ALGEBRA I B

Władysław Narkiewicz

Notatki do wykładu dla II roku matematyki w semestrze zimowym 2005/2006

I. Pojęcia wstępne

1.1. Działania

1. *Działaniem* w niepustym zbiorze X nazywamy każde przekształcenie produktu $X \times X$ w X:

$$\Phi: \ X \times X \longrightarrow X.$$

Zamiast $\Phi(x, y)$ używa się zwykle jednego z zapisów

$$x \cdot y, \ xy, \ x + y, \ x \circ y, \ x \star y, \ x \bullet y.$$

Można też używać innych symboli.

Przykłady: a) Dodawanie, odejmowanie i mnożenie w zbiorach liczb całkowitych, wymiernych, rzeczywistych, zespolonych, w zbiorze wszystkich wielomianów o współczynnikach w tych zbiorach,

b) Dodawanie, odejmowanie i mnożenie macierzy $n \times n$,

c) Dodawanie i odejmowanie w przestrzeniach liniowych, w szczególności w przestrzeniach $\mathbb{R}^K$ i w przestrzeniach funkcyjnych,

d) Składanie w zbiorze wszystkich przekształceń ustalonego zbioru Ω w siebie,

e) Składanie w zbiorze wszystkich izometrii przekształcających ustaloną figurę geometryczną na siebie.

Rozpatruje się także działania n-argumentowe, będące odwzorowaniami $X^n \longrightarrow X$. Przykładem działania jednoargumentowego może być branie liczby przeciwnej w zbiorze liczb całkowitych. Z kolei branie średniej arytmetycznej trzech liczb w zbiorze liczb wymiernych jest działaniem 3-argumentowym. Działanie dwuargumentowe nazywa się też *działaniem binarnym*. My będziemy rozpatrywali głównie zbiory z działaniami binarnymi.

W zadanym zbiorze można rozpatrywać równocześnie kilka działań. I tak np. w zbiorze liczb całkowitych naturalne jest rozpatrywanie 2 działań – dodawania i mnożenia. Prowadzi to do pojęcia *algebry*: algebrą nazywamy parę $(X; \{f_1, f_2, \ldots, f_k\})$, gdzie X jest niepustym zbiorem, a $f_1, f_2, \ldots, f_k$ są działaniami. Badaniem takich algebr zajmuje się dział matematyki zwany *algebrą ogólną* lub *algebrą uniwersalną*. Nie mieści się ona w programie naszego wykładu. Jest ona przedstawiona np. w podręczniku P.M.Cohna "*Universal Algebra*".

2. W dalszym ciągu X będzie niepustym zbiorem, a $\Phi(x, y) = x \cdot y$ będzie oznaczać działanie w X.

Mówimy, że działanie Φ jest *łączne*, jeśli dla $x, y, z \in X$ zachodzi równość $x \cdot (y \cdot z) = (x \cdot y) \cdot z$. Jest ono *przemienne*, jeśli zawsze mamy $x \cdot y = y \cdot x$.

Twierdzenie 1.1. *Jeśli działanie Φ jest łączne, to przy dowolnym ustawieniu nawiasów w wyrażeniu $x_1 \cdot x_2 \cdots x_n$ wartość tego wyrażenia nie ulega zmianie.*

Dowod: Dla $n = 3$ teza twierdzenia wynika z definicji łączności, załóżmy przeto, że jest ona prawdziwa dla $n = k \geq 3$. Zatem w iloczynach conajwyżej k elementów nie musimy mieć nawiasów. Przypuśćmy, że istnieją elementy $x_1, \cdots, x_{k+1} \in X$ takie, że przy pewnych $1 \leq r < s \leq k$ mamy

$$(x_1 \cdots x_r)(x_{r+1} \cdots x_{k+1}) \neq (x_1 \cdots x_s)(x_{s+1} \cdots x_{k+1}). \tag{1.1}$$

Na mocy założenia indukcyjnego możemy napisać

$$x_1 \cdots x_s = (x_1 \cdots x_r)(x_{r+1} \cdots x_s),$$

a zatem, korzystając z łączności, otrzymujemy

$$(x_1 \cdots x_s)(x_{s+1} \cdots x_{k+1}) = ((x_1 \cdots x_r)(x_{r+1} \cdots x_s))(x_{s+1} \cdots x_{k+1}) = (x_1 \cdots x_r)(x_{r+1} \cdots x_s \cdot x_{s+1} \cdots x_{k+1}),$$

wbrew (1.1*). $\square$

3. Jeśli w zbiorze X istnieje element e taki, że dla wszystkich $x \in X$ zachodzą równości $x \cdot e = e \cdot x = x$, to mówimy, że e jest *elementem neutralnym* dla działania Φ. W przypadku dodawania liczb takim elementem jest liczba 0, a w przypadku mnożenia liczb jest nim 1. Nie każde działanie ma element neutralny. Jeśli np. X jest zbiorem $\mathbb{Z}$ liczb całkowitych, a działaniem jest odejmowanie, to element neutralny e musiałby spełniać warunek $1 - e = e - 1 = 1$, co prowadzi do $0 = e = 2$.

Twierdzenie 1.2. *Może istnieć conajwyżej jeden element neutralny.*

Dowód: Gdyby istniały dwa elementy neutralne $e_1, e_2 \in X$, to mielibyśmy

$$e_1 = e_1 \cdot e_2 = e_2. \qquad \square$$

Jeśli e jest elementem neutralnym, to *elementem odwrotnym* do elementu $x \in X$ nazywamy element $y \in X$, dla którego $x \cdot y = y \cdot x = e$. Jeśli działaniem jest dodawanie liczb, to elementem odwrotnym do x będzie liczba $-x$, a jeśli działaniem jest mnożenie, to elementem odwrotnym do $x \neq 0$ jest $1/x$.

Twierdzenie 1.3. *Jeśli działanie jest łączne to może istnieć conajwyżej jeden element odwrotny do zadanego elementu.*

Dowód: Jeśli y, z są elementami odwrotnymi do $x \in X$, to $x \cdot y = e$ i $z \cdot x = e$, gdzie e jest elementem neutralnym. Korzystając z łączności, otrzymujemy

$$z = z \cdot e = z \cdot (x \cdot y) = (z \cdot x) \cdot y = e \cdot y = y,$$

a więc $z = y$. $\square$

Uwaga: Założenie łączności jest tutaj istotne, o czym świadczy następujący przykład: Niech X będzie zbiorem 3-elementowym: $X = \{a, b, e\}$, a działanie $\circ$ niech będzie zdefiniowane następująco:

$$x \circ y = \begin{cases} x & \text{jeśli } y = e, \\ y & \text{jeśli } x = e, \\ e & \text{w pozostałych przypadkach.} \end{cases}$$

Działanie to jest przemienne, element e jest elementem neutralnym, a przy tym elementy a, b mają po dwa elementy odwrotne.

3. Rozpatrzmy dwie algebry z jednym działaniem dwuargumentowym: $\mathcal{X} = (X, \{\cdot\})$ i $\mathcal{Y} = (Y, \{\circ\})$. Odwzorowanie $f: \; X \longrightarrow Y$, spełniające warunek

$$f(a \cdot b) = f(a) \circ f(b)$$

dla wszystkich $a, b \in X$, nazywamy *homomorfizmem* algebry $\mathcal{X}$ na $\mathcal{Y}$.

