

$$A_m:=\{g^i \pmod m:\ i\in\{0,\dots,\varphi(m)-1\}\}=\{a\in\{1,\dots,m\}:\ \mathrm{NWD}(a,m)=1\},$$

czyli $\#A_m=\varphi(m)$. Zgodnie z poprzednią własnością g^k, gdzie $k\in\{0,\dots,\phi(m)-1\}$, jest pierwiastkiem prymitywnym dla m wtedy i tylko wtedy, gdy $\mathrm{NWD}(k,\varphi(m))=1$. Oznacza to, że mamy $\varphi(\varphi(m))$ pierwiastków prymitywnych dla m, gdyż jest dokładnie $\varphi(\#A_m)=\varphi(\varphi(m))$ liczb k, które są względnie pierwsze z $\varphi(m)$. □

Uwaga 6.1.8. Nie każda liczba $m\in\mathbb{N}_{\geqslant 2}$ ma pierwiastek prymitywny. Przykładowo, jeśli $m=8$, to $\varphi(8)=4$, ale

$$\mathrm{ord}_8(1)=1,\quad \mathrm{ord}_8(3)=\mathrm{ord}_8(5)=\mathrm{ord}_8(7)=2.$$

Oznacza to, że liczba 8 nie ma pierwiastka prymitywnego.

Zauważmy, że liczba $m=14$ ma dwa pierwiastki prymitywne: $g=3$ i $g=5$.

6.2 Problem istnienia pierwiastka prymitywnego

W tym rozdziale udowodnimy, że każda liczba pierwsza posiada pierwiastek prymitywny. By to zrobić najpierw uzasadnimy bezpośrednio twierdzenie, które można też uznać za konsekwencję własności 5.3.2 zastosowanej do wielomianu stopnia n o współczynnikach w ciele $\mathbb{Z}_p$.

Twierdzenie 6.2.1 (Lagrange)**.** *Niech $p\in\mathbb{P}$, $f=\sum_{i=0}^{n}a_iX^i\in\mathbb{Z}_p[X]$, $n\in\mathbb{N}$, gdzie $p\nmid a_n$. Wówczas kongruencja*

$$f(x)\equiv 0 \pmod p \tag{6.1}$$

ma co najwyżej n rozwiązań w $\mathbb{Z}_p$.

Dowód. Zastosujemy indukcję względem n. Dla $n = 1$ rozważamy kongruencję $a_1x+a_0 \equiv 0 \pmod p$, gdzie z założenia $\mathrm{NWD}(p, a_1) = 1$ Na podstawie 1.4.6 wiemy, że wówczas istnieje dokładnie jedno rozwiązanie modulo p.

Załóżmy teraz, że teza zachodzi dla wszystkich wielomianów stopnia $\leqslant n-1$ i $f = \sum_{i=0}^{n} a_iX^i \in \mathbb{Z}_p[X]$, gdzie $p \nmid a_n$. Jeśli (6.1) nie ma pierwiastka w $\mathbb{Z}_p$, to teza jest spełniona. Niech zatem $x_0 \in \mathbb{Z}_p$ będzie pierwiastkiem kongruencji (6.1). Mamy wówczas

$$f(X) = f(X) - f(x_0) = \sum_{i=0}^{n} a_i(X^i - x_0^i) = (X - x_0)g(X),$$

gdzie $g \in \mathbb{Z}_p[X]$ jest wielomianem stopnia $n-1$, którego współczynnikiem wiodącym jest a_n. Z założenia indukcyjnego kongruencja $g(x) \equiv 0 \pmod p$ ma co najwyżej $n-1$ rozwiązań, a w konsekwencji kongruencja (6.1) ma co najwyżej $(n-1)+1 = n$ rozwiązań. □

Przykład 6.2.2. Warto zauważyć, że powyższe twierdzenie, choć bardzo proste, jest optymalne. Dokładniej, jeśli $p \in \mathbb{P}$, to kongruencja $x^p - x \equiv 0 \pmod p$ ma dokładnie p rozwiązań w $\mathbb{Z}_p$. Innymi słowy, każdy element $a \in \mathbb{Z}_p$ jest pierwiastkiem wielomianu $X^p - X \in \mathbb{Z}_p[X]$. Własność ta jest natychmiastową konsekwencją małego twierdzenia Fermata.

Warto również zwrócić uwagę na to, że dla dowolnego $a \in \{1, \ldots, p-1\}$, wielomian $g = X^p - X - a \in \mathbb{Z}_p[X]$ stopnia p, nie ma pierwiastków w $\mathbb{Z}_p$.

Twierdzenie 6.2.3. *Niech $p \in \mathbb{P}, f = \sum_{i=0}^{n} a_iX^i \in \mathbb{Z}_p[X], n \leqslant p$, gdzie $p \nmid a_n$. Wówczas kongruencja (6.1) ma dokładnie n rozwiązań wtedy i tylko wtedy, gdy $f|(X^p - X)$.*

Dowód. Z małego twierdzenia Fermata mamy, że dla dowolnego $x \in \mathbb{Z}$ zachodzi

$$x^p - x \equiv x(x-1) \cdot \ldots \cdot (x-(p-1)) \pmod p.$$

Niech teraz $x_1, \ldots, x_k \in \mathbb{Z}_p$ będą (różnymi modulo p) pierwiastkami wielomianu f. Możemy zatem napisać

$$f = (X - x_1)(X - x_2) \cdot \ldots \cdot (X - x_k)g,$$

gdzie wielomian g nie ma pierwiastków w $\mathbb{Z}_p$. Mamy zatem, że

$$\mathrm{NWD}(f, X^p - X) = (X - x_1) \cdot \ldots \cdot (X - x_k).$$

Widzimy więc, że $k = n$ wtedy i tylko wtedy, gdy $(f, X^p - X) = f$, co oznacza, że $f|(X^p - X)$. □

Lemat 6.2.4. *Niech $p \in \mathbb{P}$. Jeśli $t \in \mathbb{N}$ spełnia warunek $t|(p-1)$, to liczba takich $a \in \{1, \ldots, p-1\}$, dla których $\mathrm{ord}_p(a) = t$ jest równa 0 lub $\varphi(t)$.*

Dowód. Niech $t|(p-1), a \in \{1, \ldots, p-1\}$ i załóżmy, że $\mathrm{ord}_p(a) = t$. Wówczas kongruencja $x^t \equiv 1 \pmod p$ ma dokładnie t rozwiązań $a, a^2, \ldots, a^t$ i z twierdzenia 6.2.1 wiemy, że są to wszystkie rozwiązania. W szczególności oznacza to, że każdy element, który ma rząd t, jest kongruentny z a^i dla pewnego $i \in \{1, \ldots, t\}$. Dodatkowo, $\mathrm{ord}_p(a^k) = t$ wtedy i tylko wtedy, gdy $\mathrm{NWD}(k, t) = 1$ – takich liczb jest dokładnie $\varphi(t)$. □

Twierdzenie 6.2.5 (istnienie pierwiastka prymitywnego dla liczby pierwszej)**.** *Niech $p \in \mathbb{P}, t \in \mathbb{N}_+$ i załóżmy, że $t|(p-1)$. Wtedy liczba tych $a \in \{1, \ldots, p-1\}$, dla których $\mathrm{ord}_p(a) = t$, wynosi dokładnie $\varphi(t)$. Oznacza to w szczególności, że jest dokładnie $\varphi(p-1)$ pierwiastków prymitywnych dla p.*

Dowód. Dla $t|(p-1)$ przez $\psi(t)$ oznaczmy liczbę tych elementów zbioru $\{1, \ldots, p-1\}$, które są rzędu t. Ponieważ każdy element zbioru $\{1, \ldots, p-1\}$ ma dokładnie określony rząd, więc prawdziwa jest równość (por. 1.5.5):

$$\sum_{t|p-1} \psi(t) = p - 1 = \sum_{t|p-1} \varphi(t).$$

Z lematu 6.2.4 wiemy, że $\psi(t) \in \{0, \varphi(t)\}$ co oznacza, że $\psi(t) \leqslant \varphi(t)$. Powyższa równość implikuje, że musi być $\psi(t) = \varphi(t)$ dla każdego $t|(p-1)$. □

W tabeli poniżej prezentujemy zbiory pierwiastków prymitywnych dla początkowych 20 nieparzystych liczb pierwszych.

p	$\phi(p-1)$	pierwiastki prymitywne dla p
3	1	2
5	2	2, 3
7	2	3, 5
11	4	2, 6, 7, 8
13	4	2, 6, 7, 11
17	8	3, 5, 6, 7, 10, 11, 12, 14
19	6	2, 3, 10, 13, 14, 15
23	10	5, 7, 10, 11, 14, 15, 17, 19, 20, 21
29	12	2, 3, 8, 10, 11, 14, 15, 18, 19, 21, 26, 27
31	8	3, 11, 12, 13, 17, 21, 22, 24
37	12	2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35
41	16	6, 7, 11, 12, 13, 15, 17, 19, 22, 24, 26, 28, 29, 30, 34, 35
43	12	3, 5, 12, 18, 19, 20, 26, 28, 29, 30, 33, 34
47	22	5, 10, 11, 13, 15, 19, 20, 22, 23, 26, 29, 30, 31, 33, 35, 38, 39, 40, 41, 43, 44, 45
53	24	2, 3, 5, 8, 12, 14, 18, 19, 20, 21, 22, 26, 27, 31, 32, 33, 34, 35, 39, 41, 45, 48, 50, 51
59	28	2, 6, 8, 10, 11, 13, 14, 18, 23, 24, 30, 31, 32, 33, 34, 37, 38, 39, 40, 42, 43, 44, 47, 50, 52, 54, 55, 56
61	16	2, 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59
67	20	2, 7, 11, 12, 13, 18, 20, 28, 31, 32, 34, 41, 44, 46, 48, 50, 51, 57, 61, 63
71	24	7, 11, 13, 21, 22, 28, 31, 33, 35, 42, 44, 47, 52, 53, 55, 56, 59, 61, 62, 63, 65, 67, 68, 69
73	24	5, 11, 13, 14, 15, 20, 26, 28, 29, 31, 33, 34, 39, 40, 42, 44, 45, 47, 53, 58, 59, 60, 62, 68

Tabela. Liczby pierwsze $3 \leqslant p \leqslant 73$ i odpowiadające im zbiory pierwiastków prymitywnych.

Warto w tym miejscu wspomnieć najbardziej znaną hipotezę dotyczącą pierwiastków prymitywnych.

Hipoteza 6.2.6 (hipoteza Artina)**.** *Niech $a \in \mathbb{Z} \setminus \{-1, 0, 1\}$. Jeśli a nie jest kwadratem, to a jest pierwiastkiem prymitywnym dla nieskończenie wielu liczb pierwszych.*

Przedstawimy teraz algorytm Gaussa, który umożliwia, dla danej liczby pierwszej p, wyznaczenie pierwiastka prymitywnego dla p.

Algorytm Gaussa wyznaczania pierwiastka prymitywnego dla $p \in \mathbb{P}$.

Krok 1: Wybieramy $a \in \{2, \ldots, p-1\}$ i dla $i = 1, 2, \ldots, \mathrm{ord}_p(a)$ obliczamy $a^i \pmod p$. Jeżeli $t := \mathrm{ord}_p(a) = p-1$, to a jest pierwiastkiem prymitywnym dla p i kończymy sprawdzanie. Zgodnie z wnioskiem 6.1.6, każdy inny pierwiastek prymitywny dla p jest postaci a^k, gdzie $\mathrm{NWD}(k, p-1) = 1$. Jeśli $t \neq p-1$, to przechodzimy do kroku (2).

Krok 2: Wybieramy $b \in \{2, \ldots, p-1\}$ w taki sposób, że $b \not\equiv a^i \pmod p$ dla $i = 1, \ldots, t$. Niech $u := \mathrm{ord}_p(b)$. Jeśli $u \neq p-1$, to wyznaczamy $v = \mathrm{NWW}(t, u)$. Oznacza to, że $v = v_1 v_2$, gdzie $v_1 | t$ i $v_2 | u$ i $\mathrm{NWD}(v_1, v_2) = 1$. Niech teraz a_1, b_1 będą najmniejszymi nieujemnymi resztami modulo $a^{\frac{t}{v_1}}$ oraz $b^{\frac{u}{v_2}}$ odpowiednio. Oznacza to, że element $g = a_1 b_1$ ma rząd $\mathrm{ord}_p(g) = v_1 v_2 = v$. Jeśli $v = p-1$, to g jest pierwiastkiem prymitywnym dla p i kończymy procedurę. Jeśli $v \neq p-1$, to przechodzimy do kroku (3).

Krok 3: Powtarzamy krok (2) zastępując a przez $a_1 b_1$ i t przez v.
Jest jasne, że powyższy algorytm się skończy, gdyż w każdym kroku $v > t$.

Przykład 6.2.7. Pokażemy sposób działania algorytmu Gaussa znajdując pierwiastek prymitywny dla $p = 71$. Wybieramy $a = 2$ i znajdujemy, że $\mathrm{ord}_{71}(2) = 35$. Ponadto zbiór reszt $A = \{2^i \pmod{71} : i = 0, \ldots, 34\}$ ma postać

$$A = \{1, 2, 4, 8, 16, 32, 64, 57, 43, 15, 30, 60, 49, 27, 54, 37, 3, 6, 12,$$
$$24, 48, 25, 50, 29, 58, 45, 19, 38, 5, 10, 20, 40, 9, 18, 36\}.$$

Ponieważ $t = \mathrm{ord}_{71}(2) = 35 < 70$, więc wybieramy $b = 7$ jako najmniejszy element, który nie leży w A. Bezpośrednie sprawdzenie pokazuje, że $u = \mathrm{ord}_{71}(7) = 70$ i dostajemy, że $g = 7$ jest pierwiastkiem prymitywnym dla $p = 71$.

Naturalnym pytaniem jest jak mały może być najmniejszy pierwiastek prymitywny dla liczby pierwszej p?

Twierdzenie 6.2.8. *Niech $g(p)$ oznacza najmniejszy pierwiastek prymitywny dla liczby pierwszej p. Wówczas $g(p) \leqslant p^{0.68}$.*

Dowód powyższego twierdzenia opiera się na wyrafinowanym zastosowaniu technik analitycznej teorii liczb.

Do tej pory udowodniliśmy, że jeśli $p \in \mathbb{P}$, to p ma dokładnie $\varphi(p-1)$ pierwiastków prymitywnych. Kolejnym naturalnym pytaniem jest kwestia charakteryzacji liczb $m \in \mathbb{N}$, dla których istnieje pierwiastek prymitywny. Na początek przedstawimy negatywny rezultat. Dokładniej, prawdziwa jest następująca:

Obserwacja 6.2.9. *Niech $m = 2^k, k \geqslant 3$. Wówczas m nie ma pierwiastka prymitywnego.*

Dowód. Zauważmy, że $\varphi(2^k) = 2^{k-1}$. Pokażemy, że jeśli $a \equiv 1 \pmod 2$, to dla dowolnego $k \in \mathbb{N}_{\geqslant 3}$ zachodzi

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}. \tag{6.2}$$

Dowód poprowadzimy przez indukcję ze względu na k. Dla $k = 3$ to jest dokładnie nasza uwaga 6.1.8. Załóżmy teraz, że kongruencja (6.2) jest prawdziwa dla k. Możemy zatem napisać, że dla pewnego $u \in \mathbb{N}_0$ zachodzi $a^{2^{k-2}} = 1 + u2^k$. Stąd

$$a^{2^{k-1}} = (1 + u2^k)^2 = 1 + 2^{k+1}u + 2^{2k}u^2 \equiv 1 \pmod{2^{k+1}}.$$

Dowodzi to, że $\operatorname{ord}_{2^{k+1}}(a) | 2^{k-1} = \frac{\varphi(2^{k+1})}{2}$ i dostajemy tezę. □

Zanim sformułujemy charakteryzację tych m, dla których istnieje pierwiastek prymitywny, w kilku lematach wskażemy te sytuacje, w których pierwiastek takowy istnieje.

Lemat 6.2.10. *Jeśli $p \in \mathbb{P}_{\geqslant 3}$ i g jest pierwiastkiem prymitywnym dla p, to g lub $g+p$ jest pierwiastkiem prymitywnym dla p^2.*

Dowód. Niech g będzie pierwiastkiem prymitywnym dla p i niech $n = \operatorname{ord}_{p^2}(g)$. W szczególności $g^n \equiv 1 \pmod p$ i dostajemy, że $(p-1)|n$. Ponieważ $\varphi(p^2) = p(p-1)$, więc $n|p(p-1)$. Wobec tego $n = p(p-1)$ albo $n = p-1$. Jeśli $n = p(p-1)$, to g jest pierwiastkiem prymitywnym dla p^2 i dowód jest zakończony. W przypadku gdy $n = p-1$, czyli $g^{p-1} \equiv 1 \pmod{p^2}$ wykażemy, że $\operatorname{ord}_{p^2}(g+p) = p(p-1) = \varphi(p^2)$. Skoro g jest pierwiastkiem prymitywnym dla p, to $g+p$ również, co znowu implikuje, że $\operatorname{ord}_{p^2}(g+p) = p-1$ albo $\operatorname{ord}_{p^2}(g+p) = p(p-1)$. Mamy jednak, że

$$\begin{aligned}(g+p)^{p-1} &= \sum_{i=0}^{p-1} \binom{p-1}{i} g^{p-1-i}p^i \equiv g^{p-1} + (p-1)pg^{p-2} \\ &\equiv g^{p-1} - pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \pmod{p^2},\end{aligned}$$

bo $p \nmid g$. Oznacza to, że $\operatorname{ord}_{p^2}(g+p) = p(p-1)$ co kończy dowód. □

Przykład 6.2.11. Można sprawdzić, że $g = 2, 6, 7, 8$ są pierwiastkami prymitywnymi zarówno dla $p = 11$ jak i $p^2 = 121$.

Zauważmy jednak, że $g = 10$ jest pierwiastkiem prymitywnym dla $p = 487$, ale g nie jest pierwiastkiem prymitywnym dla p^2. Nasze rozumowanie pokazuje, że $g' = g + p = 497$ jest pierwiastkiem prymitywnym dla 487^2.

Lemat 6.2.12. *Jeśli $p \in \mathbb{P}_{\geqslant 3}$ i $g \in \mathbb{Z}$ jest pierwiastkiem prymitywnym dla p^2, to g jest pierwiastkiem prymitywnym dla p^k dla dowolnego $k \in \mathbb{N}_{\geqslant 2}$.*

Dowód. Zauważmy, że nasza teza może być zapisana jako implikacja: jeśli $g^{p-1} \not\equiv 1 \pmod{p^2}$, to $g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$. Dowód poprowadzimy indukcyjnie względem k. Dla $k = 1$ teza to wprost nasze założenie, że g jest pierwiastkiem prymitywnym dla p^2. Załóżmy, że teza zachodzi dla k, tzn. $g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$. Z twierdzenia Eulera wiemy, że $g^{\varphi(p^k)} \equiv 1 \pmod{p^k}$, a stąd i z założenia indukcyjnego otrzymujemy istnienie takiej liczby $u \in \mathbb{N}$ niepodzielnej przez p, że $g^{\varphi(p^k)} = 1 + up^k$. Stąd i ze związku $\varphi(p^{k+1}) = p^k(p-1) = p\varphi(p^k)$ otrzymujemy

$$\begin{aligned}g^{\varphi(p^{k+1})} = g^{p\varphi(p^k)} &= (1 + up^k)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} u^i p^{ki} \equiv 1 + up^{k+1} \not\equiv 1 \pmod{p^{k+2}},\end{aligned}$$

co kończy dowód naszego lematu. □

Podsumowując nasze dotychczasowe rozważania widzimy, że jeśli $m = 2, 4$ lub $m = p^k, p \in \mathbb{P}_{\geqslant 3}$ i $k \in \mathbb{N}$, to m ma pierwiastek prymitywny.

Lemat 6.2.13. *Niech $p \in \mathbb{P}_{\geqslant 3}$ i $k \in \mathbb{N}$. Niech g będzie pierwiastkiem prymitywnym dla p^k. Wtedy:*

(1) jeśli $g \equiv 1 \pmod 2$, to g jest pierwiastkiem prymitywnym dla $2p^k$,

(2) jeśli $g \equiv 0 \pmod 2$, to $g + p^k$ jest pierwiastkiem prymitywnym dla $2p^k$.

Dowód. Niech $g \equiv 1 \pmod 2$. Ponieważ $\varphi(p^k) = \varphi(2p^k)$ oraz $g^{\varphi(2p^k)} \equiv 1 \pmod{2p^k}$, to g jest pierwiastkiem prymitywnym dla $2p^k$.

Jeśli zaś $g \equiv 0 \pmod 2$, to $g + p^k \equiv 1 \pmod 2$ i $g + p^k$ jest pierwiastkiem prymitywnym dla p^k. Stosując (1) dostajemy tezę. □

Przykład 6.2.14. Liczba $g = 7$ jest pierwiastkiem prymitywnym dla $11^k, k \in \mathbb{N}$. Ponieważ g jest liczbą nieparzystą, to jest to również pierwiastek prymitywny dla $2 \cdot 7^k$.

Liczba $g = 2$ jest pierwiastkiem prymitywnym dla $13^k, k \in \mathbb{N}_+$. Ponieważ g jest liczbą parzystą, to liczba $g' = 2 + 13^k$ jest pierwiastkiem prymitywnym dla $2 \cdot 13^k$.

Twierdzenie 6.2.15 (charakteryzacja istnienia pierwiastka prymitywnego dla dowolnej liczby naturalnej)**.** *Liczba $m \in \mathbb{N}_{\geqslant 2}$ ma pierwiastek prymitywny wtedy i tylko wtedy, gdy $m = 2, 4, p^k, 2p^k$ dla $p \in \mathbb{P}_{\geqslant 3}, k \in \mathbb{N}$.*

Dowód. Jest jasne, że z naszych wcześniejszych przygotowań wynika, że wystarczy udowodnić implikację ($\Longrightarrow$). By dowieść naszej tezy wykażemy, że jeśli m ma nieparzysty dzielnik pierwszy p, to $m = p^k$ lub $m = 2p^k$.

Niech $m = np^k$, gdzie $p \nmid n$ i załóżmy, że $n \geqslant 3$. Ponieważ $\varphi(m) = \varphi(n)\varphi(p^k)$, p jest nieparzysta i $n \geqslant 3$, więc $2|\varphi(m)$ i $2|\varphi(p^k)$. Niech teraz $a \in \mathbb{Z}$ i $\mathrm{NWD}(a, m) = 1$. Wówczas:

$$a^{\frac{\varphi(m)}{2}} = (a^{\varphi(n)})^{\frac{\varphi(p^k)}{2}} \equiv 1 \pmod n,$$
$$a^{\frac{\varphi(m)}{2}} = (a^{\varphi(p^k)})^{\frac{\varphi(n)}{2}} \equiv 1 \pmod{p^k}.$$

Ponieważ układ kongruencji

$$x \equiv 1 \pmod n, \quad x \equiv 1 \pmod{p^k}$$

ma dokładnie jedno rozwiązanie modulo $m = np^k$ i $x = a^{\frac{\varphi(m)}{2}}$ jest tym rozwiązaniem, więc $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod m$, co dowodzi, że $\mathrm{ord}_m(a) \leqslant \frac{\varphi(m)}{2} < \varphi(m)$. Oznacza to, że m nie ma pierwiastka prymitywnego i otrzymujemy tezę. □

6.3 Zadania

1. Znaleźć pierwiastek prymitywny dla m, gdzie $m \in \{4, 5, 10, 13, 14, 18\}$.
2. Wykazać, że liczby $12, 20$ nie mają pierwiastka prymitywnego.
3. Odpowiedzieć na pytanie, ile niekongruentnych pierwiastków prymitywnych ma liczba 14? Wyznaczyć je wszystkie.
4. Odpowiedzieć na pytanie, ile niekongruentnych pierwiastków prymitywnych ma liczba 18? Wyznaczyć je wszystkie.
5. Wykazać, że jeśli a^{-1} jest multiplikatywną odwrotnością a modulo m, to $\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$. Wywnioskować stąd, że a jest pierwiastkiem prymitywnym modulo m wtedy i tylko wtedy, gdy a^{-1} jest pierwiastkiem prymitywnym modulo m.
6. Wykazać, że jeśli $m \in \mathbb{N}$ oraz liczby $a, b \in \mathbb{Z}$ są takie, że $(ab, m) = 1, (\mathrm{ord}_m a, \mathrm{ord}_m b) = 1$, to $\mathrm{ord}_m(ab) = \mathrm{ord}_m a \cdot \mathrm{ord}_m b$.
7. Wykazać, że jeśli $m \in \mathbb{N}, a \in \mathbb{Z}$ są takie, że $(a, m) = 1$ i $\mathrm{ord}_m a = m - 1$, to m jest liczbą pierwszą.
8. Wykazać, że r jest pierwiastkiem prymitywnym modulo $p \in \mathbb{P}_{\geqslant 3}$ wtedy i tylko wtedy, gdy $(r, p) = 1$ i $r^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ dla każdego dzielnika pierwszego q liczby $p - 1$.
9. Wykazać, że jeśli F_n jest n-tą liczba Fermata, to $\mathrm{ord}_{F_n} 2 \leqslant 2^{n+1}$.
10. Wykazać, że $\mathrm{ord}_{2^k}(3) = 2^{k-2}$ dla $k \in \mathbb{N}_{\geqslant 3}$.

Rozdział 7

Reszty kwadratowe i prawo wzajemności reszt kwadratowych

W tym rozdziale skupimy się na teorii reszt kwadratowych, czyli problemie *istnienia* rozwiązań kongruencji kwadratowych postaci $x^2 \equiv a \pmod{m}$, gdzie $a \in \mathbb{Z}, m \in \mathbb{N}_{\geqslant 2}$. Interesować nas będzie sytuacja, gdy $m = p$ jest nieparzystą liczbą pierwszą.

7.1 Reszty kwadratowe

Zaczniemy od definicji obiektu naszych zainteresowań w sposób precyzyjny.

Definicja 7.1.1 (reszta kwadratowa)**.** Niech $p \in \mathbb{P}_{\geqslant 3}$. Liczbę $a \in \mathbb{Z}$ spełniającą warunek $\mathrm{NWD}(a, p) = 1$, nazywamy **resztą kwadratową modulo** p, jeżeli istnieje $x \in \mathbb{Z}$, dla którego $x^2 \equiv a \pmod{p}$.

Jeżeli kongruencja $x^2 \equiv a \pmod{p}$ nie ma rozwiązania, to a nazywamy **niereszą kwadratową.**

Definicja 7.1.2 (symbol Legendre'a)**.** Niech $p \in \mathbb{P}_{\geqslant 3}$ i $a \in \mathbb{Z}$. Wówczas liczbę

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & p|a, \\ 1, & a \text{ jest resztą kwadratową modulo } p, \\ -1, & \text{w przeciwnym przypadku,} \end{cases}$$

nazywamy **symbolem Legendre'a z** a **modulo** p**.**

Obserwacja 7.1.3. *Niech $p \in \mathbb{P}_{\geqslant 3}$ i g będzie pierwiastkiem prymitywnym dla p (z twierdzenia 6.2.5 wiemy, że g istnieje). Wówczas zbiór reszt kwadratowych pokrywa się ze zbiorem $R = \{g^{2i} \pmod{p} : \ i = 0, 1, \ldots, \frac{p-3}{2}\}$. W szczególności, zbiór niereszt kwadratowych pokrywa się ze zbiorem $R' = \{g^{2i+1} \pmod{p} : i = 0, 1, \ldots, \frac{p-3}{2}\}$.*

Dowód. Ponieważ g jest pierwiastkiem prymitywnym, więc elementy zbioru R są parami niekongruentne, co oznacza, że $|R| = \frac{p-1}{2}$. Zauważmy, że nie ma też innych reszt kwadratowych. Istotnie, gdyby potęga g^{2i+1} była resztą kwadratową, to istniałoby takie $x_0 \in \mathbb{Z}$, że $x_0^2 \equiv g^{2i+1} \pmod{p}$, skąd $(x_0 g^{-i})^2 \equiv g \pmod{p}$. Po podniesieniu obu stron tej kongruencji do potęgi $\frac{p-1}{2}$, dostajemy na mocy małego twierdzenia Fermata, że

$$g^{\frac{p-1}{2}} \equiv (x_0 g^{-1})^{p-1} \equiv 1 \pmod{p}.$$

Wobec tego $\mathrm{ord}_p(g) \leqslant \frac{p-1}{2} < p - 1$, co jest sprzeczne z założeniem, że g jest pierwiastkiem prymitywnym. □

Dzięki powyższej obserwacji mamy natychmiastowy zestaw wniosków, dotyczących własności reszt kwadratowych.

Wniosek 7.1.4 (liczba reszt i niereszt kwadratowych)**.** *Dla dowolnego $p \in \mathbb{P}_{\geqslant 3}$ liczba reszt kwadratowych i niereszt kwadratowych modulo p jest równa $\frac{1}{2}(p-1)$.*

Wniosek 7.1.5. *Dla dowolnego $p \in \mathbb{P}_{\geqslant 3}$ zachodzą następujące własności:*

(1) jeśli a_1, a_2 są resztami kwadratowymi modulo p, to $a_1 a_2$ jest resztą kwadratową modulo p,

(2) jeśli a_1, a_2 są nieresztami kwadratowymi modulo p, to $a_1 a_2$ jest resztą kwadratową modulo p,

(3) jeśli a_1 jest resztą kwadratową modulo p i a_2 jest niereszą kwadratową modulo p, to a_1a_2 jest niereszą kwadratową modulo p.

Przykład 7.1.6. Dla $p = 11$ reszty kwadratowe modulo 11 to: $1, 3, 4, 5, 9$, zaś dla $p = 13$ reszty kwadratowe modulo 13 to: $1, 2, 3, 4, 9, 10$.

Twierdzenie 7.1.7 (kryterium Eulera dla reszt kwadratowych)**.** *Dla dowolnych $p \in \mathbb{P}_{\geqslant 3}$ i $a \in \mathbb{Z}$ zachodzi równość:*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Dowód. Jeśli $p|a$, to nie ma czego dowodzić. Jeśli a jest resztą kwadratową modulo p, to $\left(\frac{a}{p}\right) = 1$ i istnieje $x_0 \in \mathbb{Z}$, że $x_0^2 \equiv a \pmod{p}$. Stąd

$$a^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Niech $a \in \mathbb{Z}$ będzie niereszą kwadratową, czyli $\left(\frac{a}{p}\right) = -1$. Niech g będzie pierwiastkiem prymitywnym dla p. Wtedy dla pewnego $i \in \{0, 1, \ldots, (p-3)/2\}$ mamy $a \equiv g^{2i+1} \pmod{p}$ (zgodnie z obserwacją 7.1.3). Stąd

$$a^{\frac{p-1}{2}} \equiv \left(g^{2i+1}\right)^{\frac{p-1}{2}} \equiv g^{i(p-1)} g^{\frac{p-1}{2}} \equiv \left(g^{p-1}\right)^i g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod{p}.$$

Ponieważ $g^{p-1} - 1 = (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$, to $g^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ lub $g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}$. Pierwsza równość jest niemożliwa, gdyż wtedy $\mathrm{ord}_p(g) < p - 1$ i mamy sprzeczność z prymitywnością elementu g. Musi być zatem $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, czyli

$$a^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}.$$

We wszystkich przypadkach jest więc $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$ i dostajemy tezę. □

Kryterium Eulera umożliwia szybką odpowiedź na pytanie, kiedy -1 jest resztą kwadratową modulo p, gdzie $p \in \mathbb{P}_{\geqslant 3}$. Dokładniej mówiąc, mamy równość

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{gdy } p \equiv 1 \pmod{4}, \\ -1, & \text{gdy } p \equiv 3 \pmod{4}. \end{cases}$$

Oznacza to, że kongruencja $x^2 \equiv -1 \pmod{p}$ ma rozwiązanie wtedy i tylko wtedy, gdy $p \equiv 1 \pmod{4}$.

Twierdzenie 7.1.8 (własności symbolu Legendre'a)**.** *Dla dowolnych $p \in \mathbb{P}_{\geqslant 3}$ oraz $a, b \in \mathbb{Z}$ zachodzą własności:*

(1) jeśli $a \equiv b \pmod{p}$, to $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (multiplikatywność symbolu Legendre'a),

(3) jeśli $p \nmid a$, to $\left(\frac{a^2}{p}\right) = 1$.

Dowód. Wobec oczywistości punktu (3) uzasadnimy pierwsze dwie części tezy.

(1) Korzystając z kryterium Eulera mamy, że

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) \pmod{p}.$$

Jednak $p \geqslant 3$, więc oznacza to, że $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2) Ponownie, korzystając z kryterium Eulera mamy ciąg równoważności modulo:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

I ponownie teza wynika z faktu, że $p \geqslant 3$. □

Uwaga 7.1.9. Warto również zauważyć, że problem istnienia rozwiązania ogólnej kongruencji stopnia 2 postaci

$$Ax^2 + Bx + C \equiv 0 \pmod{p}, \tag{7.1}$$

gdzie $A, B, C \in \mathbb{Z}, p \nmid A$, sprowadza się do wyznaczenia odpowiedniego symbolu Legendre'a. Dokładniej, mnożąc strony kongruencji przez $4A$, a następnie dopełniając do kwadratu otrzymujemy

$$(2Ax + B)^2 + 4AC - B^2 \equiv 0 \pmod{p} \iff X^2 \equiv \Delta \pmod{p},$$

gdzie $\Delta = B^2 - 4AC$ i $X = 2Ax + B$. Widzimy zatem, że (7.1) ma rozwiązanie wtedy i tylko wtedy, gdy

$$\left(\frac{\Delta}{p}\right) = 1.$$

Mając rozwiązanie $X = X_0$ odzyskujemy rozwiązanie dla wyjściowej kongruencji rozwiązując kongruencję liniową $2Ax \equiv X_0 - B \pmod{p}$, które istnieje, bo $p \nmid 2A$.

Nasze następne twierdzenie, udowodnione przez Gaussa, znajdzie zastosowanie w dowodzie jednego z fundamentalnych twierdzeń teorii liczb: prawa wzajemności reszt kwadratowych.

Twierdzenie 7.1.10 (Lemat Gaussa)**.** *Niech $p \in \mathbb{P}_{\geqslant 3}, a \in \mathbb{Z}$ gdzie $p \nmid a$ oraz niech*

$$S = \left\{ai \bmod p : \ i \in \{1, \ldots, (p-1)/2\}, \ ai \bmod p > \frac{p}{2}\right\}$$

i $s := \#S$. Wówczas $\left(\frac{a}{p}\right) = (-1)^s$.

Dowód. Zapiszmy $S = \{u_1, \ldots, u_s\}$ i niech $V = \{v_1, \ldots, v_t\}$ będzie dopełnieniem zbioru S w zbiorze $R = \{a \cdot 1 \bmod p, \ldots, a \cdot (p-1)/2 \bmod p\}$. Zachodzi równość $t = \frac{1}{2}(p-1) - s$, co jest konsekwencją faktu, że $\mathrm{NWD}(ia, p) = 1$ dla $0 < i < p$. Na początek wykażemy, że zachodzi równość

$$L := \{p - u_1, \ldots, p - u_s, v_1, \ldots, v_t\} = R.$$

Istotnie, gdyby L było istotnym podzbiorem R, to istniałyby liczby $i, j \in \mathbb{N}, i \neq j$, dla których spełniony jest jeden z warunków: (1) $u_i \equiv u_j \pmod{p}$; (2) $v_i \equiv v_j \pmod{p}$; (3) $p - u_i \equiv v_j \pmod{p}$. Jest jasne, że jedynie warunek (3) ma szansę być spełniony. Ale skoro $u_i = ai_1 \bmod p$ oraz $v_j = aj_1 \bmod p$ dla pewnych $i_1, j_1 \in R$, to (3) implikuje, że $-ai_1 \equiv aj_1 \pmod{p}$. Równoważnie, ponieważ $p \nmid a$, mamy, że $i_1 + j_1 \equiv 0 \pmod{p}$. Ponieważ $0 < i_1 + j_1 < p$, więc dostajemy sprzeczność.

Skoro $L = R$, to prawdziwa jest równość

$$(p - u_1) \cdot \ldots \cdot (p - u_s) \cdot v_1 \cdot \ldots \cdot v_t \equiv \prod_{i=1}^{\frac{p-1}{2}} i \equiv \left(\frac{p-1}{2}\right)! \pmod{p}$$

lub równoważnie

$$(-1)^s u_1 \cdot \ldots \cdot u_s \cdot v_1 \cdot \ldots \cdot v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Z określenia liczb u_i, v_j dostajemy, że

$$(-1)^s u_1 \cdot \ldots \cdot u_s \cdot v_1 \cdot \ldots \cdot v_t \equiv \prod_{i=1}^{\frac{p-1}{2}} (ai) \pmod{p}.$$

Ostatecznie

$$(-1)^s \prod_{i=1}^{\frac{p-1}{2}} (ai) \equiv (-1)^s a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)! \pmod{p},$$

co po podzieleniu stronami przez $\left(\frac{p-1}{2}\right)!$ prowadzi do kongruencji $(-1)^s a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Korzystając z kryterium Eulera i faktu, że $(-1)^s, \left(\frac{a}{p}\right) \in \{-1, 1\}$ dostajemy równość z tezy. □

Korzystając z lematu Gaussa możemy wyprowadzić przydatny wniosek.

Wniosek 7.1.11. *Dla dowolnego $p \in \mathbb{P}_{\geqslant 3}$ zachodzi* $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. *Dokładniej:*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & gdy \;\; p \equiv \pm 1 \pmod 8, \\ -1, & gdy \;\; p \equiv \pm 3 \pmod 8. \end{cases}$$

Dowód. W dowodzie wykorzystamy lemat Gaussa (7.1.10) dla przypadku $a = 2$. Ponieważ $\{2i : \; i \in \{1, \ldots, (p-1)/2\} = \{2, 4, \ldots, p-1\}$, więc zbiór elementów $2i$, których reszty modulo p są $> p/2$ odpowiada zbiorowi tych i, że $i > p/4$. Stąd liczba takich par wynosi

$$s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor.$$

Zachodzi zatem równość $\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor}$. Rozważając możliwe reszty p modulo 8 łatwo sprawdzić bezpośrednio, że

$$\frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod 2,$$

co daje tezę. □

Kolejny rezultat podaje jawny wzór na wyznaczenie $\left(\frac{a}{p}\right)$.

Lemat 7.1.12. *Niech $p \in \mathbb{P}_{\geqslant 3}, a \in \mathbb{Z}, 2 \nmid a$, i załóżmy, że $p \nmid a$. Wówczas* $\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$, *gdzie*

$$T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right].$$

Dowód. Będziemy korzystać z oznaczeń wprowadzonych w dowodzie lematu Gaussa (7.1.10). Dokładniej, przez $u_1, \ldots, u_s$ będziemy oznaczać te reszty $ai \bmod p, i \in R = \{1, \ldots, \frac{p-1}{2}\}$, które są większe od $\frac{p}{2}$, zaś przez $v_1, \ldots, v_t$ oznaczamy pozostałe reszty. Z algorytmu dzielenia z resztą możemy napisać

$$ja = p \left[\frac{ja}{p} \right] + r_j,$$

gdzie $r_j \in \{u_1, \ldots, u_s, v_1, \ldots, v_t\}$ dla dowolnego $j \in R$. Sumując stronami te równości (jest ich $\frac{p-1}{2}$) otrzymujemy

$$\sum_{j=1}^{\frac{p-1}{2}} ja = p \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p} \right] + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{7.2}$$

Ponieważ $R = \{p - u_1, \ldots, p - u_s, v_1, \ldots, v_t\}$ możemy napisać

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{s} (p - u_j) + \sum_{j=1}^{t} v_j = pj - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j.$$

Wyznaczając z powyższej równości $\sum_{j=1}^{t} v_j$ i wstawiając ją do równości (7.2), po niezbędnych przekształceniach, dostajemy

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} = pT(a,p) - ps + 2 \sum_{j=1}^{s} u_j.$$

Ponieważ liczby a, p są nieparzyste, więc redukując powyższą równość modulo 2 otrzymujemy $s \equiv T(a,p) \pmod 2$, co po zastosowaniu lematu Gaussa, implikuje równość z tezy. □

Uwaga 7.1.13. Choć interesujący, wzór z powyższego lematu, nie jest zbyt użyteczny do bezpośredniego wyznaczania $\left(\frac{a}{p}\right)$. Przyczyna tego jest bardzo prozaiczna. Jeśli p jest dużą liczbą pierwszą, to nie jest jasne jak wyznaczyć $T(a,p) \bmod 2$ bez wyznaczania wartości $T(a,p)$. Niemniej jednak, przedstawiony wynik jest kluczem do dowodu jednego z fundamentalnych twierdzeń teorii liczb: prawa wzajemności reszt kwadratowych.

Twierdzenie 7.1.14 (prawo wzajemności reszt kwadratowych)**.** *Dla $p,q \in \mathbb{P}_{\geqslant 3}, p \neq q$ zachodzi:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{q}\frac{q-1}{2}}.$$

Dowód. Rozważamy pary liczb $(x,y) \in R_p \times R_q$, gdzie dla nieparzystej liczby k określamy $R_k = \left\{1,\ldots,\frac{k-1}{2}\right\}$. Liczba par, które rozważamy wynosi $\frac{p-1}{2}\cdot\frac{q-1}{2}$. Interesować nas będzie liczba par $(x,y) \in R_p \times R_q$, które spełniają warunek $qx > py$. Zauważmy, że są to dokładnie te pary, dla których

$$x \in R_p \quad \text{oraz} \quad 1 \leqslant y \leqslant \frac{q}{p}x.$$

Zauważmy, że dla każdego ustalonego $x \in R_p$, wskazana nierówność ma dokładnie $\left[\frac{qx}{p}\right]$ rozwiązań. Oznacza to, że liczba interesujących nas par jest równa

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] = T(q,p).$$

Rozumując w sposób analogiczny wykazujemy, że liczba par $(x,y) \in R_p \times R_q$, które spełniają warunek $qx < py$ wynosi

$$\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right] = T(p,q).$$

Zauważając teraz, że nie istnieje para $(x,y) \in R_p \times R_q$, dla której spełniona jest równość $qx = py$ dostajemy, że $T(p,q) + T(q,p) = \frac{p-1}{2}\cdot\frac{q-1}{2}$. Z lematu 7.1.12 dostajemy równość

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{T(q,p)}(-1)^{T(p,q)} = (-1)^{T(q,p)+T(p,q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

i nasze twierdzenie jest udowodnione. □

Uwaga 7.1.15. Pierwszy poprawny dowód prawa wzajemności reszt kwadratowych podał C. F. Gauss (we wspominanym już wcześniej słynnym dziele *Disquisitiones arithmeticae*). Gauss podał siedem (!) różnych dowodów tego prawa. Przedstawiony powyżej dowód jest adaptacją trzeciego dowodu Gaussa i pochodzi od G. Eisensteina. Warto dodać, że hipoteza dotycząca własności równoważnej twierdzeniu 7.1.14 została sformułowana przez Eulera w 1772 r. (w pracy *Observationes circa divisionem quadratorum per numeros primos*). Obecnie znanych jest co najmniej sto dowodów prawa wzajemności reszt kwadratowych.

Przykład 7.1.16. Prawo wzajemności reszt kwadratowych umożliwia szybkie wyznaczenie symbolu Legendre'a nawet dla dużych liczb pierwszych p. Policzmy dla przykładu $\left(\frac{174}{541}\right)$. Zauważmy, że $174 = 2\cdot 3\cdot 29$. Mamy następujący ciąg równości:

$$\begin{aligned}
\left(\frac{174}{541}\right) &= \left(\frac{2}{541}\right)\left(\frac{3}{541}\right)\left(\frac{29}{541}\right)\\
&= (-1)^{\frac{541^2-1}{8}}(-1)^{\frac{3-1}{2}\frac{541-1}{2}}\left(\frac{541}{3}\right)(-1)^{\frac{29-1}{2}\frac{541-1}{2}}\left(\frac{541}{29}\right)\\
&= -\left(\frac{1}{3}\right)\left(\frac{19}{29}\right) = -\left(\frac{19}{29}\right) = -(-1)^{\frac{19-1}{2}\frac{29-1}{2}}\left(\frac{29}{19}\right)\\
&= -\left(\frac{10}{19}\right) = -\left(\frac{2}{19}\right)\left(\frac{5}{19}\right) = -(-1)^{\frac{19^2-1}{8}}(-1)^{\frac{5-1}{2}\frac{19-1}{2}}\left(\frac{19}{5}\right)\\
&= \left(\frac{19}{5}\right) = \left(\frac{4}{5}\right) = \left(\frac{2}{5}\right)^2 = 1.
\end{aligned}$$

Nasze obliczenia oznaczają, że 174 jest resztą kwadratową modulo 541.

7.2 Zadania

1. Znaleźć reszty kwadratowe modulo n, gdzie $n \in \{3, 5, 7, 8, 13, 15, 18, 19\}$.
2. Wyznaczyć wartość symbolu Legendre'a $\left(\frac{a}{11}\right)$ dla $a \in \{1, \ldots, 10\}$.
3. Niech $p \in \mathbb{P}_{\geqslant 3}$, $a, b \in \mathbb{Z}$, $p \nmid a$. Wykazać, że $\sum_{i=1}^{p-1} \left(\frac{ai+b}{p}\right) = 0$.
4. Wykazać, że dla każdej liczby pierwszej $p > 5$ istnieje taka liczba całkowita a, że a i $a+1$ sa resztami kwadratowymi modulo p.
5. Wykazać, że jeśli $p = 4n+3 \in \mathbb{P}$ i a jest resztą kwadratową modulo p, to $x = a^{n+1}$ jest rozwiązaniem kongruencji $x^2 \equiv a \pmod{p}$.
6. Wykazać, że jeśli $p \equiv 5 \pmod 8$ oraz a jest resztą kwadratową modulo p, to rozwiązaniem kongruencji $x^2 \equiv a \pmod{p}$ jest $x = a^{(p+3)/8} \bmod p$ lub $x = 2a(4a)^{(p-5)/8} \bmod p$.
7. Znaleźć wszystkie rozwiązania następujących kongruencji wielomianowych:
   (a) $x^2 \equiv 1 \pmod{15}$;
   (b) $x^2 \equiv 31 \pmod{75}$;
   (c) $x^2 \equiv 58 \pmod{77}$;
   (d) $x^2 \equiv 16 \pmod{105}$;
   (e) $x^2 \equiv 46 \pmod{231}$;
   (f) $x^2 \equiv 207 \pmod{1001}$.
8. Wyznaczyć wartość symboli Legendre'a: $\left(\frac{3}{53}\right)$, $\left(\frac{7}{79}\right)$, $\left(\frac{15}{101}\right)$, $\left(\frac{31}{641}\right)$, $\left(\frac{111}{991}\right)$, $\left(\frac{105}{1009}\right)$.
9. Korzystając z prawa reszt kwadratowych wyznaczyć wartość symbolu Legendre'a $\left(\frac{2}{p}\right)$.
10. Scharakteryzować te liczby pierwsze p, że $\left(\frac{5}{p}\right) = 1$.
11. Scharakteryzować te liczby pierwsze p, dla których kongruencja $x^4 \equiv -4 \pmod{p}$ ma rozwiązanie w liczbach całkowitych.

Rozdział 8

Zadania dodatkowe (z odpowiedziami)

Przedstawione tutaj zadania są troche trudniejsze od zadań, które znajdują się na końcu wcześniejszych rozdziałów. W zwiazku z tym postanowiliśmy dodać do nich odpowiedzi, gdyż uważamy, że w sytuacji, gdy Czytelnik nie potrafi znaleźć odpowiedz sam, dokładne przestudiowanie tej zaprezentowanej poszerzy jego wiedzę tak w zakresie rozumienia przedstawionej wcześniej teorii, jak i technik dowodowych. Przedstawione zadania nie są w większości oryginalne i pochodzą z różnych zbiorów zadań dotyczących teorii liczb i algebry [9, 4, 15]. Dla krótkości zapisu używamy notacji $(a_1, \ldots, a_n) := \mathrm{NWD}(a_1, \ldots, a_n)$ oraz $[a_1, \ldots, a_n] := \mathrm{NWW}(a_1, \ldots, a_n)$

8.1 Zadania z teorii liczb

1. Dla dowolnych $a, b, c \in \mathbb{N}$ dowieść równości

$$([a,b],[b,c],[c,a]) = [(a,b),(b,c),(c,a)]$$

i

$$\frac{[a,b,c]^2}{[a,b][b,c][c,a]} = \frac{(a,b,c)^2}{(a,b)(b,c)(c,a)}.$$

Rozwiązanie: Zapiszmy każdą z liczb $a, b, c \in \mathbb{N}$ zgodnie z zasadniczym twierdzeniem arytmetyki w postaci rozkładów na różne liczby pierwsze (przyjmując $\alpha_j, \beta_j, \gamma_j \in \mathbb{N}_0$):

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}, \quad b = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}, \quad c = p_1^{\gamma_1} \cdot \ldots \cdot p_k^{\gamma_k}.$$

Wtedy mamy, że $[a,b] = \prod_{i=1}^{k} p_i^{\max\{\alpha_i,\beta_i\}}$ oraz $(a,b) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i,\beta_i\}}$ (wraz z analogicznymi równościami dla pozostałych kombinacji liczb a, b, c). By dowieść pierwszej tożsamości wystarczy wykazać, że dla dowolnego $i \in \{1, \ldots, k\}$ prawdziwa jest równość

$$\begin{aligned}&\min\{\max\{\alpha_i,\beta_i\},\max\{\beta_i,\gamma_i\},\max\{\gamma_i,\alpha_i\}\}\\ &\quad = \max\{\min\{\alpha_i,\beta_i\},\min\{\beta_i,\gamma_i\},\min\{\gamma_i,\alpha_i\}\}.\end{aligned}$$

Ponieważ wyrażenia po obu stronach powyższej równości są symetryczne, więc bez straty dla ogólności możemy założyć, że $\alpha_i \leqslant \beta_i \leqslant \gamma_i$. Przy tym założeniu bezpośrednie sprawdzenie pokazuje, że dla dowolnego $i \in \{1, \ldots, k\}$, obie strony są równie β_i, co dowodzi naszej tezy.

W analogiczny sposób dowodzimy drugiej tożsamości. Istotnie, wystarczy wykazać, że dla dowolnego $i \in \{1, \ldots, k\}$ prawdziwa jest równość

$$\begin{aligned}&2\max\{\alpha_i,\beta_i,\gamma_i\} - \max\{\alpha_i,\beta_i\} - \max\{\beta_i,\gamma_i\} - \max\{\gamma_i,\alpha_i\}\\ &\quad = 2\min\{\alpha_i,\beta_i,\gamma_i\} - \min\{\alpha_i,\beta_i\} - \min\{\beta_i,\gamma_i\} - \min\{\gamma_i,\alpha_i\}.\end{aligned}$$

Ponieważ wyrażenia po obu stronach są symetryczne w zmiennych $\alpha_i, \beta_i, \gamma_i$, więc bez straty dla ogólności możemy założyć, że $\alpha_i \leqslant \beta_i \leqslant \gamma_i$. Bezpośrednie przeliczenie pokazuje, że dla dowolnego $i \in \{1, \ldots, k\}$ obie strony są równe $-\beta_i$, co dowodzi naszej tezy.

2. Udowodnić, że jeśli p_n jest n-tą liczbą pierwszą, to $p_n < 2^{2^{n-1}}$.

   Rozwiązanie: Niech p_i oznacza i-tą liczbę pierwszą. Podobnie jak w dowodzie Euklidesa nieskończoności zbioru liczb pierwszych (por. 1.3.6) możemy uzasadnić, że liczba $p_1p_2 \cdot \ldots \cdot p_n + 1$ jest pierwsza lub podzielna przez liczbę pierwszą większą lub równą p_{n+1}. Oznacza to, że dla dowolnego n prawdziwa jest nierówność

   $$p_{n+1} \leqslant p_1p_2 \cdot \ldots \cdot p_n + 1.$$

   Zauważmy teraz, że $p_1 \leqslant 2 = 2^{2^0}$ i załóżmy, że $p_n \leqslant 2^{2^{n-1}}$ dla $n \geqslant 1$. Mamy zatem

   $$p_{n+1} \leqslant p_1p_2 \cdot \ldots \cdot p_n + 1 \leqslant 2^{2^0}2^{2^1} \cdot \ldots \cdot 2^{2^{n-1}} + 1 = 2^{2^{2^n-1}} + 1 \leqslant 2^{2^n}$$

   co kończy dowód indukcyjny.

3. Udowodnić, że istnieje nieskończenie wiele liczb parzystych k o tej własności, że dla każdej liczby pierwszej $p \in \mathbb{P}$, liczba $p^2 + k$ jest złożona.

   Rozwiązanie: W poszukiwaniu postaci liczb k, zauważmy najpierw, że każda liczba pierwsza $p \geqslant 5$ daje resztę 1 lub 2 przy dzieleniu przez 3, co oznacza, że $p^2 \equiv 1 \pmod 3$. Stąd natychmiast otrzymujemy, że jeśli $a \in \mathbb{N}$, to $p^2 + 6a + 2 \equiv 0 \pmod 3$ i w konsekwencji liczba $p^2 + 6a + 2$ jako większa od 3 i podzielna przez 3 jest liczbą złożoną. Analogicznie, gdy $p = 2$, to liczba $2^2 + 6a + 2$ jest złożona (bo podzielna przez 2 i większa od 2). Możemy więc przypuszczać, że liczby postaci $k = 6a + 2$ dla $a \in \mathbb{N}$ mogą spełniać tezę. Pozostaje przyjrzenie się przypadkowi $p = 3$.

   Liczba postaci $3^2 + 6a + 2$ jest złożona dla liczb a, które spełniają kongruencję $a \equiv 4 \pmod 7$, innymi słowy, gdy $a = 7b + 4$. Ostatecznie, jeśli $k = 6(7b + 4) + 11 = 7(6b + 5)$, to dla każdej liczby pierwszej p liczba postaci $p^2 + k$ jest złożona.

4. Niech $m \in \mathbb{N}$ i przez $\pi(m)$ oznaczmy liczbę liczb pierwszych nieprzekraczających m. Dowieść, że

   $$\pi(m) = \sum_{j=2}^{m} \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right],$$

   gdzie $[x]$ oznacza część całkowitą liczby x.

   Rozwiązanie: Niech

   $$a(j) = \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right].$$

   Wykażemy równość

   $$a(j) = \begin{cases} 1, & \text{gdy } \ j \in \mathbb{P}, \\ 0, & \text{gdy } \ j \notin \mathbb{P}. \end{cases}$$

   Jeśli liczba j jest pierwsza, to z twierdzenia Wilsona (1.6.5) wiemy, że $(j-1)! + 1 \equiv 0 \pmod j$ i tym samym liczba $\frac{(j-1)!+1}{j}$ jest całkowita. Ponieważ $\frac{(j-1)!+1}{j} - \frac{(j-1)!}{j} = \frac{1}{j}$ oraz $j \geqslant 2$, więc otrzymujemy, że

   $$\left[\frac{(j-1)!}{j} \right] = \frac{(j-1)! + 1}{j} - 1$$

   i tym samym

   $$a(j) = \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right] = \left[\frac{(j-1)! + 1}{j} - \left(\frac{(j-1)! + 1}{j} - 1 \right) \right] = 1.$$

   Niech teraz j będzie liczbą złożoną. Jeśli $j = 4$, to bezpośrednie przeliczenie pokazuje, że $a(4) = 0$. Możemy zatem założyć, że $j \geqslant 6$. Zauważmy, że oznacza to, że $j = ab, 1 < a \leqslant b \leqslant j - 1$ i $j = ab | (j-1)!$. Istotnie, jeśli $a \neq b$, to nie ma czego dowodzić, bo liczby te są różnymi czynnikami występującymi w rozkładzie $(j-1)!$. Jeśli zaś $a = b$, to mamy, że $a = b \leqslant \sqrt{j}$ i wówczas liczby $a, 2a = 2b \leqslant 2\sqrt{j} \leqslant j - 1$ (bo $j \geqslant 6$) wchodzą w rozkład wyrażenia $(j-1)!$, co oznacza, że $ab | 2ab | (j-1)!$. Podsumowując, liczba $\frac{(j-1)!}{j}$ jest całkowita i dostajemy, że

   $$\begin{aligned} a(j) &= \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right] = \left[\frac{(j-1)! + 1}{j} \right] - \frac{(j-1)!}{j} \\ &= \frac{(j-1)!}{j} - \frac{(j-1)!}{j} = 0. \end{aligned}$$

Widzimy więc, że rozważana suma $\sum_{j=2}^{m} a(j)$ przyjmuje wartość $\pi(m)$.

5. Wykazać, że dla dowolnego $k \in \mathbb{N}$, liczba $e_k = \sum_{n=0}^{\infty} \frac{1}{n!^k}$ jest niewymierna.

Rozwiązanie: Przypuśćmy, że dla pewnego k liczba e_k jest wymierna. Oznacza to, że istnieją takie względnie pierwsze liczby $a, b \in \mathbb{N}$, że $e_k = \frac{a}{b}$. Wynika stąd, że liczba

$$x = b!^k \left(e_k - \sum_{i=0}^{b} \frac{1}{i!^k} \right) = \sum_{i=b+1}^{\infty} \frac{b!^k}{i!^k}$$

jest całkowita i dodatnia. Wykażemy, że $x < 1$. Istotnie, dla $i \geqslant b+1$, to

$$\frac{b!^k}{i!^k} < \frac{1}{\prod_{j=1}^{i-b}(b+j)} \leqslant \frac{1}{(b+1)^{k(i-b)}}.$$

Stąd otrzymujemy, że

$$\begin{aligned} x = \sum_{i=b+1}^{\infty} \frac{b!^k}{i!^k} &< \sum_{i=b+1}^{\infty} \frac{1}{(b+1)^{k(i-b)}} \leqslant \sum_{i=1}^{\infty} \frac{1}{(b+1)^{ki}} \\ &= \frac{1}{(b+1)^k} \frac{1}{1 - \frac{1}{(b+1)^k}} = \frac{1}{(b+1)^k - 1} < 1. \end{aligned}$$

Wykazaliśmy, że $x \in (0,1)$, a ponieważ $x \in \mathbb{Z}$, to mamy sprzeczność.

6. Niech p będzie dowolną nieparzystą liczbą pierwszą.

   (a) Wykazać równość
   $$\left(\frac{p-1}{2}\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

   (b) Wykazać, że dla dowolnego $k \in \{0, \ldots, p-1\}$ zachodzi
   $$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

Rozwiązanie: (a) Z twierdzenia Wilsona (1.6.5) mamy, że $(p-1)! \equiv -1 \pmod{p}$. Zauważmy teraz, że zbiory $\{\frac{p-1}{2} + i : \ i = 1, \ldots, (p-1)/2\}, \{p - i : \ i = 1, \ldots, (p-1)/2\}$ się pokrywają, możemy zatem napisać

$$-1 \equiv (p-1)! \equiv \left(\prod_{i=1}^{\frac{p-1}{2}} i \right) \left(\prod_{i=1}^{\frac{p-1}{2}} (p-i) \right) \equiv \left(\frac{p-1}{2}\right)!^2 (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Biorąc pod uwagę ostatnie przystawanie i mnożąc obie strony przez $(-1)^{\frac{p-1}{2}}$ otrzymujemy kongruencję z tezy naszego zadania.

(b) Niech $N = \binom{p-1}{k}$ i zauważmy, że

$$\begin{aligned} k!N = k!\binom{p-1}{k} &= k!\frac{(p-1)(p-2)\cdot\ldots\cdot(p-k)}{k!} \\ &= (p-1)(p-2)\cdot\ldots\cdot(p-k) \\ &\equiv (-1)(-2)\cdot\ldots\cdot(-k) \equiv (-1)^k k! \pmod{p}. \end{aligned}$$

Ponieważ $k \in \{0, \ldots, p-1\}$, więc $\mathrm{NWD}(k!, p) = 1$ i w konsekwencji możemy podzielić skrajne strony naszej kongruencji przez $k!$ otrzymując $N \equiv (-1)^k \pmod{p}$.

7. Niech $a, b \in \mathbb{Z}, p \in \mathbb{P}_{\geqslant 3}$ i załóżmy, że $p \nmid a$. Wykazać następujące równości:

(a)
$$\sum_{i=0}^{p-1}\left(\frac{ai+b}{p}\right)=0;$$

(b)
$$\sum_{i=0}^{p-1}\left(\frac{i(i+a)}{p}\right)=\begin{cases}-1, & \text{gdy } p\nmid a,\\ p-1, & \text{gdy } p|a.\end{cases}$$

Rozwiązanie:

(a) Oznaczmy naszą sumę z lewej strony tezy przez $S(p)$. Bez straty ogólności możemy założyć, że $a,b\in\{0,\ldots,p-1\}, a\neq 0$. Niech $\overline{a}:=a^{-1} \pmod p$. Z multiplikatywności symbolu Legendre'a mamy, że

$$\left(\frac{\overline{a}}{p}\right)S(p)=\sum_{i=0}^{p-1}\left(\frac{\overline{a}}{p}\right)\left(\frac{ai+b}{p}\right)=\sum_{i=0}^{p-1}\left(\frac{i+\overline{a}b}{p}\right).$$

Z równości $\{(i+\overline{a}b) \pmod p:\ i\in\{0,\ldots,p-1\}=\{0,\ldots,p-1\}$ i faktu, że w tym zbiorze jest tyle samo reszt co niereszt kwadratowych (i dokładnie jedna z tych liczb jest podzielna przez p), dostajemy, że $\left(\frac{\overline{a}}{p}\right)S(p)=0$ i w konsekwencji $S(p)=0$.

(b) Jeśli $p|a$, to $\left(\frac{i(i+a)}{p}\right)=\left(\frac{i^2}{p}\right)=\left(\frac{i}{p}\right)^2=1$ dla $i>0$. Oznacza to, że $S(p)=0+\sum\limits_{i=1}^{p-1}1=p-1$. Załóżmy zatem, że $p\nmid a$. Dla $i\in\{1,\ldots,p-1\}$ niech $\overline{i}:=i^{-1} \pmod p$. Jest jasne, że $\overline{i}\not\equiv 0 \pmod p$ i stąd

$$\begin{aligned}S(p)&=\sum_{i=1}^{p-1}\left(\frac{i(i+a)}{p}\right)=\sum_{i=1}^{p-1}\left(\frac{\overline{i}^2}{p}\right)\left(\frac{i(i+a)}{p}\right)\\&=\sum_{i=1}^{p-1}\left(\frac{\overline{i}i(\overline{i}i+a\overline{i})}{p}\right)=\sum_{i=1}^{p-1}\left(\frac{a\overline{i}+1}{p}\right).\end{aligned}$$

Ponieważ i przebiega układ niezerowych reszt modulo p, więc $\overline{i}$ również, a ponieważ $p\nmid a$, więc mamy równość zbiorów $\{(a\overline{i}) \pmod p:\ i\in\{1,\ldots,p-1\}\}=\{1,\ldots,p-1\}$. Stąd i punktu (a) wynika, że

$$\sum_{i=1}^{p-1}\left(\frac{a\overline{i}+1}{p}\right)=\sum_{i=1}^{p-1}\left(\frac{i+1}{p}\right)=\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)-\left(\frac{1}{p}\right)=-1$$

i dostajemy tezę.

8. Dla $f\in\mathbb{Z}[X]\setminus\mathbb{Z}$ i $k\in\mathbb{N}$ definiujemy zbiór:

$$\mathcal{P}_f=\{p\in\mathbb{P}:\ \text{istnieje takie } n\in\mathbb{N},\ \text{że } p|f(n)\}.$$

Udowodnić, że zbiór $\mathcal{P}_f$ jest nieskończony.

Rozwiązanie: Niech $f=\sum\limits_{i=0}^{d}a_iX^i$. Bez straty dla ogólności możemy założyć, że wielomian f jest nierozkładalny. Załóżmy, że zbiór $\mathcal{P}_f$ jest skończony i zapiszmy $\mathcal{P}_f=\{q_1,\ldots,q_m\}$. Niech $M=a_0q_1\cdot\ldots\cdot q_m$. Ponieważ $|M|>|a_0|$ i f jest nierozkładalny, więc $f(M)\neq 0$ (nierozkładalność pociąga brak pierwiastka w $\mathbb{Q}$ jako, że jest to ciało) i mamy

$$f(M)=a_0\left(1+\sum_{i=1}^{d}a_ia_0^{i-1}M^i\right).$$

Z naszego założenia o skończoności zbioru $\mathcal{P}_f$ wynika, że dla pewnego układu m nieujemnych liczb całkowitych $\alpha_1,\ldots,\alpha_m$, prawdziwa jest równość

$$1+\sum_{i=1}^{d}a_ia_0^{i-1}M^i=q_1^{\alpha_1}\cdot\ldots\cdot q_m^{\alpha_m}.$$

Ponieważ $f(M) \neq 0$, więc co najmniej jedna z liczb $\alpha_1, \ldots, \alpha_m$ jest > 0, powiedzmy $\alpha_j > 0$. Oznacza to, że q_j jest dzielnikiem liczby $1 + \sum_{i=1}^{d} a_i a_0^{i-1} M^i$ i w konsekwencji $q_j|1$ (bo dzieli również M), co prowadzi do sprzeczności.

9. Niech $a \in \mathbb{N}_{\geqslant 2}, b \in \mathbb{Z} \setminus \{0\}, \mathrm{NWD}(a,b) = 1$ i rozważmy ciąg o wyrazach $A_n = a^n + b$. Udowodnić, że zbiór

$$\mathcal{P}(a,b) = \{p \in \mathbb{P} : \text{ istnieje takie } n \in \mathbb{N}, \text{ że } p|A_n\}$$

jest nieskończony.

Rozwiązanie: Załóżmy, że zbiór $\mathcal{P}(a,b)$ jest skończony i napiszmy

$$\mathcal{P}(a,b) = \{q_1, \ldots, q_m\}.$$

Dla danego n oraz $i \in \{1, \ldots, m\}$ niech $q_i^{\alpha_i(n)}$ oznacza największą potęgę liczby pierwszej dzielącą A_n. Ponieważ zbiór $\mathcal{P}(a,b)$ jest skończony, więc istnieje taki indeks $i_0 \in \{1, \ldots, m\}$, że dla dowolnych n_1, n_2 spełniających warunki: $n_1 < n_2$ i $n_2 - n_1 < m$ prawdziwe są podzielności

$$q_{i_0}^{\alpha_{i_0}(n_1)} | A_{n_1} \quad \text{oraz} \quad q_{i_0}^{\alpha_{i_0}(n_2)} | A_{n_2}.$$

Niech teraz $u = \min\{\alpha_{i_0}(n_1), \alpha_{i_0}(n_2)\}$, co oznacza, że

$$q_{i_0}^{u} | A_{n_1} \quad \text{oraz} \quad q_{i_0}^{u} | A_{n_2}$$

i w konsekwencji $q_{i_0}^u | (a^{n_2} - a^{n_1}) = a^{n_1}(a^{n_2-n_1} - 1)$. Ponieważ q_{i_0} nie dzieli a, więc $q_{i_0}^u | (a^{n_2-n_1} - 1)$ i prawdziwa jest nierówność $q_{i_0}^u < a^m - 1$. Z drugiej strony, ponieważ zbiór $\mathcal{P}(a,b)$ jest skończony, więc prawdziwa jest nierówność $q_{i_0}^{mu} > a^n$. Ponieważ m jest ustalone otrzymujemy nierówność

$$a^m - 1 > q_{i_0}^u > a^{\frac{n}{m}},$$

która dla dostatecznie dużych n nie może być prawdziwa.

8.2 Zadania z teorii grup

1. Niech $a, b, c \in \mathbb{R}$ będą ustalonymi parametrami. W zbiorze $G = \mathbb{R}$ definiujemy działanie $\cdot$ w następujący sposób: $x \cdot y = ax + by + c$.

   (a) Znaleźć wszystkie trójki a, b, c, że działanie $\cdot$ jest łączne.

   (b) Znaleźć wszystkie trójki a, b, c, że para $(G, \cdot)$ jest grupą.

   Rozwiązanie: (a) Działanie jest oczywiście wewnętrzne. Bezpośrednie sprawdzenie pokazuje, że dla dowolnych $x, y, z \in G$ mamy równości

$$(x \cdot y) \cdot z = a(x \cdot y) + bz + c = a^2 x + aby + bz + c(a+1),$$
$$x \cdot (y \cdot z) = ax + b(y \cdot z) + c = ax + aby + b^2 z + (b+1)c.$$

   Oznacza to, że nasze działanie jest łączne wtedy i tylko wtedy, gdy spełnione są równości

$$a = a^2, \quad b = b^2, \quad c(b-a) = 0.$$

   Rozwiązania tego układu równań mają postać $(a, b, c) \in \mathcal{A}$, gdzie

$$\mathcal{A} = \{(0,0,t), (0,1,0), (1,0,0), (1,1,t)\},$$

   gdzie $t \in \mathbb{R}$ jest dowolne ustalone.

   (b) Skoro działanie jest wewnętrzne, to naszym pierwszym krokiem jest znalezienie elementu neutralnego. Oznaczmy go przez e. Zgodnie z definicją, dla dowolnego $x \in G$ musi być $e \cdot x = x \cdot e = x$. Równoważnie

$$e \cdot x = ea + bx + c = x \quad \text{oraz} \quad x \cdot e = ax + be + c = x.$$

Skoro $e \cdot x = x \cdot e$, to musi być $ae + bx = ax + be$ lub równoważnie $(a-b)(x-e) = 0$. Ponieważ x jest dowolnym elementem G, więc $a = b$. Oczywiście $a = b \neq 0$. Następnie, skoro $e \cdot x = x$ oraz $a = b$, to mamy równość $ae + ax + c = x$. W konsekwencji $a = b = 1$ oraz $e = -c$.

Korzystając z wyniku otrzymanego w punkcie (a) dostajemy, że jeśli $a = b = 1$ i c jest dowolne, to nasze działanie ma element neutralny $e = -c$ i jest łączne. Pozostaje znaleźć teraz warunki na c, które gwarantują istnienie elementu odwrotnego. Niech zatem x' oznacza element odwrotny do x. Skoro $a = b = 1$, to $x \cdot x' = -c$ wtedy i tylko, gdy $x + x' + c = -c$ i w konsekwencji $x' = -x - 2c$ jest elementem odwrotnym.

Podsumowując: G z działaniem $x \cdot y = ax + by + c$ jest grupą wtedy i tylko wtedy, gdy $a = b = 1$ i c jest dowolnym elementem $\mathbb{R}$. Zauważmy również, ze przy takim wyborze a, b, c, grupa G jest abelowa.

2. Wykazać, że jeśli dla dowolnego elementu x grupy G zachodzi równość $x^2 = 1$, to G jest abelowa.

Rozwiązanie: Niech x, y będą dowolnymi elementami grupy G. Naszym celem jest wykazanie, że $xy = yx$. Z założenia $1 = (xy)^2 = xyxy$. Mnożąc skrajne strony równości przez x z prawej strony dostajemy $x = x^2(yxy) = yxy$. Mnożąc otrzymaną równość z prawej strony przez y dostajemy $xy = (yxy)y = yxy^2 = yx$ i stąd $xy = yx$, co kończy dowód.

3. Wykazać, że jeśli istnieje taka liczba $k \in \mathbb{N}$, że dla dowolnych elementów x, y grupy G zachodzi równość

$$(xy)^n = x^n y^n \quad \text{dla} \quad n = k, k+1, k+2,$$

to G jest grupą abelową.

Rozwiązanie: Skoro $x^k y^k = (xy)^k$, to mnożąc obie strony tej równości przez xy, a następnie korzystając z równości $(xy)^{k+1} = x^{k+1}y^{k+1}$, otrzymujemy

$$xyx^k y^k = (xy)^{k+1} = x^{k+1}y^{k+1}$$

lub równoważnie, po skróceniu z lewej przez x, a z prawej przez y^k, dochodzimy do równości $(*)$ $yx^k = x^k y$. Rozumując w analogiczny sposób, po zastąpieniu k przez $k+1$, otrzymujemy równość $(**)$ $yx^{k+1} = x^{k+1}y$. Z równości $(*)$ i $(**)$ mamy

$$x^{k+1}y = yx^{k+1} = (yx^k)x = (x^k y)x,$$

co po skróceniu przez x^k z lewej daje równość $xy = yx$. Ponieważ x, y były dowolnymi elementami grupy G dowodzi to, że G jest abelowa.

4. Niech G będzie grupą generowaną przez dwa elementy x, y.

   (a) Odpowiedzieć na pytanie, jaki jest rząd grupy G, jeśli generatory spełniają relacje $x^3 = y^2 = (xy)^2 = 1$?

   (b) Odpowiedzieć na pytanie, jaki jest rząd grupy G, jeśli generatory spełniają relacje $x^3 = y^2 = (xy)^3 = 1$?

Rozwiązanie: (a) Ponieważ x i y są generatorami i spełniają zależności $x^3 = y^2 = 1$, to każdy element w grupie G daje się zapisać jako iloczyn postaci $x^{a_1}y^{b_1} \cdot \ldots \cdot x^{a_k}y^{b_k}$, gdzie $a_i \in \{0, 1\}, b_i \in \{0, 1, 2\}$. Zauważmy jednak, że z równości $(xy)^2 = 1$, po przemnożeniu z lewej strony przez x^2 dostajemy równość $yxy = x^2$ lub równoważnie $yx = x^2 y$ (i tym samym $xyx = y$). Oznacza to, że każdy element po redukcji jest postaci $1, x, y, xy, yx = x^2y, x^2$, a jako że elementy te są różne między sobą otrzymujemy, że rząd grupy G wynosi 6.

(b) Stosujemy podobne rozumowanie jak w punkcie (a). Równość $(xy)^3 = 1$ po przemnożeniu z prawej przez y i lewej przez x^2 prowadzi nas do związku $(xy)^2 = yx^2$ i analogicznie $(yx)^2 = x^2y$. Rozważając ogólną postać elementu w grupie G, wnioskujemy, że G składa się z elementów $1, x, y, xy, yx, xyx, yxy, x^2, x^2y, yx^2, x^2yx, yx^2y$, zaś sprawdzając bezpośrednio widzimy, że żadne dwa z nich nie są sobie równe. Otrzymujemy stąd, że rząd G wynosi 12.

5. Ustalmy $k \geqslant 3$. Niech grupa U_k będzie generowana przez elementy x, y spełniające relacje $x^2 = y^k = (xy)^2 = 1$. Wykazać, że grupa U_k ma rząd $2k$ i jest izomorficzna z grupą macierzy 2×2 generowaną przez elementy X, Y postaci:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} \zeta_k & 0 \\ 0 & \zeta_k^{-1} \end{pmatrix},$$

gdzie $\zeta_k = e^{\frac{2\pi i}{k}}$.

Rozwiązanie: Zauważmy najpierw, że każdy element grupy U_k jest postaci $x^\alpha y^\beta$, gdzie $\alpha \in \{0,1\}$ oraz $\beta \in \{0,\ldots,k-1\}$. Jest tak bowiem ze związku $(xy)^2 = 1$ mamy, że $yx = x^{-1}y^{-1} = xy^{-1}$ i w konsekwencji dla dowolnego $\beta \in \mathbb{Z}$ mamy równość $y^\beta x = xy^{-\beta}$. Stąd natychmiast wnioskujemy, że rząd U_k wynosi $2k$. Zauważmy, że $X^2 = I$, gdzie I jest macierzą jednostkową. Analogicznie sprawdzamy, że $Y^k = I$ (jest to konsekwencja tożsamości

$$\begin{pmatrix} p & 0 \\ 0 & q \end{pmatrix}^k = \begin{pmatrix} p^k & 0 \\ 0 & q^k \end{pmatrix},$$

która zachodzi dla dowolnego $k \in \mathbb{Z}$ oraz $a, b \in \mathbb{C}$). Zauważmy teraz, że $XY = \begin{pmatrix} 0 & \zeta_k \\ \zeta_k^{-1} & 0 \end{pmatrix}$, a stąd $(XY)^2 = I$. Niech teraz $G = \langle X, Y\rangle < M(2,2,\mathbb{C})$. By pokazać, że $U_k \cong G$ wystarczy bezpośrednio sprawdzić, że odwzorowanie $\phi : U_k \to G$ zadane jako: $\phi(x^\alpha y^\beta) = X^\alpha Y^\beta$ jest poszukiwanym izomorfizmem.

6. Niech G będzie grupą skończoną i $H \subset G$ będzie jej podgrupą właściwą. Wykazać, że $\bigcup\limits_{x\in G} x^{-1}Hx \subsetneq G$.

   Rozwiązanie: Niech $|G| = n$ i połóżmy $h := [G : H]$ – zauważmy, że $h > 1$, gdyż H jest podgrupą właściwą. Ponieważ $H \subset \{g \in G : gHg^{-1} = H\}$, więc wiadomo, że istnieje co najwyżej h podgrup sprzężonych z H w G. Zauważmy jednak, że wszystkie te podgrupy mają co najmniej jeden element wspólny: element neutralny. Oznacza to, że liczba elementów w podgrupach sprzężonych z H wynosi co najwyżej $1+(|H|-1)h = 1+|H|[G : H] - h = n + 1 - h < n$ co kończy dowód.

7. Niech G będzie grupą skończoną, $N = |G|$ i $n \in \mathbb{N}$ spełnia warunek $\mathrm{NWD}(n, N) = 1$. Wykazać, że dla każdego elementu $x \in G$ istnieje taki element $y \in G$, że $x = y^n$.

   Rozwiązanie: Ponieważ G jest skończona, więc dla dowolnego elementu $z \in G$ zachodzi równość $z^N = 1$. Skoro $\mathrm{NWD}(n, N) = 1$, więc istnieją takie liczby całkowite a, b, że $1 = an + bN$. Stąd $x = x^{an+bN} = (x^a)^n(x^N)^b = (x^a)^n$ i wystarczy przyjąć $y = x^a$.

8. Podgrupę H grupy G nazywamy *specjalną*, jeśli dla każdej pary elementów $x, y \in G, x \notin H$, istnieje dokładnie jeden taki element $z \in H$, że $y^{-1}xy = z^{-1}xz$. Wykazać, że każda specjalna podgrupa grupy G jest podgrupą normalną w G.

   Rozwiązanie: Niech H będzie podgrupą specjalną G. Chcemy wykazać, że dla dowolnych $g \in G, h \in H$ jest $ghg^{-1} \in H$ lub równoważnie $g^{-1}hg \in H$. Oznaczmy $x = ghg^{-1}$ i przypuśćmy, że $x \notin H$. Ponieważ H jest podgrupa specjalną, więc istnieje dokładnie jeden taki element $z \in H$, że $h = g^{-1}xg = z^{-1}xz$. W konsekwencji $x = zhz^{-1} \in H$ i dostajemy tezę.

9. Niech G będzie grupą i $H < C(G)$, gdzie $C(G)$ jest centrum grupy G. Wykazać, że H jest podgrupą normalną grupy G oraz, że jeśli dodatkowo G/H jest grupą cykliczną, to G jest abelowa.

   Rozwiązanie: Na początek dowiedziemy normalności H. Wystarczy wykazać, że dla dowolnego $h \in H, g \in G$ mamy $ghg^{-1} \in H$. Ponieważ $h \in H < C(G)$, to dla dowolnego $g \in G$ mamy, że $gh = hg$. Stąd $ghg^{-1} = (hg)g^{-1} = h \in H$ i dostajemy tezę.