Homomorfizm różnowartościowy (injektywny) nazywa się *monomorfizmem*, homomorfizm surjektywny ("na") nazywa się *epimorfizmem*, a homomorfizm, który jest równocześnie różnowartościowy i surjektywny nazywa się *izomorfizmem*. Izomorfizm jest zatem homomorfizmem, dającym wzajemnie jednoznaczne odwzorowanie zbioru X na Y. W przypadku $\mathcal{X} = \mathcal{Y}$ homomorfizm nazywa się *endomorfizmem*, a endomorfizm będący izomorfizmem nazywa się *automorfizmem*. Mówimy, że dwie algebry $\mathcal{X}$ i $\mathcal{Y}$ są *izomorficzne*, jeśli istnieje izomorfizm $\Phi: \; \mathcal{X} \longrightarrow \mathcal{Y}$. Piszemy wówczas $\mathcal{X} \sim \mathcal{Y}$.

Fakt 1.4. *(i) Złożenie homomorfizmów (monomorfizmów, epimorfizmów, izomorfizmów, endomorfizmów, automorfizmów) jest homomorfizmem (monomorfizmem epimorfizmem, izomorfizmem, endomorfizmem, automorfizmem).*

(ii) Jeśli $\Phi: \; (X, \{\cdot\}) \longrightarrow (Y, \{\circ\})$ *jest izomorfizmem, to odwzorowanie odwrotne*

$$\Phi^{-1}: \; (Y, \{\circ\}) \longrightarrow (X, \{\cdot\})$$

jest również izomorfizmem.

Dowód: (i) Jeśli $f : (X, \{\cdot\}) \longrightarrow (Y, \{\circ\})$ i $g : (Y, \{\circ\}) \longrightarrow (Z, \{\star\})$ są homomorfizmami, a $h(x) = g(f(x))$ jest ich złożeniem, to dla $a, b \in X$ mamy

$$h(a \cdot b) = g(f(a \cdot b)) = g(f(a) \circ f(b)) = g(f(a)) \star g(f(b)) = h(a) \star h(b),$$

a więc h jest homomorfizmem. Pozostałe stwierdzenia wynikają teraz z własności odwzorowań różnowartościowych, surjektywnych i wzajemnie jednoznacznych.

(ii) Wystarczy pokazać, że Φ^{-1} jest homomorfizmem. Niech więc $a, b \in Y$ i niech $a_1, b_1 \in X$ spełniają $\Phi(a_1) = a, \Phi(b_1) = b$. Wówczas

$$ab = \Phi(a_1)\Phi(b_1) = \Phi(a_1 b_1),$$

tj. $\Phi^{-1}(ab) = a_1 b_1$, a ponieważ $\Phi^{-1}(a) = a_1$ i $\Phi^{-1}(b) = b$, zatem

$$\Phi^{-1}(ab) = \Phi^{-1}(a)\Phi^{-1}(b). \qquad \square$$

1.2. Podstawowe struktury: grupy, pierścienie, ciała

1. Omówimy teraz najważniejsze typy zbiorów z działaniami, pojawiającymi się w naturalny sposób w różnych działach matematyki.

Zbiór z działaniem łącznym nazywa się *półgrupą*. Niech Ω będzie niepustym zbiorem, a X niech będzie zbiorem wszystkich przekształceń $\Omega \longrightarrow \Omega$, przy czym działaniem jest składanie przekształceń. Nietrudno widzieć, że X z tym działaniem jest półgrupą.

Najważniejszą klasę półgrup tworzą *grupy*. *Grupą* nazywamy niepusty zbiór z działaniem, które jest łączne, posiada element neutralny a przy tym do każdego elementu istnieje element odwrotny. Działanie w grupie oznacza się zazwyczaj kropką $\cdot$, tak jak zwykłe mnożenie, a w praktyce tę kropkę się pomija, o ile nie doprowadzi to do nieporozumienia. Jeśli działanie jest przemienne (a wówczas grupę nazywamy *grupą przemienną* lub *grupą abelową*), to często działanie w niej oznacza się symbolem dodawania $+$.

Zatem zbiór G z działaniem $\cdot$ jest grupą, jeśli spełnione są następujące warunki:

(i) Dla wszystkich $a, b, c \in G$ mamy

$$a(bc) = (ab)c,$$

(i) Istnieje element $e \in G$ taki, że dla wszystkich $a \in G$ mamy

$$ae = ea = a,$$

(iii) Do każdego elementu $a \in G$ istnieje element $b \in G$ taki, że

$$ab = ba = e.$$

W grupie abelowej jest spełniony dodatkowo warunek

(iv) Dla wszystkich $a, b \in G$ mamy $ab = ba$.

Przykłady grup:

(a) Zbiory liczb całkowitych, wymiernych, rzeczywistych lub zespolonych z dodawaniem,

(b) Zbiory niezerowych liczb wymiernych, rzeczywistych lub zespolonych z mnożeniem,

(c) Zbiór reszt z dzielenia przez ustaloną liczbę naturalną N z dodawaniem modulo N,

(d) Zbiór $S(\Omega)$ wszystkich wzajemnie jednoznacznych przekształceń ustalonego zbioru $\Omega \neq \emptyset$ na siebie, w szczególności zbiór S_n wszystkich permutacji zbioru n-elementowego,

(e) Zbiór $Sym(\Gamma)$ wszystkich izometrii, przekształcających ustalony podzbiór Γ płaszczyzny na siebie,

(f) Zbiór $GL_n(\mathbb{R})$ wszystkich odwracalnych macierzy $n \times n$ o elementach rzeczywistych z mnożeniem,

(g) Zbiór $SL_2(\mathbb{Z})$ wszystkich macierzy 2×2 o elementach całkowitych i wyznaczniku równym 1 z mnożeniem.

2. Inną ważną klasą zbiorów z działaniami są *pierścienie*. Niepusty zbiór X z dwoma działaniami oznaczonymi przez "$+$" i "$\cdot$", zwanymi dodawaniem i mnożeniem, nazywamy pierścieniem, jeśli są spełnione następujące warunki:

(i) Zbiór X z dodawaniem jest grupą przemienną z elementem neutralnym 0,

(ii) Mnożenie jest łączne,

oraz

(iii) Dla dowolnych $x, y, z \in X$ zachodzi rozdzielność mnożenia względem dodawania:

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad (y + z) \cdot x = y \cdot x + y \cdot z.$$

Pierścień nazywa się *pierścieniem przemiennym*, jeśli jego mnożenie jest działaniem przemiennym. Jeśli w pierścieniu istnieje element neutralny dla mnożenia, to mówimy, że jest to *pierścień z jednością*.

Przykłady pierścieni:

(a) Zbiór $\mathbb{Z}$ liczb całkowitych, zbiór $\mathbb{Q}$ liczb wymiernych, zbiór $\mathbb{R}$ liczb rzeczywistych, zbiór $\mathbb{C}$ liczb zespolonych ze zwykłym dodawaniem i mnożeniem,

(b) Zbiór wszystkich wielomianów o współczynnikach z $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ze zwykłymi działaniami,

(c) Zbiór $\mathfrak{M}_n(R)$ wszystkich macierzy $n \times n$ o elementach ze zbioru $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$,

(d) Zbiór $C(I)$ wszystkich funkcji ciągłych o wartościach rzeczywistych na odcinku I ze zwykłym dodawaniem i mnożeniem,

(e) Zbiór reszt z dzielenia przez ustaloną liczbę naturalną N z dodawaniem i mnożeniem modulo N.

(f) Zbiór wszystkich liczb parzystych, czy też ogólniej, zbiór wszystkich liczb podzielnych przez zadaną liczbę naturalną.

3. Szczególnie ważną rolę odgrywają pierścienie K, które obok podanych wyżej warunków (i) – (iii) są przemienne, mają jedność, a nadto każdy element różny od 0 posiada element odwrotny. Warunki te można sformułować prosto w następjący sposób:

(I) Zbiór K jest grupą przemienną względem dodawania,

(II) Zbiór $K \setminus \{0\}$ jest grupą przemienną względem mnożenia,

(III) Dla dowolnych $x, y, z \in K$ zachodzi równość $x \cdot (y + z) = x \cdot y + x \cdot z$.