   Jeśli G/H jest cykliczna, to istnieje taki element $x \in G$, że xH jest generatorem grupy G/H. Zauważmy, że oznacza to, że $G = \langle x, H\rangle$. Istotnie, załóżmy, że istnieje taki element $y \in G$, że $y \notin \langle x, H\rangle$ i rozważmy $yH \in G/H$. Wtedy $yH = x^kH$ dla pewnego k, więc w szczególności $y = x^kh' \in \langle x, H\rangle$ co prowadzi do sprzeczności. Skoro $G = \langle x, H\rangle$, to wiemy, że G jest generowana przez elementy, które są parami przemienne. Dowodzi to, że G jest abelowa.

10. Wyznaczyć grupę automorfizmów grupy C_n.

    Rozwiązanie: Na początek zauważmy, że jeśli $f \in \mathrm{End}(C_n)$, to istnieje taki element $a \in \mathbb{Z}$, że $f(x) = ax$ dla $x \in C_n$, co jest natychmiastową konsekwencją cykliczności grupy C_n. Jeśli odwzorowanie $f(x) = ax$ jest odwracalne, to oznacza, że istnieje takie $b \in \mathbb{Z}$, że dla dowolnego $x \in \mathbb{C}_n$ mamy $abx = x$. W szczególności, biorąc $1 \in C_n$ mamy, że $ab = 1 \in C_n$, zaś równoważnie $ab \equiv 1 \pmod n$. Dla danego a rozważana kongruencja ma rozwiązanie wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, n) = 1$. Stąd wnioskujemy, że $f(x) = ax$ jest automorfizmem wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, n) = 1$, co oznacza, że $\mathrm{Aut}(C_n) = \{f_a : f_a(x) = ax \text{ dla } x \in C_n\}$. Z tego opisu natychmiast wnioskujemy, że $\mathrm{Aut}(C_n) \cong \Phi(n) = \{a \in \{1,\ldots,n\} : \mathrm{NWD}(a, n) = 1\}$, gdzie działaniem w $\Phi(n)$ jest mnożenie (modulo n).

11. Podać przykład dwóch nieizomorficznych grup G_1, G_2 dla których $\mathrm{Aut}(G_1) \cong \mathrm{Aut}(G_2)$.

Rozwiązanie: Korzystając z poprzedniego zadania wnioskujemy, że jeśli p jest nieparzystą liczba pierwszą, to $\mathrm{Aut}(C_p) \cong \Phi(p)$ oraz $\mathrm{Aut}(C_{2p}) \cong \Phi(2p)$. Oczywiście $C_p \ncong C_{2p}$, niemniej jednak $|\Phi(p)| = \phi(p) = \phi(2p) = |\Phi(2p)|$ i z twierdzenia o istnieniu pierwiastka prymitywnego (6.2.15) wiemy, że grupy $\Phi(p), \Phi(2p)$ są cykliczne, a więc izomorficzne.

8.3 Zadania z teorii pierścieni

1. Niech I, J, K będą ideałami w pierścieniu R. Wykazać, że jeśli $I \subset K$, to $(I + J) \cap K = I + (J \cap K)$.

Rozwiązanie: Niech $x \in (I + J) \cap K$. Oznacza to, że istnieją takie elementy $u \in I \subset K, v \in J$, że $x = u + v$. Ponieważ $x \in K$, więc $v = x - u \in K$. Jednocześnie, $x - u = v \in J$, więc możemy napisać $x = u + v \in I + (J \cap K)$. Dowodzi to zawierania $(I + J) \cap K \subset I + (J \cap K)$. Jeśli teraz $x \in I + (J \cap K)$, to istnieją takie elementy $u \in I, k \in J \cap K$, że $x = u + k$. Mamy oczywiście $u \in I + J$ oraz $k \in J \cap K \subset J \subset I + J$, co oznacza, że $x \in I + J$. Jednocześnie, $u \in I \subset K$ oraz $k \in K$, a stąd $x = u + v \in K + K = K$. W konsekwencji $x \in (I + J) \cap K$ i dostajemy tezę.

2. Niech R będzie pierścieniem oraz I takim skończenie generowanym ideałem w R, że $I = I^2$. Znaleźć taki element $x \in R$, że $x^2 = x$ oraz $I = Rx$. (Element x pierścienia R, który spełnia równość $x^2 = x$ nazywamy idempotentem.)

Rozwiązanie: Skoro I jest skończenie generowany, to istnieją takie elementy $a_1, \ldots, a_n \in I$, że $I = Ra_1 + \ldots + Ra_n$. Zauważmy również, że $I = Ia_1 + \ldots + Ia_n$. Istotnie, zawieranie $\supseteq$ jest trywialne. Z drugiej strony, skoro $x \in I = I^2$, to istnieją takie elementy $u_i, v_i \in I$, że $x = \sum_{i=1}^{n} u_i v_i$. Jednakże, dla dowolnego $i \in \{1, \ldots, n\}$, każdy z elementów u_i, v_i jest kombinacją liniową $a_1, \ldots, a_n$ o współczynnikach z R, więc $u_i v_i = \sum_{i,j=1}^{n} r_{i,j} a_i a_j$ dla pewnych $r_{i,j} \in R$. Stąd natychmiast otrzymujemy, że $u_i v_i \in Ia_1 + \ldots + Ia_n$, i w konsekwencji $x \in Ia_1 + \ldots + Ia_n$. Skoro więc zachodzi $(\star)$ $I = Ia_1 + \ldots + Ia_n (\star)$, to dla dowolnego $i \in \{1, \ldots, n\}$ istnieje takie element $b_i \in I$, że $(1 - b_i)I \subset Ia_i + Ia_{i+1} + \ldots + Ia_n$. Dowód przeprowadzić można indukcyjnie względem i, korzystając z faktu, że dla $i = 1$ rozważana własność jest konsekwencją równości $(\star)$ (wystarczy wziąć $b_1 = 0$). Z rozumowania indukcyjnego wynika, że istnieje element $x = b_{n+1} \in I$ spełniający warunek $(1 - x)I = (0)$ – ten właśnie element x spełnia warunki naszego zadania. Istotnie, skoro $(1 - x)I = (0)$, to $x(1 - x) = 0$ i $x = x^2$, czyli $I = Ix$ i ostatecznie $I = Rx$.

3. Niech R będzie pierścieniem i dla ideału I w R zdefiniujmy radykał ideału I w następujący sposób:

$$\mathrm{rad}(I) = \{x \in R : \ x^n \in I\}.$$

   (a) Wykazać, że $\mathrm{rad}(I)$ jest ideałem w R.

   (b) Wykazać, że $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$.

   (c) Wykazać, że $\mathrm{rad}(I \cap J) = \mathrm{rad}(I) \cap \mathrm{rad}(J)$, gdzie J jest ideałem w R.

   (d) Wykazać, że $\mathrm{rad}(I + J) = \mathrm{rad}(\mathrm{rad}(I) + \mathrm{rad}(J))$, gdzie J jest ideałem w R.

Rozwiązanie: (a) Jeśli $r \in R$, $x \in \mathrm{rad}(I)$ i $m \in \mathbb{N}$ jest takie, że $x^m \in I$, to $(rx)^m = r^m x^m \in I$ i tym samym $rx \in \mathrm{rad}(I)$. Jeśli teraz $x, y \in \mathrm{rad}(I)$ oraz $m, n \in \mathbb{N}$ są takie, że $x^m, y^n \in I$, to wówczas

$$(x + y)^{m+n} = \sum_{i=0}^{m+n} \binom{m+n}{i} x^i y^{m+n-i}.$$

Zauważmy teraz, że jeśli $i < m$, to $m + n - i \geqslant n$, co oznacza, że każdy z elementów $\binom{m+n}{i} x^i y^{m+n-i}$ należy do ideału I (bo $y^{m+n-i} \in I$). Tym samym ich suma również należy do I. Jeśli zaś $i \geqslant m$, to $x^i \in I$ i dostajemy analogiczną własności. Tym samy cała rozważana suma, a więc i element $(x + y)^{m+n}$ należą do I. Oznacza to, że $x + y \in \mathrm{rad}(I)$.

(b) Jest jasne, że $I \subset \mathrm{rad}(I)$. W szczególności $\mathrm{rad}(I) \subset \mathrm{rad}(\mathrm{rad}(I))$. Niech zatem $x \in \mathrm{rad}(\mathrm{rad}(I))$. Istnieje więc takie $m \in \mathbb{N}$, że $x^m \in \mathrm{rad}(I)$. Z definicji radykału wynika, że istnieje też takie $n \in \mathbb{N}$, że $(x^m)^n = x^{mn} \in I$. Oznacza to jednak, że $x \in \mathrm{rad}(I)$.

(c) Ponieważ $I \cap J \subset I, J$, więc $\mathrm{rad}(I \cap J) \subset \mathrm{rad}(I) \cap \mathrm{rad}(J)$. Niech zatem $x \in \mathrm{rad}(I) \cap \mathrm{rad}(J)$. Onzacza to, że istnieją takie liczby $m, n \in \mathbb{N}$, że $x^m \in I, x^n \in J$. Stąd $(x^m)^n = x^{mn} = (x^n)^m \in I \cap J$, co implikuje, że $x \in \mathrm{rad}(I \cap J)$.

(d) Ponieważ $I, J \subset I+J$, więc $\mathrm{rad}(I)+\mathrm{rad}(J) \subset \mathrm{rad}(I+J)$ i w konsekwencji $\mathrm{rad}(\mathrm{rad}(I)+\mathrm{rad}(J)) \subset \mathrm{rad}(I+J)$. Niech teraz $x \in \mathrm{rad}(I+J)$. Oznacza to, że istnieje takie $n \in \mathbb{N}$, że $x^n \in I+J$. Równoważnie, istnieją takie elementy $u \in I \subset \mathrm{rad}(I), v \in J \subset \mathrm{rad}(J)$, że $x^n = u + v \in \mathrm{rad}(I) + \mathrm{rad}(J)$. Otrzymujemy zatem, że $x \in \mathrm{rad}(\mathrm{rad}(I) + \mathrm{rad}(J))$ i stąd teza.

4. Niech
$$A = \left\{ \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix} : \ z_1, z_2 \in \mathbb{C} \right\}.$$
Wykazać, że A jest pierścieniem bez dzielników zera.

Rozwiązanie: Zauważmy, że jeśli $z_1 = a + bi, z_2 = c + di$, to możemy napisać
$$M = \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix} = aI_2 + bI + cJ + dK,$$
gdzie
$$I = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$
Bezpośrednie sprawdzenie pokazuje, że zachodzą relacje
$$I^2 = J^2 = K^2 = -I_2, \ IJ = -JI = K, KI = -IK = J, JK = -KJ = I.$$
Korzystając z tych relacji można sprawdzić, że A istotnie jest pierścieniem (nieprzemiennym). Ponieważ dla macierzy M zachodzi równość $\det(M) = a^2 + b^2 + c^2 + d^2$, więc dla $M \in A \setminus \{0\}$, M jest odwracalna. Implikuje to, że w A nie ma dzielników zera. (Rozważany pierścień jest przykładem tzw. pierścienia z dzieleniem, czyli pierścienia nieprzemiennego, w którym każdy niezerowy element jest odwracalny).

5. Niech R będzie pierścieniem. Wykazać, że następujące warunki są równoważne

   (a) jedynym elementem nilpotentym w R (tzn. takim dla którego istnieje $n \in N$ że $x^n = 0$) jest 0;

   (b) $U(R[X]) = U(R)$.

Rozwiązanie: $(a) \implies (b)$ Oczywiście, do obu zbiorów należą elementy odwracalne w pierścieniu R. Niech więc $f = \sum_{i=0}^{m} a_i X^i, g = \sum_{i=0}^{n} b_i X^i \in R[X]$, gdzie $\deg(f) = m, \deg(g) = n$ i przynajmniej jeden z wielomianów nie jest stałą. Załóżmy, że $fg = 1$. W szczególności $a_0 b_0 = 1$, czyli $a_0, b_0 \in U(R)$ oraz $a_m b_n = 0$. Napiszmy
$$fg = 1 + \sum_{j=1}^{m+n} c_j X^j, \quad \text{gdzie} \quad c_j = \sum_{i=0}^{j} a_j b_{i-j}.$$
W powyższym zapisie przyjeliśmy konwencję, że $a_j = 0$ dla $j > n$ i analogicznie dla b_j. Ponieważ $fg = 1$, więc $c_j = 0$ dla $j > 0$. Zauważmy, że skoro $c_{m+n} = a_m b_n = 0$ i $c_{m+n-1} = a_m b_{n-1} + a_{m-1} b_n = 0$, to po przemnożeniu przez b_n stronami, otrzymujemy równość $a_{m-1} b_n^2 = 0$. Rozumując dalej analogicznie (indukcyjnie względem i) otrzymujemy, że
$$0 = a_m b_n = a_{m-1} b_n^2 = a_{m-2} b_n^3 = \ldots = a_1 b_n^m = a_0 b_n^{m+1}.$$
Ponieważ a_0 jest jednością, więc oznacza to, że b_n jest elementem nilpotentnym i stąd $b_n = 0$ – sprzeczność.

$(b) \implies (a)$ Dla dowodu nie wprost załóżmy, że $a \in R^*$ jest elementem nilpotentym, tzn. istnieje takie $n \in \mathbb{N}$, że $a^n = 0$ i $a^i \neq 0$ dla $i < n$. Zauważmy, że wówczas wielomian $f = 1 + a^{n-1} X \in U(R[X])$. Istotnie
$$(1 + a^{n-1} X)(1 - a^{n-1} X) = 1 - a^{2(n-1)} X^2 = 0,$$
bo $2(n-1) \geqslant n$ dla $n \geqslant 2$. Jako, że stopień f jest dodatni mamy sprzeczność.

6. Wykazać, że $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ jest pierścieniem Euklidesa.

   Rozwiązanie: Niech $\phi : \mathbb{Z}[i] \ni a + bi \mapsto a^2 + b^2 \in \mathbb{N}_0$. Jest jasne, że jeśli $z_j = a_j + b_j i$ dla $j = 1, 2$, to $\phi(z_1 z_2) = \phi(z_1)\phi(z_2)$, (de facto $\phi(z) = |z|^2$). Zauważmy, że

$$\frac{z_1}{z_2} = \frac{a_1 + b_1 i}{a_2 + b_2 i} = \frac{a_1 a_2 + b_1 b_2 - (a_1 b_2 - a_2 b_1)i}{\phi(z_2)}.$$

   Z algorytmu dzielenia z resztą wynika, że istnieją takie liczby całkowite $q_i, r_i, i = 1, 2$, że

$$a_1 a_2 + b_1 b_2 = q_1 \phi(z_2) + r_1, \quad a_1 b_2 - a_2 b_1 q_2 \phi(z_2) + r_2$$

   oraz $-\frac{1}{2}\phi(z_2) \leqslant r_i \leqslant \frac{1}{2}\phi(z_2)$. Niech zatem $q = q_1 - q_2 i, r = r_1 - r_2 i$. Przy takim określeniu q, r zachodzi równość

$$z_1 = q z_2 - \frac{r}{\overline{z_2}} \implies R := \frac{r}{\overline{z_2}} \in \mathbb{Z}[i], \quad (\overline{z} \text{ oznacza sprzężenie liczby zespolonej})$$

   By zakończyć dowód, wystarczy wykazać, że $\phi(R) < \phi(z_2)$. By zaś tego dowieść wystarczy zauważyć, że $\phi(r) = \phi(R\overline{z_2}) = \phi(R)\phi(\overline{z_2}) = \phi(R)\phi(z_2)$. Ponieważ

$$\phi(r) = r_1^2 + r_2^2 \leqslant 2 \cdot \left(\frac{1}{2}\phi(z_2)\right)^2 = \frac{1}{2}\phi(z_2)^2,$$

   więc

$$\phi(R) = \frac{\phi(r)}{\phi(z_2)} \leqslant \frac{1}{2}\phi(z_2) < \phi(z_2)$$

   i dostajemy tezę.

7. Niech R będzie pierścieniem i I ideałem w R. Wykazać, że

$$J := \left\{ \sum_{i=0}^{n} a_i X^i \in R[X] : \ a_0 \in I \ \text{ oraz } \ a_i \in R, i = 1, \ldots, n \right\}$$

   jest ideałem w $R[X]$. Wykazać, że jeśli I jest ideałem pierwszym (maksymalnym), to J jest ideałem pierwszym (maksymalnym).

   Rozwiązanie: By dowieść pierwszej części tezy rozważmy odwzorowanie

$$\Phi : \ R[X] \ni f \mapsto f(0) \in R,$$

   które jest epimorfizmem pierścieni. Zauważmy, że $J = \Phi^{-1}(I)$, co implikuje, że J jest ideałem w $R[X]$. Rozważmy teraz naturalny epimorfizm $\pi : \ R \to R/I$ oraz odwzorowanie

$$\Phi \circ \pi : \ R[X] \to R/I,$$

   które jest więc również epimorfizmem pierścieni. Mamy również, że

$$\mathrm{Ker}(\Phi \circ \pi) = \{f \in R[X] : \ \Phi \circ \pi(f) = I\} = J.$$

   Oznacza to na podstawie twierdzenia o izomorfizmie, że $R[X]/J \cong R/I$. Jeśli I jest ideałem pierwszym (maksymalnym), to również $R[X]/J$ jest ideałem pierwszym (maksymalnym).

8. Niech $n \in \mathbb{N}_{\geqslant 3}$ będzie liczbą nieparzystą, która nie jest kwadaratem liczby naturalnej. Wykazać, że element $2 \in \mathbb{Z}[i\sqrt{n}]$ jest nierozkładalny, ale nie jest pierwszy.

   Rozwiązanie: Na początek zauważmy, że $(1 + i\sqrt{n})(1 - i\sqrt{n}) = n + 1 = 2k$ dla pewnego $k \in \mathbb{N}$. Ponieważ $2|n + 1$ i $2 \nmid 1 \pm i\sqrt{n}$, więc 2 nie jest elementem pierwszym w $\mathbb{Z}[i\sqrt{n}]$. Pokażemy teraz, że 2 jest elementem nierozkładalnym. Dla dowodu nie wprost przypuśćmy, że $2 = xy$ dla pewnych $x, y \in \mathbb{Z}[i\sqrt{n}]$. Obkładając tę równość stronami przez sprzężenie, dostajemy równość $2 = \overline{xy}$. Jeśli $x = a + bi\sqrt{n}, y = c + di\sqrt{n}$ dla $a, b, c, d \in \mathbb{Z}$, to

$$4 = x\overline{x}y\overline{y} = (a^2 + nb^2)(c^2 + nd^2).$$

   Oznacza to, że $a^2 + nb^2 | 4$, więc $a^2 + nb^2 \in \{1, 2, 4\}$. Jeśli $a^2 + nb^2 = 1$, to $a = \pm 1, b = 0$ i x jest jednością. Równość $a^2 + nb^2 = 2$ jest niemożliwa, więc musi być $a^2 + nb^2 = 4$. Wówczas jednak $c^2 + nd^2 = 1$ i y jest jednością.

9. Niech L będzie ciałem i $f, g \in \mathrm{End}(L)$. Wykazać, że $K = \{x \in L : \ f(x) = g(x)\}$ jest podciałem ciała L.

   Rozwiązanie: Każdy endomorfizm ciała jest monomorfizmem jako, że gdy $f(x) = 0$ to gdyby $x \neq 0$ oznaczałoby to, że $1 = f(x \cdot x^{-1}) = f(x) \cdot [f(x)]^{-1} = 0$ mielibyśmy sprzeczność. Stąd f, g są monomorfizmami. Zauważmy, że zbiór K jest zamknięty ze względu na działania dodawania i mnożenia. Istotnie, jeśli $x_1, x_2 \in K$, to $f(x_1) = g(x_1), f(x_2) = g(x_2)$, więc $f(x_1 \circ x_2) = g(x_1 \circ x_2)$, gdzie $\circ \in \{+, \cdot\}$. Ponadto $0, 1 \in K$. Pozostaje wykazać, że każdy element z K jest odwracalny w K. Jeśli jednak $x \in K$ oraz $y \in L$ jest taki, że $xy = 1$, to oczywiście $f(y) = f(x)^{-1} = g(x)^{-1} = g(y)$ i dostajemy tezę.

10. Niech $d \in \mathbb{N}$ będzie liczbą bezkwadratową. Wyznaczyć $\mathrm{Aut}(\mathbb{Q}[\sqrt{d}])$.

    Rozwiązanie: Na początek zauważmy, że $\mathrm{Aut}(\mathbb{Q}) = \{id\}$. Istotnie, ponieważ $f(0) = f(0+0) = f(0) + f(0)$, to $f(0) = 0$. Następnie, $f(1) = f(1 \cdot 1) = f(1)f(1) = f(1)^2$, a ponieważ f jest automorfizmem, więc $f(1) = 1$. Ponadto $1 = f(1) = f((-1)(-1)) = f(-1)f(-1)$ i stąd $f(-1) = -1$ (bo f monomorfizm). W konsekwencji, dla $m \in \mathbb{Z}$ zachodzi równość $f(m) = m$. Jeśli teraz $m \in \mathbb{Z}$ i $n \in \mathbb{N}$, to

$$m = f(m) = f\left(n \cdot \frac{m}{n}\right) = f(n) f\left(\frac{m}{n}\right) = n f\left(\frac{m}{n}\right).$$

    Stąd $f(m/n) = m/n$ i widzimy, że jedyny automorfizm $\mathbb{Q}$, to automorfizm identycznościowy.

    Niech teraz $f \in \mathrm{Aut}(\mathbb{Q}[\sqrt{d}])$. Rozumując jak wyżej dostajemy, że dla dowolnego $a \in \mathbb{Q}$ mamy $f(a) = a$. Jeśli teraz $x = a + b\sqrt{d}$, to

$$f(x) = f(a + b\sqrt{d}) = f(a) + f(b) f(\sqrt{d}) = a + b f(\sqrt{d}).$$

    Wiemy jednak, że $d = f(d) = f(\sqrt{d}^2) = f(\sqrt{d})^2$ i w konsekwencji $f(\sqrt{d}) = \sqrt{d}$ lub $f(\sqrt{d}) = -\sqrt{d}$. Wobec tego $f = id$ lub $f(a + b\sqrt{d}) = a - b\sqrt{d}$, co daje, że $\mathrm{Aut}(\mathbb{Q}[\sqrt{d}]) \cong \mathbb{Z}_2$.

8.4 Zadania z teorii ciał

1. Dla wielomianu $f = X^4 + pX^2 + qX + r \in K[X]$ podać warunek konieczny i wystarczający na istnienie rozkładu postaci $f = (X^2 + aX + b)(X^2 + cX + d)$, gdzie a, b, c, d leżą w pewnym rozszerzeniu ciała K.

   Rozwiązanie: Niech $h_1 := X^2 + aX + b, h_2 := X^2 + cX + d$. Porównując współczynniki stojące przy tych samych potęgach zmiennej X po obu stronach równości $f = h_1 h_2$ otrzymujemy układ równań

$$-bd + r = 0, \quad -bc - ad + q = 0, \quad -b - ac - d + p = 0, \quad a + c = 0. \tag{$\star$}$$

   Z dwóch ostatnich równań wyznaczamy c, d otrzymując $c = -a, d = a^2 - b + p$. Wstawiając wyznaczone wartość do pozostałych równań, nasz układ redukujemy do postaci

$$a^2 b = b^2 - bp + r, \quad 2ab = a^3 + ap - q.$$

   Przemnażając pierwsze równanie przez $4a^2$ i wykorzystując drugie równanie otrzymujemy

$$\begin{aligned} 2a^3(a^3 + ap - q) = 2a^3(2ab) &= (2ab)^2 - 2a(2ab)p + 4a^2 r \\ &= (a^3 + ap - q)^2 - 2a(a^3 + ap - q)p + 4a^2 r. \end{aligned}$$

   Porównując skrajne wyrażenia widzimy, że a^2 jest pierwiastkiem wielomianu $g = X^3 + 2pX^2 + (p^2 - 4r)X - q^2$. Twierdzimy zatem, że $f = h_1 h_2$, gdzie f, h_1, h_2 są jak wyżej, wtedy i tylko wtedy, gdy a^2 jest pierwiastkiem wielomianu g.

   Przedstawione rozumowanie pokazuje, że jest to warunek konieczny. Pokażemy, że jest to również warunek wystarczający. Przypuśćmy zatem, że a^2 jest zerem wielomianu g. Jeśli $a = 0$, to $q = 0$ i układ równań $(\star)$ redukuje się do postaci $c = 0, \ b + d = p, \ bd = r$. Eliminując d widzimy, że b spełnia równanie kwadratowe $b^2 - bp + r = 0$ i teza zachodzi (bo b, a więc i d, leżą w ciele L, gdzie $[L : K] \leqslant 2$). Jeśli $a \neq 0$, to wyznaczamy c, d, b z trzech ostatnich równań układu $(\star)$ i widzimy, że a^2 musi być zerem wielomianu g.

   Uwaga: Zauważmy, że jeśli $q \neq 0$, to istnienie $a \in K$ dla którego $g(a^2) = 0$ gwarantuje, że wielomiany h_1, h_2 są określone nad K. Istotnie, jeśli $q \neq 0$, to $a \neq 0$ i elementy c, d, b wyznaczone z trzech ostatnich równań układu $(\star)$ leżą w K. Wtedy $g(a^2) = 0$, ale z założenia $a \in K$, więc rozkład jest określony nad K.

2. Wyznaczyć element odwrotny do $x = 1 + \sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

   Rozwiązanie: Ponieważ $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : \ a, b, c, d \in \mathbb{Q}\}$, to szukamy takiego $y = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, że $xy = 1$. Mamy, że

$$\begin{aligned} 1 = xy &= (1 + \sqrt{2} + \sqrt{3})(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) \\ &= a + 2b + 3c + (a + b + 3d)\sqrt{2} + (a + c)\sqrt{3} + (b + c + d)\sqrt{6}. \end{aligned}$$

   Ponieważ elementy $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ są $\mathbb{Q}$-liniowo niezależne, więc

$$1 = xy \iff a + 2b + 3c = 1, \quad a + b + 3d = 0, \quad a + c + 2d = 0, \quad b + c + d = 0.$$

   Łatwo sprawdzić, że otrzymany układ równań ma dokładnie jedno rozwiązanie: $a = \frac{1}{2}, b = \frac{1}{4}$, $c = 0, d = -\frac{1}{4}$ i dostajemy postać elementu y, który jest odwrotny do x w $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

3. Niech L/K będzie rozszerzeniem ciał i $u \in L$ będzie taki, że $2 \nmid [K(u) : K]$. Wykazać, że $K(u) = K(u^2)$.

   Rozwiązanie: Ponieważ $K(u^2) \subset K(u)$, więc

$$[K(u) : K] = [K(u) : K(u^2)][K(u^2) : K].$$

   Zauważmy również, że u jest pierwiastkiem wielomianu $f \in K(u^2)[X]$, gdzie $f = X^2 - u^2$. Oznacza to, że $[K(u) : K] \leqslant 2$. Jednakże, równość $[K(u) : K] = 2$ jest niemożliwa (bo $2 \nmid [K(u) : K]$), więc $[K(u) : K(u^2)] = 1$ i w konsekwencji $K(u) = K(u^2)$.

4. Niech $n \in \mathbb{N}_{\geqslant 3}, n \equiv 1 \pmod 2$ i $a \in \mathbb{Q}$ będzie liczbą dodatnią. Wykazać, że ciało $\mathbb{Q}(a^{1/n})$ nie ma nietrywialnych automorfizmów.

   Rozwiązanie: Niech $\alpha = a^{1/n}$ i oznaczmy $K = \mathbb{Q}(\alpha)$. Mamy oczywiście, że

$$\mathbb{Q}(\alpha) = \left\{ \sum_{i=0}^{n-1} b_i \alpha^i : \ b_0, b_1, \ldots, b_{n-1} \in \mathbb{Q} \right\}$$

   Niech teraz $\phi \in \mathrm{Aut}(K)$ i zdefiniujmy $\beta = \phi(\alpha)/\alpha$. Jest jasne, że $f(\alpha) = $ dla $f = X^n - a$ oraz $\phi|_{\mathbb{Q}} = \mathrm{id}\,|_{\mathbb{Q}}$. W szczególności, jeśli $x = \sum\limits_{i=0}^{n-1} b_i \alpha^i$, to $\phi(x) = \sum\limits_{i=0}^{n-1} b_i \phi(\alpha)^i$. Ponieważ $\alpha^n = a$, więc

$$\alpha^n = a = \phi(a) = \phi(\alpha^n) = \phi(\alpha)^n \Longrightarrow \left(\frac{\phi(\alpha)}{\alpha} \right)^n = a.$$

   Oznacza to, że β jest pierwiastkiem wielomianu $g = X^n - 1$. Ponieważ $\beta \in \mathbb{R}, n$ jest nieparzyste i $\beta^n = 1$, więc $\beta > 0$. Mamy również

$$0 = \beta^n - 1 = (\beta - 1) \left(\sum_{i=0}^{n-1} \beta^i \right).$$

   Ponieważ $\sum\limits_{i=0}^{n-1} \beta^i > 0$, więc $\beta = 1$, co oznacza, że $\phi(\alpha) = \alpha$ i $\phi = \mathrm{id}$.

5. Niech $p, q \in \mathbb{Q}, p \neq q$. Wykazać, że $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$.

   Rozwiązanie: Jest jasne, że $\mathbb{Q}(\sqrt{p} + \sqrt{q}) \subset \mathbb{Q}(\sqrt{p}, \sqrt{q})$. Oznaczmy $u = \sqrt{p} + \sqrt{q}$. By wykazać zawieranie w drugą stronę wystarczy udowodnić, że $\sqrt{p}, \sqrt{q} \in \mathbb{Q}(u)$. Proste przeliczenie pokazuje, że

$$u^2 = p + q + 2\sqrt{pq}, \quad u^3 = (p + 3q)\sqrt{p} + (q + 3p)\sqrt{q}.$$

   Rozwiazując teraz układ $u = \sqrt{p} + \sqrt{q}, u^3 = (p + 3q)\sqrt{p} + (q + 3p)\sqrt{q}$ ze względu na $\sqrt{p}, \sqrt{q}$ znajdujemy, że

$$\sqrt{p} = \frac{-3pu - qu + u^3}{2(q - p)} \in \mathbb{Q}(u), \quad \sqrt{q} = \frac{pu + 3qu - u^3}{2(q - p)} \in \mathbb{Q}(u),$$

   co było do pokazania.

6. Scharakteryzować wszystkie takie wielomiany $f \in \mathbb{Z}_3[X]$ stopnia dwa, że $\mathbb{Z}_3[X]/(f)$ jest ciałem.

   Rozwiązanie: Na początek zauważmy, że jeśli u jest jednością w $\mathbb{Z}_3$ (czyli $u = 1, 2$), to $(uf) = (f)$ dla dowolnego $f \in \mathbb{Z}_3[X]$. Możemy zatem rozważać wielomian f postaci $f = X^2 + aX + b$. Ponieważ $\mathbb{Z}_3$ jest ciałem, więc $\mathbb{Z}_3[X]$ jest pierścieniem ideałów głównych i ideał (f) jest maksymalny, czyli $\mathbb{Z}_3[X]/(f)$ jest ciałem wtedy i tylko wtedy, gdy f jest nierozkładalny w $\mathbb{Z}_3[X]$, co wobec jego stopnia jest równoważne brakowi pierwiastków w $\mathbb{Z}_3$. Bezpośrednie sprawdzenie pokazuje, że by wielomian spełniał ten wymóg muci być $(a, b) \in A$, gdzie $A = \{(0, 1), (1, 2), (2, 2)\}$. W konsekwencji liczba interesujących nas wielomianów wynosi $3 + 3 = 6$.

7. Niech $f = X^4 - X^3 + X^2 - X + 1 \in \mathbb{Z}[X]$ i $u \in \mathbb{C}$ będzie pierwiastkiem f. Dla dowolnej liczby $a \in \mathbb{Q}$ wyznaczyć stopień rozszerzenia $[L : \mathbb{Q}]$, gdzie $L = \mathbb{Q}\left(u + au^{-1}\right)$.

   Rozwiązanie: Na początek wykażemy, że f jest wielomianem nierozkładalny w $\mathbb{Q}[X]$. Ponieważ $f(\pm 1) \neq 0$, więc f nie ma czynników stopnia 1. Ponieważ f jest stopnia 4, to jeśli f byłby rozkładalny, to z lematu Gaussa, istniałyby takie liczby całkowite $p, q, r, s \in \mathbb{Z}$, że

   $$X^4 - X^3 + X^2 - X + 1 = (X^2 + pX + q)(X^2 + rX + s).$$

   Porównując współczynniki po obu stronach powyższej równości dostajemy układ równań

   $$qs = 1, \quad qr + ps = -1, \quad q + pr + s = 1, \quad p + r = -1.$$

   Ponieważ $q, s \in \mathbb{Z}$, więc $q = s = \pm 1$. Jeśli $q = s = -1$, to otrzymujemy układ sprzeczny. Musi być zatem $q = s = 1$. Nasz układ redukuje się zatem do układu $p + r = -1, pr = -1$ i dostajemy, że liczby p, r są pierwiastkami wielomianu $T^2 + T - 1 = 0$, który nie ma pierwiastków w liczbach całkowitych. Oznacza to, że f jest nierozkładalny nad $\mathbb{Q}$ i w konsekwencji $[\mathbb{Q}(u) : \mathbb{Q}] = 4$.

   Jest jasne, że dla dowolnego $a \in \mathbb{Q}$, element $v_a = u + au^{-1} \in \mathbb{Q}(u)$ i wobec tego $\mathbb{Q}(v_a) < \mathbb{Q}(u)$. Stąd $[\mathbb{Q}(v_a) : \mathbb{Q}]$ jest dzielnikiem $[\mathbb{Q}(u) : \mathbb{Q}] = 4$. Oznaczmy $D_a = [\mathbb{Q}(v_a) : \mathbb{Q}]$. Gdyby $D_a = 1$ dla pewnego $a \in \mathbb{Q}$, to by oznaczało, że $v_a \in \mathbb{Q}$. Równoważnie istniałaby taka liczba $b \in \mathbb{Q}$, że $u + au^{-1} = b$ i wówczas $u^2 - bu + a = 0$, co oznaczałoby, że u jest stopnia co najwyżej 2 nad $\mathbb{Q}$, podczas gdy wykazaliśmy, że u ma stopień 4 sprzeczność. Oznacza to, że $D_a = 2$ lub $D_2 = 4$. Jeżeli $D_a = 2$, to oznacza, że elementy $1, v_a, v_a^2$ są liniowo zależne nad $\mathbb{Q}$ czyli istnieją takie $p, q \in \mathbb{Q}$, że

   $$\begin{aligned} v_a^2 + pv_a + q = 0 &\iff u^4 + pu^3 + (2a + q)u^2 + apu + a^2 = 0 \\ &\iff (p + 1)u^3 + (2a + q - 1)u^2 + (ap + 1)u + a^2 - 1 = 0, \end{aligned}$$

   (jest to konsekwencja równości $u^4 = u^3 - u^2 + u - 1$). Stąd $p = -1, a = 1, q = 1$, co oznacza, że $D_a = 2$ wtedy i tylko wtedy, gdy $a = 1$. W konsekwencji $D_a = 4$ dla $a \in \mathbb{Q} \setminus \{1\}$.

8. Niech $u = 2 + \sqrt{5 + \sqrt{-5}} \in \mathbb{C}$. Wyznaczyć wielomian minimalny dla u nad $\mathbb{Q}$ oraz wyznaczyć stopnie rozszerzeń $[\mathbb{Q}(u) : \mathbb{Q}], [\mathbb{Q}(u^2) : \mathbb{Q}]$.

   Rozwiązanie: Mamy, że $(u - 2)^2 = 5 + \sqrt{-5}$ wobec tego $(u^2 - 4u - 1)^2 = -5$ tym samym u jest pierwiastkiem wielomianu $f = X^4 - 8X^3 + 14X^2 + 8X + 6 \in \mathbb{Z}[X]$. Korzystając z kryterium Eisensteina dla $p = 2$ widzimy, że wielomian f jest nierozkładalny w $\mathbb{Q}[X]$. Jako, że f jest unitarny, to jest to wielomian minimalny elementu u nad $\mathbb{Q}$ i $[\mathbb{Q}(u) : \mathbb{Q}] = 4$.

   Rozważmy teraz wieżę rozszerzeń $\mathbb{Q} \subset \mathbb{Q}(u^2) \subset \mathbb{Q}(u)$. Zauważmy, że $\mathbb{Q}(u^2) \subset \mathbb{Q}(u)$ jest rozszerzeniem stopnia co najwyżej 2. Istotnie, element u jest zerem wielomianu $g = X^2 - u^2 \in \mathbb{Q}(u^2)[X]$, skąd $[\mathbb{Q}(u) : \mathbb{Q}(u^2)] \leqslant 2$. Mamy jednak równość

   $$4 = [\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(u) : \mathbb{Q}(u^2)][\mathbb{Q}(u^2) : \mathbb{Q}].$$

   Oznacza to, że $[\mathbb{Q}(u^2) : \mathbb{Q}] = 2$ lub 4. Gdyby $[\mathbb{Q}(u^2) : \mathbb{Q}] = 2$, to oznaczałoby istnienie takiego wielomianu $h = X^2 + pX + q \in \mathbb{Q}[X]$, że $h(u) = 0$. Jednakże f jest wielomianem minimalnym dla u, więc $h | f$. Ale $\deg f = \deg h = 4$, więc dostajemy sprzeczość. Oznacza to, że $[\mathbb{Q}(u^2) : \mathbb{Q}] = 4$.

9. Niech K będzie ciałem, $f = X^5 + 3X + 3 \in K[X]$, zaś u będzie pierwiastkiem wielomianu f. Wyznaczyć stopnie rozszerzeń $[K(u) : K], [K(u^7) : K]$, gdzie $K = \mathbb{Q}$ lub $K = \mathbb{F}_2$.

   Rozwiązanie: Niech $K = \mathbb{Q}$. Korzystając z kryterium Eisensteina z $p = 3$ widzimy, że wielomian f jest nierozkładalny w $\mathbb{Q}[X]$ i tym samym $[\mathbb{Q}(u) : \mathbb{Q}] = 5$. Ponieważ $u^7 \in \mathbb{Q}(u)$ i $5 = [\mathbb{Q}(u) : \mathbb{Q}] = [\mathbb{Q}(u) :$

$\mathbb{Q}(u^7)][\mathbb{Q}(u^7):\mathbb{Q}]$, to $[\mathbb{Q}(u^7):\mathbb{Q}]|5$. Gdyby $[\mathbb{Q}(u^7):\mathbb{Q}]=1$, to istniałaby taka liczba wymierna p, że $u^7+p=0$. Mamy jednak, że $f(u)=0$, więc

$$u^7 = u^2 f(u) - 3u^2(u+1) = -3u^2(u+1)$$

i liczba $-3u^2(u+1)$ jest wymierna. Prowadzi to jednak do sprzeczności, gdyż liczby $1, u, u^3$ są $\mathbb{Q}$-liniowo niezależne (bo $[\mathbb{Q}(u):\mathbb{Q}]=5$). Oznacza to, że $[\mathbb{Q}(u^7):\mathbb{Q}]=5$.

Niech teraz $K=\mathbb{F}_2$. Z postaci wielomianu f łatwo widać, że f nie ma pierwiastka w $\mathbb{F}_2$. Jeśli f jest rozkładalny, to musi być podzielny przez wielomian stopnia 2. Bezpośrednie sprawdzenie pokazuje, że jedyny wielomiany nierozkładalny w $\mathbb{F}_2[X]$ stopnia 2, ma postać X^2+X+1 i otrzymujemy równość

$$X^5+3X+3 = (X^2+X+1)(X^3+X^2+1).$$

Oznacza to, że $[\mathbb{F}_2(u):\mathbb{F}_2]=2$ lub 3, w zależności od tego, czy u jest pierwiastkiem wielomianu $f_1=X^2+X+1$, czy $f_2=X^3+X^2+1$. Jeśli $f_1(u)=0$, to $\mathbb{F}_2(u)=\mathbb{F}_4$ i oczywiście $u^7=u$, czyli $[\mathbb{F}_2(u^7):\mathbb{F}_2]=[\mathbb{F}_2(u):\mathbb{F}_2]=2$. Jeśli $f_2(u)=0$, to $\mathbb{F}_2(u)=\mathbb{F}_8$. Zauważmy, że jednocześnie w $\mathbb{F}_2(u)$ zachodzi równość $u^7=(u^4+u^3+u^2+1)(u^3+u^2+1)+1$, co oznacza, że $u^7=1$ i wobec tego $[\mathbb{F}_2(u^7):\mathbb{F}_2]=1$.

10. Niech K będzie ciałem i $f\in K[X]$ będzie wielomianem stopnia dodatniego. Wykazać, że każdy dzielnik zera w $K[X]/(f)$ jest nilpotentny wtedy i tylko wtedy, gdy f jest potęgą elementu nierozkładalnego w $K[X]$.

Rozwiązanie: Na początek zauważmy, że jeśli $\overline{g}:=g+(f)\in K[X]/(f)$ jest dzielnikiem zera, to $\mathrm{NWD}(f,g)\neq 1$ (równoważnie: f i g mają wspólny pierwiastek w pewnym rozszerzeniu K). Oznacza to, że $g+(f)$ jest dzielnikiem zera wtedy i tylko wtedy, gdy g jest podzielny przez co najmniej jeden z czynników nierozkładalnych wielomianu f. Jednocześnie, zauważmy, że $g+(f)$ jest nilpotentny wtedy i tylko wtedy, gdy jest podzielny przez każdy czynnik nierozkładalny wielomianu f.

Po tych obserwacjach jesteśmy gotowi by dowieść naszej tezy. Zaczniemy od wynikania ($\Longrightarrow$). Przypuśćmy, że f nie jest potęgą elementu nierozkładalnego. Oznacza to, że wielomian f jest podzielny przez dwa względnie pierwsze elementy nierozkładalne, powiedzmy h_1, h_2. Widzimy więc, że $h_1+(f)$ jest dzielnikiem zera w $K[X]/(f)$, ale nie jest elementem nilpotentnym, co prowadzi do sprzeczności.

Przejdźmy do dowodu ($\Longleftarrow$). Jeśli $f(X)=h(X)^n$ dla pewnego $h\in K[X]$ i $g+(f)$ jest dzielnikiem zera w $K[X]/(f)$, to istnieje taki wielomian $h_1\in K[X]$, że $g=h\cdot h_1$. Wówczas $g^n+(f)=h^n\cdot h_1^n+(f)=(f)=(0)+(f)$ i rozważny element jest nilpotentny.

Rozdział 9

Wybrane zagadnienia teorii grup

9.1 Twierdzenia o izomorfizmach dla grup

Nasze rozważania zaczniemy od uzyskania (istotnych dla dalszej części) wniosków z podstawowego twierdzenia o izomorfizmie (por. 3.5.2). Jak wiadomo, suma mnogościowa podgrup danej grupy nie musi tworzyć struktury grupy, ale wygodnym pojęciem jest zbudowana na bazie tej sumy grupa zwana złączeniem wyjściowych podgrup.

Definicja 9.1.1 (złączenie podgrup)**.** Jeśli G jest grupą, $(H_i)_{i\in I}$ niepustą rodziną podgrup grupy G to **złączeniem podgrup** H_i nazywamy grupę oznaczaną przez $\bigvee_{i\in I} H_i$ zadaną następująco:

$$\bigvee_{i\in I} H_i = \left\langle \bigcup_{i\in I} H_i \right\rangle.$$

Inaczej mówiąc, jest to najmniejsza podgrupa G zawierająca elementy wszystkich podgrup z rodziny (H_i).

Własność 9.1.2 (własności złączenia)**.** *Nich H, K będą podgrupami grupy G, przy czym H dodatkowo normalna w G. Wtedy:*

(1) $HK = KH = H \vee K$,

(2) jeśli dodatkowo K także normalna w G oraz $H \cap K = \{1_G\}$, to $hk = kh$ dla $h \in H$ oraz $k \in K$.

Dowód. (1) Wykażemy, że $HK = H \vee K$. Oczywiście, $HK = \{hk : \ h \in H, k \in K\} \subset H \vee K$ wprost z definicji złączenia podgrup. Zauważmy teraz, że każdy element $x \in H \vee K$ jest postaci:

$$x = a_1 \cdot \ldots \cdot a_n,$$

gdzie $a_i \in H \cup K$ oraz możemy założyć, że elementy tych podgrup ułożone są naprzemiennie (jeśli obok siebie byłyby elementy z tej samej podgrupy to zastępujemy go ich iloczynem). Możemy założyć, że $a_1 \in K$, gdyż jeśli $a_1 \in H$ to wystarczy rozważyć $a_1^{-1}x = a_2 \cdot \ldots \cdot a_n$. Niech więc:

$$x = k_1h_1k_2h_2 \cdot \ldots \cdot k_mh_m, \qquad h_i \in H, k_j \in K.$$

Z założenia H jest normalną podgrupą G, czyli $k_1h_1k_1^{-1} \in H$ więc istnieje takie $\overline{h_1} \in H$, że $k_1h_1 = \overline{h_1}k_1$, czyli

$$x = \overline{h_1}k_1k_2h_2 \cdot \ldots \cdot k_mh_m.$$

Stosujemy analogiczne rozumowanie do elementu $k_1k_2h_2$ i otrzymujemy ponownie taki element $\overline{h_2} \in H$, że $k_1k_2h_2 = \overline{h_2}k_1k_2$, czyli

$$x = \overline{h_1} \cdot \overline{h_2} \cdot k_1k_2k_3h_3 \cdot \ldots \cdot k_mh_m.$$

Postępując dalej analogicznie po skończonej liczbie kroków dostaniemy:

$$x = \overline{h_1} \cdot \ldots \cdot \overline{h_m} \cdot k_1 \cdot \ldots \cdot k_m \in HK$$

dla pewnych $\overline{h_1}, \ldots, \overline{h_m} \in H$. Zauważamy na koniec $KH = K \vee H = H \vee K = HK$. Dowód drugiej części twierdzenia pozostawiamy jako proste ćwiczenie. □

Twierdzenie 9.1.3 (II twierdzenie o izomorfizmie)**.** *Jeśli G – grupa, K, H – podgrupy G oraz dodatkowo $H \lhd G$, to $HK/H \cong K/(H \cap K)$.*

Dowód. Skorzystamy ze znanego nam już podstawowego twierdzenia o izomorfizmie (por. 3.5.2) dla odwzorowania:

$$f : K \ni k \longrightarrow kH \in HK/H.$$

Po pierwsze zauważamy, że $k \in \operatorname{Ker} f$ wtedy i tylko wtedy, gdy $kH = H$ co oznacza, że $k \in H \cap K$ (skoro k wyjściowo jest z K), więc $\operatorname{Ker} f = H \cap K$. Dalej, $gH \in HK/H$ wtedy i tylko wtedy, gdy istnieją takie elementy $h \in H$ oraz $k \in K$, że $gH = (hk)H$ czyli

$$gH = h(kH) = h(Hk) = (hH)k = Hk = kH = f(k) \in \operatorname{Im} f.$$

Wobec tego f jest epimorfizmem o jądrze $H \cap K$, czyli z twierdzenia 3.5.2 mamy tezę. □

Twierdzenie 9.1.4 (III twierdzenie o izomorfizmie)**.** *Jeśli G – grupa, H, K – normalne podgrupy G oraz $K \subset H$, to $H/K \lhd G/K$ oraz $(G/K)/(H/K) \cong G/H$.*

Dowód. Fakt, że H/K jest podgrupą normalną w G/K wynika z tego, że jest to obraz podgrupy normalnej $H \lhd G$ przez epimorfizm kanoniczny $\pi : G \longrightarrow G/K$ (por. twierdzenie 3.5.1). Aby wykazać drugą część twierdzenia ponownie skorzystamy z podstawowego twierdzenia o izomorfizmie (3.5.2) tym razem dla odwzorowania:

$$f : G/K \ni aK \longrightarrow aH \in G/H.$$

Zauważmy najpierw, że to odwzorowanie jest poprawnie określone dzięki temu, że $K \subset H$. Ponadto oczywiście jest ono epimorfizmem. Trzeba jedynie wyznaczyć jego jądro. Otóż, $gK \in \operatorname{Ker} f$ wtedy i tylko wtedy, gdy $gH = H$ co jest równoważne temu, że $g \in H$ albo inaczej $gK \in H/K$, słowem jądro to H/K. Stosujemy twierdzenie 3.5.2 i mamy tezę. □

Twierdzenie 9.1.5 (homomorfizmy iloczynów i sum prostych)**.** *Niech $(f_i : G_i \longrightarrow H_i)_{i \in I}$ będzie niepustą rodziną homomorfizmów grup, $N_i \lhd G_i$ dla $i \in I$ i niech $G = \prod_{i \in I} G_i$, $H = \prod_{i \in I} H_i$ oraz $f := \prod_{i \in I} f_i : G \longrightarrow H$. Wtedy:*

(1) $f \in Hom(G, H)$ oraz $\operatorname{Ker} f = \prod_{i \in I} \operatorname{Ker} f_i$ oraz $\operatorname{Im} f = \prod_{i \in I} \operatorname{Im} f_i$,

(2) $f(\bigoplus_{i \in I} G_i) \subset \bigoplus_{i \in I} H_i$,

(3) homomorfizm f jest monomorfizmem (epimorfizmem, izomorfizmem) wtedy i tylko wtedy, gdy f_i jest monomorfizmem (epimorfizmem, izomorfizmem) dla każdego $i \in I$,

(4) $\prod_{i \in I} N_i \lhd \prod_{i \in I} G_i$ oraz $\left(\prod_{i \in I} G_i\right) / \left(\prod_{i \in I} N_i\right) \cong \prod_{i \in I} (G_i/N_i)$,

(5) $\bigoplus_{i \in I} N_i \lhd \bigoplus_{i \in I} G_i$ oraz $\left(\bigoplus_{i \in I} G_i\right) / \left(\bigoplus_{i \in I} N_i\right) \cong \bigoplus_{i \in I} (G_i/N_i)$.

Dowód. Punkty (1)–(3) łatwo wynikają wprost z definicji działań w produkcie oraz sumie prostej. Skomentujemy dowód (4) – analogicznie dowodzi się (5). Ponieważ dla każdego $i \in I$ homomorfizm naturalny $\pi_i : G_i \longrightarrow G_i/N_i$ jest epimorfizmem o jądrze N_i, więc na podstawie (1) i (2) mamy, że

$$\prod_{i \in I} \pi_i : \prod_{i \in I} G_i \longrightarrow \prod_{i \in I} G_i/N_i$$

jest epimorfizmem o jądrze $\prod_{i \in I} N_i$, dzięki czemu zgodnie z podstawowym twierdzeniem o izomorfizmie 3.5.2 mamy tezę. □

9.2 Działanie grupy na zbiorze

Podstawowym narzędziem w dowodach wielu ważnych zastosowań teorii grup (m.in. w teorii Galois, ale także np. w geometrii różniczkowej) jest pojęcie działania grupy na zbiorze. W tym rozdziale wprowadzimy definicję, podamy ważne przykłady oraz udowodnimy najważniejsze własności związane z tym pojęciem.

Definicja 9.2.1 (działanie grupy na zbiorze)**. Działaniem grupy** G na zbiorze $X \neq \emptyset$ nazywamy odwzorowanie:

$$G \times X \ni (g, x) \longrightarrow g.x \in X$$

spełniające następujące warunki:

(1) $g.(h.x) = (g \cdot h).x$ dla dowolnych g, $h \in G$ oraz $x \in X$ (łączność),

(2) $1.x = x$ dla dowolnego $x \in X$ (element neutralny).

Przykład 9.2.2. Przyjrzyjmy się kilku podstawowym przykładom działania grupy na zbiorze.

(1) Każda grupa G działa na siebie za pomocą translacji:

$$G \times G \ni (g, x) \longrightarrow gx \in G$$

(2) Każda grupa G działa na siebie za pomocą sprzężenia:

$$G \times G \ni (g, x) \longrightarrow gxg^{-1} \in G$$

(3) Każda grupa G działa na rodzinie swoich podzbiorów $\mathcal{P}(G)$ za pomocą sprzężenia

$$G \times \mathcal{P}(G) \ni (g, A) \longrightarrow gAg^{-1} \in \mathcal{P}(G)$$

(4) Jeśli $X \neq \emptyset$, to grupa $S(X)$ ((6)) działa na zbiorze X za pomocą ewaluacji:

$$S(X) \times X \ni (\sigma, x) \longrightarrow \sigma(x) \in X$$

Definicja 9.2.3 (stabilizator i orbita)**.** Jeśli grupa G działa na zbiorze X oraz $x \in X$, to zbiór

$$\mathrm{Stab}_G(x) := G_x := \{g \in G : \ gx = x\}$$

nazwamy **stabilizatorem**[1] elementu x. Zbiór

$$O(x) := O_G(x) := \{g.x, \ g \in G\}$$

nazywamy **orbitą elementu** x.

Dla dalszej analizy własności działania grupy na zbiorze wprowadzamy na elementach zbioru X przydatną relację. Jeśli grupa G działa na zbiorze X, to definiujemy:

$$x \sim_G y \iff \exists\, g \in G : \ y = g.x.$$

Własność 9.2.4 (własności orbit i stabilizatorów)**.** *Niech grupa G działa na zbiorze X oraz x, y będą dowolnymi elementami X. Wtedy zachodzą własności:*

(1) relacja $\sim_G$ jest relacją równoważności na zbiorze X,

(2) zbiór $\mathrm{Stab}(x)$ *jest podgrupą grupy G,*

(3) $O_G(x) = [x]_{\sim_G}$ *oraz* $\#(O(x)) = [G : \mathrm{Stab}(x)]$,

(4) jeśli $x \sim_G y$, to podgrupy $\mathrm{Stab}(x)$ *i* $\mathrm{Stab}(y)$ *są sprzężone tzn. istnieje takie $a \in G$, że:*

$$\mathrm{Stab}(y) = a\,\mathrm{Stab}(x)a^{-1}.$$

[1] Czasem stabilizator jest nazywany grupą izotropii.

Dowód. (1) Ponieważ $1.x = x$, więc $x \sim_G x$ i mamy zwrotność. Jeśli $x \sim_G y$, to istnieje takie $g \in G$, że $y = g.x$ czyli $g^{-1}.y = g^{-1}.(g.x) = (g^{-1}g).x = 1.x = x$. Stąd $y \sim_G x$. Ostatecznie, jeśli $x \sim_G y$, $y \sim_G z$, to istnieją takie $g, h \in G$, że $y = g.x$, $z = h.y$. Wobec tego $z = h.(g.x) = (hg).x$, co pokazuje, że $x \sim_G z$.

(2) Wprost z definicji działania grupy na zbiorze mamy, że $1 \in \mathrm{Stab}(x)$. Jeśli g, $h \in \mathrm{Stab}(x)$, to $(gh^{-1}).x = g.(h^{-1}.(h.x)) = g.x = x$, więc $gh^{-1} \in \mathrm{Stab}(x)$.

(3) Wprost z definicji relacji $\sim_G$ mamy równość $O(x) = [x]_{\sim_G}$. Określmy teraz odwzorowanie:

$$(G/\mathrm{Stab}(x))_l \ni g\,\mathrm{Stab}(x) \longrightarrow g.x \in O(x).$$

Zauważmy, że $g\,\mathrm{Stab}(x) = h\,\mathrm{Stab}(x)$ wtedy i tylko wtedy, gdy $g^{-1}h \in \mathrm{Stab}(x)$, a to ma miejsce dokładnie, gdy $g.x = h.x$. Nasze odwzorowanie jest więc poprawnie określone i injektywne. Surjektywność odwzorowania wynika z definicji.

(4) Niech $y = a.x$ dla pewnego $a \in G$. Wtedy $g \in \mathrm{Stab}(y)$ wtedy i tylko wtedy gdy $g.(a.x) = a.x$, czyli wtedy i tylko wtedy, gdy $a^{-1}ga \in \mathrm{Stab}(x)$ lub równoważnie $g \in a\,\mathrm{Stab}(x)a^{-1}$. □

Bezpośrednio z udowodnionych własności wynikają kolejne, które łatwo widać (jeśli pamiętamy np. o twierdzeniu Lagrange'a (3.4.5) oraz o definicji centrum grupy (3.1.14.(4))).

Wniosek 9.2.5 (ważne własności orbit i stabilizatorów)**.** *Dla działania grupy G na zbiorze X zachodzą własności:*

(1) jeśli G jest skończona, to dla $x \in X$ mamy $\#(O(x))||G|$,

(2) jeśli G działa na siebie za pomocą translacji, to $\mathrm{Stab}(x) = \{1\}$ oraz $O(x) = G$ dla dowolnego $x \in G$,

(3) jeśli G działa na siebie za pomocą sprzężenia, to dla $x \in G$ mamy

$$C(x) := \mathrm{Stab}(x) = \{g \in G : \ gx = xg\}^2$$

oraz $O(x) = \{gxg^{-1} : \ g \in G\} =: x^G$. Zauważmy ponadto, że $\#(O(x)) = 1$ wtedy i tylko wtedy, gdy $x \in C(G)$.

Twierdzenie 9.2.6 (uogólnione równanie klas)**.** *Jeśli grupa skończona G działa na zbiorze skończonym X oraz elementy $x_1, \ldots, x_r \in X$ są takie, że $X = O(x_1) \cup \ldots \cup O(x_r)$ gdzie $O(x_i) \neq O(x_j)$ dla $i \neq j$, to prawdziwa jest równość:*

$$\#(X) = \sum_{i=1}^{r} [G : \mathrm{Stab}(x_i)].$$

Dowód. Zauważmy, że przedstawienie $X = O(x_1) \cup \ldots \cup O(x_r)$ jest zgodnie z własnościami klas równoważności przedstawieniem w postaci sumy zbiorów parami rozłącznych więc:

$$\#(X) = \#(O(x_1) + \ldots + \#(O(x_r).$$

Pozostaje więc zauważyć, że z poprzedniej własności mamy $\#(O(x_i) = [G : \mathrm{Stab}(x_i)]$, co kończy dowód. □

Wniosek 9.2.7 (równanie klas)**.** *Jeśli skończona grupa G działa na siebie za pomocą sprzężenia ((2)), to zachodzą własności:*

(1) dla elementów $x_1, \ldots, x_r \in G$ takich, że $G = O(x_1) \cup \ldots \cup O(x_r)$, gdzie $O(x_i) \neq O(x_j)$ dla $i \neq j$, mamy:

$$|G| = \sum_{i=1}^{r} [G : C(x_i)].$$

(2) jeśli ponadto $I = \{i \in \{1, \ldots, r\} : \ \#O(x_i) > 1\}$, to

$$|G| = |C(G)| + \sum_{i \in I} [G : C(x_i)].$$

Wniosek 9.2.8. *Jeśli p jest liczbą pierwszą oraz $k \in \mathbb{N}$, to grupa rzędu p^k ma nietrywialne centrum.*

[2] $C(x)$ nazywamy centralizatorem elementu x

Dowód. Niech G będzie grupą rzędu p^k. Jeśli jest to grupa abelowa, to nie mamy czego dowodzić, gdyż w tym wypadku $G = C(G)$ i jest to nietrywialna grupa. Jeśli G nie jest abelowa, to $I \neq \emptyset$ (gdzie I oznacza zbiór indeksów z wypowiedzi równania klas (9.2.7)), zaś $[G : C(x_i)] = p^{k_i}$ dla pewnego $k_i \in \mathbb{N}$, gdyż, jak wiadomo, indeks podgrupy musi dzielić rząd grupy. Wobec tego z równania klas otrzymujemy równość:

$$|C(G)| = |G| - \sum_{i=1}^{r} [G : C(x_i)] = p^k - \sum_{i=1}^{r} p^{k_i}$$

i jako, że prawa strona jest podzielna przez p, to $p||C(G)|$. Oznacza to, że centrum jest nietrywialne. □

Z punktu widzenia zastosowań bardzo ważnym działaniem grupy na zbiorze jest działanie G na zbiorze wszystkich jej podgrup za pomocą sprzężenia. Niech $\mathcal{G}(G)$ będzie zbiorem wszystkich podgrup grupy G. Wówczas chodzi nam o działanie:

$$G \times \mathcal{G}(G) \ni (g, H) \longrightarrow gHg^{-1} \in \mathcal{G}(G).$$

Definicja 9.2.9 (normalizator podgrupy)**.** Jeśli H jest podgrupą grupy G i G działa na zbiór wszystkich swoich podgrup przez sprzężenie, to stabilizator H nazywamy **normalizatorem** podgrupy H i oznaczamy $N(H)$. Innymi słowy:

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

Własność 9.2.10 (własności normalizatora)**.** *Niech G będzie grupą, zaś H jej podgrupą. Wtedy zachodzą własności:*

(1) $H \lhd N(H)$ i $N(H)$ jest największą (w sensie inkluzji) podgrupą G, w której H jest normalna,

(2) $H \lhd G$ wtedy i tylko wtedy, gdy $N(H) = G$,

(3) moc zbioru wszystkich podgrup grupy G sprzężonych z H (tzn. podgrup postaci: gHg^{-1} dla pewnego $g \in G$) jest równa $[G : N(H)]$.

Dowód. (1) wynika wprost z definicji normalizatora, zaś (2) to wniosek z (1). Dla dowodu (3) zauważmy, że moc zbioru podgrup sprzężonych z H to moc orbity H, a ta jak wiemy jest równa indeksowi stabilizatora H. Jako, że w tym przypadku stabilizator to normalizator, obserwacja ta kończy dowód. □

Definicja 9.2.11 (punkty stałe działania)**.** Jeśli grupa G działa na zbiorze X, to zbiór:

$$X^G := \{x \in X : \ g.x = x, \ \forall \ g \in G\}$$

nazywamy **zbiorem punktów stałych** działania G na X.

Własność 9.2.12 (moc zbioru punktów stałych)**.** *Jeśli p jest liczbą pierwszą, $k \in \mathbb{N}$, zaś grupa G rzędu p^k działa na zbiór skończony X, to*

$$\#(X) \equiv \#(X^G) \pmod{p}.$$

Dowód. Element $x \in X$ należy do zbioru X^G wtedy i tylko wtedy, gdy $O(x) = \{x\}$, czyli $\#(X^G)$ to moc zbioru orbit jednoelementowych. Podobnie jak przy badaniu centrum w dowodzie 9.2 otrzymujemy z ogólnego równania klas:

$$\#(X) = \#(X^G) + \sum_{i=1}^{r} \#(O(x_i)),$$

gdzie w sumie z prawej strony występują reprezentacje orbit o mocy większej od 1 (parami rozłącznych). Wynika stąd, że dla każdego $i = 1, \ldots, r$ liczba $\#(O(x_i)) = [G : \mathrm{Stab}(x_i)]$ jest większa od 1 i dzieli rząd grupy G, czyli jest podzielna przez p. □

Twierdzenie 9.2.13 (lemat Burnside'a)**.** *Niech G będzie grupą skończoną działającą na zbiorze skończonym X. Wtedy liczba orbit działania G na X wyraża się wzorem:*

$$\frac{1}{|G|} \sum_{g \in G} S(g),$$

gdzie $S(g) = \#\{x \in X : \ g.x = x\}$.

Dowód. Rozbijmy X na N orbit rozłącznych: $X = O_1 \cup \ldots \cup O_N$. Jeśli ustalimy orbitę O_i oraz punkt $x_0 \in O_i$, to dla dowolnego $y \in O_i$: $\#(g \in G : \ g.y = y) = |\operatorname{Stab}(y)| = |\operatorname{Stab}(x_0)|$, zaś a liczba punktów w O_i, to $[G : \operatorname{Stab}(x_0)]$. Wobec tego:

$$\sum_{g\in G} \#(\{y \in O_i : \ g.y = y\}) = |\operatorname{Stab}(x_0)|[G : \operatorname{Stab}(x_0)] = |G|.$$

Tym samym: $S(g) = \#(\bigcup_{i=1}^{N} \{x \in O_i : \ g.x = x\}) = \sum_{i=1}^{N} \#(\{x \in O_i : \ g.x = x\})$, a stąd

$$\begin{aligned}\sum_{g\in G} S(g) &= \sum_{g\in G}\sum_{i=1}^{N} \#(\{x \in O_i : \ g.x = x\}) \\ &= \sum_{i=1}^{N}\sum_{g\in G} \#(\{x \in O_i : \ g.x = x\}) = \sum_{i=1}^{N} |G| = N|G|,\end{aligned}$$

co kończy dowód. □

9.3 Problem odwrócenia twierdzenia Lagrange'a

Zwracaliśmy uwagę na fakt, że w grupie skończonej G może nie być podgrup pewnego rzędu dzielącego rząd G. Klasycznym (i najmniejszym w sensie liczebności rozpatrywanej grupy) przykładem jest grupa alternująca A_4 (por. 3.6.7), która ma 12 elementów, ale można łatwo nawet bezpośrednio stwierdzić, że nie ma w niej podgrupy rzędu 6 (choć istnieje wiele różnych dowodów tego faktu). Około 100 lat temu matematyk norweski Sylow [3] odkrył pewne prawidłowości, dzięki którym można stwierdzić, że w niektórych sytuacjach twierdzenie Lagrange'a można we wspomnianym sensie odwrócić. Będziemy dążyli do wykazania twierdzeń, które w literaturze znane są jako twierdzenia Sylowa. Zaczniemy od własności przypisywanej Cauchy'emu i prawdziwej ogólniej niż tylko w sytuacji, dla której ją poniżej udowodnimy.

Twierdzenie 9.3.1 (Cauchy)**.** *Jeśli liczba pierwsza p dzieli rząd skończonej grupy abelowej G, to w grupie G istnieje element rzędu p.*

Dowód. Dowód przeprowadzimy indukcyjnie względem rzędu grupy G. Jeśli $|G| = 2$, to oczywiście twierdzenie się trywializuje. Niech więc $|G| > 2$. Wtedy istnieje w G element $a \neq 1$ i wobec tego $|a| = r > 1$. Jeśli p dzieli r, to $r = pq$ dla pewnego $q > 0$ i element $b := a^q$ jest dobrym, poszukiwanym elementem. Mamy bowiem $b^p = (a^q)^p = a^r = 1$, czyli $|b| \leqslant p$, a nie może być mniejszy, gdyż wtedy mniejszy byłby rząd a.

Jeśli p nie dzieli r, to, biorąc $H := \langle a\rangle$, mamy $p||G| = [G : H]|H| = |G/H||H|$ (ostatni zapis ma sens bo grupa G jest abelowa, czyli podgrupa H jest normalna w G) i wobec tego $p||G/H|$. Jednak $|G/H| < |G|$, wobec czego możemy wykorzystać założenie indukcyjne i wybrać taki element $b \in G$, że $|bH| = p$. Jeśli $|b| = s$, to $(bH)^s = b^sH = H$. Zatem p musi dzielić s, skąd $s = pt$ dla pewnego $t > 0$ i wracamy do poprzedniego przypadku otrzymując analogicznie, że rząd elementu b^t jest równy p. □

Twierdzenie 9.3.2 (I twierdzenie Sylowa)**.** *Jeśli p jest liczbą pierwszą, $k \in \mathbb{N}$, zaś G to grupa skończona, której rząd jest podzielny przez p^k, to w G istnieje podgrupa rzędu p^k.*

Dowód. Dowód przeprowadzimy stosując podwójną indukcję: względem rzędu grupy G i wykładnika k. Jeśli $|G| = 2$, to twierdzenie jest oczywiste. Niech więc $|G| > 2$ i wypiszmy równanie klas (9.2) dla G:

$$|G| = |C(G)| + \sum_{i=1}^{r}[G : C(x_i)], \qquad [G : C(x_i)] > 1, \ i = 1, \ldots, r.$$

Jeśli p nie dzieli $|C(G)|$, to istnieje takie $i \in \{1, \ldots, r\}$, że p nie dzieli $[G : C(x_i)]$ i tym samym z twierdzenia Lagrange'a mamy, że $p^k||C(x_i)|$. Centralizator $C(x_i)$ jest podgrupą G i jej rząd jest mniejszy niż rząd G – tym samym z założenia indukcyjnego istnieje w tej grupie podgrupa rzędu p^k i jest to poszukiwana podgrupa w G.

Jeśli p dzieli $|C(G)|$, to na mocy twierdzenia Cauchy'ego (9.3) w $C(G)$ istnieje element a rzędu p. Podgrupa $H := \langle a\rangle$ jest normalna w G (gdyż zawiera się w centrum). Jeśli $k = 1$, to H jest już dobrą podgrupą. Niech więc $k > 1$ – wtedy:

$$|G| = [G : H]|H| = |G/H|p,$$

[3] Peter Ludwig Mejdell Sylow (1832-1918).

czyli $p^{k-1}||G/H|$ i grupa G/H jest niższego rzędu niż G. Z założenia indukcyjnego G/H zawiera podgrupę rzędu p^{k-1}. Podgrupa ta (z twierdzenia o przenoszeniu podgrup 3.5.1) jest postaci K/H dla pewnej podgrupy K grupy G zawierającej H (jądro rzutowania kanonicznego). Wtedy K spełnia tezę, gdyż:

$$|K| = [K : H]|H| = |F/H||H| = p^{k-1}p = p^k. \qquad \square$$

Przykład 9.3.3. Niech G będzie grupą rzędu n. Zbadajmy, gdzie mamy szansę znaleźć kontrprzykład dla odwrócenia twierdzenia w wersji ogólnej. Jeśli $n = 1, 2, 3, 5, 7, 11$ to odwrócenie jest prawdziwe: są to grupy cykliczne. Jeśli $n = 4 = 2^2$, $n = 6 = 2 \cdot 3$, $n = 8 = 2^3$, $n = 9 = 3^2$ i $n = 10 = 2 \cdot 5$, to wszystkie te sytuacji podpadają pod twierdzenie Sylowa, zatem odwrócenie będzie prawdziwe. Pierwszy przypadek gdy twierdzenie Sylowa nie może zostać zastosowane, pojawia się przy grupach rzędu $n = 12$ i faktycznie, jak wspomnieliśmy, A_4 ma 12 elementów i nie posiada podgrupy rzędu 6.

Definicja 9.3.4 (podgrupa Sylowa)**.** Jeśli p jest liczbą pierwszą, to grupę skończoną, której rząd jest potęgą p nazywamy p-**grupą**. Przez p-**podgrupę** rozumiemy każdą taką podgrupę, która jest p-grupą. Podgrupy będące p-podgrupami maksymalnego rzędu w danej grupie nazywamy jej p-**podgrupami Sylowa**. Zbiór wszystkich p-podgrup Sylowa w grupie G będziemy oznaczać dalej przez $S_p(G)$.

Innymi słowy, jeśli $|G| = p^k n$, gdzie p jest liczbą pierwszą, $k \in \mathbb{N}$ oraz $p \nmid n$, to H jest p-podgrupą Sylowa grupy G, jeśli $|H| = p^k$ lub jeszcze inaczej, jeśli H jest p-podgrupą grupy G i $p \nmid [G : H]$.

Zauważmy najpierw prostą własność charakteryzującą p-grupy.

Własność 9.3.5. *Niech p będzie liczbą pierwszą. Grupa G jest p-grupą wtedy i tylko wtedy, gdy dla dowolnego $a \in G$, rząd elementu a jest pewną potęgą naturalną (bądź zerową) liczby p.*

Dowód. Oczywiście, fakt że dla dowolnego $a \in G \setminus \{1_G\}$ rząd tego elementu jest potęgą liczby p, gdy G jest p-grupą wynika wprost z twierdzenia Lagrange'a. Wynikanie w drugą stronę wykazujemy wykorzystując kontrapozycję. Jeśli bowiem $n = |G|$ nie jest potęgą liczby p, to istnieje różna od p liczba pierwsza q dzieląca n. Na podstawie pierwszego twierdzenia Sylowa (9.3.2) istnieje więc podgrupa G rzędu q. Jako, że q jest pierwsza, to podgrupa ta jest cykliczna, tym samym istnieje w G element, którego rząd nie jest potęgą liczby a. [4] $\square$

Własność 9.3.6 (maksymalność podgrup Sylowa)**.** *Jeśli P jest p-podgrupą Sylowa skończonej grupy G, zaś H jest p-podgrupą zawartą w $N(P)$, to $H \subset P$. W szczególności, jeśli Q jest p-podgrupą Sylowa zawartą w $N(P)$, to $P = Q$.*

Dowód. Wiemy, że $H < N(P)$ oraz $P \lhd N(P)$. Na podstawie II twierdzenia o izomorfizmie (9.1.3) dostajemy $HP/P \cong H/(H \cap P)$. Oczywiście, $|H|$ jest potęgą p, zatem na mocy twierdzenia Lagrange'a wiemy, że liczba $|HP/P| = |H/(H \cap P)| = [H : H \cap P]$ dzieli rząd grupy H, czyli istnieje takie $k \geqslant 0$, że $|HP/P| = p^k$. Wobec tego dostajemy równość:

$$|HP| = |HP/P||P| = p^k|P|.$$

Ponieważ P jest p-grupą, to jest nią również HP. Ponieważ $P \subset HP$, więc z maksymalności P wśród p-podgrup wynika, że $HP = P$ i dalej $H \subset P$. $\square$

Twierdzenie 9.3.7 (II twierdzenie Sylowa)**.** *Niech G będzie grupą rzędu $p^k n$, gdzie p jest liczbą pierwszą, $k \in \mathbb{N}$ oraz $p \nmid n$. Wtedy zachodzą własności:*

(1) każde dwie p-podgrupy Sylowa grupy G są sprzężone,

(2) każda p-podgrupa grupy G jest zawarta w pewnej p-podgrupie Sylowa grupy G,

(3) liczba $\#(S_p(G))$ p-podgrup Sylowa grupy G jest dzielnikiem n oraz $\#(S_p(G)) \equiv 1 \pmod p$.

Dowód. Zanim dowodzić będziemy konkretnych własności, przedstawmy kilka użytecznych faktów. Niech P będzie p-podgrupą Sylowa grupy G, zaś Q dowolną p-podgrupą G. Rozważmy działanie grupy Q na zbiorze $(G/P)_l$ za pomocą translacji:

$$Q \times (G/P)_l \ni (a, gP) \longrightarrow (ag)P \in (G/P)_l.$$

Przedstawmy teraz $(G/P)_l$ jako rozłączną sumę orbit:

$$(G/P)_l = O(g_1P) \cup \ldots \cup O(g_rP),$$

[4] Dla dowodu można także oczywiście skorzystać bezpośrednio z twierdzenia Cauchy'ego w wersji nieabelowej.

gdzie $g_1, \ldots, g_r \in G$. Niech $|Q| = p^s$ dla pewnego $1 \leqslant s \leqslant k$. Moc każdej orbity jest dzielnikiem rzędu grupy Q, więc $\#(O(g_iP)) = p^{k_i}$ dla pewnego $0 \leqslant k_i \leqslant s$ $(1 \leqslant i \leqslant r)$. Z twierdzenia Lagrange'a mamy:

$$n = |(G/P)_l| = p^{k_1} + \ldots + p^{k_r},$$

czyli przynajmniej jedna z potęg musi być równe zeru, oznaczmy ją przez k_{i_0}. Wtedy jednak $O(g_{i_0}P) = \{g_{i_0}P\}$, skąd $Qg_{i_0}P = g_{i_0}P$ lub równoważnie $Qg_{i_0}Pg_{i_0}^{-1} = g_{i_0}Pg_{i_0}^{-1}$, co daje $Q \subset g_{i_0}Pg_{i_0}^{-1}$.

Przejdźmy teraz do dowodu podpunktów tezy, opierając się na powyższym rozumowaniu.

(1) Jeśli rozważana (dowolna) podgrupa Q to p-podgrupa Sylowa, to $|Q| = |P| = |g_{i_0}Pg_{i_0}^{-1}| = p^k$ i mamy $Q = g_{i_0}Pg_{i_0}^{-1}$, co oznacza, wobec dowolności P i Q, że wszystkie p-podgrupy Sylowa G są sprzężone.

(2) Ponieważ $g_{i_0}Pg_{i_0}^{-1}$ jest też p-podgrupą Sylowa i $Q \subset g_{i_0}Pg_{i_0}^{-1}$, więc dowolna p-grupa zawiera się w pewnej p-grupie Sylowa.

(3) Rozważmy działanie G na zbiorze $S_p(G)$ wszystkich p-podgrup Sylowa grupy G (wobec pierwszego twierdzenia Sylowa jest to zbiór niepusty) za pomocą sprzężenia:

$$G \times S_p(G) \ni (g, P) \longrightarrow gPg^{-1} \in S_p(G).$$

Ustalmy $P \in S_p(G)$. Wiemy już, że wszystkie p-podgrupy Sylowa są sprzężone, więc dostajemy:

$$\#(S_p(G)) = \#(O(P)) = [G : \mathrm{Stab}(P)] = [G : N(P)],$$

gdyż $\mathrm{Stab}(P) = N(P)$. Ponieważ

$$[G : P] = [G : N(P)][N(P) : P] = \#(S_p(G))[N(P) : P],$$

to wynika stąd, że $\#(S_p(G))$ dzieli indeks podgrupy P w G. Rozważmy teraz działanie grupy P na zbiorze $S_p(G)$ za pomocą sprzężenia

$$P \times S_p(G) \ni (a, Q) \longrightarrow aQa^{-1} \in S_p(G).$$

Niech $S := S_p(G)^P$ będzie zbiorem punktów stałych tego działania. Wiemy wtedy, że (por. 9.2):

$$\#(S_p(G)) \equiv \#(S) \pmod{p}.$$

Ale jeśli Q jest p-podgrupą Sylowa, to Q należy do S wtedy i tylko wtedy, gdy $Q = aQa^{-1}$ dla dowolnego $a \in P$, czyli dokładnie wtedy, gdy $P \subset N(Q)$. Wiemy jednak, że $N(Q)$ zawiera tylko jedną p-podgrupę Sylowa i jest nią oczywiście Q. Stąd $P = Q$ oraz $\#(S) = 1$. □

9.4 Twierdzenia o klasyfikacji grup abelowych

W podstawowej części twierdzenie o klasyfikacji grup abelowych przyjęliśmy bez dowodu (por. 3.3.19) – teraz nadrobimy te zaległości i zobaczymy też, jak można je zastosować do wyznaczania wszystkich grup abelowych danego rzędu. Jest to jednak bardzo ważne twierdzenie także z punktu widzenia zastosowań w teorii liczb i topologii algebraicznej. Najpierw wprowadzimy zestaw pomocniczych własności.

Twierdzenie 9.4.1 (charakteryzacja iloczynu podgrup)**.** *Jeśli G jest grupą, zaś $H_1, \ldots, H_n$ jej podgrupami, to odwzorowanie:*

$$\phi : H_1 \times \ldots \times H_n \ni (h_1, \ldots, h_n) \mapsto h_1 \cdot \ldots \cdot h_n \in G$$

jest izomorfizmem wtedy i tylko wtedy, gdy spełnione są następujące warunki:

(1) $H_1, \ldots, H_n$ są normalnymi podgrupami G,

(2) $H_i \cap H_{i+1} \cdot \ldots \cdot H_n = \{1\}$ dla $i = 1, \ldots, n-1$,

(3) $H_1 \cdot \ldots \cdot H_n = G$.