Pierścienie, spełniające te warunki nazywamy *ciałami*.

Najprostsze przykłady ciał, to dobrze znane zbiory $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ze zwykłym dodawaniem i mnożeniem. Inne przykłady pojawią się w poniższych prostych twierdzeniach:

Twierdzenie 1.5. *Zbiór $\mathbb{Q}(\beth)$ wszystkich liczb zespolonych postaci $a + bi$ z wymiernymi a, b jest ciałem ze zwykłymi działaniami.*

Dowód: Wystarczy sprawdzić, że zbiór ten jest zamknięty na dodawanie i mnożenie, a każdy jego element różny od zera posiada element odwrotny. Fakty te wynikają natychmiast z równości

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \quad (a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

$$\frac{1}{a + bi} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i$$

i uwagi, że zbiór liczb wymiernych jest zamknięty na dodawanie, mnożenie i dzielenie przez swe niezerowe elementy, a z $a + bi \neq 0$ wynika $a^2 + b^2 \neq 0$. $\square$

Twierdzenie 1.6. *Jeśli p jest liczbą pierwszą, to zbiór reszt z dzielenia przez p z dodawaniem i mnożeniem modulo p jest ciałem.*

Dowód: Rozpoczniemy od dwóch prostych faktów:

Lemat 1.7. (Dzielenie z resztą.) *Jeśli $a \in \mathbb{Z}$, zaś b jest liczbą naturalną, to istnieją liczby całkowite q, r takie, że*

$$a = qb + r, \quad 0 \leq r < b.$$

Dowód: Istnieje liczba całkowita N, spełniająca

$$Nb \leq a < (N+1)b,$$

możemy więc przyjąć $q = N$, $r = a - Nb$, gdyż $0 \leq a - Nb < (N+1)b - Nb = b$. □

Lemat 1.8. *Jeśli a, b są liczbami całkowitymi, nie mającymi wspólnego dzielnika większego od 1, to istnieją liczby całkowite x_0, y_0 takie, że*

$$ax_0 + by_0 = 1.$$

Dowód: Niech A będzie zbiorem wszystkich liczb dających się przedstawić w postaci $ax + by$ przy całkowitych x, y i niech d będzie najmniejszą dodatnią liczbą w zbiorze A. Zatem $d = ax + by$ przy pewnych $x, y \in \mathbb{Z}$. Zauważmy, że każdy element zbioru A dzieli się przez d. W istocie, jeśli $c \in A$ i $d \nmid c$, to z lematu 1.7 wynika istnienie liczb $q, r \in \mathbb{Z}$, spełniających $c = qd + r$ i $0 < r < d$. Ponieważ przy pewnych $t, u \in \mathbb{Z}$ mamy $c = at + bu$, przeto

$$r = c - qd = (t - qx)a + (u - qy)p$$

leży w A, co z uwagi na $0 < r < d$ przeczy wyborowi liczby d. Ponieważ $a = 1 \cdot a + 0 \cdot b$ i $b = 0 \cdot a + 1 \cdot b$, przeto $a, b \in A$, a więc obie liczby a, b dzielą się przez $d > 0$, co jest możliwe jedynie, gdy $ax + by = d = 1$. □

Oprzemy się na lemacie, pochodzącym od Euklidesa, aczkolwiek podany przez niego jest błędny:

Lemat 1.9. *Jeśli p jest liczbą pierwszą dzielącą iloczyn ab, to p dzieli conajmniej jedną z liczb a, b.*

Dowód: Jeśli $p|ab$, ale $p \nmid a$, to z lematu 1.8 wynika istnienie liczb całkowitych x, y spełniających $1 = ax + py$. Mnożąc tę równość obustronnie przez b dochodzimy do $b = (ab)x + p(by)$, ale prawa strona ostatniej równości dzieli się przez p i otrzymujemy $p|b$. □

Oznaczmy przez $\bar{a}$ resztę z dzielenia liczby całkowitej a przez p. Łatwo sprawdzić, że $\overline{a+b} = \bar{a} + \bar{b}$ i $\overline{ab} = \bar{a} \cdot \bar{b}$, a elementem neutralnym dla mnożenia jest $\bar{1}$. Do dowodu twierdzenia wystarczy pokazać, że jeśli $p \nmid a$, to istnieje $b \in \mathbb{Z}$ takie, że $\overline{ab} = \bar{1}$. Niech więc $p \nmid a$ i rozpatrzmy reszty

$$\bar{a}, \overline{2a}, \overline{3a}, \overline{(p-1)a}. \tag{1.2}$$

Gdyby dwie z nich były równe, powiedzmy $\overline{ra} = \overline{sa}$, przy czym $r < s$, to mielibyśmy $\overline{(s-r)a} = 0$, a więc liczba $(s-r)a$ dzieliłaby się przez p. Wobec $p \nmid a$ z lematu 1.9 wynika podzielność $s - r$ przez p, ale to nie jest możliwe, ponieważ $0 < s - r < p$. Zatem reszty występujące w (1.2) są wszystkie różne, a przy tym poprzednie rozumowanie pokazuje, że są one niezerowe. Jest ich $p - 1$, więc jest to zbiór wszystkich niezerowych reszt modulo p, a zatem reszta $\bar{1}$ musi wśród nich wystąpić, tj. istnieje b, spełniające $\bar{\cdot}b = \bar{1}$. □

II. Elementy teorii grup

2.1. Podstawowe własności

1. Udowodnimy teraz parę prostych faktów o grupach. Niech G będzie dowolną grupą z elementem neutralnym e. Element ten będziemy nazywali *jednością grupy* G. Działanie w G będziemy oznaczać przez xy, a element odwrotny do $a \in G$ oznaczamy przez a^{-1}. Tak więc dla dowolnego $a \in G$ mamy $aa^{-1} = a^{-1}a = e$. Z twierdzenia 1.3 wynika, że element a^{-1} jest jednoznacznie wyznaczony przez a. W przypadku, gdy G jest abelowa, a jej działanie oznaczone jest przez "$+$", to element przeciwny do a jest oznaczany przez $-a$.

Twierdzenie 2.1. *Jeśli $a, b \in G$, to każde z równań*

$$ax = b, \quad ya = b$$

ma w G dokładnie jedno rozwiązanie.

Dowód: Jeśli $ax = b, ya = b$, to

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

oraz

$$y = ye = y(aa^{-1}) = (ya)a^{-1} = ba^{-1},$$

co dowodzi jedyności rozwiązania. Powyższe wzory pokazują też, że elementy $x = a^{-1}b$ i $y = ba^{-1}$ spełniają nasze równania. □

Twierdzenie 2.2. *Jeśli $a, b \in G$, to $(ab)^{-1} = b^{-1}a^{-1}$.*

Dowód: Korzystając z twierdzenia 1.1 otrzymujemy

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e. \qquad \square$$

Potęgowanie w grupach definujemy, przyjmując $a^0 = e$ oraz $a^{n+1} = a \cdot a^n$ dla $n = 0, 1, 2, \ldots$, tak więc dla $k = 1, 2, 3, \ldots$ mamy

$$a^k = \underbrace{a \cdot a \cdots a}_{k \text{ razy}}. \tag{2.1}$$

Ponadto dla $n = 2, 3, \ldots$ kładziemy $a^{-n} = (a^{-1})^n$.

Twierdzenie 2.3. *(i) Dla $a \in G$ oraz $n = 1, 2, \ldots$ mamy $(a^n)^{-1} = a^{-n}$.*
(ii) Dla $a \in G$ i całkowitych m, n mamy

$$a^{m+n} = a^m a^n.$$

(iii) Dla $a, b \in G$ i całkowitych m, n mamy

$$(a^m)^n = a^{mn}.$$

(iv) Jeśli grupa G jest abelowa, to dla całkowitych n mamy

$$(ab)^n = a^n b^n. \tag{2.2}$$

Dowód: (i) Kładąc $b = a^{-1}$ otrzymamy

$$a^n a^{-n} = a^n b^n = \underbrace{a \cdot a \cdots a}_{n \text{ razy}} \underbrace{b \cdot b \cdots b}_{n \text{ razy}} = e.$$

(ii) Jeśli obie liczby m, n są nieujemne, to równości te wynikają z (2.1). Jeśli obie są ujemne, powiedzmy $m = -M, n = -N$ przy $M, N \geq 0$, to kładąc $b = a^{-1}$ i korzystając z (i) i (2.1) otrzymamy

$$a^m a^n = a^{-M} a^{-N} = b^M b^N = b^{M+N} = (a^{-1})^M (a^{-1})^N = (a^{-1})^{M+N} = a^{m+n}.$$

Jeśli m i n mają różne znaki, np. $m \geq 0$, $n < 0$ i $n = -N$ z dodatnim N, to

$$a^m a^n = a^m a^{-N} = a^m b^N = \underbrace{a \cdot a \cdots a}_{m \text{ razy}} \underbrace{b \cdot b \cdots b}_{N \text{ razy}} = \left\{ \begin{array}{ll} a^{m-N} & \text{gdy } m \geq N \\ b^{N-m} & \text{gdy } m < N \end{array} \right\} = a^{m+n}.$$

(iii) Jeśli $n \geq 0$, to wystarczy zastosować (2.1) i (i). Jeśli zaś $n < 0$ i $N = -n$ i przyjmiemy $b = a^{-1}$, to z (i) wynika

$$(a^m)^n = (a^m)^{-N} = ((a^m)^{-1})^N = (a^{-m})^N = a^{-mN} = a^{mn}.$$

(iv) Wynika z (i) i przemienności mnożenia. □

Uwaga 1: Zachodzenie równości (2.2) dla każdego n jest charakterystyczne dla grup abelowych. Jeśli bowiem G nie jest abelowa, to istnieją w niej elementy a, b spełniające $ab \neq ba$, a w przypadku $n = 2$ równość (2.2) dawałaby

$$abab = (ab)^2 = a^2 b^2 = aabb,$$

zatem

$$ba = a^{-1}(abab)b^{-1} = a^{-1}(aabb)b^{-1} = (a^{-1}a)(ab)(bb^{-1}) = ab,$$

wbrew wyborowi a, b.

Uwaga 2: Jeśli grupa G jest abelowa, a działanie jest oznaczane znakiem dodawania, to zamiast a^n piszemy na, tak więc wzory z powyższego twierdzenia przyjmą następującą postać:

$$-(-a) = a, \ (m+n)a = ma + na, \ m(na) = (mn)a, \ n(a+b) = na + nb.$$

2. Niepusty podzbiór H grupy G nazywa się *podgrupą* grupy G, jeśli jest grupą ze względu na te same działania. Piszemy wtedy $H < G$.

Twierdzenie 2.4. *Na to by niepusty zbiór $H \subset G$ był podgrupą grupy G potrzeba i wystarcza, by dla dowolnych $a, b \in H$ zachodziło $ab^{-1} \in H$.*

Dowód: Jeśli podzbiór H grupy G jest jej podgrupą, to zawiera jedność e grupy G, wraz z każdym swym elementem zawiera element do niego odwrotny, a nadto jest zamkniety na działanie, tj. z $a, b \in H$ wynika $ab \in H$. Stąd wynika spełnienie warunku $ab^{-1} \in H$ dla dowolnych $a, b \in H$.

Załóżmy teraz spełnienie tego warunku. Kładąc w nim $b = a$ otrzymamy $e = aa^{-1} \in H$. Przyjmując $a = e$ widzimy, że wraz z dowolnym elementem $b \in H$ również element $eb^{-1} = b^{-1}$ leży w H. Jeśli teraz a, b leżą w H, to $b^{-1} \in H$ oraz $ab = a(b^{-1})^{-1} \in H$. Łączność działania wynika z łączności działania w większej grupie G. □

3. Jeśli $a \in G$ i istnieją liczby naturalne $n \geq 1$ spełniające $a^n = e$, to najmniejszą z nich nazywamy *rzędem elementu* a i oznaczamy[1] $o(a)$. Jeśli takich liczb nie ma, to mówimy, że a ma *rząd nieskończony* i piszemy $o(a) = \infty$. Grupa, której każdy element ma rząd skończony nazywa się *grupą torsyjną*, a grupa, w której każdy element różny od jedności ma rząd nieskończony nazywa się *grupą beztorsyjną*.

Twierdzenie 2.5. *(i) Jeśli $a \in G$ i $o(a) = n < \infty$ to każda liczba całkowita N, spełniająca $a^N = e$ dzieli się przez n, elementy $a, a^2, \ldots, a^n = e$ są parami różne i tworzą podgrupę grupy G.*

(ii) Jeśli $a \in G$ jest rzędu nieskończonego, to elementy a^k $(k \in \mathbb{Z})$ są wszystkie różne i tworzą podgrupę grupy G.

[1] Od angielskiego słowa *order*.

Dowód: Jeśli $a^N = e$, to stosując Lemat 1.7 napiszmy $N = qn + r$, przy czym $0 \leq r < n$. Wówczas, korzystając z Twierdzenia 2.3, otrzymamy

$$e = a^N = a^{qn+r} = (a^n)^q a^r = ea^r = a^r,$$

co wobec $0 \leq r < n$ jest możliwe jedynie w przypadku $r = 0$, a to daje podzielność N przez n.

Gdyby elementy a^s, a^t były równe przy pewnych $1 \leq s < t \leq n$, to korzystając z Twierdzenia 2.3 mielibyśmy $e = a^{t-s}$, co wobec $0 < t - s < n$ nie jest możliwe. To rozumowanie działa także w przypadku gdy rząd elementu a jest nieskończony. To, że zbiór wszystkich potęg o wykładniku całkowitym ustalonego elementu tworzy grupę wynika z Twierdzenia 2.4 i z uwagi, że jeśli $o(a) = n < \infty$, to $(a^k)^{-1} = a^{n-k}$. □

Grupa, złożona z wszystkich potęg ustalonego elementu a nazywa się *grupą cykliczną* generowaną przez a, zaś a nazywa się *generatorem* tej grupy. Nietrudno zauważyć, że wszystkie grupy cykliczne są abelowe. Z Twierdzenia 2.5 wynika, że ilość elementów w grupie cyklicznej generowanej przez element a jest równa $o(a)$.

Przykłady grup cyklicznych:

a) Grupa utworzona przez wszystkie liczby całkowite z dodawaniem jest grupą cykliczną nieskończoną, generowaną przez liczbę 1. Jest ona też generowana przez liczbę -1, tak więc widzimy, że generator grupy cyklicznej nie jest wyznaczony jednoznacznie. Grupę tę oznacza się przez C_∞.

b) Dla $N = 1, 2, \ldots$ rozpatrzmy zbiór $\{0, 1, 2, \ldots, N-1\}$, w którym działaniem jest dodawanie modulo N, które można formalnie określić wzorem

$$a +_N b = \begin{cases} a+b & \text{gdy } a+b < N, \\ a+b-N & \text{gdy } a+b \geq N. \end{cases}$$

Grupę tę można traktować jako grupę reszt z dzielenia przez N. Oznaczamy ją przez C_N.