Dowód. Zauważmy najpierw, że w oczywisty sposób surjektywność odwzorowania ϕ jest równoważna warunkowi (3). Załóżmy najpierw, że ϕ jest izomorfizmem. Wykażemy, że dla $i \neq j$ i dowolnych $h_i \in H_i$, $h_j \in H_j$ zachodzi równość $h_i h_j = h_j h_i$. Istotnie:

$$h_i h_j h_i^{-1} h_j^{-1} = \phi(1, \ldots, h_i, \ldots, h_j, \ldots, 1)\phi(1, \ldots, h_i^{-1}, \ldots, h_j^{-1}, \ldots, 1) = \varphi(1, \ldots, 1) = 1.$$

Dalej, jeśli $h \in H_i$ oraz $g \in G$, to z surjektywności ϕ mamy $g = h_1 \cdot \ldots \cdot h_n$ dla pewnych $h_i \in H_i, 1 \leqslant i \leqslant n$. Otrzymujemy zatem:

$$ghg^{-1} = h_1 \cdot \ldots \cdot h_n h h_n^{-1} \cdot \ldots \cdot h_1^{-1} = h_i h h_i^{-1} \in H_i,$$

czyli $H_i \lhd G$ dla $i = 1, \ldots, n$. Na koniec, jeśli $h_i = h_{i+1} \cdot \ldots \cdot h_n \in H_i \cap H_{i+1} \cdot \ldots \cdot H_n$, to

$$1 = h_i^{-1} h_{i+1} \cdot \ldots \cdot h_n = \phi(1, \ldots, 1, h_i^{-1}, h_{i+1}, \ldots, h_n),$$

czyli z injektywności ϕ mamy $h_i = h_{i+1} = \ldots = h_n = 1$.

Załóżmy teraz odwrotnie, że zachodzą warunki (1)–(3). Z własności 9.1.2 wynika, że wtedy $h_i h_j = h_j h_i$ dla dowolnych $h_i \in H_i, h_j \in H_j, i \neq j$, czyli ϕ jest homomorfizmem. Warunek (3) zapewnia surjektywność ϕ i wreszcie jeśli $\phi(h_1, \ldots, h_n) = h_1 \cdot \ldots \cdot h_n = 1$, to

$$h_1^{-1} = h_2 \cdot \ldots \cdot h_n \in H_1 \cap H_2 \cdot \ldots \cdot H_n = \{1\},$$

czyli $h_1 = 1$ i $h_2 \cdot \ldots \cdot h_n = 1$. Podobnie jest

$$h_2^{-1} = h_3 \cdot \ldots \cdot h_n \in H_2 \cap H_3 \cdot \ldots \cdot H_n = \{1\},$$

czyli $h_2 = 1$. Kontynuując analogicznie przekonujemy się, że $h_1 = h_2 = \ldots = h_n = 1$, co oznacza injektywność homomorfizmu ϕ. □

Twierdzenie 9.4.2. *Niech G będzie grupą skończoną rzędu $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$, gdzie liczby $p_1, \ldots, p_r$ są parami różnymi liczbami pierwszymi oraz $k_1, \ldots, k_r \in \mathbb{N}$. Jeśli P_i to p_i-podgrupa Sylowa grupy G dla $i = 1, \ldots, r$, to odwzorowanie:*

$$\varphi : P_1 \times \ldots \times P_r \ni (a_1, \ldots, a_r) \mapsto a_1 \cdot \ldots \cdot a_r \in G$$

jest izomorfizmem wtedy i tylko wtedy, gdy podgrupy $P_1, \ldots, P_r$ są normalne.

Dowód. Jeśli powyższe odwzorowanie jest izomorfizmem, to z poprzedniego twierdzenia wynika, że podgrupy $P_1, \ldots, P_r$ są normalne. Odwrotnie, gdy podgrupy te są normalne, to $P_i \cap P_j = \{1\}$ dla $i \neq j$ ze względu na fakt, że rzędy tych grup są względnie pierwsze, a w rezultacie $P_i \cap P_{i+1} \cdot \ldots \cdot P_r = \{1\}$ (na podstawie normalności elementy różnych podgrup P_k, P_l są ze sobą przemienne z 9.1.2, czyli rząd $P_{i+1} \cdot \ldots \cdot P_r$ jest względnie pierwszy z rzędem P_i). Warunki te, podobnie jak w dowodzie poprzedniego twierdzenia, dają injektywność φ, zaś równość $|G| = |P_1 \times \ldots \times P_r|$ kończy dowód. □

Jako, że w grupie abelowej mamy zagwarantowaną normalność każdej podgrupy, to bezpośrednio z naszego twierdzenia wynika następujący wniosek.

Wniosek 9.4.3. *Jeśli G jest grupą abelową rzędu $n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$, gdzie p_i są parami różnymi liczbami pierwszymi oraz $k_1, \ldots, k_r \in \mathbb{N}$, to istnieją takie podgrupy $H_1, \ldots, H_r$ grupy G, że $|H_i| = p_i^{k_i}$ dla $i = 1, \ldots, r$ oraz $G \cong H_1 \oplus \ldots \oplus H_r$.*

Dla skończonych grup abelowych uzyskamy nieco dokładniejszą charakteryzację, rozkładając je w sposób taki jak w powyższym wniosku, z dodatkową informacją o postaci podgrup H_i. W ten uzyskamy rozkład grupt na „cegiełki" cykliczne. Przedstawione przez nas poniżej rozumowania pochodzą z [10].

Własność 9.4.4. *Niech G będzie skończoną grupą abelową rzędu p^n dla pewnego $n \in \mathbb{N}$, zaś $g \in G$ elementem maksymalnego rzędu w G. Wtedy istnieje H taka podgrupa G, że $G \cong \langle g \rangle \oplus H$.*

Dowód. Zauważmy najpierw, że teza jest w oczywisty sposób prawdziwa, gdy $\langle g \rangle = G$. Istotnie, w tym przypadku wystarczy wziąć $H := \{1_G\}$. Dowód przeprowadzimy indukcyjnie względem n.

Jeśli $n = 1$, to mamy do czynienia ze skomentowaną sytuacją $G = \langle g \rangle$.

Niech $n > 1$ i niech $|g| = p^m$ dla pewnego $m \in \mathbb{N}$. Wtedy, wobec maksymalności m, dla dowolnego $a \in G$ zachodzi $a^{p^m} = 1_G$. Jeśli $G = \langle g \rangle$, to nie mamy co dowodzić, więc niech $h \notin \langle g \rangle$ będzie elementem minimalnego rzędu spoza $\langle g \rangle$. Twierdzimy, że wystarczy przyjąć $H = \langle h \rangle$.

Udowodnimy najpierw, że $H \cap \langle g \rangle = \{1_G\}$. Zauważmy, że wystarczy wykazać, że $|H| = p$. Jest tak, gdyż w takim przypadku $H = \{1_G, h, \ldots, h^{p-1}\}$, więc jeśli $a \in \langle h \rangle \cap \langle g \rangle$, to $a = h^k$ dla pewnego $k \in \{0, \ldots, p-1\}$ względnie pierwszego z p. Tym samym $H = \langle a \rangle \subset \langle g \rangle$, co prowadzi do sprzeczności.

Zauważmy, że jeśli $|h| = s$, to $(h^p)^{\frac{s}{p}} = 1_G$. Stąd $|h^p| = \frac{|h|}{p}$, a tym samym rząd h^p jest mniejszy niż rząd h. Wobec wyboru h mamy $h^p \in \langle g \rangle$, tzn. $h^p = g^r$ dla pewnego r. Stąd:

$$(g^r)^{p^{m-1}} = (h^p)^{p^{m-1}} = h^{p^m} = 1_G,$$

i wobec tego rząd g^r jest mniejszy lub równy od p^{m-1}. Oznacza to, że g^r nie może generować grupy $\langle g \rangle$. Jednocześnie, $r = ps$ dla pewnego $s \in \mathbb{N}$, więc $h^p = g^r = g^{ps}$. Określmy teraz $b := g^{-s}h$. Element ten nie może należeć do $\langle g \rangle$, gdyż w przeciwnym wypadku także h należałoby do $\langle g \rangle$. Mamy jednak:

$$b^p = g^{-sp}h^p = g^{-r}h^p = h^{-p}h^p = 1_G.$$

Otrzymaliśmy więc element b rzędu p spoza $\langle g \rangle$. Ponieważ h było minimalnego spośród elementów spoza $\langle g \rangle$, mamy $|H| = p$.

Zauważmy dalej, że $|gH| = |g|$. Oczywiście, $|gH| \leqslant |g|$, więc przypuśćmy że $|gH| < p^m$. Wtedy $H = 1_{G/H} = (gH)^{p^{m-1}} = g^{p^{m-1}}H$, czyli $g^{p^{m-1}} \in H \cap \langle g \rangle$, więc $g^{p^{m-1}} = 1_G$, wbrew temu, że $|g| = p^m$.

Oznacza to, że element gH jest elementem maksymalnego rzędu w grupie ilorazowej G/H, która jest p-grupą rzędu mniejszego niż rząd G. Możemy więc zastosować założenie indukcyjne i korzystając z 3.5.1 znaleźć taką K – podgrupę G, że $G/H \cong \langle gH \rangle \oplus (K/H)$, gdzie $H \subset K$. Dowolny element aH z G/H można więc przedstawić w postaci $(g^sH)(kH)$ dla pewnego $s \in \mathbb{Z}$ oraz $k \in K$. Oznacza to, że $a = g^skh$ dla pewnego $h \in H$, czyli $G = \langle g \rangle K$. Jednocześnie, jeśli $c \in \langle g \rangle \cap K$, to $cH \in \langle gH \rangle \cap K/H = \{1_{G/H}\}$, więc $c \in \langle g \rangle \cap H = \{1_G\}$, czyli ostatecznie $G \cong \langle g \rangle \oplus K$. □

Twierdzenie 9.4.5 (charakteryzacja skończonych grup abelowych)**.** *Dla każdej skończonej grupy abelowej G istnieją takie niekoniecznie różne między sobą liczby pierwsze $p_1, \ldots, p_r$ oraz takie liczby $k_1, \ldots, k_r \in \mathbb{N}$, że $G \cong \mathbb{Z}/p_1^{k_1}\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/p_r^{k_r}\mathbb{Z}$.*

Dowód. Jest to bezpośredni efekt poprzedniej własności. Jeśli bowiem G jest skończoną grupą abelową, zaś g jest elementem G maksymalnego rzędu, to albo $\langle g \rangle = G$, co kończy dowód, albo na podstawie 9.4.4 mamy $G \cong \mathbb{Z}_{|g|} \oplus H$ dla pewnej podgrupy H zawartej w G. Ponieważ $|H| < |G|$, indukcja kończy rozumowanie. □

Inaczej mówiąc, każda skończona grupa abelowa jest sumą prostą grup cyklicznych. Jak się okazuje, własność ta dotyczy również nieskończonych grup abelowych, gdy tylko są one skończenie generowane, o czym przekonamy się w kolejnym twierdzeniu. Zamieścimy tu jedynie szkic dowodu tego twierdzenia.

Zauważmy najpierw, że jeśli grupa abelowa G jest skończenie generowana i ustalimy pewien układ jej generatorów $g_1, \ldots, g_n$, to naturalny homomorfizm

$$\mathbb{Z}^n := \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{n\text{-krotnie}} \ni (k_1, \ldots, k_n) \longrightarrow k_1g_1 + \ldots + k_ng_n \in G^5$$

jest epimorfizmem. Odwrotnie, jeśli dla ustalonych elementów grupy $g_1, \ldots, g_n$ rozważane odwzorowanie jest epimorfizmem grup, to grupa G jest skończenie generowana, zaś jeśli K jest jądrem tego epimorfizmu, to $G \cong \mathbb{Z}^n/K$.

Skoro chcemy scharakteryzować grupy abelowe skończenie generowane, to wobec powyższych faktów wydaje się, że dobrze byłoby lepiej poznać strukturę podgrup grupy $\mathbb{Z}^n$ (tak jak to uczyniliśmy dla $n = 1$ w twierdzeniu 3.1.15).

Wykażemy, że za pomocą zmiany układu generującego można dowolną nietrywialną podgrupę K grupy $\mathbb{Z}^n$ przekształcić tak, aby:

$$K \cong d_1\mathbb{Z} \oplus \ldots \oplus d_r\mathbb{Z},$$

gdzie $d_1, \ldots, d_r > 0$ i $d_i | d_{i+1}$ dla $i = 1, \ldots, r$. W szczególności, otrzymamy pożądaną informację o grupie ilorazowej. Istotnie, konsekwencją tej własności jest równość $\mathbb{Z}^n/K \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^{n-r}$.

Zaczniemy od udowodnienia ważnej własności podgrup w $\mathbb{Z}^n$.

[5] Stosujemy zapis addytywny tzn. kg oznacza k-tą potęgę elementu g w G.

Własność 9.4.6 (liczebność generatorów podgrup w $\mathbb{Z}^n$)**.** *Każda podgrupa w $\mathbb{Z}^n$ jest generowana przez co najwyżej n elementów.*

Dowód. Zastosujemy indukcję względem n. Dla $n = 1$ teza jest prawdziwa, co wykazaliśmy w 3.1.15. Niech więc $K < \mathbb{Z}^n$ $(n > 1)$ oraz niech $H = \pi(K) < \mathbb{Z}$, gdzie π jest rzutem na pierwszą współrzędną. Wtedy istnieje taki $a_1 \in \mathbb{Z}$, że $H = a_1\mathbb{Z}$ i istnieją $a_2, \ldots, a_n \in \mathbb{Z}$ takie, że $(a_1, \ldots, a_n) \in K$. Niech $(k_1, \ldots, k_n) \in K$ oraz $k_1 = sa_1$ dla pewnego $s = s(k_1) \in \mathbb{Z}$. Wtedy

$$(k_1, k_2, \ldots, k_n) = s(a_1, a_2, \ldots, a_n) + (0, k_2 - sa_2, \ldots, k_n - sa_n).$$

Oczywiście, zbiór elementów postaci $(k_2 - s(k_1)a_2, \ldots, k_n - s(k_1)a_n)$ tworzy podgrupę w $\mathbb{Z}^{n-1}$ i podgrupa ta, na mocy założenia indukcyjnego, jest generowana przez co najwyżej $(n-1)$ elementów. Oznacza to, że K jest generowana przez co najwyżej n elementów. □

Twierdzenie 9.4.7 (rzutowania $\mathbb{Z}^n$)**.** *Jeśli K jest niezerową podgrupą w $\mathbb{Z}^n$, to istnieją takie $d_1, \ldots, d_r \in \mathbb{N}$, że $d_i | d_{i+1}$ dla $i = 1, \ldots, r-1$ oraz $K \cong d_1\mathbb{Z} \oplus \ldots \oplus d_r\mathbb{Z}$. W szczególności otrzymujemy izomorfizm:*

$$\mathbb{Z}^n / K \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^{n-r}.$$

Dowód. (Szkic) Wiemy, że podgrupa K jest skończenie generowana, wybierzmy więc generatory $g_1, \ldots, g_r$ grupy K. Wiemy już, że $r \leqslant n$. Jeśli

$$g_i = (k_{i,1}, \ldots, k_{i,n}), \qquad i = 1, \ldots, r,$$

to utwórzmy macierz:

$$\begin{pmatrix} k_{1,1} & k_{1,2} & \ldots & k_{1,n} \\ k_{2,1} & k_{2,2} & \ldots & k_{2,n} \\ \vdots & \vdots & & \vdots \\ k_{r,1} & k_{r,2} & \ldots & k_{r,n} \end{pmatrix}.$$

Sprowadzamy tę macierz do postaci normalnej

$$\begin{pmatrix} d_1 & l_{1,2} & \ldots & l_{1,r-1} & l_{1,r} & l_{1,r+1} & \ldots & l_{1,n} \\ 0 & d_2 & \ldots & l_{2,r-1} & l_{2,r} & l_{2,r+1} & \ldots & l_{2,n} \\ \vdots & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & d_{r-1} & l_{r-1,r} & l_{r-1,r+1} & \ldots & l_{r-1,n} \\ 0 & 0 & \ldots & 0 & d_r & l_{r,r+1} & \ldots & l_{r,n} \end{pmatrix},$$

takiej, aby $d_i | d_{i+1}$ dla $i = 1, \ldots, r-1$ gdzie $l_{i,j} \in \mathbb{Z}$ dla $1 \leqslant i < \min\{j, r+1\}$ oraz $2 \leqslant j \leqslant n$ [6]. Powstały układ wektorów (wierszy) o współczynnikach całkowitych tworzy poszukiwany układ generatorów podgrupy K. □

Bezpośrednio z poprzednich rozważań i ostatniego twierdzenia dostajemy wniosek.

Wniosek 9.4.8 (charakteryzacja grup abelowych skończenie generowanych)**.** *Każda skończenie generowana grupa abelowa jest izomorficzna z grupą postaci $\mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^d$, gdzie $d_i \in \mathbb{N}$ można wybrać tak, by $d_i | d_{i+1}$ oraz $d \in \mathbb{N}_0$.*

Przykład 9.4.9. Jak wyznaczyć wszystkie grupy abelowe rzędu 120 ? Niech G będzie taką grupą. Wiemy, że istnieją takie $d_1, \ldots, d_r > 1$, że $G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}/d_r\mathbb{Z}$ (bo grupa jest skończona) oraz $d_i | d_{i+1}$ dla $i = 1, \ldots, r-1$. Rozkładamy $k = 120 = 2^3 \cdot 3 \cdot 5$. Każdy z dzielników pierwszych liczby k musi dzielić d_r. Wobec tego mamy następujące możliwości:

(1) $d_r = 2^3 \cdot 3 \cdot 5$ czyli $r = 1$ i $G \cong \mathbb{Z}_{120}$,

(2) $d_r = 2^2 \cdot 3 \cdot 5$, wtedy $r = 2$ i $d_1 = 2$ oraz $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_{60}$,

(3) $d_r = 2 \cdot 3 \cdot 5$ i wtedy $r = 3$, $d_1 = d_2 = 2$ i mamy $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{30}$.

Wykazaliśmy w ten sposób, że istnieją dokładnie 3 grupy abelowe rzędu 120.

[6] Można to zrobić za pomocą operacji (wykonywanych na wyjściowej macierzy) dodawania, odejmowania oraz zamiany miejscami wierszy i kolumn, ewentualnie mnożenia przez (-1). Chcemy jedynie, by rząd tej macierzy się nie zmienił

9.5 Grupy rozwiązalne

Na koniec bardziej zaawansowanych rozważań z zakresu teorii grup przyjrzyjmy się specjalnemu typowi grupy: grupie rozwiązalnej. Nazwa tej grupy usprawiedliwiona jest jej związkiem z problemem, który leży u historycznych podstaw powstania teorii grup – problem rozwiązalności równań wielomianowych, czyli poszukiwania metod wyliczania pierwiastków wielomianu za pomocą jego współczynników. O tych związkach opowiemy dalej (por. 12.6).

Z każdą grupą G możemy związać pewną szczególną podgrupę normalną G', nazywaną pochodną grupy G. Jedną z charakterystycznych cech tej grupy jest fakt, że G/G' jest grupą abelową.

Definicja 9.5.1 (komutant/pochodna grupy)**.** Jeśli G jest grupą oraz x, $y \in G$, to element:

$$[x, y] := xyx^{-1}y^{-1}$$

nazywamy **komutatorem** elementów x, y. **Komutantem (pochodną)** grupy G nazywamy grupę G' generowaną przez wszystkie komutatory tzn.

$$G' := \langle [x, y] : \ x, y \in G \rangle \ ^{7}.$$

Analogicznie określamy wyższe pochodne:

$$G^{(0)} := G, \quad G^{(n+1)} := (G^{(n)})', \quad n \in \mathbb{N}_0.$$

Własność 9.5.2 (podstawowe własności komutanta grupy)**.** *Jeśli G jest grupą, zaś H jej podgrupą, to następujące warunki są równoważne:*

(1) $G' \subset H$,

(2) $H \lhd G$ oraz G/H jest grupą abelową.

Dowód. (1) $\Longrightarrow$ (2) Jeśli $h \in H$ oraz $g \in G$, to

$$ghg^{-1} = (ghg^{-1}h^{-1})h = [g, h]h \in G'H \subset H.$$

Jeśli natomiast a, $b \in G$, to wtedy:

$$(aH)(bH) = abH = (baa^{-1}b^{-1}ab)H = ba[a^{-1}, b^{-1}]H = baH = (bH)(aH).$$

(2) $\Longrightarrow$ (1) Dla a, $b \in G$ mamy:

$$[a, b]H = (aba^{-1}b^{-1})H = (aH)(bH)(a^{-1}H)(b^{-1}H) = (aH)(a^{-1}H)(bH)(b^{-1}H) = H,$$

czyli $[a, b] \in H$, więc $G' \subset H$ jako grupa generowana przez komutatory. □

Definicja 9.5.3 (grupa rozwiązalna)**.** Mówimy, że grupa G jest **rozwiązalna**, jeśli istnieje takie $n \in \mathbb{N}_0$, że $G^{(n)} = \{1\}$. Najmniejszą całkowitą liczbę nieujemną o tej własności nazywamy wtedy **stopniem rozwiązalności** grupy G.

Przykład 9.5.4. (1) Każda grupa abelowa jest rozwiązalna, bowiem jej pierwsza pochodna jest równa $\{1\}$. Jeśli taka grupa jest nietrywialna, to stopień jej rozwiązalności wynosi 1.

(2) Można łatwo sprawdzić, że $S_4' = A_4$, $A_4' = V := \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$[8] i wreszcie $V' = \{1\}$, skąd S_4 jest grupą rozwiązalną stopnia 3.

Twierdzenie 9.5.5 (charakteryzacja rozwiązalności grupy)**.** *Grupa G jest rozwiązalna wtedy i tylko wtedy, gdy istnieje taki ciąg:*

$$\{1\} = G_0 \lhd G_1 \lhd \ldots \lhd G_n = G$$

w którym G_i/G_{i-1} jest grupą abelową dla $i = 1, \ldots, n$.

[7] Gdy A jest podzbiorem grupy G, to piszemy $\langle A \rangle = \langle a : \ a \in A \rangle$ pomijając dla uproszczenia parę nawiasów klamrowych.

[8] Jest to tzw. czwórkowa grupa Kleina, izomorficzna z niecykliczną grupą $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Dowód. Zauważmy, że twierdzenie oczywiście jest prawdziwe, gdy G jest grupą trywialną. Zakładamy więc dalej, iż G jest nietrywialna.

Jeśli grupa G jest rozwiązalna, to niech $n \in \mathbb{N}$ będzie takie, że $G^{(n)} = \{1\}$. Wtedy z poprzedniej własności szukanym ciągiem jest:

$$\{1\} = G^{(n)} \lhd G^{(n-1)} \lhd \ldots \lhd G^{(0)} = G.$$

Odwrotnie, załóżmy, że istnieje ciąg z tezy. Ponieważ $G_{n-1} \lhd G_n$ i grupa G_n/G_{n-1} jest abelowa, to na podstawie poprzedniej własności mamy $G^{(1)} = G_n^{(1)} \subset G_{n-1}$. Podobnie dalej $G_{n-2} \lhd G_{n-1}$ oraz grupa G_{n-1}/G_{n-2} jest abelowa i znów w takim razie $G_{n-1}^{(1)} \subset G_{n-2}$, czyli $G^{(2)} \subset G_{n-1}^{(1)} \subset G_{n-2}$. Kontynuując rozumowanie w ten sposób, otrzymamy $G^{(n)} \subset G_0 = \{1\}$, co kończy dowód. □

Twierdzenie 9.5.6 (dziedziczenie rozwiązalności)**.** *Niech $f : G \longrightarrow \widetilde{G}$ będzie homomorfizmem grup, H – podgrupa G, $N \lhd G$. Wtedy zachodzą własności:*

(1) jeśli G jest rozwiązalna, to H i $f(G)$ są grupami rozwiązalnymi,

(2) jeśli grupy N i G/N są rozwiązalne, to również G jest rozwiązalna.

Dowód. (1) Z definicji łatwo widać, że $H^{(n)} \subset G^{(n)}$ dla $n \in \mathbb{N}_0$, więc H jest grupą rozwiązalną stopnia nie większego niż stopień G. Podobnie sprawdzamy, że $(f(G))^{(n)} = f(G^{(n)})$ dla $n \in \mathbb{N}_0$ i znów stopień rozwiązalności $f(G)$ nie przewyższa stopnia dla G.

(2) Jeśli G/N jest trywialna, to oznacza, że $G = N$, więc twierdzenie jest prawdziwe. Załóżmy więc, że G/N jest nietrywialna. Skoro jest rozwiązalna, to istnieje takie $n \in \mathbb{N}$, że $(G/N)^{(n)} = \{1\}$. Stosując analogiczne rozumowanie jak w (1) do rzutowania kanonicznego $\pi : G \longrightarrow G/N$ dostaniemy, że $\pi(G^{(n)}) = (G/N)^{(n)} = \{1\}$ czyli $G^{(n)} \subset N$ – jednak N jest grupą rozwiązalną, a jak wiemy z (1) jej podgrupa też musi być rozwiązalna. Oznacza to, że G jest rozwiązalna ze względu na rekurencyjną definicję pochodnej. □

Wniosek 9.5.7 (nierozwiązalność S_n)**.** *Grupy S_n dla $n \geqslant 5$ są nierozwiązalne.*

Dowód. Gdyby $S_n, n \geqslant 5$, była grupą rozwiązalną, to zgodnie z poprzednią własnością rozwiązalna byłaby także grupa A_n. Jedyny ciąg podgrup normalnych w A_n, to $\{1\} \lhd A_n$ (por. twierdzenie 3.6.10). Wiemy jednak, że $A_n/\{1\} = A_n$ nie jest abelowa dla $n \geqslant 5$. □

Rozdział 10

Wybrane zagadnienia teorii pierścieni

10.1 Pierścień wielomianów wielu zmiennych

10.1.1 Konstrukcja pierścienia wielomianów wielu zmiennych

Niech P będzie pierścieniem. W tym rozdziale skonstruujemy pierścień wielomianów n-zmiennych w ogólnej postaci. Nasza konstrukcja doprowadzi do powstania pierścienia izomorficznego z rozważanym w 5.1.3. Będziemy dalej operować na wielowskaźnikach naturalnych, tzn. elementach zbioru $\mathbb{N}_0^n$. Jeśli $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$, to liczbę:

$$|\alpha| := \alpha_1 + \ldots + \alpha_n$$

nazywamy **długością** wielowskaźnika α. Ustalmy teraz $n \in \mathbb{N}$ i niech

$$W_n(P) := \{f : \mathbb{N}_0^n \longrightarrow P : \ f(\alpha) = 0, \ \text{ dla prawie wszystkich } \ \alpha \in \mathbb{N}_0^n\}.$$

Na zbiorze tym wprowadzamy dwa działania. Dla f, $g \in W_n(P)$ oraz $\alpha \in \mathbb{N}_0^n$ określamy:

$$(f+g)(\alpha) := f(\alpha) + g(\alpha), \qquad (fg)(\alpha) := \sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma).$$

Twierdzenie 10.1.1. *Niech P – pierścień, $n \in \mathbb{N}$. Wtedy:*

(1) zbiór $W_n(P)$ z określonymi powyżej działaniami ma strukturę pierścienia przemiennego z jedynką różną od zera,

(2) odwzorowanie: $\varphi : P \longrightarrow W_n(P)$ określone wzorem:

$$\varphi(a) := f_a, \quad f_a(\alpha) := \begin{cases} a, & gdy \ \ \alpha = 0 \\ 0, & gdy \ \ \alpha \neq 0 \end{cases}$$

jest monomorfizmem pierścieni.

Dowód. (1) Oczywiście $(W_n(P), +)$ jest grupą abelową, gdyż taką grupą jest $(P, +)$. Ponadto, dla dowolnych f, g, $h \in W_n(P)$, mamy

$$\begin{aligned}(f(gh))(\alpha) &= \sum_{\beta+\varepsilon=\alpha} f(\beta)(gh)(\varepsilon) = \sum_{\beta+\varepsilon=\alpha} f(\beta) \left(\sum_{\gamma+\delta=\varepsilon} g(\gamma)h(\delta) \right) \\ &= \sum_{\beta+\gamma+\delta=\alpha} f(\beta)g(\gamma)h(\delta) = \sum_{\delta+\varepsilon=\alpha} \left(\sum_{\beta+\gamma=\delta} f(\beta)g(\gamma) \right) h(\varepsilon)\end{aligned}$$

oraz

$$\begin{aligned}(f(g+h))(\alpha) &= \sum_{\beta+\gamma=\alpha} f(\beta)(g+h)(\gamma) = \sum_{\beta+\gamma=\alpha} (f(\beta)g(\gamma) + f(\beta)h(\gamma)) \\ &= \sum_{\beta+\gamma=\alpha} f(\beta)g(\gamma) + \sum_{\beta+\gamma=\alpha} f(\beta)h(\gamma) = (fg)(\alpha) + (fh)(\alpha) = (fg+fh)(\alpha).\end{aligned}$$

Analogicznie przeliczamy równość $(g+h)f = gf + hf$. Jedynką pierścienia $W_n(P)$ jest

$$1_{W_n(P)}(\alpha) = \begin{cases} 1, & \text{gdy } \alpha = 0 \\ 0, & \text{gdy } \alpha \neq 0 \end{cases},$$

gdyż $(1_{W_n(P)} f)(\alpha) = \sum\limits_{\beta+\gamma=\alpha} 1_{W_n(P)}(\beta) f(\gamma) = f(\alpha)$.

(2) Gdy $f_a = 0$, to wtedy $0 = f_a(0) = a$. □

Wyróżnimy teraz w pierścieniu $W_n(P)$ specjalne elementy nazywane zmiennymi. Niech:

$$\varepsilon_i := (\delta_{i,j})_{j=1,\ldots,n} = (0,\ldots,1,\ldots,0), \qquad i = 1,\ldots,n.$$

Wobec tego dla dowolnego $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}_0^n$, mamy $\alpha = \alpha_1\varepsilon_1 + \ldots + \alpha_n\varepsilon_n$.

Definicja 10.1.2 (zmienna nad pierścieniem II)**.** (por. definicja 4.5.2) Jeśli P jest pierścieniem, $n \in \mathbb{N}$, to ***i*-tą zmienną** nad tym pierścieniem $(1 \leqslant i \leqslant n)$ nazywamy element pierścienia $W_n(P)$ określony wzorem:

$$X_i(\alpha) := \begin{cases} 1, & \text{gdy } \alpha = \varepsilon_i \\ 0, & \text{gdy } \alpha \neq \varepsilon_i \end{cases}.$$

Definicja 10.1.3 (pierścień wielomianów n-zmiennych)**.** Jeśli P – pierścień, $n \in \mathbb{N}$, to pierścień $(W_n(P), +, \cdot)$ wprowadzony powyżej nazywamy **pierścieniem wielomianów n-zmiennych** nad pierścieniem P (lub o współczynnikach z P) i oznaczamy $W_n(P) = P[X_1,\ldots,X_n]$. Każdy element tego pierścienia nazywamy **wielomianem**.

Wprowadzamy dodatkowo oznaczenia:

$$X := (X_1,\ldots,X_n), \qquad X^\alpha := X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n}, \qquad \alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{N}_0^n.$$

10.1.2 Ogólne własności pierścienia wielomianów

Przedstawimy teraz dowód równoważności przedstawionej konstrukcji pierścienia wielomianów wielu zmiennych z jego konstrukcją indukcyjną, polegającą na rozważaniu pierścienia wielomianów jednej zmiennej nad pierścieniem wielomianów mniejszej liczby zmiennych. Rozumowania przedstawione poniżej powstały w oparciu o [8].

Własność 10.1.4. *Niech P – pierścień, $n \in \mathbb{N}$, $1 \leqslant i \leqslant n$. Dla $k \in \mathbb{N}_0$ oraz $\beta = (\beta_1,\ldots,\beta_n) \in \mathbb{N}_0^n$ zachodzi:*

$$X_i^k(\alpha) = \begin{cases} 1, & gdy \ \ \alpha = k\varepsilon_i \\ 0, & gdy \ \ \alpha \neq k\varepsilon_i \end{cases}, \qquad X^\beta(\alpha) = \begin{cases} 1, & gdy \ \ \alpha = \beta \\ 0, & gdy \ \ \alpha \neq \beta \end{cases}.$$

Dowód. Pierwszą część udowodnimy indukcyjnie względem k. Jeśli $k = 0$, to oczywiście mamy $X_i^0 = 1_{P[X_1,\ldots,X_n]}$. Dla $k = 1$ jest zaś $X_i^1 = X_i$. Niech $k > 1$ i teza będzie prawdziwa dla $k-1$. Zauważmy, że

$$X_i^{k-1}(\beta)X_i(\gamma) = \begin{cases} 1\cdot 1, & \text{gdy } \beta = (k-1)\varepsilon_i \ \text{ oraz } \ \gamma = \varepsilon_i \\ 1\cdot 0, & \text{gdy } \beta = (k-1)\varepsilon_i \ \text{ oraz } \ \gamma \neq \varepsilon_i \\ 0\cdot 1, & \text{gdy } \beta \neq (k-1)\varepsilon_i \ \text{ oraz } \ \gamma = \varepsilon_i \\ 0\cdot 0, & \text{gdy } \beta \neq (k-1)\varepsilon_i \ \text{ oraz } \ \gamma \neq \varepsilon_i \end{cases}$$
$$= \begin{cases} 1, & \text{gdy } \beta = (k-1)\varepsilon_i \ \text{ oraz } \ \gamma = \varepsilon_i \\ 0, & \text{gdy } \beta \neq (k-1)\varepsilon_i \ \text{ lub } \ \gamma \neq \varepsilon_i \end{cases}.$$

Zatem

$$X_i^k(\alpha) = (X_i^{k-1}X_i)(\alpha) = \sum_{\beta+\gamma=\alpha} X_i^{k-1}(\beta)X_i(\gamma) = \begin{cases} 1, & \text{gdy } \alpha = k\varepsilon_i \\ 0, & \text{gdy } \alpha \neq k\varepsilon_i \end{cases}.$$

Podobnie:

$$X^\beta(\alpha) = (X_1^{\beta_1} \cdot \ldots \cdot X_n^{\beta_n})(\alpha) = \sum_{\gamma_1+\ldots+\gamma_n=\alpha} X_1^{\beta_1}(\gamma_1) \cdot \ldots \cdot X_n^{\beta_n}(\gamma_n),$$

co jest równe:

$$= \begin{cases} 1, & \text{gdy } \gamma_1 = \beta_1\varepsilon_1,\ldots,\gamma_n = \beta_n\varepsilon_n \\ 0, & \text{w pozostałych przypadkach} \end{cases} = \begin{cases} 1, & \text{gdy } \alpha = \beta \\ 0, & \text{w pozostałych przypadkach} \end{cases}.$$

□

Ustalimy teraz standardową terminologię. Wielomian postaci aX^α nazywamy **jednomianem** lub **formą**. Każdy wielomian $f \in P[X_1, \ldots, X_n]$ można jednoznacznie przedstawić w postaci sumy jednomianów, mianowicie:

$$f = \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha X^\alpha, \qquad \text{gdzie prawie wszystkie } \ a_\alpha = f(\alpha) \ \text{ są równe zero.}$$

Często będziemy upraszczać zapis do $f = \sum\limits_{\alpha} a_\alpha X^\alpha$ lub nawet $f = \sum a_\alpha X^\alpha$ gdy wiadomo ilu zmiennych jest wielomian. **Stopniem wielomianu** f nazywamy liczbę:

$$\deg f := \begin{cases} \max\{|\alpha| : \ a_\alpha \neq 0\}, & \text{gdy } f \neq 0 \\ -\infty, & \text{gdy } f = 0 \end{cases}.$$

Wielomian $f \neq 0$ nazywamy **jednorodnym stopnia** $s \geqslant 0$, jeśli $f = \sum\limits_{|\alpha|=s} a_\alpha X^\alpha$.

Twierdzenie 10.1.5 (o uniwersalności pierścienia wielomianów)**.** *Dla dowolnego homomorfizmu pierścieni $\varphi : P \longrightarrow R$ i układu elementów $t_1, \ldots, t_n \in R$ istnieje jedyny taki homomorfizm pierścieni $\Phi : P[X_1, \ldots, X_n] \longrightarrow R$, że $\Phi(X_i) = t_i$ dla $i = 1, \ldots, n$ oraz $\Phi|_P = \varphi$.*

Dowód. Zauważmy, że homomorfizm pojawiający się w tezie jest jednoznacznie wyznaczony przez swoje własności, gdyż:

$$\Phi\left(\sum_{\alpha \in \mathbb{N}_0^n} a_\alpha X^\alpha\right) = \sum_{\alpha \in \mathbb{N}_0^n} \Phi(a_\alpha X^\alpha) = \sum_{\alpha \in \mathbb{N}_0^n} \Phi(a_\alpha)\Phi(X^\alpha) = \sum_{\alpha \in \mathbb{N}_0^n} \varphi(a_\alpha) t^\alpha,$$

gdzie $t^\alpha = t_1^{\alpha_1} \cdot \ldots \cdot t_n^{\alpha_n}$ dla $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}_0^n$. Pozostaje więc sprawdzić, że zadane w ten sposób odwzorowanie spełnia tezę. W oczywisty sposób jest to homomorfizm grup z dodawaniem. Ponadto, dla α, β, $\gamma \in \mathbb{N}_0^n$:

$$\begin{aligned} \Phi(\sum_\alpha a_\alpha X^\alpha \sum_\beta b_\beta X^\beta) &= \Phi(\sum_\gamma (\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta) X^\gamma) \\ &= \sum_\gamma \varphi(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta) t^\gamma = \sum_\gamma (\sum_{\alpha+\beta=\gamma} \varphi(a_\alpha)\varphi(b_\beta)) t^\gamma \\ &= \sum_\alpha \varphi(a_\alpha) t^\alpha \sum_\beta \varphi(b_\beta) t^\beta = \Phi(\sum_\alpha a_\alpha X^\alpha)\Phi(\sum_\beta b_\beta X^\beta), \end{aligned}$$

czyli Φ jest homomorfizmem pierścieni. Ostatecznie, jeśli $a \in P$, to $\Phi(a) = \varphi(a)t^0 = \varphi(a)$ zatem $\Phi|_P = \varphi$. □

Przeliczone własności pozwolą nam na wyciągnięcie wniosku, którego należało się spodziewać.