Twierdzenie 2.6. *(i) Każda grupa cykliczna mająca nieskończenie wiele elementów jest izomorficzna z grupą C_∞.*

(ii) Każda grupa cykliczna mająca $N < \infty$ elementów jest izomorficzna z grupą C_N.

Dowód: Z twierdzenia 2.5 wynika, że jeśli a jest generatorem grupy cyklicznej nieskończonej A, to pokrywa się ona ze zbiorem $\{e, a, a^2, \ldots, a^{-1}, a^{-2}, \ldots\}$. Z Twierdzenia 2.3 (ii) otrzymujemy, że $\Phi: C_\infty \longrightarrow A$ zadane przez $n \mapsto a^n$ jest homomorfizmem i pozostaje zauważyć, że Φ jest odwzorowaniem wzajemnie jednoznacznym.

Podobnie postępujemy w przypadku, gdy $o(a) = N$. Wtedy grupa A generowana przez a jest postaci $\{e, a, a^2, \ldots, a^{N-1}\}$, a korzystając ponownie z Twierdzenia 2.3 (ii) widzimy, tak jak w poprzednim przypadku, że odwzorowanie $\Phi: C_N \longrightarrow A$ zadane przez $n \mapsto a^n$ jest izomorfizmem. □

2.2. Grupy permutacji.

1. Bardzo ważnymi grupami są *grupy permutacji* zbiorów skończonych. Możemy przy tym ograniczyć się do zbiorów postaci $X_n = \{1, 2, \ldots, n\}$, gdyż każdej permutacji zbioru n-elementowego $\{x_1, x_2, \ldots, x_n\}$ odpowiada w sposób wzajemnie jednoznaczny permutacja zbioru indeksów X_n. Grupa wszystkich permutacji zbioru X_n nazywa się n-tą *grupą symetryczną* i jest oznaczana przez S_n. Ma ona $n!$ elementów.

Jeśli $P \in S_n$ i dla $i = 1, 2, \ldots, n$ mamy $P(i) = a_i$, to piszemy

$$P = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

Kolejność elementów w górnym wierszu może być dowolna, tak więc np. permutacje

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \text{ i } \begin{pmatrix} 3 & 2 & 1 \\ 2 & 1 & 3 \end{pmatrix}$$

są równe.

Wygodę tego zapisu widać przy mnożeniu i odwracaniu permutacji, gdyż zachodzą równości

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & \cdots & c_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix} \tag{2.3}$$

i

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}^{-1} = \begin{pmatrix} b_1 & b_2 & \cdots & b_n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}. \tag{2.4}$$

Zbiór elementów $k \in X_n$, spełniających $P(k) = k$ nazywamy *zbiorem elementów niezmienniczych* permutacji P, lub też *zbiorem fixpunktów* P i oznaczamy przez $F(P)$, a jego dopełnienie $X_n \setminus F(P)$ oznaczamy przez $M(P)$. Zauważmy, że zbiór $M(P)$ jest pusty jedynie dla permutacji identycznościowej E ($E(k) = k$ dla $k = 1, 2, \ldots, n$), zaś zbiór $F(P)$ może być pusty dla wielu permutacji z S_n.

Permutacja C nazywa się *cyklem k-elementowym*, jeśli istnieją elementy $a_1, a_2, \ldots, a_k \in X_n$ takie, że

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

a dla $j \notin \{a_1, a_2, \ldots, a_k\}$ mamy $C(j) = j$. Taki cykl zapisujemy w postaci $(a_1, a_2, \ldots, a_k)$. Z definicji cyklu wynika łatwo, że rząd cyklu k-elementowego jest równy k, a zatem jedynym cyklem jednoelementowym jest identyczność. Cykle 2-elementowe nazywamy *transpozycjami*. Warto pamiętać, że jeśli T jest transpozycją, to $T^{-1} = T$.

Dwie permutacje P_1, P_2 nazywają się *rozłączne*, jeśli $M(P_1) \cap M(P_2) = \emptyset$.

Twierdzenie 2.7. (i) *Jeśli C_1, C_2 są cyklami rozłącznymi, to $C_1C_2 = C_2C_1$,*

(ii) *Każda permutacja $P \in S_n$ jest bądź cyklem, bądź też iloczynem cykli rozłącznych.*

Dowód: (i) Prosty rachunek pokazuje, że jeśli $C_1 = (a_1, a_2, \ldots, a_r)$ i $C_2 = \{b_1, b_2, \ldots, b_s)$, a zbiory $\{a_1, \ldots, a_r\}$ i $\{b_1, \ldots, b_s\}$ są rozłączne oraz

$$X_n = \{a_1, \ldots, a_r\} \cup \{b_1, \ldots, b_s\} \cup \{c_1, c_2, \ldots, c_t\}$$

jest rozkładem X_n na zbiory rozłączne, to zarówno C_1C_2, jak i C_2C_1 jest równe

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_r & b_1 & b_2 & \cdots & b_s & c_1 & c_2 & \cdots & c_t \\ a_2 & a_3 & \cdots & a_1 & b_2 & b_3 & \cdots & b_1 & c_1 & c_2 & \cdots & c_t \end{pmatrix}.$$

(ii) Zastosujemy indukcję ze względu na liczbę elementów zbioru $M(P)$.

Jeśli $\#M(P) = 0$, to P jest identycznością, a więc jest cyklem 1-elementowym. Załóżmy, że przy pewnym $k \geq 1$ teza jest prawdziwa dla wszystkich permutacji P z $\#M(P) < k$ i niech $Q \in S_n$ spełnia $M(Q) = k$. Ponieważ $Q \neq E$, zatem istnieje $i \in X_n$ z $Q(i) \neq i$. Weźmy pod uwagę ciąg $a_1 = i, a_2 = Q(a_1), a_3 = Q(a_2), \ldots$. Ze skończoności zbioru X_n wynika, że w ciągu tym muszą wystąpić powtarzające się elementy. Niech r będzie najmniejszym indeksem, dla którego istnieje $s > r$ takie, że $a_r = a_s$. Gdyby było $r > 1$, to mielibyśmy

$$Q(a_{r-1}) = a_r = a_s = Q(a_{s-1}),$$

co dałoby

$$a_{r-1} = Q^{-1}(Q(a_{r-1})) = Q^{-1}(Q(a_{s-1})) = a_{s-1},$$

wbrew wyborowi r. Zatem $r = 1$ i widzimy, że Q jest postaci

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{s-1} & b_1 & \cdots & b_{n-s+1} \\ a_2 & a_3 & \cdots & a_1 & c_1 & \cdots & c_{n-s+1} \end{pmatrix},$$

przy czym zbiory $\{a_1, \ldots, a_{s-1}\}$ i $\{b_1, c_1, \ldots, b_{n-s+1}, c_{n-s+1}\}$ są rozłączne. Jeśli $C = (a_1, a_2, \ldots, a_{s-1})$, to dla permutacji $Q_1 = C^{-1}Q$ mamy $F(Q_1) = F(Q) \cup \{a_1, a_2, \ldots, a_{s-1}\}$, a zatem $\#M(Q_1) < \#M(Q) = k$ i z założenia indukcyjnego wynika, że Q_1 jest bądź cyklem, bądź też iloczynem cykli rozłącznych, powiedzmy

$Q_1 = C_1 \cdots C_t$. To prowadzi do $Q = CQ_1 = CC_1 \cdots C_t$ i pozostaje zauważyć, że cykl C jest rozłączny z każdym z cykli C_i. □

Wniosek. *Każda permutacja jest iloczynem transpozycji.*

Dowód: Wystarczy pokazać, że każdy cykl jest iloczynem transpozycji i zastosować twierdzenie. Zastosujemy indukcję ze względu na długość k cyklu. W przypadku $k = 2$ nie ma czego dowodzić, załóżmy zatem, że każdy cykl o długości mniejszej od k jest iloczynem transpozycji i niech $C = (a_1, a_2, \ldots, a_k)$ będzie cyklem k-elementowym. Jeśli $T = (a_k, a_1)$, to

$$C_1 = CT = \begin{pmatrix} a_1 & a_2 & \ldots & a_{k-1} & a_k \\ a_1 & a_3 & & a_k & a_2 \end{pmatrix} = (a_2, a_3, \ldots, a_k)$$

jest cyklem $(k-1)$-elementowym, a więc jest iloczynem transpozycji. Ponieważ T jest transpozycją, zatem $T^{-1} = T$, a więc $C = C_1 T^{-1} = C_1 T$ jest iloczynem transpozycji. □

Uwaga: Powyższy dowód pokazuje, że jeśli C jest cyklem k-elementowym przy $k \geq 1$, to jest on iloczynem $k-1$ transpozycji.

2. Ważną podgrupę grupy S_n tworzą tzw. *permutacje parzyste*. Permutacja

$$P = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & & a_n \end{pmatrix}$$

nazywa się permutacją parzystą, jeśli iloczyn

$$\prod_{i<j} (a_j - a_i)$$

jest liczbą dodatnią. Pozostałe permutacje nazywa się *permutacjami nieparzystymi*. *Znak permutacji* definiujemy przez

$$\operatorname{sgn} P = \begin{cases} +1 & \text{gdy } P \text{ jest parzysta,} \\ -1 & \text{gdy } P \text{ jest nieparzysta.} \end{cases}$$

Nietrudno spostrzec, że jeśli permutację P zapiszemy w postaci

$$P = \begin{pmatrix} b_1 & b_2 & \ldots & b_n \\ c_1 & c_2 & & c_n \end{pmatrix},$$

to

$$\operatorname{sgn} P = \prod_{i<j} \frac{b_j - b_i}{c_j - c_i}. \tag{2.5}$$

Twierdzenie 2.8. (i) *Dla dowolnych permutacji P_1, P_2 mamy*

$$\operatorname{sgn} P_1 P_2 = \operatorname{sgn} P_1 \cdot \operatorname{sgn} P_2$$

i

$$\operatorname{sgn} P_1^{-1} = \operatorname{sgn} P_1.$$

(ii) Cykl k-elementowy jest permutacją parzystą wtedy i tylko wtedy, gdy $2 \nmid k$.

Dowód: (i) To wynika z wzorów (2.3), (2.4) i (2.5).

(ii) Wprost z definicji znaku permutacji wynika, że transpozycja jest permutacją nieparzystą. Z uwagi po Wniosku z Twierdzenia 2.7 wiemy, że dla $k \geq 3$ cykl k-elementowy jest iloczynem $k-1$ transpozycji, wystarczy więc zastosować (i), by otrzymać tezę. □

Wniosek. (i) *Zbiór wszystkich permutacji parzystych zawartych w S_n jest podgrupą S_n.*

(ii) Przy $n \geq 2$ podgrupa ta ma $n!/2$ elementów.

Dowód: (i) Wynika z Twierdzeń 2.4 i 2.8.

(ii) Niech $A = \{P_1, \dots, P_N\}$ będzie zbiorem wszystkich parzystych permutacji w S_n i niech T oznacza transpozycję $(1, 2)$. Jeśli $P \in S_n$ jest dowolną permutacją nieparzystą, to na mocy Twierdzenia 2.8 (i) iloczyn PT jest permutacją parzystą, a więc $PT \in A$, tj. przy pewnym i mamy $PT = P_i$, tj. $P = P_iT$. Ponieważ permutacje $P_1T, P_2T, \dots, P_NT$ są wszystkie różne (gdyż z $P_iT = P_jT$ wynika $P_i = P_j$), zatem zbiór $\{P_1T, \dots, P_NT\}$ pokrywa się ze zbiorem wszystkich permutacji nieparzystych, a więc takich permutacji jest tyle samo co permutacji parzystych. Zatem A ma $n!/2$ elementów. $\square$

Podgrupa grupy S_n złożona z wszystkich permutacji parzystych nazywa się *n-tą grupą alternującą* i jest oznaczana przez A_n.

3. Okazuje się, że przy badaniu grup skończonych można się ograniczyć do grup permutacji zbiorów skończonych i ich podgrup:

Twierdzenie 2.9. (Arthur Cayley) *Jeśli G jest grupą n-elementową, to jest ona izomorficzna z pewną podgrupą grupy S_n wszystkich permutacji zbioru n-elementowego.*

Dowód: Niech $G = \{g_1 = e, g_2, \dots, g_n\}$. Każdemu elementowi $g \in G$ przyporządkujemy permutację P_g zbioru $\{1, 2, \dots, n\}$ w następujący sposób: ponieważ dla $i = 1, 2, \dots, n$ mamy $gg_i = g_{n_i}$ przy pewnym $1 \leq n_i \leq n$, a elementy gg_i są wszystkie różne, zatem odwzorowanie $i \mapsto n_i$ jest permutacją zbioru $\{1, 2, \dots, n\}$, którą oznaczymy przez P_g. Zauważmy, że z uwagi na $(gh)g_i = g(hg_i)$ zachodzi równość $P_{gh} = P_gP_h$. Mamy ponadto $P_e = E$ i $P_{g^{-1}} = P_g^{-1}$. To pokazuje, że zbiór $H = \{P_g : g \in G\}$ jest podgrupą S_n. Odwzorowanie $\Psi : G \longrightarrow H$ zadane przez $g \mapsto P_g$ jest wzajemnie jednoznaczne i pozostaje zauważyć, że dla $g, h \in G$ mamy

$$\Psi(gh) = P_{gh} = P_gP_h = \Psi(g)\Psi(h),$$

co dowodzi, że Ψ jest izomorfizmem. $\square$

2.3. Dzielniki normalne. Grupy ilorazowe. Twierdzenia o homomorfizmach i izomorfizmach.

1. Niech H będzie podgrupą grupy G i niech $g \in G$. Zbiór wszystkich iloczynów gh, gdzie h przebiega wszystkie elementy grupy H oznaczamy gH i nazywamy *prawostronną warstwą grupy G względem podgrupy H wyznaczoną przez g*. Podobnie, zbiór

$$Hg = \{hg : h \in H\}$$

nazywamy *lewostronną warstwą grupy G względem podgrupy H wyznaczoną przez g*. Oczywiście, w przypadku grup abelowych pojęcia te się pokrywają.

Twierdzenie 2.10. *Niech G będzie grupą, a H jej podgrupą.*

(i) *Dla każdego $g \in G$ warstwy gH i Hg są równoliczne ze zbiorem H.*

(ii) *Zbiór warstw prawostronnych grupy G względem jej podgrupy H jest równoliczny ze zbiorem warstw lewostronnych.*

(iii) *Jeśli $g_1, g_2 \in G$, to warstwy g_1H i g_2H są bądź rozłączne, bądź równe i to samo dotyczy warstw Hg_1 i Hg_2.*

(iv) *Dwa elementy g_1, g_2 wyznaczają tę samą warstwę prawostronną (lewostronną) względem H wtedy i tylko wtedy, gdy $g_1^{-1}g_2 \in H$ ($g_1g_2^{-1} \in H$).*

Dowód: (i) Odwzorowania $\Psi : H \longrightarrow Hg$ i $\Xi : H \longrightarrow gH$ zadane przez $\Psi(h) = hg$, $\Xi(h) = gh$ są wzajemnie jednoznaczne.