Wniosek 10.1.6. *Jeśli pierścienie P i R są izomorficzne, to również pierścienie wielomianów $P[X_1, \ldots, X_n]$ oraz $R[X_1, \ldots, X_n]$ są izomorficzne.*

Dowód. Jeśli $f : P \longrightarrow R$ to izomorfizm, to określamy dwa homomorfizmy:

$$\varphi := \iota_R \circ f : P \longrightarrow R[X_1, \ldots, X_n], \qquad \psi := \iota_P \circ f^{-1} : R \longrightarrow P[X_1, \ldots, X_n].$$

Zgodnie z poprzednim twierdzeniem istnieją homomorfizmy rozszerzające te odwzorowania tzn.

$$\Phi : P[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n], \ \Phi|_P = \varphi, \ \Phi(X_i) = X_i$$

$$\Psi : R[X_1, \ldots, X_n] \longrightarrow P[X_1, \ldots, X_n], \ \Psi|_P = \psi, \ \Psi(X_i) = X_i.$$

Dla $\sum\limits_{\alpha \in \mathbb{N}_0^n} a_\alpha X^\alpha \in P[X_1, \ldots, X_n]$ mamy:

$$\begin{aligned} (\Psi \circ \Phi)(\sum_\alpha a_\alpha X^\alpha) &= \Psi(\sum_\alpha \varphi(a_\alpha) X^\alpha) = \Psi(\sum_\alpha f(a_\alpha) X^\alpha) \\ &= \sum_\alpha \psi(f(a_\alpha)) X^\alpha = \sum_\alpha f^{-1}(f(a_\alpha)) X^\alpha = \sum_\alpha a_\alpha X^\alpha. \end{aligned}$$

Podobnie wykazujemy, że $\Phi \circ \Psi = id$, co kończy dowód. □

Wniosek 10.1.7. *Niech $\varphi : P \longrightarrow R$ będzie homomorfizmem pierścieni, I ideałem w P, zaś $\pi : P \longrightarrow P/I$ epimorfizmem kanonicznym. Wtedy:*

(1) istnieje dokładnie jeden homomorfizm $\Phi : P[X_1, \ldots, X_n] \longrightarrow R[X_1, \ldots, X_n]$ taki, że $\Phi|_P = \varphi$, $\Phi(X_i) = X_i$ dla $i = 1, \ldots, n$; dodatkowo, gdy φ jest monomorfizmem (epimorfizmem), to również Φ jest monomorfizmem (epimorfizmem),

(2) jedyny homomorfizm pierścieni $\Pi : P[X_1, \ldots, X_n] \longrightarrow (P/I)[X_1, \ldots, X_n]$ spełniający $\Pi|_P = \pi$ oraz $\Pi(X_i) = X_i$ dla $i = 1, \ldots, n$ jest epimorfizmem o jądrze $I[X_1, \ldots, X_n]$ – w szczególności więc $P[X_1, \ldots, X_n]/I[X_1, \ldots, X_n] \cong (P/I)[X_1, \ldots, X_n]$.

Dowód. (1) Pierwsza część tezy to wniosek z twierdzenia o uniwersalności 10.1.5, zaś druga wynika z postaci Φ.

(2) Zauważmy, że $\sum\limits_{\alpha \in \mathbb{N}_0^n} a_\alpha X^\alpha \in \mathrm{Ker}(\Pi)$ wtedy i tylko wtedy, gdy $\sum\limits_{\alpha}(a_\alpha + I)X^\alpha = 0$, czyli gdy $a_\alpha + I = I$ co oznacza, że $a_\alpha \in I$ dla dowolnego α. □

Wniosek 10.1.8. *Niech P pierścień, $\{i_1, \ldots, i_n\} = \{1, \ldots, n\}$ oraz niech $0 < k < n$. Wtedy*

(1) istnieje monomorfizm $P[X_{i_1}, \ldots, X_{i_k}] \longrightarrow P[X_1, \ldots, X_n]$,

(2) $P[X_{i_1}, \ldots, X_{i_k}][X_{i_{k+1}}, \ldots, X_{i_n}] \cong P[X_1, \ldots, X_n]$.

Dowód. (1) Niech $\varphi : P \longrightarrow P[X_1, \ldots, X_n]$ będzie naturalnym monomorfizmem. Stosując twierdzenie 10.1.5 otrzymujemy taki homomorfizm $\Phi : P[X_{i_1}, \ldots, X_{i_k}] \longrightarrow P[X_1, \ldots, X_n]$, że $\Phi|_P = \varphi$ oraz $\Phi(X_{i_j}) = X_{i_j}$ dla $j = 1, \ldots, k$. Z poprzedniego wniosku wiemy, że Φ jest monomorfizmem.

(2) Zachowując oznaczenia i stosując ponownie twierdzenie o uniwersalności do Φ otrzymujemy dodatkowo taki monomorfizm $\Psi : P[X_{i_1}, \ldots, X_{i_k}][X_{i_{k+1}}, \ldots, X_{i_n}] \longrightarrow P[X_1, \ldots, X_n]$, że $\Psi|_{P[X_{i_1}, \ldots, X_{i_k}]} = \Phi$ oraz $\Psi(X_{i_j}) = X_{i_j}$ dla $j = k+1, \ldots, n$. W szczególności $\Psi(X_i) = X_i$ dla $i = 1, \ldots, n$.

Jeśli zaś $f = \sum\limits_{\alpha} a_\alpha X^\alpha \in P[X_1, \ldots, X_n]$, to

$$f = \sum_{\alpha} a_\alpha X_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot X_{i_k}^{\alpha_{i_k}} X_{i_{k+1}}^{\alpha_{i_{k+1}}} \cdot \ldots \cdot X_{i_n}^{\alpha_{i_n}} = \Psi(\sum_{\alpha} A_\alpha X_{i_{k+1}}^{\alpha_{i_{k+1}}} \cdot \ldots \cdot X_{i_n}^{\alpha_{i_n}}),$$

gdzie $A_\alpha = a_\alpha X_{i_1}^{\alpha_{i_1}} \cdot \ldots \cdot X_{i_k}^{\alpha_{i_k}} \in P[X_{i_1}, \ldots, X_{i_k}]$. □

Jako prosty wniosek z sytuacji dla jednej zmiennej (por. 4.5.10) otrzymujemy następującą własność.

Własność 10.1.9. *Jeśli P jest pierścieniem całkowitym, to $P[X_1, \ldots, X_n]$ też jest pierścieniem całkowitym.*

10.1.3 Własności stopnia i ich konsekwencje

Własność 10.1.10. *Niech P będzie pierścieniem, $f, g \in P[X_1, \ldots, X_n]$. Wtedy*

(1) jeśli wielomiany f, g są jednorodne stopnia s, to $f + g = 0$ lub $f + g$ jest jednorodny stopnia s,

(2) jeśli wielomiany f, g są jednorodne oraz $fg \neq 0$, to fg jest jednorodny stopnia $\deg f + \deg g$,

(3) jeśli $\deg f = n$, to istnieją takie (wyznaczone jednoznacznie) wielomiany $f_0, \ldots, f_n \in P[X_1, \ldots, X_n]$, że $f_n \neq 0$, $f = \sum\limits_{i=0}^{n} f_i$ oraz $\deg f_i = i$ o ile $f_i \neq 0$ dla $i = 0, \ldots, n$.

Dowód. Wymienione własności wynikają bezpośrednio z definicji, podamy więc tylko krótkie komentarze. Dowodząc (2) zauważmy, że jeśli $f = \sum\limits_{|\alpha|=s} a_\alpha X^\alpha$ oraz $g = \sum\limits_{|\beta|=t} b_\beta X^\beta$, to $fg = \sum\limits_{|\gamma|=s+t} (\sum\limits_{\alpha+\beta=\gamma} a_\alpha b_\beta) X^\gamma$, zatem w szczególności $\deg(fg) = \deg f + \deg g$ dla $fg \neq 0$.

(3) Jeśli $f = \sum\limits_{\alpha} a_\alpha X^\alpha$, to wystarczy przyjąć $f_i := \sum\limits_{|\alpha|=i} a_\alpha X^\alpha$ dla $i = 0, \ldots, n$. □

Wniosek 10.1.11. *Niech P – pierścień, $f, g \in P[X_1, \ldots, X_n]$. Wtedy*

(1) $\deg(f + g) \leqslant \max\{\deg f, \deg g\}$,

(2) $\deg(fg) \leqslant \deg f + \deg g$ *i dodatkowo przy całkowitości pierścienia zachodzi równość.*

Dowód. Przedstawmy najpierw nasze wielomiany w postaci sumy form: $f = f_0 + \ldots + f_k$, $g = g_0 + \ldots + g_l$ - $f_k \neq 0$, $g_l \neq 0$, gdzie składniki to formy jednorodne. Gdy $k \neq l$ i przykładowo $k < l$, to

$$f + g = (f_0 + g_0) + \ldots + (f_k + g_k) + g_{k+1} + \ldots + g_l,$$

skąd teza. Oczywiście, gdy $k = l$ i $g_k = -f_k$ to mamy nierówność silną.

Dla dowodu (2) zauważmy, że:

$$fg = f_0g_0 + (f_0g_1 + f_1g_0) + \ldots + (f_{k-1}g_l + f_kg_{l-1}) + f_kg_l.$$

Jeśli $f_kg_l \neq 0$, to $\deg(fg) = \deg f + \deg g$. Jeśli $f_kg_l = 0$ to nierówność jest słaba. Gdy pierścień jest całkowity, to $f_kg_l \neq 0$. □

Wniosek 10.1.12. *Jeśli P jest całkowity, to $U(P[X_1, \ldots, X_n]) = U(P)$.*

Dowód. Oczywiście $U(P) \subset U(P[X_1, \ldots, X_n])$. Jeśli $f \in P[X_1, \ldots, X_n]$ jest elementem odwracalnym, to istnieje taki $g \in P[X_1, \ldots, X_n]$, że $fg = 1$. Porównanie stopni po obu stronach, dzięki całkowitości pierścienia daje $\deg f + \deg g = 0$, czyli ponieważ oba wielomiany muszą być niezerowe mamy $\deg f = \deg g = 0$, w szczególności f jest stałą odwracalną w perścieniu P. □

10.2 Pierścienie noetherowskie

W podstawowej części naszego wykładu udowodniliśmy, że każdy pierścień euklidesowy jest pierścieniem ideałów głównych (por. twierdzenie 4.6.3). Przyjrzyjmy się dalszym własnościom tych ciekawych pierścieni. Szczególnie ważna jest następująca własność, która prowadzi do definicji kolejnego typu pierścienia.

Własność 10.2.1. *Niech P będzie pierścieniem ideałów głównych. Wtedy:*

(1) każdy wstępujący ciąg ideałów w P stabilizuje się,

(2) każda niepusta rodzina ideałów w P ma element maksymalny względem relacji inkluzji.

Dowód. (1) Niech $(I_n)_{n=1}^{\infty}$ będzie wstępującym ciągiem ideałów.

Wtedy ponieważ suma $J := \bigcup_{n=1}^{\infty} I_n$ jest też ideałem (ze względu na monotoniczność), to suma także jest generowana przez jeden element $a \in P$, czyli $J = (a)$. Wobec tego istnieje taki wskaźnik $n_0 \in \mathbb{N}$, że $a \in I_{n_0}$. Ale dla dowolnego $p \geqslant n_0$ mamy $I_{n_0} \subset I_p \subset J = (a) \subset I_{n_0}$. Stąd od tego momentu ciąg musi się stabilizować.

(2) Dla dowodu nie wprost załóżmy, że $\mathcal{F}$ jest niepustą rodziną ideałów, w której nie ma elementu maksymalnego i wybierzmy $I_1 \in \mathcal{F}$. Skoro nie jest to element maksymalny to oznacza, że istnieje taki element $I_2 \in \mathcal{F}$, że $I_1 \subsetneq I_2$. Kontynuujemy w ten sam sposób rekurencyjnie i otrzymujemy wstępujący ciąg ideałów w P, który się nie stabilizuje, co stoi w sprzeczności z (1). □

Definicja 10.2.2 (pierścień noetherowski)**.** [1] Pierścień, w którym każdy wstępujący ciąg ideałów stabilizuje się nazywamy **pierścieniem noetherowskim**.

Bezpośrednio z udowodnionej przez nas własności otrzymujemy wniosek.

Wniosek 10.2.3. *Każdy pierścień ideałów głównych jest pierścieniem noetherowskim.*

Często przyjmuje się nieco inną definicję pierścienia noetherowskiego, którą wyraża warunek równoważny omówiony w poniższym twierdzeniu.

Twierdzenie 10.2.4. *Pierścień P jest pierścieniem noetherowskim wtedy i tylko wtedy, gdy każdy ideał w P jest skończenie generowany.*

[1] Amalie Emmy Noether (1882-1935) – niemiecka matematyczka i fizyczka.

Dowód. Załóżmy najpierw, że P jest pierścieniem noetherowskim, w którym znajdziemy pewien ideał I, który nie jest skończenie generowany. Wybierzmy $a_1 \in I$ i dalej rekurencyjnie wybierzmy taki ciąg $a_2, \ldots$, że $a_{i+1} \in I \setminus (a_1, \ldots, a_i)$ (skoro $a_1, \ldots, a_i$ nie mogą wygenerować I, to taki element a_{i+1} istnieje). Mamy wtedy:

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \ldots \subsetneq (a_1, \ldots, a_n) \subsetneq \ldots$$

wstępujący ciąg ideałów w P, który się nie stabilizuje, co jest sprzeczne z noetherowskością P.

Dla dowodu wynikania przeciwnego rozumujemy analogicznie jak w dowodzie własności 10.2.1 z tym, że dla sumy wybieramy zamiast jednego generatora skończony układ generatorów. □

Przykład 10.2.5. (1) Pierścienie $\mathbb{Z}$, $K[X]$ (K – ciało) jako pierścienie ideałów głównych są pierścieniami noetherowskimi i jak zobaczymy w kolejnym twierdzeniu także $K[X_1, \ldots, X_n]$ jest noetherowski.

(2) Pierścień $K[X_1, X_2, \ldots] := \bigcup_{n=1}^{\infty} K[X_1, \ldots, X_n]$ nie jest pierścieniem noetherowskim, jako że ciąg $(X_1) \subsetneq (X_1, X_2) \subsetneq \ldots$ nie stabilizuje się.

Zauważymy teraz, że własność noetherowskości pierścienia dziedziczy się na nowe struktury.

Własność 10.2.6. *Niech P będzie pierścieniem noetherowskim, $f : P \longrightarrow R$ homomorfizmem pierścieni, zaś I ideałem w P. Wtedy*

(1) $f(P)$ jest pierścieniem noetherowskim,

(2) P/I jest pierścieniem noetherowskim,

Dowód. Część (1) jest oczywista ze względu na postać ideałów w $f(P)$. Istotnie, każdy ideał w $f(P)$ jest postaci $f(I)$ dla pewnego ideału $I \subset P$ zawierającego $\mathrm{Ker}(f)$ (por. 4.3.2). Wobec tego, jeśli $I = (a_1, \ldots, a_n)$, to $f(I) = (f(a_1), \ldots, f(a_n)))$, czyli każdy ideał w $f(P)$ jest skończenie generowany.

(2) wynika z (1) zastosowanej do $f := \pi$, gdzie π jest rzutowaniem kanonicznym. □

Twierdzenie 10.2.7 (Hilberta o bazie)**.** *Jeśli P jest pierścieniem noetherowskim, to jest nim też pierścień wielomianów $P[X]$.*

Dowód. Przypuśćmy, że mamy w $P[X]$ ideał I, który nie jest skończenie generowany.

Utworzymy rekurencyjnie ciąg wielomianów, wybierając f_1 – wielomian z I najniższego stopnia spośród wielomianów z $I \setminus \{0\}$ i dalej po wyborze $f_1, \ldots, f_k$ wybieramy f_{k+1} – wielomian najniższego stopnia spośród wielomianów ze zbioru $I \setminus (f_1, \ldots, f_k)$.

Niech $n_k := \deg f_k$, a_k – współczynnik wiodący f_k.

Z konstrukcji dostajemy, że $n_1 \leqslant n_2 \leqslant \ldots$ oraz zauważamy, że ciąg

$$(a_1) \subsetneq (a_1, a_2) \subsetneq \ldots \subsetneq \ldots,$$

nie stabilizuje się w P. Faktycznie, zawierania są istotne, gdyż gdyby dla pewnego k było $(a_1, \ldots, a_k) = (a_1, \ldots, a_{k+1})$, to $a_{k+1} = \sum_{i=1}^{k} b_i a_i$ dla pewnych $b_i \in P$. Ale wtedy $g := f_{k+1} - \sum_{i=1}^{k} b_i X^{n_{k+1}-n_i} f_i \in I \setminus (f_1, \ldots, f_k)$ i $\deg g < \deg f_{k+1}$, co prowadziłoby do sprzeczności z wyborem f_{k+1}. □

Przykład 10.2.8. Zauważmy, że dzięki poprzedniemu twierdzeniu wiemy, że $\mathbb{Z}[X]$ jest pierścieniem noetherowskim i w ten sposób otrzymujemy przykład takiego pierścienia, który nie jest pierścieniem ideałów głównych (np. ideał $(X, 3)$ nie jest ideałem generowanym przez jeden element).

Rozdział 11

Elementy teorii eliminacji

11.1 Różniczkowanie i krotność pierwiastka wielomianów

W podstawowej części wspominaliśmy o pierwiastku wielomianu oraz o związanym z tym pojęciem twierdzeniu Bezouta (por. rozdział 4.8.1). Mówiliśmy również o krotności pierwiastka (por. definicja 5.3.1). Teraz scharakteryzujemy krotność za pomocą pochodnej wielomianu. Musimy jednak najpierw taką pochodną wielomianu określić. Na gruncie algebry nie mamy pojęcia granicy wobec tego nie możemy wykorzystywać definicji pochodnej wielomianu, jaką znamy z analizy. Możemy jednak sformułować to pojęcie w taki sposób, aby było zgodne ze znanym nam różniczkowaniem.

Definicja 11.1.1 (pochodna wielomianu)**.** Niech P będzie pierścieniem całkowitym, $f = a_0 + a_1X + \ldots + a_nX^n \in P[X]$. **Pochodną wielomianu** f nazywamy wielomian:

$$f' := a_1 + 2a_2X + \ldots + na_nX^{n-1} \in P[X],$$

przy czym rozumiemy tę równość tak, że dla wielomianów stałych pochodna wielomianu jest wielomianem zerowym.

Uwaga 11.1.2. (1) Indukcyjnie możemy określić kolejne pochodne wielomianu f jako $f^{(k)} = (f^{(k-1)})'$.

(2) W przypadku znanych nam pierścieni $P = \mathbb{R}$ lub $P = \mathbb{C}$ powyższa pochodna wielomianu pokrywa się ze znanym nam pojęciem pochodnej z analizy.

Jako ćwiczenie pozostawimy sprawdzenie wzorów na pochodne wielomianów, które pokrywają się ze znanymi wzorami z analizy matematycznej. Pamiętajmy, że musimy to zrobić w oparciu o algebraiczną definicję pochodnej.

Własność 11.1.3. *Dla wielomianów f, g z pierścienia $P[X]$ oraz elementów $\alpha, \beta \in P$, zachodzą wzory:*

(1) $(\alpha f + \beta g)' = \alpha f' + \beta g'$,

(2) $(fg)' = f'g + fg'$.

Twierdzenie 11.1.4. *Niech R będzie pierścień całkowitym, P jego podpierścieniem, $c \in R$ i $f \in P[X]$. Wówczas c jest pierwiastkiem wielokrotnym f wtedy i tylko wtedy, gdy $f(c) = f'(c) = 0$.*

Dowód. Wykonajmy najpierw dzielenie f przez $(X-c)^2$ w pierścieniu $R[X]$ (możemy to zrobić bo współczynnik wiodący w $(X-c)^2$ jest odwracalny). Oznacza to, że istnieją takie elementy $q \in R[X]$, $r \in R[X]$, że

$$f = q \cdot (X-c)^2 + r$$

i $\deg r < 2$, czyli $r = \alpha X + \beta$ dla pewnych $\alpha, \beta \in R$.

Zapiszmy nieco inaczej f:

$$f = q \cdot (X-c)^2 + \alpha(X-c) + \alpha c + \beta$$

i policzmy teraz pochodną f:

$$f' = q' \cdot (X-c)^2 + 2q \cdot (X-c) + \alpha = (X-c)[q' \cdot (X-c) + 2q] + \alpha.$$

Podstawmy w obu równościach $X = c$. Wtedy dostaniemy: $f(c) = \alpha c + \beta$ (z pierwszej równości) i $f'(c) = \alpha$, czyli

$$f = q \cdot (X-c)^2 + f'(c)(X-c) + f(c).$$

Jeśli $f(c) = f'(c) = 0$, to $(X-c)^2 | f$, czyli c jest co najmniej dwukrotnym pierwiastkiem f.

Na odwrót, jeśli c jest co najmniej dwukrotnym pierwiastkiem f, to oczywiście $f(c) = 0$ i $(X-c)^2 | f$, ale także $(X-c)^2 | q \cdot (X-c)^2$ czyli $(X-c)^2 | f'(c)$, a ponieważ $f'(c)$ jest stałą, więc $f'(c) = 0$ (zauważmy, że wykorzystujemy w tym momencie całkowitość pierścienia, w którym pracujemy). □

11.2 Rugownik i jego własności

Niech K będzie dowolnym ciałem, $f,\ g \in K[X]$ – wielomiany jednej zmiennej postaci:

$$f = a_nX^n + \ldots + a_1X + a_0,\ g = b_mX^m + \ldots + b_1X + b_0, \qquad a_nb_m \neq 0. \tag{$\star$}$$

Definicja 11.2.1 (rugownik wielomianów)**.** W sytuacji ($\star$) **rugownikiem** wielomianów f i g nazywamy wyrażenie $R(f,g) := \det(S_{f,g})$, gdzie:

$$S_{f,g} = \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \ldots & a_0 & 0 & \ldots & 0 \\ 0 & a_n & a_{n-1} & \ldots & a_1 & a_0 & \ldots & 0 \\ \ldots & & & & & & & \\ 0 & 0 & \ldots & a_n & a_{n-1} & a_{n-2} & \ldots & a_0 \\ b_m & b_{m-1} & b_{m-2} & \ldots & b_0 & 0 & \ldots & 0 \\ 0 & b_m & b_{m-1} & \ldots & b_1 & b_0 & \ldots & 0 \\ \ldots & & & & & & & \\ 0 & 0 & \ldots & b_m & b_{m-1} & b_{m-2} & \ldots & b_0 \end{pmatrix},$$

gdzie współczynniki wielomianu f są wypisywane m razy, zaś wielomianu g n razy. Macierz $S_{f,g}$ nazywana jest **macierzą Sylvestera wielomianów** f, g. Jeżeli $\deg f = \deg g = 0$, to kładziemy $R(f,g) = 1$.

Przykład 11.2.2. Przyjrzyjmy się jak wygląda rugownik wielomianów w prostych sytuacjach.

(1) Jeśli $f = a_0$ oraz $g = b_mX^m + b_{m-1}X^{m-1} + \ldots + b_0$, gdzie $b_m \neq 0$, to

$$R(f,g) = a_0^m.$$

(2) Jeśli $f = a_1X + a_0, g = b_1X + b_0$, to

$$R(f,g) = a_1b_0 - a_0b_1.$$

(3) Analogicznie, jeśli $f = a_2X^2 + a_1X + a_0, g = b_1X + b_0$, to

$$R(f,g) = a_2b_0^2 - a_1b_1b_0 + a_0b_1^2.$$

Własność 11.2.3. *Przy oznaczeniach jak wyżej, zachodzi równość* $R(f,g) = (-1)^{nm}R(g,f)$.

Dowód. Korzystając z definicji rugownika oraz przenosząc $(m+1)$-szy wiersz macierzy $S_{f,g}$ na pierwszą pozycję mamy równość

$$R(f,g) = \det S_{f,g} = (-1)^m \det \begin{pmatrix} b_m & b_{m-1} & b_{m-2} & \ldots & 0 & 0 & 0 \\ a_n & a_{n-1} & a_{n-2} & \ldots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & a_1 & a_0 \\ 0 & b_m & b_{m-1} & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \ldots & 0 & b_1 & b_0 \end{pmatrix}.$$

Rozumując w sposób analogiczny, czyli przenosząc $m+i$-ty wiersz na miejsce wiersza i-tego otrzymujemy ciąg równości

$$R(f,g) = \det S_{f,g} = (-1)^{2m} \det \begin{pmatrix} b_m & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \dots & 0 & 0 & 0 \\ a_n & a_{n-1} & a_{n-2} & \dots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \dots & 0 & a_1 & a_0 \\ 0 & 0 & b_m & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & 0 & b_1 & b_0 \end{pmatrix}$$

$$= \dots = (-1)^{nm} \det \begin{pmatrix} b_m & b_{m-1} & b_{m-2} & \dots & 0 & 0 & 0 \\ 0 & b_m & b_{m-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & b_1 & b_0 & 0 \\ 0 & 0 & 0 & \dots & 0 & b_1 & b_0 \\ a_n & a_{n-1} & a_{n-2} & \dots & 0 & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & a_1 & a_0 & 0 \\ 0 & 0 & 0 & \dots & 0 & a_1 & a_0 \end{pmatrix}$$

$$= (-1)^{mn} \det S_{g,f} = (-1)^{mn} R(g,f),$$

i dostajemy tezę. □

Własność 11.2.4. *Przy oznaczeniach jak wyżej, niech* $f^*(X) = X^n f(1/X), g^*(X) = X^m g(1/X)$. *Wówczas* $R(f^*, g^*) = R(g,f) = (-1)^{mn} R(f,g)$.

Dowód. Wystarczy dowieść pierwszą równość. Zauważmy jednak, że macierz Sylvestera S_{f^*,g^*} powstaje z macierzy $S_{g,f}$ przez zamianę kolejności wszystkich wierszy i kolumn (poprzez cykliczną permutację). □

Własność 11.2.5. *Niech* K *będzie ciałem,* $f,\ g \in K[X]$, *gdzie* $\deg f = n$, $\deg g = m$. *Wtedy* $\mathrm{NWD}(f,g) \neq 1$ *wtedy i tylko wtedy, gdy istnieją takie niezerowe wielomiany* $\bar{f}$ *i* $\bar{g}$, *że:*

(1) $\deg(\bar{f}) < n, \quad \deg(\bar{g}) < m,$

(2) $f\bar{g} = \bar{f}g.$

Dowód. Najpierw załóżmy, że $h := \mathrm{NWD}(f,g)$ jest wielomianem dodatniego stopnia. Wówczas $f = h\bar{f}$, $g = h\bar{g}$ dla pewnych wielomianów $\bar{f}$, $\bar{g}$ i $f\bar{g} = h\bar{g}\bar{f} = g\bar{f}$, skąd teza.

Dla dowodu wynikania w drugą stronę, niech $\bar{f}$, $\bar{g}$ będą wielomianami spełniającymi odpowiednie założenia i niech $f = p_1 \dots p_s$, $\bar{g} = p_{s+1} \dots p_r$ będą ich rozkładami na czynniki nierozkładalne. Wówczas mamy:

$$f\bar{g} = (p_1 \dots p_s)(p_{s+1} \dots p_r) = \bar{f}g.$$

Ponieważ $\deg(\bar{f}) < \deg(f)$, to jeden z czynników p_i, gdzie $1 \leqslant i \leqslant s$, musi wystąpić w rozkładzie g na czynniki nierozkładalne. Oznacza to, że $p_i | f$ i $p_i | g$, skąd $\deg(\mathrm{NWD}(f,g)) > 1$. □

Mając powyższy techniczny lemat możemy łatwo wykazać ważną własność rugownika, dzięki której możemy wychwytywać istnienie istotnych wspólnych podzielników wielomianów.

Twierdzenie 11.2.6. *Niech* K *będzie ciałem,* $f,\ g \in K[X]$. *Wtedy wielomiany* f *i* g *mają wspólny dzielnik dodatniego stopnia wtedy i tylko wtedy, gdy* $R(f,g) = 0$.

Dowód. Będziemy chcieli skorzystać z poprzedniej własności. Wykażemy więc najpierw, że $R(f,g)=0$ wtedy i tylko wtedy, gdy istnieją odpowiednie dwa wielomiany z jej tezy.

Niech najpierw $\bar{f}$ i $\bar{g}$ będą wielomianami takimi, że $\bar{g}f=\bar{f}g$, gdzie

$$\begin{aligned}\bar{f}&=c_0+c_1X+\ldots+c_{n-1}X^{n-1},\\ \bar{g}&=d_0+d_1X+\ldots+d_{m-1}X^{m-1}.\end{aligned}$$

Z równości iloczynów wynika, że

$$\begin{aligned}(a_nX^n+\ldots+a_1X+a_0)&(d_{m-1}X^{m-1}+\ldots+d_1X+d_0)\\ &=(b_mX^m+\ldots+b_1X+b_0)(c_{n-1}X^{n-1}+\ldots+c_1X+c_0),\end{aligned}$$

co daje po porównaniu współczynników równania:

$$\begin{aligned}&a_0d_0=b_0c_0,\\ &a_1d_0+a_0d_1=b_1c_0+b_0c_1,\\ &a_2d_0+a_1d_1+a_0d_2=b_2c_0+b_1c_1+b_0c_2,\\ &\ldots\\ &a_nd_{m-1}=b_mc_{n-1}.\end{aligned}$$

Układ równań, który otrzymaliśmy traktujemy jako jednorodny układ równań liniowych z $n+m$ niewiadomymi $c_0,\ldots,c_{n-1},d_0,\ldots,d_{m-1}$. Układ ten ma niezerowe rozwiązania (bo wielomiany f i g są niezerowe), czyli wyznacznik tego układu musi być równy zero. Tym samym rugownik, jako wyznacznik macierzy transponowanej, też jest równy zero, co kończy dowód wynikania w jedną stronę.

Dla dowodu drugiej implikacji przyjmijmy $R(f,g)=0$. Wtedy układ równań, który przed chwilą rozważaliśmy posiada niezerowe rozwiązanie $(c_0,\ldots,c_0,\ldots,c_{n-1},d_0,\ldots,d_{m-1})$ i w ten sposób łatwo odzyskujemy wielomiany $\bar{f}$ i $\bar{g}$.

Poprzednia własność kończy dowód twierdzenia. □

Twierdzenie 11.2.7. *Niech K będzie ciałem, f, g wielomianami z $K[X]$ w postaci $(\star)$. Wtedy istnieją takie wielomiany F, $G\in K[X]$, że $\deg F<\deg f$, $\deg G<\deg g$ oraz $R(f,g)=Ff+Gg$.*

Dowód. Domnóżmy najpierw f kolejno przez $1,X,X^2,\ldots,X^{m-1}$, zaś wielomian g przez $1,X,X^2,\ldots,X^{n-1}$ i zapiszmy otrzymane równania:

$$\begin{aligned}f&=a_0+a_1X+\ldots+a_nX^n,\\ Xf&=a_0X+a_1X^2+\ldots+a_nX^{n+1},\\ &\ldots\\ X^{m-1}f&=a_0X^{m-1}+\ldots+a_nX^{m+n-1},\\ g&=b_0+b_1X+\ldots+b_mX^m,\\ Xg&=b_0X+b_1X^2+\ldots+b_mX^{m+1},\\ &\ldots\\ gX^{n-1}&=b_0X^{n-1}+\ldots+b_mX^{n+m-1}.\end{aligned}$$

Niech $D_1,\ldots,D_{m+n}$ będą dopełnieniami algebraicznymi elementów pierwszej kolumny rugownika $R(f,g)$.

Zauważmy, że mnożąc obie strony uzyskanego wyżej i-tego równania przez D_i i dodając równania stronami dostaniemy

$$\begin{aligned}&(D_1+D_2X+\ldots+D_mX^{m-1})f+(D_{m+1}+D_{m+2}X+\ldots+D_{n+m}X^{n-1})g\\ &\quad=(D_1a_0+D_{m+1}b_0)+(D_1a_1+D_2a_0+D_{m+1}b_1+D_{m+2}b_0)X+\ldots+(D_ma_n+D_{m+n}b_m)X^{m+n-1}\\ &\quad=R(f,g).\end{aligned}$$

Istotnie, wyraz wolny tego wielomianu to rugownik $R(f,g)$ rozwinięty względem pierwszej kolumny, podczas gdy współczynnik przy X^k jest rozwinięciem wyznacznika powstałego z rugownika przez zastąpienie pierwszej kolumny $(k+1)$-szą dla $k=1,2,\ldots,n+m-1$. Oznacza to, że współczynnik przy X^k jest równy zero, jako rozwnięcie wyznacznika o dwóch jednakowych kolumnach (pierwszej i $(k+1)$-szej). □

Niech $f,\ g \in K[X_1,\ldots,X_n]$. Roboczo, dla potrzeb omówienia jednego z zastosowań (por. 11.2.14), rugownik wielomianów $f,\ g \in K[X_1,\ldots,X_{s-1},X_s,X_{s+1},\ldots,X_n]$ względem zmiennej X_s, który dla ustalonego $s \in \{1,\ldots,n\}$ będziemy oznaczać przez $R_s(f,g)$. Jest to z definicji wielomian zmiennych $X_1,\ldots,X_{s-1},X_{s+1},\ldots,X_n$.

Twierdzenie 11.2.8. *Niech $F = A_k + A_{k-1}X_n + \ldots + A_0X_n^s$, $A_0 \neq 0$, $G = B_l + B_{l-1}X_n + \ldots + B_0X_n^l$, $B_0 \neq 0$, $A_i, B_j \in K[X_1,\ldots,X_{n-1}]$ – wielomiany jednorodne stopnia i, j odpowiednio.*

Wtedy wielomian $r(X_1,\ldots,X_{n-1}) := R_n(F,G)$ jest wielomianem jednorodnym stopnia kl względem zmiennych $X_1,\ldots,X_{n-1}$.

Dowód. Zauważmy, że

$$r(tX_1,\ldots,tX_{n-1}) = \begin{pmatrix} t^kA_k & t^{k-1}A_{k-1} & t^{k-2}A_{k-2} & \ldots & A_0 & 0 & \ldots & 0 \\ 0 & t^kA_k & t^{k-1}A_{k-1} & \ldots & tA_1 & A_0 & \ldots & 0 \\ \ldots & & & & & & & \\ 0 & 0 & \ldots & t^kA_k & t^{k-1}A_{k-1} & t^{k-2}A_{k-2} & \ldots & A_0 \\ t^lB_l & t^{l-1}B_{l-1} & t^{l-2}B_{l-2} & \ldots & B_0 & 0 & \ldots & 0 \\ 0 & t^lB_l & t^{l-1}B_{l-1} & \ldots & tB_1 & B_0 & \ldots & 0 \\ \ldots & & & & & & & \\ 0 & 0 & \ldots & t^lB_l & t^{l-1}B_{l-1} & t^{l-2}B_{l-2} & \ldots & B_0 \end{pmatrix}.$$

Jeśli pomnożymy i-ty wiersz z pierwszych l wierszy przez t^{l-i+1}, zaś j-ty z pozostałych k wierszy przez t^{k-j+1}, to dostaniemy

$$\begin{aligned} &t^pr(tX_1,\ldots,tX_{n-1}) \\ &\quad= \begin{pmatrix} t^{k+l}A_k & t^{k+l-1}A_{k+l-1} & t^{k+l-2}A_{k-2} & \ldots & t^lA_0 & \ldots & 0 \\ \ldots & & & & & & \\ 0 & 0 & \ldots & t^{k+1}A_n & t^kA_{k-1} & \ldots & tA_0 \\ t^{k+l}B_l & t^{k+l-1}B_{l-1} & t^{k+l-2}B_{l-2} & \ldots & t^kB_0 & \ldots & 0 \\ \ldots & & & & & & \\ 0 & 0 & \ldots & t^{l+1}B_l & t^lB_{l-1} & \ldots & tB_0 \end{pmatrix} \\ &\quad= t^{(k+l)+(k+l-1)+\ldots+1}r(X_1,\ldots,X_{n-1}) = t^qr(X_1,\ldots,X_{n-1}), \end{aligned}$$

gdzie

$$p = \frac{1}{2}(l(l+1)+k(k+1)), \quad q = \frac{1}{2}(l+k+1)(l+k).$$

Wobec tego, ponieważ $q-p = kl$, dostajemy, że

$$r(tX_1,\ldots,tX_{n-1}) = t^{kl}r(X_1,\ldots,X_{n-1}).$$ □

Omówimy teraz użyteczne twierdzenie, które jest punktem wyjścia do swoistego rodzaju metody redukcji, używanej do obliczania rugowników.

Twierdzenie 11.2.9. *Niech K będzie ciałem, $f,\ g \in K[X]$ wielomiany stopnia odpowiednio n, m, gdzie $m \leqslant n$. Niech $f = qg + r$, dla pewnych $q,\ r \in K[X]$, przy czym $\deg r < \deg g$. Wówczas $R(g,f) = b_m^{n-\deg r}R(g,r)$.*

Dowód. Z naszych założeń wynika, że $j = \deg q = n-m$. Zauważmy, że dla ustalonego $k \in \{1,\ldots,m\}$ odejmując od wiersza $(n+k)$-tego sumę $w_{(s)}c_j + w_{(k+1)}c_{j-1} + \ldots + w_{(k+j)}c_0$ wyzerujemy wszystkie elementy na miejscach $(n+i,i)$ dla $i = 1,2,\ldots,j$. Oznacza to, że od wierszy o numerach $n+1,n+2,\ldots,n+j$ macierzy $S_{g,f}$ odejmujemy odpowiednie kombinacje liniowe innych j wierszy otrzymując

$$\det S_{g,f} = \det S_{g,qg+r} = \det \begin{pmatrix} M_1 & M_2 \\ 0 & S_{g,r} \end{pmatrix},$$

gdzie, jak wynika z naszej dyskusji $M_1 \in M(n-m,n-m)$ jest macierzą trójkątną, której główną przekątną tworzą wyrazy b_m, zaś M_2 jest pewną macierzą. Stąd $R(g,f) = \det(S_{g,f}) = \det(M_1)\det(S_{g,r})$ i dostajemy tezę.

□

Twierdzenie 11.2.10. *Niech K ciało, $f = a_n(X-\alpha_1)\dots(X-\alpha_n) \in K[X]$, $g = b_m(X-\beta_1)\dots(X-\beta_m) \in K[X]$.*

Wtedy

$$R(f,g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j). \tag{11.1}$$

Równoważnie możemy napisać

$$R(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j).$$

Dowód. Na początek zauważmy, że jeśli nasza formuła (11.1) jest prawdziwa, to równość $R(f,g) = a_n^m \prod_{i=1}^{n} g(\alpha_i)$ jest oczywista. Druga równość również jest w tym przypadku jasna, gdyż

$$\begin{aligned} R(f,g) &= a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j) = b_m^n \prod_{j=1}^{m} a_n^m \prod_{i=1}^{n}(\alpha_i - \beta_j) \\ &= b_m^n \prod_{j=1}^{m} a_n^m \prod_{i=1}^{n}[-(\beta_j - \alpha_i)] = b_m^n \prod_{j=1}^{m}(-1)^n f(\beta_j) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(\beta_j). \end{aligned}$$

Wykażemy teraz, że równość (11.1) jest spełniona. Dowód przeprowadzimy indukcjnie względem $\deg f + \deg g = n+m$. Teza oczywiście zachodzi, gdy $n = m = 0$. Wówczas $R(f,g) = 1$. Załóżmy, że teza zachodzi dla wszystkich wielomianów f, g, które spełniają warunek $\deg f + \deg g < n + m$. Bez straty dla ogólności możemy założyć, że $n \leqslant m$. Dzieląc g z resztą przez wielomian f, możemy napisać $g = qf + r$, gdzie $\deg r < \deg f = n$. Korzystając teraz z Twierdzenia 11.2.9 otrzymujemy, że

$$R(f,g) = a_n^{m-\deg r} R(f, g-qf) = a_n^{m-\deg r} R(f,r).$$

Jeśli $r \neq 0$, to $n + \deg r < n + m$ i stosując założenie indukcyjne otrzymujemy równość

$$R(f,r) = a_n^{m-\deg r} a_n^{\deg r} \prod_{i=1}^{n} r(\alpha_i) = a_n^m \prod_{i=1}^{n} g(\alpha_i),$$

bo $g(\alpha_i) = q(\alpha_i)f(\alpha_i) + r(\alpha_i) = r(\alpha_i)$ dla $i = 1, \dots, n$.

Jeśli $r = 0$, to oznacza, że wielomian f dzieli wielomian g czyli $R(f,g) = 0$. Z drugiej strony, jeśli $f|g$, to istnieją i, j, że $\alpha_i = \beta_j$, więc każdy z iloczynów się zeruje.