(ii) Odwzorowanie $x \mapsto x^{-1}$ jest różnowartościowe i przeprowadza warstwę prawostronną gH na warstwę lewostroną Hg^{-1}.

(iii) Jeśli warstwy g_1H i g_2H nie są rozłączne, to istnieje $a \in (g_1H) \cap (g_2H)$. Wtedy $a = g_1h_1 = g_2h_2$ przy odpowiednich $h_1, h_2 \in H$, a zatem $g_1 = g_2h_2h_1^{-1} \in g_2H$, co prowadzi do $g_1H \subset g_2H$, a zamieniając w tym rozumowaniu elementy g_1 i g_2 otrzymujemy $g_2H \subset g_1H$, co ostatecznie daje $g_1H = g_2H$.

(iv) Warunek $g_1^{-1}g_2 \in H$ jest równoważny z $g_2 \in g_1H$, a (iii) pokazuje, że to jest równoważne z $g_1H = g_2H$. Podobne rozumowanie działa także w przypadku warstw lewostronnych. □

Ilość elementów w grupie skończonej G nazywamy *rzędem grupy*, a ilość warstw w G względem podgrupy H nazywa się *indeksem* H w G i oznacza przez $[G : H]$.

Wniosek 1. (Twierdzenie Lagrange'a) *Dla skończonych grup $H < G$ mamy*

$$\#G = [G : H] \cdot \#H. \tag{2.6}$$

Dowód: Wynika natychmiast z (i). □

Wniosek 2. *Jeśli grupa G jest skończona, to zarówno rząd jak i indeks każdej jej podgrupy są dzielnikami rzędu grupy.*

Dowód: Wynika z wzoru (2.6). □

Wniosek 3. *Jeśli G jest grupą skończoną, to dla $g \in G$ mamy $o(g)|\#G$.*

Dowód: Wynika z Wniosku 2 i Twierdzenia 2.5 (i). □

Wniosek 4. *Jeśli rząd grupy G jest liczbą pierwszą, to G jest grupą cykliczną.*

Dowód: Jeśli $g \neq e$ jest elementem G to jego rząd jest większy od 1, a ponieważ poprzedni wniosek prowadzi do $o(g)|p$, to $o(g) = p$, a więc grupa cykliczna generowana przez a pokrywa się z G. □

3. Rozpatrzmy $G = S_n$ i $H = A_n$ przy $n \geq 3$. W tym przypadku warstwa prawostronna gA_n wyznaczona przez element $g \in A_n$ pokrywa się z ze zbiorem permutacji parzystych, zaś takaż warstwa wyznaczona przez element $g \in S_n \setminus A_n$ składa się z wszystkich permutacji nieparzystych. Tak samo jest w przypadku warstw lewostronnych, a więc w tym przypadku zachodzi równość $gH = Hg$ mimo, że grupa S_n nie jest abelowa.

Ten przykład prowadzi do kolejnego pojęcia. Mówimy, że podgrupa H grupy G jest jej *dzielnikiem normalnym*, jeśli dla każdego elementu $g \in G$ zachodzi równość $gH = Hg$. Piszemy wówczas $H \triangleleft G$. Wprost z definicji otrzymujemy następujący fakt:

Fakt 2.11. *Na to by podgrupa H grupy G była jej dzielnikiem normalnym potrzeba i wystarcza, by dla wszystkich $g \in G$ i $h \in H$ element ghg^{-1} leżał w H.* □

Zajmiemy się teraz homomorfizmami grup i rozpoczniemy od prostego lematu:

Lemat 2.12. *Jeśli $f : G_1 \longrightarrow G_2$ jest homomorfizmem grup, a przez e_i oznaczymy dla $i = 1, 2$ jedność grupy G_i, to $f(e_1) = e_2$ i dla każdego $g \in G_1$ mamy $f(g^{-1}) = f(g)^{-1}$.*

Dowód: Jeśli $a = f(e_1)$, to $a \cdot a = a^2 = f(e_1^2) = f(e_1) = a = a \cdot e_2$ i z Twierdzenia 2.1 wynika $a = e_2$. Zatem dla $g \in G_1$ mamy

$$e_2 = f(e_1) = f(g)f(g^{-1}),$$

a więc $f(g)^{-1} = f(g^{-1})$. □

Jeśli G_1, G_2 są grupami, $e_2 \in G_2$ jest jednością, a $f : G_1 \longrightarrow G_2$ jest homomorfizmem, to zbiór $\{g \in G_1 : f(g) = e_2\}$ nazywa się *jądrem homomorfizmu* f i oznacza się przez*) $\operatorname{Ker} f$. Obraz grupy G_1 przez homomorfizm f oznaczamy przez $\operatorname{Im} f$.

Twierdzenie 2.13. (i) *Jeśli $f : G_1 \longrightarrow G_2$ jest homomorfizmem grup, to* $\operatorname{Im} f$ *jest podgrupą grupy G_2, a* $\operatorname{Ker} f$ *jest dzielnikiem normalnym grupy G_1.*

(ii) *Na to by homomorfizm $f : G_1 \longrightarrow G_2$ był monomorfizmem potrzeba i wystarcza, by* $\operatorname{Ker} f = \{e\}$.

Dowód: (i) Jeśli $a, b \in \operatorname{Im} f$, to istnieją $x, y \in G$ takie, że $a = f(x), b = f(y)$, a więc wobec Lematu 2.12 mamy $ab^{-1} = f(xy^{-1})$ i możemy skorzystać z Twierdzenia 2.4. Jeśli $g_1, g_2 \in \operatorname{Ker} f$, to $f(g_1g_2^{-1}) =$

*) Od angielskiego słowa "kernel".

$f(g_1)f(g_2)^{-1} = e_2$ i znów skorzystamy z Twierdzenia 2.4 by stwierdzić, że $\mathrm{Ker}\, f$ jest podgrupą G. By pokazać, że jest ona dzielnikiem normalnym zauważmy, że dla $g \in G$, $h \in \mathrm{Ker}\ f$ mamy

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)f(h)f(g)^{-1} = f(g)f(g)^{-1} = e_2,$$

a więc $ghg^{-1} \in \mathrm{Ker}\ f$.

(ii) Jeśli f nie jest monomorfizmem i elementy $a \neq b$ grupy G mają ten sam obraz, tj. $f(a) = f(b)$, to $ab^{-1} \neq e_1$, ale $f(ab^{-1}) = f(a)f(b)^{-1} = e_2$. Wynikanie w drugą stronę jest trywialne. □

Wprowadzimy teraz pojęcie *grupy ilorazowej*. Niech H będzie dzielnikiem normalnym grupy G. Wprowadzimy działanie w zbiorze G/H wszystkich warstw grupy G względem H (ponieważ $H \triangleleft G$, zatem warstwy prawo- i lewostronne się pokrywają), kładąc

$$(g_1H) \cdot (g_2H) = (g_1g_2)H. \tag{2.7}$$

Twierdzenie 2.14. *Jeśli $H \triangleleft G$, to zbiór warstw G/H z działaniem określonym wzorem* (2.7) *jest grupą, a odwzorowanie $\phi :\ G \longrightarrow G/H$ zadane przez $\phi(g) = gH$ jest epimorfizmem.*

Dowód: Musimy wpierw wykazać, że działanie na warstwach, zdefiniowane wzorem (2.7) jest dobrze określone, tj. jego wynik nie zależy od wyboru elementu wyznaczającego warstwę. Jeśli $a_1H = g_1H$ i $a_2H = g_2H$, to z Twierdzenia 2.10 (iv) wynika, że dla $i = 1, 2$ mamy $h_i = g_i^{-1}a_i \in H$. Zatem $a_i = g_ih_i$, a więc $a_1a_2 = g_1h_1g_2h_2$. Ponieważ H jest dzielnikiem normalnym, zatem $h = g_2^{-1}h_1g_2 \in H$, co daje $g_2h = h_1g_2$ oraz

$$a_1a_2 = (g_1g_2)(hh_2) \in g_1g_2H.$$

Korzystając z Twierdzenia 2.10 (iii) otrzymujemy teraz $(a_1a_2)H = (g_1g_2)H$.