□

Wniosek 11.2.11. *Niech K będzie ciałem, $f, g_1, g_2 \in K[X]$. Wówczas $R(f, g_1 g_2) = R(f,g_1)R(f,g_2)$.*

Dowód. Korzystając z formuły (11.1) otrzymujemy

$$\begin{aligned} R(f, g_1 g_2) &= a_n^{\deg g_1 + \deg g_2} \prod_{i=1}^{n} g_1(\alpha_i) g_2(\alpha_i) \\ &= a_n^{\deg g_1} \prod_{i=1}^{n} g_1(\alpha_i) \cdot a_n^{\deg g_2} \prod_{i=1}^{n} g_2(\alpha_i) = R(f,g_1)R(f,g_2) \end{aligned}$$

i stąd teza. □

Omówimy teraz kilka zastosowań rugownika. Zaczniemy od wyznaczenia rugownika $R(f,g)$ dla dowolnych dwumianów $f, g \in K[X]$.

Wniosek 11.2.12. *Niech K będzie ciałem, $r, s \in \mathbb{N}, a, b \in K$ i rozważmy $f(X) = X^r - a, g(X) = X^s - b$. Wówczas $R(f,g) = (-1)^s (a^{s_1} - b^{r_1})^d$, gdzie $d = \mathrm{NWD}(r,s), r_1 = r/s, s_1 = s/d$.*

Dowód. Dowód przeprowadzimy indukcyjnie względem $r + s$. Ponieważ $R(f,g) = (-1)^{rs} R(g,f)$ i $rs + d + r \equiv s \pmod 2$, więc bez straty dla ogólności możemy założyć, że $s \leqslant r$. Jeśli $s = 0$, to nie ma czego dowodzić i teza

zachodzi. Mamy zatem, że $r \geqslant s > 0$. Wykonując dzielenie z resztą wielomianu f przez wielomian g otrzymujemy równość $f(X) = X^{r-s}g(X) + bX^{r-s} - a$. Stąd

$$\begin{aligned} R(f(X), g(X)) &= R(bX^{r-s} - a, X^s - b) \\ &= R(b, X^s - b)R(X^{r-s} - a/b, X^s - b) = b^s R\left(X^{r-s} - \frac{a}{b}, X^s - b\right). \end{aligned}$$

Stosując teraz założenie indukcyjne dostajemy, że

$$R\left(X^{r-s} - a/b, X^s - b\right) = (-1)^s \left(\left(\frac{a}{b}\right)^{s_1} - b^{r_1 - s_1}\right)^d$$

i w konsekwencji, po koniecznych uproszczeniach, otrzymujemy

$$R(X^r - a, X^s - b) = (-1)^s (a^{s_1} - b^{r_1})^d. \qquad \square$$

Następny wniosek będzie użytecznym narzędziem w dowodzie górnego ograniczenia na liczbę wspólnych rozwiązań dwóch równań wielomianowych od dwóch zmiennych.

Wniosek 11.2.13. *Jeśli K jest ciałem, $f, g \in K[X, Y]$ – wielomiany stopni odpowiednio k, l, to* $\deg R_Y(f, g) \leqslant kl$.

Dowód. Rozważmy ujednorodnienia $\bar{f}$, $\bar{g} \in K[X, Y, Z]$ wielomianów f i g za pomocą zmiennej Z (tzn. domnażamy każdy składnik jednorodny przez potęgę Z tak, aby wielomiany były jednorodne).

Otrzymujemy w ten sposób:

$$\begin{aligned} \bar{f}(X, Y, Z) &= f_0(X, Z)Y^k + \ldots + f_k(X, Z) \\ \bar{g}(X, Y, Z) &= g_0(X, Z)Y^l + \ldots + g_l(X, Z) \end{aligned}$$

gdzie f_i, g_j są jednorodne stopni $k - i$ i $l - j$ lub zerami.

Rugownik $R_Y(\bar{f}, \bar{g})$ zgodnie z poprzednim Twierdzeniem 11.2.8 jest wielomianem stopnia co najwyżej kl. Podstawiając $Z = 1$ otrzymujemy z powrotem wielomiany f i g, a tym samym ich rugownik, co dowodzi tezy. $\square$

Twierdzenie 11.2.14 (Bezout)**.** *Niech K będzie ciałem, f, $g \in K[X, Y]$ stopni odpowiednio m, n nie posiadające wspólnego dzielnika stopnia dodatniego. Wtedy $\#V(f, g) \leqslant mn$, gdzie $V(f, g) = \{(x, y) \in K \times K : \ f(x, y) = g(x, y) = 0\}$.*

Dowód. Dla dowodu nie wprost załóżmy, że w zbiorze $V(f, g)$ jest co najmniej $mn + 1$ elementów. Oznaczmy te rozwiązania przez $(a_j, b_j) \in K \times K$. Dobierzmy element $c \in K$ tak, aby:

$$a_j + cb_j \neq a_i + cb_i, \quad \text{dla} \ \ 1 \leqslant j < i \leqslant mn + 1.$$

i zmieńmy układ współrzędnych na $K \times K$:

$$x = \bar{x} - c\bar{y}, \quad y = \bar{y}.$$

W ten sposób zmieniamy osie tak, aby na każdej osi równoległej do y leżał co najwyżej jeden punkt zbioru $V(f, g)$.

Rozważmy teraz wielomiany:

$$\bar{f}(\bar{X}, \bar{Y}) := f_0(\bar{X} - c\bar{Y})(\bar{Y})^m + f_1(\bar{X} - c\bar{Y})(\bar{Y})^{m-1} + \ldots + f_m(\bar{X} - c\bar{Y})$$

$$\bar{g}(\bar{X}, \bar{Y}) := g_0(\bar{X} - c\bar{Y})(\bar{Y})^n + g_1(\bar{X} - c\bar{Y})(\bar{Y})^{n-1} + \ldots + g_n(\bar{X} - c\bar{Y}).$$

Bezpośrednie przeliczenie pokazuje, że pary liczb $(\overline{a_j}, \overline{b_j}) = (a_j + cb_j, b_j)$ spełniają $\bar{f}(\overline{a_j}, \overline{b_j}) = 0$ i $\bar{g}(\overline{a_j}, \overline{b_j}) = 0$, czyli $\overline{a_1}, \ldots, \overline{a_{mn+1}}$ są pierwiastkami rugownika $R_Y(\bar{f}, \bar{g})$ tych dwóch wielomianów jako wielomianów zmiennej X. Ponieważ rugownik ten jest stopnia co najwyżej mn i ma $mn+1$ pierwiastków musi być wielomianem zerowym. Wobec tego wielomiany f i g mają wspólny dzielnik $h(X + cY, Y)$ stopnia dodatniego wbrew założeniom twierdzenia. $\square$

Czytelnika zainteresowanego pogłębieniem swojej wiedzy dotyczącej teorii rugownika i jego zastosowań odsyłamy do książki [1].

11.3 Wyróżnik wielomianu i jego własności

Niech K będzie dowolnym ciałem, zaś $f \in K[X]$ wielomian jednej zmiennej postaci

$$f = a_n X^n + \ldots + a_1 X + a_0. \qquad (\star)$$

Definicja 11.3.1 (wyróżnik wielomianu)**. Wyróżnikiem** wielomianu f nazywamy wyrażenie $D(f) = \frac{(-1)^{n(n-1)/2}}{a_n} R(f, f')$, gdzie $f' = \sum_{i=0}^{n} i a_i X^{i-1}$ jest pochodną wielomianu f (por. definicja 11.1.1).

Jest jasne, że $D(f) = 0$ wtedy i tylko wtedy, gdy wielomiany f, f' mają wspólny dzielnik. Równoważnie $D(f) = 0$ wtedy i tylko wtedy, gdy f ma pierwiastek wielokrotny.

Lemat 11.3.2. *Dla $f \in K[X]$ postaci $(\star)$ zachodzi równość*

$$D(f) = a_n^{2(n-1)} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Dowód. Z określenia rugownika wielomianów f, f' wiemy, że zachodzi równość $R(f, f') = a_n^{n-1} \prod_{i=1}^{n} f'(\alpha_i)$, gdzie α_i jest i-tym pierwiastkiem wielomianu f (pierwiastki liczymy z krotnościami). Łatwo widać, że skoro $f = a_n \prod_{j=1}^{n} (X - \alpha_j)$, to $f'(\alpha_i) = a_n \prod_{j \neq i} (\alpha_i - \alpha_j)$. Stąd

$$R(f, f') = a_n^{2n-1} \prod_{j \neq i} (x_j - x_i) = (-1)^{\frac{n(n-1)}{2}} a_n^{2n-1} \prod_{i<j} (x_j - x_i)^2.$$

Korzystając teraz ze związku między wyróżnikiem $D(f)$ i rugownikiem $R(f, f')$ otrzymujemy tezę. □

Lemat 11.3.3. *Niech $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{m} b_i X^i \in K[x]$. Wówczas*

$$D(fg) = D(f) D(g) R^2(f, g).$$

Dowód. Niech $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m$ będą pierwiastkami wielomianów f, g, odpowiednio. Z określenia wyróżnika otrzymujemy ciąg równości

$$\begin{aligned} D(fg) &= (a_n b_m)^{2(n+m-1)} \prod_{i_1<i_2} (\alpha_{i_1} - \alpha_{i_2})^2 \prod_{j_1<j_2} (\beta_{j_1} - \beta_{j_2})^2 \prod_{k_1<k_2} (\alpha_{k_1} - \beta_{k_2})^2 \\ &= \left(a_n^{2(n-1)} \prod_{i_1<i_2} (\alpha_{i_1} - \alpha_{i_2})^2 \right) \left(b_m^{2(m-1)} \prod_{j_1<j_2} (\beta_{j_1} - \beta_{j_2})^2 \right) \left(a_n^{2m} b_m^{2n} \right) \prod_{k_1<k_2} (\alpha_{k_1} - \beta_{k_2})^2 \\ &= D(f) D(g) R(f, g)^2. \end{aligned}$$

□

Przykład 11.3.4. Niech $f = X^n + a \in K[X]$. Wykażemy, że $D(f) = (-1)^{\frac{n(n-1)}{2}} a^{n-1} n^n$. Istotnie, korzystając ze związku miedzy wyróżnikiem i rugownikiem mamy

$$D(f) = (-1)^{\frac{n(n-1)}{2}} R(f, f') = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} n \alpha_i^{n-1}.$$

Ponieważ $\prod_{i=1}^{n} \alpha_i = (-1)^n a$, więc $\prod_{i=1}^{n} n \alpha_i^{n-1} = n^n a^{n-1}$ i dostajemy tezę.

Można również udowodnić następujące

Twierdzenie 11.3.5 (Swan [14])**.** *Niech $f = X^n + aX^m + b \in K[X]$, gdzie $0 < m < n$, $d = \mathrm{NWD}(n, m), n_1 = n/d, m_1 = m/d$. Wówczas*

$$D(f) = (-1)^{\frac{n(n-1)}{2}} b^{m-1} (n^{n_1} b^{n_1 - m_1} + (-1)^{n_1+1} (n-m)^{n_1 - m_1} m^{m_1} a^{n_1})^d.$$

Choć pozornie może się wydawać, że wyznaczanie jawnej postaci wyróżników jest łatwe, nie jest znana wyraźna postać wyróżnika ogólnego czwórmianu $f = X^n + aX^m + bX^k + c$, gdzie $0 < k < m < n$ oraz $a, b, c \in K$.

Rozdział 12

Wybrane zagadnienia teorii ciał

12.1 Jednoznaczność ciała rozkładu wielomianu

W tym rozdziale powrócimy do pojęcia ciała rozkładu wielomianu (por. definicja 5.3.5). Jak wiemy na podstawie twierdzenia 5.3.7, każdy wielomian posiada ciało rozkładu nad swoim ciałem współczynników. Wykażemy teraz kilka pomocniczych własności, które wykorzystamy w dalszych zastosowaniach, ale w szczególności udowodnimy też jednoznaczność ciała rozkładu. Zaczniemy od przygotowań.

Niech $\sigma : K \longrightarrow L$ będzie homomorfizmem ciał. Homomorfizm ten w naturalny sposób indukuje homomorfizm pierścieni wielomianów $\sigma_\star : K[X] \longrightarrow L[X]$ określony wzorem:

$$\sigma_\star(a_0 + a_1X + \ldots + a_nX^n) := \sigma(a_0) + \sigma(a_1)X + \ldots + \sigma(a_n)X^n,$$

co inaczej zapisać możemy jako $\sigma_\star f = \sigma \circ f$ dla $f \in K[X]$.

Bezpośrednio z definicji łatwo zauważyć zestaw poniżej zebranych własności.

Uwaga 12.1.1. Niech $\sigma : K \longrightarrow L$, $\tau : L \longrightarrow M$ będą homomorfizmami ciał, f, $g \in K[X]$. Wtedy zachodzą własności:

(1) $(\tau \circ \sigma)_\star = \tau_\star \circ \sigma_\star$ oraz $(id_K)_\star = id_{K[X]}$, co w szczególności prowadzi do wniosku, że jeśli σ jest izomorfizmem $(\sigma \circ \sigma^{-1} = \mathrm{id}_K)$, to $\sigma_\star$ także jest izomorfizmem,

(2) jeśli σ jest izomorfizmem, to f dzieli g wtedy i tylko wtedy, gdy $\sigma_\star f$ dzieli $\sigma_\star g$,

(3) jeśli σ jest izomorfizmem, to wielomian f jest nierozkładalny wtedy i tylko wtedy, gdy wielomian $\sigma_\star f$ jest nierozkładalny.

Twierdzenie 12.1.2 (jednoznaczność ciała rozkładu)**.** *Niech $\sigma : K_1 \longrightarrow K_2$ będzie izomorfizmem ciał, $f \in K_1[X]$, L_1 ciałem rozkładu wielomianu f nad K_1, zaś L_2 ciałem rozkładu wielomianu $\sigma_\star f$ nad K_2. Wtedy istnieje taki izomorfizm ciał $\Sigma : L_1 \longrightarrow L_2$, że $\Sigma|_{K_1} = \sigma$.*

Dowód. Dowód przebiega indukcyjnie względem $n := [L_1 : K_1]$. Jeśli $n = 1$, to $L_1 = K_1$ i $L_2 = K_2$, więc wystarczy przyjąć $\Sigma := \sigma$. Załóżmy więc, że $n > 1$, co w szczególności oznacza, że istnieje taki element $u \in L_1 \setminus K_1$, że $f(u) = 0$. Niech $p_u \in K_1[X]$ będzie wielomianem minimalnym u nad K_1. Jako, że p_u jest unitarny i nierozkładalny w $K_1[X]$, to wielomian $\sigma_\star p_u$ też jest wielomianem unitarnym i nierozkładalnym w $K_2[X]$. Dodatkowo, ponieważ p_u dzieli f, to $\sigma_\star p_u$ dzieli $\sigma_\star f$. Z założenia wiemy, że $\sigma_\star f$ rozkłada się liniowo nad L_2, czyli także $\sigma_\star p_u$ rozkłada się liniowo nad L_2.

Wybierzmy $w \in L_2$ – dowolny pierwiastek wielomianu $\sigma_\star p_u$. Wtedy, dla g, $h \in K_1[X]$, mamy

$$g(u) = 0 \iff p_u | g \iff \sigma_\star p_u | (\sigma_\star g) \iff (\sigma_\star g)(w) = 0,$$

czyli możemy poprawnie określić homomorfizm ciał, który z powyższej własności jest też automatycznie izomorfizmem:

$$\bar{\sigma} : K_1(u) \ni \frac{g(u)}{h(u)} \mapsto \frac{(\sigma_\star g)(w)}{(\sigma_\star h)(w)} \in K_2(w)$$

Zauważmy, że z definicji wynika też, że $\bar{\sigma}|_{K_1} = \sigma$. Jednocześnie mamy $K_1 \subset K_1(u) \subset L_1$ i wiemy też, że $[L_1 : K_1(u)] < n$. Dodatkowo, L_1 to ciało rozkładu wielomianu f nad $K_1(u)$, zaś L_2 to ciało rozkładu $\sigma_\star f$ nad $K_2(w)$. Z założenia indukcyjnego mamy więc, że istnieje taki izomorfizm ciał $\Sigma : L_1 \longrightarrow L_2$, że $\Sigma|_{K_1(u)} = \bar{\sigma}$, w szczególności $\Sigma|_{K_1} = \bar{\sigma}|_{K_1} = \sigma$. □

Stosując powyższe twierdzenie dla sytuacji, gdy L_1, L_2 są ciałami rozkładu wielomianu f nad K, zaś σ jest identycznością na K otrzymujemy wniosek mówiący o wspomnianej jednoznaczności ciała rozkładu.

Wniosek 12.1.3. *Każde dwa ciała rozkładu wielomianu $f \in K[X]$ nad ciałem współczynników K są K-izomorficzne.*

Dla dalszych zastosowań sformułujemy jeszcze jedną przydatną własność, wynikającą z głównego twierdzenia.

Własność 12.1.4. *Niech L/K będzie rozszerzeniem ciał takim, że L jest ciałem rozkładu pewnego wielomianu nad K. Jeśli u, $w \in L$ oraz p_u, p_w są wielomianami minimalnymi nad K elementów u, w odpowiednio, to $p_u = p_w$ wtedy i tylko wtedy, gdy istnieje Σ – taki K-automorfizm ciała L, że $\Sigma(u) = w$.*

Dowód. Przyjmijmy $p := p_u = p_w$ i zauważmy, że dla dowolnego $f \in K[X]$ mamy $f(u) = 0$ wtedy i tylko wtedy, gdy p dzieli f, a to ma miejsce dokładnie wtedy, gdy $f(w) = 0$, zatem możemy poprawnie określić izomorfizm

$$\bar{\sigma} : K(u) \ni \frac{f(u)}{g(u)} \longrightarrow \frac{f(w)}{g(w)} \in K(w).$$

Oczywiście, zachodzi $\bar{\sigma}|_K = id_K$. Ponadto L jest ciałem rozkładu tego samego wielomianu nad K jak i nad $K(u)$ oraz nad $K(w)$. Z 12.1.2 otrzymujemy istnienie takiego izomorfizmu $\Sigma : L \longrightarrow L$, że $\Sigma|_{K(u)} = \bar{\sigma}|_K = id_K$ oraz $\Sigma(u) = \bar{\sigma}(u) = w$.

Odwrotnie, jeśli Σ jest K-automorfizmem L spełniającym warune $\Sigma(u) = w$, to $\Sigma_\star p_u = p_u$, gdyż Σ jest K-automorfizmem. Stąd

$$p_u(w) = (\Sigma_\star p_u)(\Sigma(u)) = \Sigma(p_u(u)) = \Sigma(0) = 0,$$

więc $p_u = p_w$, gdyż p_u jest unitarny i nierozkładalny. □

12.2 Wielomiany i rozszerzenia rozdzielcze

Wyróżnimy teraz szczególny typ wielomianów – w skrócie mówiąc (przy odpowiednich założeniach) będą to wielomiany o wyłącznie jednokrotnych pierwiastkach (por. definicja 5.3.1).

Definicja 12.2.1 (wielomian rozdzielczy)**.** Jeśli K jest ciałem, to wielomian $f \in K[X]$ nierozkładalny nad K nazywamy **rozdzielczym** nad K, gdy nie posiada on pierwiastków wielokrotnych w żadnym swoim ciele rozkładu (por. definicja 5.3.5) nad K. Dowolny wielomian dodatniego stopnia (niekoniecznie nierozkładalny) z $K[X]$ nazywamy **rozdzielczym** nad K, gdy każdy jego czynnik nierozkładalny w $K[X]$ jest wielomianem rozdzielczym.

Jak zbadać, czy dany wielomian nierozkładalny jest rozdzielczy? Jak wiemy (por. twierdzenie 11.1.4) krotność pierwiastków danego wielomianu można badać za pomocą odpowiedniej własności pochodnej tego wielomianu. Okazuje się, że „test pochodnej" bardzo dobrze funkcjonuje przy sprawdzaniu rozdzielczości. Zanim udowodnimy odpowiednią własność przyjrzymy się przykładowi, który jest jednym z najprostszych, klasycznych przykładów wielomianu, który rozdzielczy nie jest. Jak zobaczymy niedługo, nie warto takiego przykładu szukać nad najbardziej znanymi ciałami, czy to charakterystyki zero, czy to dodatniej charakterystyki ale skończonymi, gdyż nad nimi wszystkie wielomiany są rozdzielcze.

Przykład 12.2.2. Niech $K := \mathbb{Z}_p(t)$ będzie ciałem funkcji wymiernych o współczynnikach z ciała $\mathbb{Z}_p$, gdzie p – liczba pierwsza. Rozważmy wielomian $f := X^p - t \in K[X]$. Na podstawie kryterium Eisensteina (por. twierdzenie 4.9.6, gdzie jako element nierozkładalny bierzemy t) widzimy, że jest to wielomian nierozkładalny w $K[X]$. Jeśli teraz $\alpha \in L$ jest pierwiastkiem f w dowolnym L – ciele rozkładu f nad K, to $X^p - t = (X - \alpha)^p$, gdyż $\mathrm{char}(L) = p$. Oznacza to, że f nie jest rozdzielczy nad K. Jednocześnie zaś widzimy, że $f' = pX^{p-1} = 0$.

Przykład ten sugeruje, że brak rozdzielczości wiąże się z zerowaniem się pochodnej wielomianu. Istotnie tak jest o czym przekonuje kolejne twierdzenie.

Twierdzenie 12.2.3 (charakteryzacja rozdzielczości)**.** *Jeśli K jest ciałem, zaś $f \in K[X]$ wielomianem nierozkładalnym w $K[X]$, to f jest wielomianem rozdzielczym wtedy i tylko wtedy, gdy $f' \neq 0$.*

Dowód. Dowód przeprowadzimy rozważając kontrapozycję.

Jeśli wielomian f nie jest rozdzielczy, to zgodnie z definicją posiada pierwiastek wielokrotny w pewnym ciele rozkładu L, czyli w $L[X]$ wielomiany f i f' (zgodnie z twierdzeniem 11.1.4) mają wspólny dzielnik dodatniego stopnia,

co oznacza (por. twierdzenie 11.2.6), że $R(f, f') = 0$. Jednak, ponieważ f i f' to wielomiany o współczynnikach z K, to $R(f, f') \in K$, więc oznacza to, że f i f' mają wspólny czynnik dodatniego stopnia także w $K[X]$. Istnieje zatem $g \in K[X] \setminus K$ dzielący f i f'. W szczególności, $f = cg$ dla pewnej stałej $c \in K^\star$ (gdyż f jest nierozkładalny). Tym samym $f' = c^{-1}fh$ dla pewnego $h \in K[X]$. Jednak $\deg(f') < \deg(f)$, więc podzielność f' przez f jest możliwa tylko, gdy $f' = 0$.

Odwrotnie, gdy $f' = 0$, to każdy pierwiastek wielomianu f w dowolnym jego ciele rozkładu jest jednocześnie pierwiastkiem pochodnej, czyli jest to pierwiastek wielokrotny. Korzystając ponownie z 11.1.4 wiemy, że f nie jest rozdzielczy. □

Trzeba pamiętać o tym, że w powyższym twierdzeniu założyliśmy nierozkładalność wielomianu. Bez tego założenia proponowana własność nie zachodzi: pochodna wielomianu nierozdzielczego w ogólnej postaci nie musi być zerowa, co potwierdza przykład $f = X(X^p - t) \in \mathbb{Z}_p(t)$ – jak wiemy z 12.2.2 nie jest to wielomian rozdzielczy, a mimo to $f' = X^p - t \neq 0$.

Jeśli ciało ma charakterystykę zero, to pochodna wielomianu jest wielomianem zerowym tylko wtedy, gdy jest to wielomian stały. Prowadzi to do kolejnego wniosku.

Wniosek 12.2.4 (rozdzielczość nad charakterystyką zero)**.** *Jeśli K jest ciałem charakterystyki zero, to każdy niestały wielomian z $K[X]$ jest rozdzielczy nad K.*

Nie jest jednak tak, że nie znajdziemy ciał dodatniej charakterystyki, przy których także występują wyłącznie wielomiany rozdzielcze – takie ciała mają swoją szczególną nazwę.

Definicja 12.2.5 (ciało doskonałe)**.** Mówimy, że ciało K jest **doskonałe**, gdy każdy niestały wielomian z $K[X]$ jest rozdzielczy nad K.

Przykład 12.2.6. (1) Z 12.2.4 wynika, że każde ciało charakterystyki zero jest doskonałe.

(2) Każde ciało skończone jest doskonałe.

Dowód. (2) Jeśli K jest skończone, $f \in K[X]$ jest wielomianem nierozkładalnym w $K[X], \mathrm{char}(K) = p > 0$, to musi być $f' \neq 0$. Istotnie, gdyby $f' = 0$, to mielibyśmy $f \in K[X^p]$, zatem moglibyśmy zapisać $f = a_0 + a_1X^p + \ldots + a_nX^{np}$ dla pewnych $a_0, \ldots, a_n \in K$. Ponieważ K jest ciałem skończonym, to na podstawie faktu, że monomorfizm Frobeniusa jest wówczas automorfizmem (por. uwagi po 5.4.1), dla każdego $i = 0, \ldots, n$ istnieje takie $b_i \in K$, że $a_i = b_i^p$. Tym samym:

$$f = b_0^p + b_1^pX^p + \ldots + b_n^pX^{pn} = (b_0 + b_1X + \ldots + b_nX^n)^p,$$

wbrew nierozkładalności f. □

Z powyższego przykładu wynika więc, że przykładów ciał które nie są doskonałe poszukiwać należy wśród ciał nieskończonych o charakterystyce dodatniej.

Definicja 12.2.7 (rozszerzenie rozdzielcze)**.** Jeśli L/K jest rozszerzeniem ciał, to element $u \in L$ nazywamy **rozdzielczym** nad K, gdy jest on przestępny nad K lub gdy jest on algebraiczny nad K i jego wielomian minimalny jest rozdzielczy nad K. Rozszerzenie ciał L/K nazywamy **rozdzielczym**, gdy każdy element ciała L jest rozdzielczy nad K.[1]

Przykład 12.2.8. (1) Rozszerzenie $\mathbb{C}/\mathbb{R}$ jest rozdzielcze jako że mamy do czynienia z ciałami charakterystyki zero.

(2) Jeśli $K = \mathbb{Z}_p(t)$ oraz L jest ciałem rozkładu wielomianu $f = X^p - t \in K[X]$, to rozszerzenie L/K nie jest rozdzielcze.

Na zakończenie naszych rozważań o rozszerzeniach rozdzielczych wypowiemy bez dowodu twierdzenie, które charakteryzuje liczbę możliwych rozszerzeń izomorfizmu ciał współczynników do izomorfizmu ciał rozkładu wielomianów, gdy założymy dodatkowo rozdzielczość rozważanych wielomianów (por. twierdzenie 5.3.9).

Twierdzenie 12.2.9. *Jeśli $\sigma : K_1 \longrightarrow K_2$ jest izomorfizmem ciał, $f \in K_1[X]$ jest wielomianem rozdzielczym nad K_1, L_1 jest ciałem rozkładu tego wielomianu nad K_1, zaś L_2 ciałem rozkładu $\sigma_\star f$ nad K_2, to istnieje dokładnie $[L_1 : K_1]$ takich izomorfizmów ciał $\Sigma : L_1 \longrightarrow L_2$, że $\Sigma_{K_1} = \sigma$.*

[1] Czasem w definicji rozszerzenia rozdzielczego zakłada się jego algebraiczność, nie dopuszczając tym samym elementów przestępnych.

12.3 Twierdzenie o elemencie prymitywnym

W tej części udowodnimy twierdzenie, które pozwala znacznie uprościć postać skończonego rozszerzenia ciał (por. definicja 5.1.4). Okazuje się bowiem, że rozszerzenie takie w rozsądnych sytuacjach można zastąpić rozszerzeniem prostym (por. definicja 5.1.15). Będzie to wniosek z tzw. twierdzenie o elemencie prymitywnym. Zanim je udowodnimy przyjrzymy się dokładniej podgrupom skończonym grupy multiplikatywnej ciała, które, jak zobaczymy, mają szczególną strukturę.

Twierdzenie 12.3.1 (o grupie multiplikatywnej w ciele)**.** *Każda skończona podgrupa grupy multiplikatywnej ciała jest cykliczna.*

Dowód. Niech G będzie skończoną podgrupą grupy $(K^\star, \cdot)$, gdzie K jest ciałem. Jeśli $|G| = n$ oraz $d|n$ jest ustaloną liczbą naturalną, zaś H cykliczną podgrupą grupy G rzędu d, to dla każdego elementu $x \in H$ zachodzi $x^d = 1$. Ponieważ wielomian stopnia d o współczynnikach z ciała ma co najwyżej d pierwiastków (por. 5.3.2), więc nie może istnieć druga, inna cykliczna podgrupa G rzędu d. Innymi słowy, każdemu dzielnikowi naturalnemu d liczby n, odpowiada co najwyżej jedna podgrupa cykliczna G rzędu d.

Jeśli, dla podgrupy cyklicznej H grupy G oznaczymy przez $g(H)$ zbiór generatorów H, to oczywiście G jest mnogościową sumą zbiorów $g(H)$, gdzie sumujemy po wszystkich H podgrupach cyklicznych G. Jak wiadomo (por. wniosek 3.3.14), jeśli $|H| = d$, to $\#g(H) = \varphi(d)$, zatem na podstawie własności 1.5.5 mamy:

$$n = |G| = \sum_{H \text{ – podgrupa cykliczna } G} \#g(H) \leqslant \sum_{d|n} \varphi(d) = n.$$

Oznacza to, że dla każdego podzielnika d liczby n mamy dokładnie jedną podgrupę cykliczną zadanego rzędu. W szczególności istnieje podgrupa cykliczna w G rzędu n, skąd sama grupa G jest cykliczna. □

Z udowodnionej własności płynie bardzo ważny wniosek, który odnotujemy osobno.

Wniosek 12.3.2. *Grupa multiplikatywna ciała skończonego jest grupą cykliczną.*

Twierdzenie 12.3.3 (o elemencie prymitywnym)**.** *Każde skończone rozszerzenie rozdzielcze jest rozszerzeniem prostym.*

Dowód. Niech L/K będzie skończonym rozszerzeniem rozdzielczym (12.2.7). Jeśli samo ciało K jest skończone, to również L jest ciałem skończonym, jako skończenie wymiarowa przestrzeń wektorowa nad K. Wobec tego, z poprzedniego wniosku wynika, że grupa multiplikatywna $(L^\star, \cdot)$ jest generowana przez jeden element $u \in L$. Wówczas więc $L = K(u)$ i rozszerzenie jest oczywiście proste.

Niech więc K będzie ciałem nieskończonym. Działając indukcyjnie, zauważmy, że wystarczy gdy wykażemy tezę dla ciała L postaci $L = K(a, b)$ dla pewnych elementów a, $b \in L$ algebraicznych nad K (por. twierdzenie 5.2.8). Niech M będzie ciałem rozkładu wielomianu $p_a \cdot p_b$, gdzie p_a, p_b to wielomiany minimalne odpowiednio elementów a, b nad ciałem K. Wtedy oba wielomiany p_a, p_b rozkładają się liniowo nad M. Rozważmy $a_1 := a, a_2, \ldots, a_r$, $b_1 := b, b_2, \ldots, b_s$ – wszystkie pierwiastki odpowiednio wielomianu p_a i wielomianu p_b w ciele M. Dzięki rozdzielczości rozszerzenia L/K wiemy, że pierwiastki te są jednokrotne. Wybierzmy element $c \in K$ w taki sposób, aby $c \notin \left\{ \dfrac{a_i - a}{b - b_j} : \ i = 1, \ldots, r, j = 2, \ldots, s \right\}$ – wybór ten jest możliwy dzięki temu, że K jest ciałem nieskończonym. Niech teraz

$$f(X) := p_a(u - cX), \qquad \text{gdzie } \ u = a + bc.$$

Wprost z definicji mamy $K(u) \subset K(a, b)$ oraz $f(b) = 0$, co więcej $f(b_j) \neq 0$ o ile $j \neq 1$, gdyż $u - b_j c \neq a_i$, dla $i = 1, \ldots, r$. Stąd wniosek, że b jest jedynym wspólnym pierwiastkiem wielomianów p_b i f, czyli $X - b$ jest największym wspólnym dzielnikiem tych wielomianów w $K(u)[X]$, gdyż pierwiastki największego wspólnego dzielnika dwóch wielomianów są jednocześnie pierwiastkami obu tych wielomianów. Oznacza to, że $X - b \in K(u)[X]$, czyli $b \in K(u)$, a tym samym także $a = u - bc \in K(u)$, czyli $K(a, b) \subset K(u)$. □

Zauważmy, że w przypadku ciała nieskończonego w zasadzie dowód jaki przeprowadziliśmy powyżej opisuje algorytm wyboru elementu prymitywnego danego rozszerzenia, jeśli jest to rozszerzenie o dwa elementy.

Przykład 12.3.4. Rozważmy klasyczne rozszerzenie $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$. Wykorzystując algorytm z poprzedniego dowodu łatwo otrzymujemy, że $\mathbb{Q}(\sqrt{2}, \sqrt{2}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, którą to równość łatwo także sprawdzić bezpośrednio wykazując odpowiednie zawierania.

12.4 Grupa Galois

Dalsza część skryptu dotycząca badania grup Galois oraz rozwiązalności przez pierwiastniki opracowana została w oparciu o gorąco polecany podręcznik [13], do którego warto sięgnąć po więcej informacji.

Zauważmy, że łatwo sprawdzić, że jeśli L/K jest rozszerzeniem ciał, to zbiór $\{\sigma \in \mathrm{Aut}(L) : \ \sigma|_K = \mathrm{id}_K\}$ tworzy grupę z działaniem składania. Grupa ta będzie miała w tym rozdziale specjalne znaczenie.

Definicja 12.4.1 (grupa Galois rozszerzenia/wielomianu)**.** Dla rozszerzenia ciał L/K grupę

$$G(L/K) := \{\sigma \in \mathrm{Aut}(L) : \ \sigma|_K = \mathrm{id}_K\}$$

nazywamy **grupą Galois rozszerzenia** L/K, zaś jej elementy nazywamy **K-automorfizmami ciała** L. Jeśli $f \in K[X]$, zaś L jest ciałem rozkładu f nad K, to grupę $G(L/K)$ nazywamy **grupą Galois wielomianu** f nad ciałem K. Będziemy ją dalej oznaczać przez $G_K(f)$.

Zauważmy, że oczywiście $G(L/K)$ jest podgrupą grupy wszystkich automorfizmów ciała L. Przyjrzyjmy się klasycznemu, ważnemu przykładowi, w którym widać jasno jak wygląda grupa Galois.

Przykład 12.4.2. Zauważmy, że jeśli $L = \mathbb{C}$, zaś $K = \mathbb{R}$, to oczywiście każdy $\mathbb{R}$-automorfizm ciała $\mathbb{C}$ można wyznaczyć wyliczając wartość $\sigma(a+bi)$ gdzie $a, b \in \mathbb{R}$. Jednak, skoro jest to $\mathbb{R}$-automorfizm, to $\sigma(a+bi) = a+b\sigma(i)$. Jego postać jest więc jednoznacznie wyznaczona przez $\sigma(i)$. Zauważmy jednak dalej, że $i^2 = -1$, czyli $(\sigma(i))^2+1 = 0$ więc $\sigma(i)$ musi być pierwiastkiem zespolonym równania $X^2+1 = 0$, tym samym $\sigma(a+bi) = a+bi$ lub $\sigma(a+bi) = a-bi$. Mamy więc dwa $\mathbb{R}$-automorfizmy ciała $\mathbb{C}$, zaś $G(\mathbb{C}/\mathbb{R})$ jest grupą rzędu 2, czyli jest izomorficzna z $\mathbb{Z}_2$.

Ciało $\mathbb{C}$ jest ciałem rozkładu nad $\mathbb{R}$ wielomianu $f = X^2 + 1 \in \mathbb{R}[X]$, tym samym nasze rozumowanie pokazuje, że $G_{\mathbb{R}}(f) \cong \mathbb{Z}_2$.

Przyjrzyjmy się teraz nieco dokładniej grupie Galois wielomianu $f \in K[X]$. Zauważmy, że jeśli $\sigma \in G_K(f)$, to jest to homomorfizm, który jest identycznością na współczynnikach naszego wielomianu. Jeśli zatem $\alpha \in L$ jest pierwiastkiem f, to $0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha))$, co oznacza, że $\sigma(\alpha)$ jest także pierwiastkiem naszego wielomianu. Widzimy więc, że de facto σ permutuje pierwiastki wielomianu f.

Własność 12.4.3. *Jeśli K jest ciałem, zaś wielomian $f \in K[X]$ ma n różnych pierwiastków w L swoim ciele rozkładu nad K, to $G_K(f)$ jest podgrupą S_n. W szczególności $|G_K(f)|$ jest podzielnikiem $n!$.*

Dowód. Wiemy już z poprzedzających rozważań, że $\sigma \in G_K(f)$ permutuje pierwiastki tego wielomianu, więc możemy założyć, że jeśli $X = \{\alpha_1, \ldots, \alpha_n\}$ jest zbiorem wszystkich różnych pierwiastków f w ciele L, to $\sigma|_X$ można utożsamić z permutacją elementów $\{1, \ldots, n\}$, czyli przyjąć, że $\sigma|_X \in S_n$. Odwzorowanie

$$G(L/K) \ni \sigma \longrightarrow \sigma|_X \in S_n$$

jest więc monomorfizmem (pamiętajmy, że $L = K(\alpha_1, \ldots, \alpha_n)$), którego obraz jest podgrupą S_n izomorficzną z $G(L/K) = G_K(f)$. □

Jeśli mamy do czynienia z wielomianem nierozkładalnym i rozdzielczym, to rozważając fakt, że identyczność jako automorfizm z K na K posiada (dzięki twierdzeniu 12.2.9) $[L : K]$ rozszerzeń do automorfizmu L, otrzymujemy więcej informacji o liczbie elementów grupy Galois wielomianu f.

Twierdzenie 12.4.4. *Jeśli K jest ciałem, $f \in K[X]$ jest nierozkładalny i rozdzielczy nad K, zaś L jest jego ciałem rozkładu nad K, to $|G(L/K) = |G_K(f)| = [L : K]$.*

Zobaczmy, jak wykorzystując powyższe twierdzenie łatwo można wyznaczyć grupę Galois prostego wielomianu.

Przykład 12.4.5. Wyznaczmy grupę Galois wielomianu $f = X^3 - 2$ nad ciałem $\mathbb{Q}$. Zauważmy, że jest to wielomian nierozkładalny, więc jeśli rozważymy jego jedyny rzeczywisty pierwiastek $a = \sqrt[3]{2}$ to $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Jednocześnie, wszystkie pierwiastki naszego wielomianu możemy uzyskać wykorzystując ζ – dowolny pierwiastek pierwotny stopnia 3 z jedynki, (por. definicja 12.5.1) tym samym $L = \mathbb{Q}(a, \zeta)$ jest ciałem rozkładu naszego wielomianu nad $\mathbb{Q}$. Policzmy: $|G_{\mathbb{Q}}(f)| = |G(L/\mathbb{Q})| = [L : \mathbb{Q}] = [L : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 3[L : \mathbb{Q}(a)]$. Jednak L zawiera elementy, które nie są rzeczywiste, więc $[L : \mathbb{Q}(a)] > 1$. Jednocześnie wiemy, że $G(L/\mathbb{Q})$ jest podgrupą S_3, a jedyną podgrupą S_3 rzędu większego od 3 jest cała S_3. Tym samym $G_{\mathbb{Q}}(f) \cong S_3$.

Twierdzenie 12.4.6. *Niech $K \subset L \subset M$ będzie wieżą rozszerzeń ciał, f, $g \in K[X]$ zaś L, M to ciała rozkładu odpowiednio wielomianów f, g nad K. Wtedy $G(M/L) \triangleleft G(M/K)$ oraz $G(M/K)/G(M/L) \cong G(L/K)$.*

Dowód. Zauważmy najpierw, że jeśli $\sigma \in G(M/K)$, zaś $\alpha_1, \ldots, \alpha_n$ to wszystkie różne pierwiastki f, to $\sigma(L) = K(\sigma(\alpha_1), \ldots, \sigma(\alpha_n)) = K(\alpha_1, \ldots, \alpha_n) = L$, a to oznacza, że poprawnie określić możemy odwzorowanie:

$$\Phi : G(M/K) \ni \sigma \longrightarrow \sigma|_L \in G(L/K)$$

które jest oczywiście homomorfizmem ciał o jądrze $G(M/L)$. Oznacza to, że $G(M/L)$ jest normalną podgrupą $G(M/K)$, zaś z twierdzenia o izomorfizmie dla grup dostaniemy, że $G(M/K)/G(M/L) \cong \mathrm{Im}(\Phi)$, czyli pozostaje wykazać, że $\mathrm{Im}(\Phi) = G(L/K)$. Jednak z twierdzenia 12.2.9 wiemy, że dla dowolnego $\sigma \in G(L/K)$ istnieje takie $\Sigma \in G(M/K)$, że $\Sigma|_L = \sigma$, co kończy dowód. □

12.5 Pierwiastki z jedynki w ciałach

Definicja 12.5.1 (pierwiastki pierwotne z jedynki)**.** Jeśli K jest ciałem, zaś L jest ciałem rozkładu wielomianu $X^n - 1$ nad K, (gdzie $n \in \mathbb{N}$), to zbiór:

$$U_n(K) := \{u \in L : \ u^n = 1\}$$

tworzy podgrupę skończoną grupy multiplikatywnej $(L^\star, \cdot)$. Jak wiemy (por. twierdzenie 12.3.1) jest to grupa cykliczna. Każdy generator grupy $U_n(K)$ nazywamy **pierwiastkiem pierwotnym z jedynki stopnia** n.

Zauważmy, że nasza definicja jest kompatybilna z rozważaniami prowadzonymi po 3.3.14. Zauważmy dalej, że jeśli ζ jest pierwiastkiem pierwotnym z jedynki stopnia n, to wszystkie pierwiastki wielomianu $X^n - 1$ mają postać $1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$, a co za tym idzie pierwiastki wielomianu $X^n - c$ będą postaci $\alpha, \alpha\zeta, \alpha\zeta^2, \ldots, \alpha\zeta^{n-1}$, gdzie α jest dowolnie wybranym pierwiastkiem $X^n - c$.

Kolejne dwa twierdzenia mają charakter przygotowawczy do dowodu charakteryzacji rozwiązalności wielomianu w języku jego grupy Galois.

Twierdzenie 12.5.2. *Jeśli $L = K(\zeta)$, gdzie K ciało, zaś ζ jest pierwiastkiem pierwotnym z jedynki stopna n, to $G(L/K)$ jest podgrupą grupy $U(\mathbb{Z}_n)$. W szczególności, oznacza to, że jest to grupa abelowa.*

Dowód. Oczywiście każdy K-automorfizm L jest jednoznacznie wyznaczony przez wartość na ζ. Dodatkowo wiemy, że $\sigma(\zeta)$ jest pierwiastkiem wielomianu $X^n - 1$, co oznacza, że $\sigma(\zeta) = \zeta^{k_\sigma}$ dla pewnego $k_\sigma \in \{1, \ldots, n\}$ (jednoznacznie wyznaczonego). Wiemy też, że σ permutuje pierwiastki wielomianu $X^n - 1$, czyli skoro ζ był generatorem grupy pierwiastków, to $\sigma(\zeta)$ także musi być generatorem. Oznacza to, że $\mathrm{NWD}(n, k_\sigma) = 1$, więc $k_\sigma \in U(\mathbb{Z}_n)$. Możemy więc poprawnie określić odwzorowanie:

$$s : G(L/K) \ni \sigma \mapsto k_\sigma \in U(\mathbb{Z}_n).$$

Odwzorowanie to jest homomorfizmem: $\sigma(\tau(\zeta)) = \sigma(\zeta^{k_\tau}) = (\sigma(\zeta))^{k_\tau} = \zeta^{k_\sigma \cdot k_\tau}$, czyli $k_{\sigma\circ\tau} = k_\sigma \cdot k_\tau$. Dodatkowo, jeśli $k_\sigma = 1$, to $\sigma(\zeta) = \zeta$, więc $\sigma = \mathrm{id}_L$, czyli s jest monomorfizmem, co kończy dowód. □

Grupa multiplikatywna $U(\mathbb{Z}_n)$ jest oczywiście abelowa, jednak nie musi być cykliczna (np. $U(\mathbb{Z}_8)$ nie jest). Głębokie twierdzenie Kroneckera–Webera mówi, że każde skończone i abelowe (tzn. o abelowej grupie Galois) rozszerzenie ciała $\mathbb{Q}$ może zostać zanurzone w pewnym rozszerzeniu postaci $\mathbb{Q}(\zeta)$.

Twierdzenie 12.5.3. *Dla ustalonego $n \in \mathbb{N}$, niech K będzie ciałem charakterystyki różnej od n, zawierającym pewien n-ty pierwiastek pierwotny z jedynki, $f = X^n - a \in K[X]$. Wtedy dla dowolnego L ciała rozkładu f nad K istnieje monomorfizm $\varphi : G(L/K) \longrightarrow \mathbb{Z}_n$. W szczególności oznacza to, że grupa $G(L/K)$ jest cykliczna.*

Dodatkowo, monomorfizm φ jest izomorfizmem wtedy i tylko wtedy, gdy f jest nierozkładalny nad K.

Dowód. Niech ζ będzie pierwiastkiem pierwotnym z jednynki stopnia n należącym do K, zaś $\alpha \in L$ dowolnym pierwiastkiem f. Jeśli $\sigma \in G(L/K)$, to wobec faktu, że obrazem przez σ pierwiastka f jest pierwiastek f wiemy, że $\sigma(\alpha) = \alpha\zeta^{k_\sigma}$ dla pewnego $k_\sigma \in \{1, \ldots, n\}$. Tym samym σ jest jednoznacznie wyznaczone przez k_σ. Określmy więc odwzorowanie:

$$\varphi : G(L/K) \ni \sigma \longrightarrow k_\sigma \in \mathbb{Z}_n.$$

Zauważmy, że $\sigma \circ \tau(\alpha) = \sigma(\alpha\zeta^{k_\tau}) = \sigma(\alpha)(\sigma(\zeta))^{k_\tau} = \alpha\zeta^{k_\sigma + k_\tau}$, czyli $\varphi(\sigma \circ \tau) = \varphi(\sigma) + \varphi(\tau)$. Nasze odwzorowanie jest więc homomorfizmem i tym samym w oczywisty sposób monomorfizmem, co pozwala zakończyć dowód pierwszej części twierdzenia.

Zauważmy dalej, że odwzorowanie φ jest izomorfizmem wtedy i tylko wtedy, gdy dla każdego pierwiastka $\alpha\zeta^k$ wielomianu f istnieje taki $\sigma \in G(L/K)$, że $\sigma(\alpha) = \alpha\zeta^k$. Jednak, na podstawie własności 12.1.4, ma to miejsce dokładnie wtedy, gdy wszystkie pierwiastki wielomianu f mają ten sam wielomian minimalny, co oznacza nierozkładalność wielomianu f. □

Wniosek 12.5.4. *Niech K będzie ciałem charakterystyki różnej od $p \in \mathbb{P}$, zawierającym pewien p-ty pierwiastek pierwotny z jedynki, $f = X^p - a \in K[X]$ oraz niech L będzie ciałem rozkładu wielomianu f nad K. Wtedy zachodzą własności:*

(1) jeśli wielomian f jest liniowo rozkładalny nad K, to $G(L/K)$ jest grupą trywialną,

(2) jeśli wielomian f nie rozkłada się liniowo nad K, to $G(L/K) \cong \mathbb{Z}_p$, zaś wielomian f jest nierozkładalny.

Dowód. Rozważmy ponownie odwzorowanie $\varphi : G(L/K) \longrightarrow \mathbb{Z}_p$ określone w dowodzie poprzedniego twierdzenia. Jeśli f rozkłada się liniowo nad K, to $L = K$, więc $G(L/K)$ jest trywialna.

Jeśli f nie rozkłada się liniowo nad K, to $\mathrm{Im}(\varphi)$ jest nietrywialną podgrupą $\mathbb{Z}_p$, zatem wobec pierwszości p odwzorowanie φ musi być surjekcją, czyli $G(L/K) \cong \mathbb{Z}_p$ i f jest nierozkładalny na mocy poprzedniego twierdzenia. □

12.6 Rozwiązalność przez pierwiastniki

Wykażemy teraz jak wykorzystać grupę Galois wielomianu do zbadania istnienia wzoru na na pierwiastki tego wielomianu wyrażonego za pomocą jego współczynników i podstawowych operacji: dodawania, odejmowania, mnożenia, dzielenia i pierwiastkowania.

Definicja 12.6.1 (rozszerzenie pierwiastnikowe)**.** Rozszerzenie ciał L/K nazywamy **prostym pierwiastnikowym**, gdy jest ono postaci $L = K(\alpha)$, gdzie $\alpha^n \in K$ dla pewnego $n \in \mathbb{N}$.

Powiemy, że rozszerzenie L/K **jest rozszerzeniem pierwiastnikowym**, gdy istnieje taka wieża rozszerzeń ciał: $K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \ldots \subseteq L_r = L$, że każde z rozszerzeń L_i/L_{i-1} dla $i = 1, \ldots, r$ jest proste pierwiastnikowe.

Uwaga 12.6.2. Rozważając rozszerzenie pierwiastnikowe zawsze możemy zakładać, że rozszerzenia proste jakie pojawiają się w wieży są takimi rozszerzeniami, że n jest liczbą pierwszą. Istotnie, jeśli bowiem mamy rozszerzenie postaci $K \subseteq K(\alpha)$, gdzie $\alpha^n \in K$ i $n = pq$, to wystarczy rozbić wieżę dodatkowo na $K \subseteq K(\beta) \subseteq K(\beta)(\alpha)$ dla $\beta = \alpha^p$, gdyż wtedy $\beta^q = \alpha^n \in K$ i $\alpha^p = \beta \in K(\beta)$.

Definicja 12.6.3 (rozwiązalność wielomianu)**.** Jeśli K jest ciałem, to wielomian $f \in K[X]$ nazywamy **rozwiązalnym przez pierwiastniki** (lub po prostu **rozwiązalnym**) nad K, gdy istnieje rozszerzenie pierwiastnikowe L ciała K, które zawiera jako podciało ciało rozkładu wielomianu f nad K.

Przykład 12.6.4. Rozważmy dowolny wielomian kwadratowy $f = X^2 + bX + c \in \mathbb{Q}[X]$. Zauważmy, że $L = K(\sqrt{b^2 - 4c})$ jest rozszerzeniem pierwiastnikowym K, a że L jest ciałem rozkładu naszego wielomianu nad K, to f jest rozwiązalny nad K.

W dalszych rozważaniach zakładać będziemy, że ciała są charakterystyki zero, by móc dość dowolnie korzystać m.in. z twierdzenia 12.5.3.

Własność 12.6.5. *Niech K będzie ciałem charakterystyki zero, $f \in K[X]$ wielomianem rozwiązalnym przez pierwiastniki nad K, zaś L ciałem rozkładu f nad K. Wtedy*

(1) istnieje taka wieża pierwiastnikowa $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r$, że $L \subseteq L_r$, gdzie L_r jest ciałem rozkładu pewnego wielomianu nad K, zaś $L_i = L_{i-1}(\alpha_i)$ oraz $\alpha_i^{p_i} \in L_{i-1}$ dla pewnych $p_i \in \mathbb{P}$, $i = 1, \ldots, r$,

(2) jeśli L_r/K jest rozszerzeniem pierwiastnikowym z punktu (1) oraz K zawiera p_i-te pierwiastki pierwotne z jedynki dla $i = 1, \ldots, r$, to $G(L/K)$ jest grupą rozwiązalną.

Dowód. Zauważmy najpierw, że ponieważ f jest rozwiązalny przez pierwiastniki, to istnieje taka wieża pierwiastnikowa $K = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_s$, że $L \subseteq M_s$. Rozszerzenie M_s/K jest rozszerzeniem skończonym, więc istnieją elementy $u_1, \ldots, u_n \in M_s$ algebraiczne nad K takie, że $M_s = K(u_1, \ldots, u_n)$. Wystarczy więc przyjąć jako M ciało rozkładu wielomianu będącego iloczynem wielomianów minimalnych elementów $u_1, \ldots, u_n$, a następnie zagęścić otrzymaną wieżę tak, by rozszerzenia proste w niej występujące związane były z potęgami będącymi liczbami pierwszymi.

Dla dowodu drugiej części najpierw rozważmy $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r$ rozszerzenie dobrane w części pierwszej. Określmy dla $i = 0, \ldots, r$ grupy $G_i = G(L_r/L_i)$. Dla każdego p_i ciało K zawiera pewien pierwiastek pierwotny p_i-tego stopnia z jedynki, więc każde L_i jest ciałem rozkładu wielomianu $f_i = X^{p_i} - \alpha_i^{p_i} \in L_{i-1}[X]$ nad L_{i-1}. Wobec tego z twierdzenia 12.4.6 otrzymamy ciąg:

$$\{\mathrm{id}\} = G_r \lhd \cdots \lhd G_1 \lhd G_0 = G(L_r/K), \qquad G_{i-1}/G_i < \mathbb{Z}_{p_i},\ i = 1, \ldots, r.$$

Odpowiednie grupy ilorazowe są tutaj abelowe jako podgrupy $\mathbb{Z}_{p_i}$, co oznacza rozwiązalność grupy $G(L_r/K)$. Ponownie stosując 12.4.6 do wieży $K \subseteq L \subseteq L_r$ otrzymamy, że $G(L/K)$ jest grupą ilorazową grupy rozwiązalnej $G(L_r/K)$, czyli jest to grupa rozwiązalna. □

Okazuje się, że dzięki abelowości (a tym samym rozwiązalności) grupy $G(K(\zeta)/K)$, gdzie ζ jest pierwiastkiem pierwotnym z jedynki, możemy w poprzedniej własności wyeliminować wymóg zawierania przez ciało K pierwiastków pierwotnych z jedynki.

Twierdzenie 12.6.6. *Niech K będzie ciałem charakterystyki zero, $f \in K[X]$ wielomianem rozwiązalnym nad K, zaś L ciałem rozkładu f nad K. Wtedy grupa $G(L/K)$ jest rozwiązalna.*

Dowód. Na podstawie poprzedniej własności wiemy, że istnieje taka wieża pierwiastnikowa $K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r$, że $L \subseteq L_r$ oraz $L_i = L_{i-1}(\alpha_i)$, gdzie $\alpha_i^{p_i} \in L_{i-1}$ dla pewnych liczb pierwszych p_i. Dodatkowo, możemy założyć, że L_r jest ciałem rozkładu pewnego wielomianu $g \in K[X]$ nad K. Przyjmijmy teraz $m := \mathrm{NWW}(p_1, \ldots, p_r)$ i rozważmy rozszerzenie $L_r \subseteq M$, gdzie $M = L_r(\zeta)$ dla ζ pierwiastka pierwotnego z jedynki stopnia m. Wtedy M jest ciałem rozkładu nad K wielomianu $(X^m - 1)g$ i możemy rozważyć wieżę pierwiastnikową

$$K = L_0 \subseteq K(\zeta) = L_0(\zeta) \subseteq L_1(\zeta) \subseteq \ldots \subseteq L_r(\zeta) = M,$$

dodatkowo pamiętając, że $L \subseteq M$. Ciało $K(\zeta)$ jest ciałem rozkładu wielomianu $X^m - 1$ nad K i rozważać możemy też wieżę $K \subseteq K(\zeta) \subseteq M$. Z twierdzenia 12.4.6 dostajemy $G(M/K(\zeta)) \lhd G(M/K)$ i $G(M/K)/G(M/K(\zeta)) \cong G(K(\zeta)/K)$, czyli grupa ilorazowa jest abelowa, w szczególności rozwiązalna. Patrząc teraz na wieżę

$$K(\zeta) = L_0(\zeta) \subseteq L_1(\zeta) \subseteq \ldots \subseteq L_r(\zeta) = M$$

jesteśmy w sytuacji z własności 12.6.5 (p_i-te pierwiastki pierwotne należą do $K(\zeta)$), stąd rozwiązalność grupy $G(M/K(\zeta))$. Skoro grupa ilorazowa $G(M/K)/G(M/K(\zeta))$ jak i podgrupa $G(M/K(\zeta))$ są rozwiązalne, to wiemy, że rozwiązalna jest sama grupa $G(M/K)$ (por. twierdzenie 9.5.6) i dalej a $G(L/K)$, gdyż ponownie, z twierdzenia 12.4.6, mamy $G(L/K) \cong G(M/K)/G(M/L)$. □

Twierdzenie 12.6.7 (Abel, Ruffini)**.** *Istnieje wielomian $f \in \mathbb{Q}[X]$ stopnia 5, który nie jest rozwiązalny nad $\mathbb{Q}$.*

Dowód. Rozważmy wielomian

$$f = X^5 - 4X + 2 \in \mathbb{Q}[X]$$

nierozkładalny w $\mathbb{Q}[X]$, co można łatwo sprawdzić stosując na przykład kryterium Eisensteina (por. twierdzenie 4.9.6).

Niech L będzie ciałem rozkładu f nad $\mathbb{Q}$ i niech $G := G(L/\mathbb{Q})$ będzie grupą Galois tego wielomianu. Gdyby wielomian był rozwiązalny, to jego grupa zgodnie z poprzednim twierdzeniem musiałaby być rozwiązalna. Weźmy dowolny ustalony $\alpha \in L$ pierwiastek naszego wielomianu i rozważmy wieżę rozszerzeń $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq L$. Wobec nierozkładalności f nad $\mathbb{Q}$ wiemy, że $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, więc skoro

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 5[L : \mathbb{Q}(\alpha)],$$

to $|G| = [L : \mathbb{Q}]$ jest podzielny przez 5. Z prostych przeliczeń analitycznych widzimy, że f posiada dokładnie trzy pierwiastki rzeczywiste, jako że np. $f(-2) < 0$, $f(0) > 0$, $f(1) < 0$ i $f(2) > 0$, więc pierwiastków tych jest co najmniej trzy, ale więcej być nie może, gdyż $f' = 5X^4 - 4$ ma tylko dwa pierwiastki rzeczywiste. Nasz wielomian ma więc dwa istotnie zespolone, sprzężone ze sobą pierwiastki. Jednocześnie wiemy, że na grupę G możemy patrzeć jak na podgrupę grupy S_5 (por. własność 12.4.3).

Na podstawie twierdzenia Sylowa (por. 9.3.2) wiemy, że grupa G posiada element rzędu 5, co w S_5 oznacza, że do G należy pewien cykl długości 5. Jednocześnie do G należy też transpozycja odpowiadająca odwzorowaniu sprzężenia – takie odwzorowanie po zawężeniu do L to automorfizm, który polega na zamianie miejscami sprzężonych pierwiastków istotnie zespolonych i jest identycznością na pozostałych pierwiastkach rzeczywistych. W G znajdujemy więc transpozycję oraz cykl maksymalnej długości. Łatwo w ramach ćwiczenia wykazać, że jeśli podgrupa S_n zawiera cykl długości n oraz transpozycję, to jest to cała grupa S_n. Tym samym $G = S_5$, a jak wiemy grupa ta nie jest rozwiązalna (por. wniosek 9.5.7), co prowadzi do sprzeczności. □

Wartym odnotowania jest fakt, że w dowodzie powyższego twierdzenia nieistotna była postać samego wielomianu f, natomiast kluczowe było spostrzeżenie, że ów wielomian posiada dokładnie trzy pierwiastki rzeczywiste. Co ciekawe taką konstrukcję można uogólnić na dowolny stopień $\deg f \geqslant 5$ będący liczbą pierwszą. Należy również wspomnieć, że powyższe twierdzenie jest mocniejszą wersją wyniku Abela i Ruffiniego. Twierdzenie przypisywane tym dwóch autorom mówi, że dla wielomianów stopnia większego do 4 nie istnieją ogólne (dobre dla wszystkich wielomianów) wzory, na podstawie których można wyliczyć ich pierwiastki, dysponując współczynnikami. Twierdzenie wykazane wyżej pokazuje, że nawet dla konkretnego wielomianu wskazanie takich wzorów może okazać się niewykonalne.

12.7 Konstrukcje za pomocą cyrkla i linijki

Problemy geometryczne wielokrotnie motywowały badania prowadzone w algebrze. Wiele z nich zostało postawionych w starożytności, zaś trzy najbardziej znane można sformułować następująco:

1. trysekcja kąta,
2. podwojenie sześcianu,
3. kwadratura koła.

By doprecyzować cel, który nas interesuje, przypomnijmy, że pierwszy z problemów sformułowanych wyżej dotyczy podziału danego kąta na trzy równe części, drugi dotyczy konstrukcji sześcianu, którego objętość jest dwa razy większa od objętości danego sześcianu, zaś w trzecim interesuje nas konstrukcja kwadratu, którego pole jest równe polu danego koła. To co najważniejsze, to wyjaśnienie słowa „konstrukcja", którego użyliśmy w wyjaśnieniu sformułowania naszych problemów. Dokładniej, chodzi o to by w konstrukcji używać tylko cyrkla i linijki. Warto podkreślić, że przez linijkę rozumiemy tutaj listewkę, która służy do kreślenia linii prostych i zaznaczono na niej długość jednego odcinka. Przyjmujemy, że jest to tzw. długość jednostkowa. By przeformułować powyższe problemy na język algebry należy wyjaśnić, co to znaczy skonstruować dany punkt lub odcinek, używając cyrkla i linijki.

Dokładniej, powiemy, że dana długość lub punkt są konstruowalne za pomocą cyrkla i linijki, jeżeli dają się uzyskać w wyniku zastosowania (możliwe, że wielokrotnego) czterech operacji:

(1) wyznaczenie prostej przechodzącej przez dwa ustalone punkty;

(2) wyznaczenie punktu przecięcia dwóch prostych;

(3) wyznaczenie okręgu o danym środku i promieniu;

(4) wyznaczenie punktu przecięcia prostej i okręgu lub przecięca dwóch okręgów.

Z kursu geometrii szkolnej wiemy, że używając cyrkla i linijki, dla danej prostej potrafimy skonstruować prostą prostopadłą i prostą równoległą do danej prostej i przechodzącą przez ustalony punkt. Wynika z tego, że wychodząc od punktów $P_0 = (0,0), P_1 = (0,1)$ oraz osi układu współrzędnych OX (czyli prostej zadanej równiem $x = 0$) i OY (czyli prostej zadanej równaniem $y = 0$), a następnie stosując do nich operację brania prostej prostopadłej i równoległej, jesteśmy w stanie skonstruować każdy punkt o współrzędnych całkowitych. Rozważając pozostałe operacje i stosując je do punktów o współrzędnych całkowitych, otrzymamy nowe punkty. Zbiór liczb (odległości), które otrzymamy nazywamy zbiorem długości konstruowalnych. Powiemy następnie, że dany punkt $(x, y) \in \mathbb{R}^2$ (lub równoważnie liczba zespolona $z = x + iy$) jest konstruowalny, jeżeli jego współrzędne są liczbami konstruowalnymi.

W dalszej części naszych rozważań nie będziemy rozróżniać pojęcia liczby konstruowalnej i punktu konstruowalnego. By przekonać się, że te pojęcia są istotnie równoważne zauważmy, że jeśli $P = (x, y)$ jest punktem konstruowalnym, to rozważając prostą L prostopadłą do osi OX przechodzącą przez punkt P, widzimy, że $L \cap OY = \{(x, 0)\}$. Oznacza to, że długość $|x|$ jest konstruowalna. W analogiczny sposób dostajemy, że długość $|y|$ jest konstruowalna. Z drugiej strony, jeśli potrafimy skonstruować długości x, y, to potrafimy skonstruować punkty $P = (x, 0)$ oraz $Q = (0, y)$. Niech teraz L_x będzie prostą przechodzącą przez punkt P i prostopadłą do osi OX, zaś L_y prostą przechodzącą przez punkt Q i prostopadłą do osi OY. Wówczas $L_x \cap L_y = \{(x, y)\}$, co oznacza, że punkt P jest konstruowalny. Z naszych rozważań wynika, że jesteśmy też w stanie konstruować liczby zespolone, które interpretujemy jako punkty na płaszczyźnie. Zauważmy jeszcze, że jeśli $P = (x, y)$ jest konstruowalny, to dla każdego układu znaków, punkt $(\pm x, \pm y)$ również jest konstruowalny. Przykładowo, jeśli rozważymy prostą L prostopadłą do osi OY i przechodzącą przez punkt P, to $Q = L \cap OY$ i oczywiście $Q = \{(0, y)\}$. Rozważając teraz okrąg S o środku

w punkcie Q i przechodzący przez punkt P widzimy, że $S \cap L = \{P, P'\}$, gdzie $P' = (-x, y)$, co oznacza, że punkt P' jest konstruowalny.

Jeżeli mamy skonstruowane dwie długości, powiedzmy $a, b > 0$, to potrafimy skonstruować odcinek o długości ab. Istotnie, do tego wystarczy umiejętność skonstruowania prostych równoległych. Dokładniej, rozważmy dowolny (niezerowy) kąt ostry $\measuredangle AOB$, którego długości ramion wynoszą $|AO| = 1, |BO| = b$. Następnie, na półprostej OA konstruujemy odcinek OC, którego długość wynosi $|OC| = a$. Wyznaczamy teraz prostą, powiedzmy l_{AB}, przechodzącą przez punkty A i B, a następnie wyznaczamy prostą l przechodzącą przez punkt C i równoległą do prostej l_{AB}. Zauważmy, że prosta l przecina w punkcie D półprostą zawierajacą punkty OB. Z naszej konstrukcji wynika, że trójkąty AOB oraz COD są podobne. Oznacza to, że

$$\frac{|BO|}{|AO|} = \frac{|DO|}{|CO|} \quad \Longleftrightarrow \quad \frac{b}{1} = \frac{|DO|}{a} \quad \Longleftrightarrow \quad |DO| = ab,$$

i tym samy skonstruowaliśmy odcinek o długości ab.

W analogiczny sposób, korzystając z prawa podobieństwa trójkątów, możemy skonstruować odcinek o długości a/b. Istotnie, rozważmy dowolny (niezerowy) kąt ostry $\measuredangle AOB$, którego długości ramion wynoszą $|AO| = 1, |BO| = a$. Następnie, na półprostej OA konstruujemy odcienek OC, którego długość wynosi $|OC| = b$. Wyznaczamy teraz prostą, powiedzmy l_{BC}, przechodzącą przez punkty B i C, a następnie wyznaczamy prostą l przechodzącą przez punkt A i równoległą do prostej l_{BC}. Zauważmy, że prosta l przecina w punkcie D półprostą zawierajacą punkty OB. Z naszej konstrukcji wynika, że trójkąty AOD oraz BOC są podobne. Oznacza to, że

$$\frac{|DO|}{|AO|} = \frac{|BO|}{|CO|} \quad \Longleftrightarrow \quad \frac{|DO|}{1} = \frac{a}{b} \quad \Longleftrightarrow \quad |DO| = \frac{a}{b},$$

i tym samym skonstruowaliśmy odcinek o długości a/b.

Oznaczmy teraz przez $K \subset \mathbb{C}$ zbiór liczb konstruowalnych. Z naszych dotychczasowych rozważań wynika, że $\mathbb{Q} \subset K$. W szczególności zbiór punktów konstruowalnych zawiera wszystkie punkty, których współrzędne są wymierne. Co więcej, zbiór K jest zamknięty ze względu na działanie dodawania oraz mnożenia. Do tego $0 \in K$ oraz każdy element $x \in K$ posiada element przeciwny. Ponadto, dla dowolnego $x \in K \setminus \{0\}$ istnieje element odwrotny $1/x$ względem mnożenia. Oznacza to, że K jest ciałem. Pojawia się naturalne pytanie: czy można opisać to ciało w terminach algebraicznych?

Zanim to zrobimy zauważmy, że K jest istotnie większe niż $\mathbb{Q}$, gdyż dla danego $a \in \mathbb{Q}, a > 0$ potrafimy skonstruować $\sqrt{a}$. Istotnie, rozważmy odcinek AB długości $a + 1$ oraz dwa punkty O oraz C leżące na tym odcinku. Punkt O jest środkiem odcinka AB, zaś punkt C spełnia układ równań: $|AC| = a, |BC| = 1$. Rozważmy teraz okrąg S o środku w punkcie O przechodzący przez punkt A. Wówczas AB jest średnicą okręgu S. Niech teraz L będzie prostą prostopadłą do prostej zawierającą odcinek AB i przechodzącą przez punkt C. Wówczas przecięcie prostej L oraz okręgu S zawiera dwa punkty $P = (x, y)$ oraz $Q = (x, -y)$ i każdy z nich jest konstruowalny. Co więcej $|PC| = \sqrt{a}$, i liczba $\sqrt{a}$ jest konstruowalna. Równość ta jest konsekwencją znanej własności okręgu, która mówi, że trójkąt wpisany w okrąg, którego jeden z boków jest średnicą okręgu, jest prostokątny.

Przejdźmy teraz do opisu ciała K. Na początek zauważmy, że jeśli mamy dwa punkty konstruowalne, których współrzędne leżą w pewnym podciele K' ciała K, to równanie prostej przechodzącej przez te dwa punkty ma współczynniki w ciele K'. Jeśli mamy dwie proste, powiedzmy L_1, L_2, zadane przez równania o współczynnikach z ciała $K' \subset K$, to ich punkt przecięcia również ma współrzędne w ciele K'. Oznacza to, że stosując operację (2) nie wychodzimy poza ciało K'.

Rozważmy teraz operacje (3) i (4). Jakiego typu punkty uzyskujemy w wyniku tych operacji i czy wyprowadzają nas poza ciało K'? Tutaj zakładamy, że prosta i okrąg lub oba okręgi są zadane równaniami o współczynnikach w ciele K'. W przypadku konstrukcji (3) interesuje nas rozwiązanie układu równań

$$\begin{cases} ax + by + c & = 0 \\ (x - x_1)^2 + (y - y_1)^2 & = r \end{cases},$$

gdzie $a, b, c, x_1, y_1, r \in K'$. Eliminując jedną ze zmiennych z równanie liniowego i wstawiając do równania okręgu otrzymujemy równanie kwadratowe o współczynnikach z K'. Oznacza to, że rozwiązanie takiego równania leży w ciele K'', którego stopień nad K' jest $\leqslant 2$.

W przypadku konstrukcji (3) interesuje nas rozwiązanie układu równań

$$\begin{cases} (x - x_1)^2 + (y - y_1)^2 & = r_1 \\ (x - x_2)^2 + (y - y_2)^2 & = r_2 \end{cases},$$

gdzie $x_i, y_i, r_i \in K'$ dla $i = 1, 2$. Odejmując od równanie pierwszego równanie drugie nasz układ redukuje się do układu

$$\begin{cases} 2(x_2 - x_1)x + 2(y_2 - y_1)y &= x_2^2 - x_1^2 + y_2^2 - y_1^2 + r_1 - r_2 \\ (x - x_2)^2 + (y - y_2)^2 &= r_2 \end{cases},$$

czyli przecięcia prostej i okręgu. Oznacza to, że operacja (4) prowadzi do rozszerzenia K'' ciała K', którego stopień nad K' jest $\leqslant 2$.

Z naszych rozważań wynika następująca obserwacja. Jeżeli mamy dany skończony ciąg punktów konstruowalnych oraz K' jest najmniejszym ciałem zawierającym współrzędne tych punktów, to po wykonania operacji (1), (2), (3), (4) jesteśmy w stanie wyprodukować punkty, których współrzędne leżą w co najwyżej kwadratowym rozszerzeniu ciała K'. Oznacza to, że jeśli mamy liczbę konstruowalną $\alpha \in \mathbb{C}$ otrzymaną po skończonej liczbie naszych operacji na prostych i okręgach o współczynnikach z ustalonego ciała K', to istnieje takie $m \in \mathbb{N}$ oraz ciało K'', że $[K'' : K'] = 2^m$. Ponieważ $[K'(\alpha) : K']$ dzieli 2^m, więc również $[K'(\alpha) : K']$ jest potęgą dwójki. Tym samym udowodniliśmy następujące

Twierdzenie 12.7.1. *Jeśli liczba $\alpha \in \mathbb{C}$ jest konstruowalna nad ciałem K', to dla pewnego m zachodzi równość $[K'(\alpha) : K'] = 2^m$.*

Uwaga 12.7.2. Należy znaznaczyć, że jeśli $\alpha \in \mathbb{C}$ oraz $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^m$, to α nie musi być liczbą konstruowalną. Istotnie, nasze rozumowanie, które doprowadziło nas do Twierdzenia 12.7.1, pokazuje, że α musi być elementem ciała, powiedzmy F, które powstało jako ciąg rozszerzeń kwadratowych ciała $\mathbb{Q}$. Rzecz jasna wtedy $[F : \mathbb{Q}] = 2^m$ dla pewnego m. Nietrudno jednak wskazać takie $\alpha \in \mathbb{C}$, że $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ i ciało $\mathbb{Q}(\alpha)$ nie ma podciała kwadratowego. Istotnie, niech α będzie zerem wielomianu $f(X) = X^4 + 3X + 3$. Wielomian f jest nierozkładalny w $\mathbb{Q}[X]$ (dlaczego?) i można sprawdzić, że grupa Galois jego ciała rozkładu to A_4 – grupa permutacji parzystych na czterech elementach. Jak wiadomo w A_4 nie ma podgrup indeksu 2, co oznacza, że nie istnieje ciało kwadratowe F, że $\mathbb{Q} \subset F \subset \mathbb{Q}(\alpha)$. Oznacza to, że α nie jest liczbą konstruowalną.

Twierdzenie 12.7.1 umożliwia dowód następującego.

Wniosek 12.7.3. *Podwojenie sześcianu nie może być przeprowadzone za pomocą cyrkla i linijki.*

Dowód. Jeśli mamy dany sześcian o boku $a > 0$, to podwojenie sześcianu oznacza skonstruowanie takiego $b \in \mathbb{R}$, że $b^3 = 2a^3$. Równoważnie, należy skonstruować długość $d = \sqrt[3]{2}$. Jednakże $[\mathbb{Q}(d) : \mathbb{Q}] = 3$, a ponieważ liczba 3 nie jest potęgą dwójki, więc konstrukcja jest niemożliwa. □

Wniosek 12.7.4. *Konstrukcja tryskekcji kąta nie jest na ogół wykonalna za pomocą cyrkla i linijki.*

Dowód. Zauważmy, że jeśli kąt θ jest konstruowalny, to punkt o współrzędnych $(\cos\theta, \sin\theta)$ również jest konstruowalny, jako punkt leżący w odległości jednostkowej od środka układu współrzędnych i na prostej przechodzącej przez środek układu współrzędnych i nachylonej do osi OX pod kątem α. Na odwrót, jeśli punkt $(\cos\theta, \sin\theta)$ jest konstruowalny, to każda ze współrzędnych jest liczbą konstruowalną, a więc i kąt α jest konstruowalny. Z naszych rozważań wynika, że problem trysekcji danego kąta θ jest równoważny pytaniu o konstruowalność kąta $\theta/3$ lub równoważnie konstruowalność liczby $\cos\theta/3$. Niech teraz θ będzie dane i rozważmy $a = \cos\theta$ oraz $t = \cos\theta/3$. Ze wzorów trygonometrycznych mamy równość

$$\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3 \quad \Longleftrightarrow \quad F_a(t) := 4t^3 - 3t - a = 0.$$

Widzimy zatem, że trysekcja kąta θ jest wykonalna wtedy i tylko wtedy, gdy równanie $F_a(t) = 0$ ma pierwiastek wymierny. Jeśli rozważymy teraz $\theta = 60^0$, to $a = \cos\theta = 1/2$ i rozważamy równanie $F_{1/2}(t) = 0$ lub równoważnie, po przemnożeniu przez 2, równanie

$$8t^3 - 6t - 1 = 0.$$

Zauważmy jednak, że równanie to nie ma pierwiastków wymiernych (bo te muszą być postaci $\pm 1/2^i$ dla pewnego $i = 0, 1, 2, 3$). Oznacza to, że wielomian definiujący nasze równanie jest nierozkładalny i stopień rozszerzenia $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$, gdzie $8\beta^3 - 6\beta - 1 = 0$. Stąd trysekcja kąta θ nie jest wykonalna za pomocą cyrkla i linijki. □

W przypadku kwadratury koła lub równoważnie konstrukcji liczby π prawdziwe jest następujące.

Twierdzenie 12.7.5. *Kwadratura koła jest niewykonalna za pomocą cyrkla i linijki. Dokładniej, liczba π jest przestępna.*

Nie będziemy dowodzić tego twierdzenia, gdyż metody jego dowodu, w przeciwieństwie do dwóch poprzednich problemów, nie są algebraiczne, a analityczne. Nawet dowód niewymierności liczby π jest nietrywialny i został przeprowadzony po raz pierwszy przez J. H. Lamberta w 1760 r. Prosty dowód wykorzystujący jedynie elementarną analizę zaproponował Ch. Hermite [7]. Dowód, że liczba π jest przestępna został przeprowadzony przez von Lindemanna w 1882 r. [12].

Innym ciekawym problemem geometrii, z którym można sobie poradzić za pomocą zaprezentowanych przez nas technik, jest konstruowalność n-kąta foremnego. W szczególności okazuje się, że prawdziwe jest następujące kryterium.

Twierdzenie 12.7.6 (Gauss)**.** *Niech $n \geqslant 3$ będzie ustaloną liczbą naturalną. Niech $n = 2^k n_0$, gdzie n_0 jest liczbą nieparzystą. Wówczas n-kąt foremny jest konstruowalny za pomocą cyrkla i linijki wtedy i tylko wtedy, gdy n_0 jest iloczynem różnych liczb pierwszych Fermata.*

Pierwszy dowód stwierdzenia, że liczba n w zaprezentowanej wyżej postaci jest konstruowalna, został przedstawiony przez Gaussa w roku 1801. Ciekawostką jest fakt, że 17-kąt foremny zdobi pomnik Gaussa w Brunszwiku, lecz tylko wprawne oko jest w stanie odróżnić go od okręgu.

Bibliografia

[1] A. G. Akrias, *Elemens of Computer Algebra with Applications*, John Wiley and Sons, New York, 1989.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, UTM Springer, New York, 1976.

[3] M. Bryński, *Elementy teorii Galois*, Alfa, 1985.

[4] J. D. Dixon, *Problems in Group Theory*, Dover Books on Mathematics, 1973.

[5] R. L. Graham, D. E. Knuth, O. Patashnik, *Matematyka konkretna*, PWN, Warszawa, 2011.

[6] D. Guin, *Algèbre, Groupes et Anneaux*, Édition BELIN, 1997.

[7] Ch. Hermite, Extrait d'une lettre de Monsieur Ch. Hermite à Monsieur Paul Gordan, Journal für die reine und angewandte Mathematik (in French) **76** (1873), 303–311.

[8] T.W. Hungerford, *Algebra*, Springer Science and Business Media, 2003.

[9] J.-M. De Koninck, A. Mercier, *1001 Problems in Classical Number Theory*, Amer. Math. Soc., Providence, RI, 2007.

[10] T.W. Judson, *Abstract Algebra, Theory and Applications*, Lightning Source iNC; Edycja 2015.

[11] R. Lidl, G. Pilz, *Applied Abstract Algebra*, New York, Berlin, Heidelberg, Tokyo: Springel-Verlag, 1984.

[12] F. von Lindemann, Über die Zahl π, Mathematische Annalen 20 (1882), 213–225.

[13] J. Rotman, *Galois theory*, Springer-Verlag, New York, 1998.

[14] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math., 12 (1962), 1099–1106.

[15] K. Szymiczek, *Zbiór zadań z teorii grup*, PWN, Warszawa, 1989.

Indeks