Łączność działania w G/H wynika z łączności działania w G, a z (2.7) wynika, że H jest elementem neutralnym w G/H, zaś elementem odwrotnym do gH jest $g^{-1}H$. Widzimy więc, że G/H jest grupą, a stwierdzenie, że ϕ jest homomorfizmem wynika natychmiast z (2.7). Jego surjektywność jest oczywista. □

Odwzorowanie ϕ, występujące w tym twierdzeniu nazywa się *kanonicznym homomorfizmem G na G/H*.

Następujące twierdzenie daje opis wszystkich epimorfizmów zaczynających się w grupie G. Nazywa się go często *zasadniczym twierdzeniem o homomorfizmach dla grup*:

Twierdzenie 2.15. *Niech $f :\ G \longrightarrow G_1$ będzie epimorfizmem i niech H będzie jego jądrem. Oznaczmy przez $\phi :\ G \longrightarrow G/H$ homomorfizm opisany w Twierdzeniu* 2.14. *Wówczas grupy G_1 i G/H są izomorficzne i istnieje dokładnie jeden izomorfizm $\psi :\ G/H \longrightarrow G_1$, taki, że dla $g \in G$ mamy $f(g) = \psi(\phi(g))$, tj.*

$$f = \psi \circ \phi. \tag{2.8.}$$

Dowód: Pokażemy najpierw, że jeśli $gH = g_1H$, to $f(g) = f(g_1)$. W istocie, mamy wówczas $g_1 = gh$ z pewnym $h \in H$, a więc

$$f(g_1) = f(gh) = f(g)f(h) = f(g).$$

To pokazuje, że odwzorowanie $\psi :\ G/H \longrightarrow G_1$ dane wzorem $\psi(gH) = f(g)$ jest dobrze określone. To, że ψ jest homomorfizmem wynika teraz z

$$\psi(g_1H \cdot g_2H) = \psi((g_1g_2)H) = f(g_1g_2) = f(g_1)f(g_2) = \psi(g_1H)\psi(g_2H).$$

Surjektywność ψ jest konsekwencją surjektywności homomorfizmu $f : G \longrightarrow G_1$, a gdyby ψ nie był monomorfizmem, to z Twierdzenia 2.13 (ii) otrzymalibyśmy element $gH \in G/H$, różny od H, spełniający $\psi(gH) = e$, ale wówczas $e = \psi(gH) = f(g)$, co prowadzi do $g \in \mathrm{Ker}\ f = H$, a więc $gH = H$, sprzeczność.

Pozostaje wykazać jedyność izomorfizmu ψ, spełniającego (2.8). Jeśli $\Psi :\ G/H \longrightarrow G_1$ spełnia $f = \Psi \circ \phi$ i $\Psi \neq \psi$, to istnieje warstwa $gH \in G/H$, dla której mamy $\Psi(gH) \neq \psi(gH)$, ale wobec $\phi(g) = gH$ prowadzi to do

$$f(g) = \Psi(\phi(g)) = \Psi(gH) \neq \psi(gH) = \psi(\phi(g)) = f(g),$$

co jest jawnie niemożliwe. $\square$

Przykłady:

1. *Jeśli* $\mathbb{R}^+, \mathbb{Z}^+$ *są grupami liczb rzeczywistych i całkowitych z dodawaniem, zaś* T *jest grupą liczb zespolonych o module* 1 *z mnożeniem, to*

$$\mathbb{R}^+/\mathbb{Z}^+ \sim \mathbb{T}.$$

Rozpatrzmy odwzorowanie $f:\ \mathbb{R}^+ \longrightarrow \mathbb{T}$ zadane wzorem $f(x) = e^{2\pi ix}$. Ponieważ $f(x+y) = e^{2\pi i(x+y)} = e^{2\pi ix} \cdot e^{2\pi iy} = f(x)f(y)$, zatem f jest homomorfizmem. Surjektywność jest jasna, a

$$\text{Ker } f = \{x \in \mathbb{R}^+ :\ {\nvDash\pi\sqsupset\frown} = \nVdash\} = \mathbb{Z}^+$$

i pozostaje zastosować twierdzenie 2.15.

2. *Jeśli* $GL_n(\mathbb{R})$ *jest grupą odwracalnych macierzy* $n \times n$ *o elementach z* $\mathbb{R}$ *z mnożeniem, a* $SL_n(\mathbb{R})$ *jest jej podgrupą złożoną z macierzy o wyznaczniku* 1*, to*

$$GL_n(\mathbb{R})/\mathbb{SL}_{\ltimes}(\mathbb{R}) \sim \mathbb{R}^*,$$

gdzie $\mathbb{R}^*$ *jest grupą niezerowych liczb rzeczywistych z mnożeniem.*

To wynika z rozpatrzenia homomorfizmu $f:\ GL_n(\mathbb{R}) \longrightarrow \mathbb{R}^*$ zadanym przez wyznacznik ($f(\mathfrak{A}) = \det \mathfrak{A}$).

3. $S_n/A_n \sim C_2$.

Bo $[S_n : A_n] = 2$, a z Wniosku 4 z Twierdzenia 2.10 wynika, że każda grupa 2-elementowa jest cykliczna.

3. Udowodnimy teraz dwa twierdzenia, które dotyczą podgrup ustalonej grupy G. Jeśli H, K są podgrupami G, to łatwo sprawdzić, korzystając z Twierdzenia 2.4, że ich część wspólna $K \cap H$ również jest podgrupą G. Będziemy także rozpatrywać najmniejszą podgrupę G, zawierającą zarówno H jak i K. Jej istnienie wynika z pierwszej części następującego lematu:

Lemat 2.16. (i) *Jeśli* A *jest niepustym podzbiorem grupy* G*, a* $G(A)$ *jest częścią wspólną wszystkich podgrup grupy* G*, zawierających* A*, to* $G(A)$ *jest podgrupą o tej własności, że jeśli* $G_1 < G$ *zawiera* A*, to* $G(A) < G_1$.

(ii) Jeśli $K \lhd G$ *i* $H \lhd G$*, to najmniejsza podgrupa* G*, zawierająca* H *i* K *pokrywa się ze zbiorem*

$$KH := \{kh :\ k \in K, h \in H\}.$$

Dowód: (i) Wystarczy pokazać, że $G(A)$ jest podgrupą G. Jeśli $a, b \in G(A)$, to a, b leżą w każdej podgrupie zawierającej A, a więc ab^{-1} ma tę samą własność.

(ii) Wystarczy wykazać, że KH jest podgrupą G. W tym celu rozpatrzmy dla $k_i \in K$, $h_i \in H$ $(i = 1, 2)$ element

$$(k_1h_1)(k_2h_2)^{-1} = k_1h_1h_2^{-1}k_2^{-1} = (k_1k_2^{-1})(k_2h_1h_2^{-1}k_2^{-1})$$

i zauważmy, że $k_2h_1h_2^{-1}k_2^{-1} \in H$. $\square$

Twierdzenie 2.17. (Pierwsze twierdzenie o izomorfizmach.) *Jeśli* $K \lhd G$ *i* $H \lhd G$*, to*

(i) $K < KH = HK < G$,

(ii) $H \cap K \lhd H$ *i* $K \lhd KH$,

(iii) Odwzorowanie $\phi :\ hK \mapsto h(K \cap H)$ *indukuje izomorfizm*

$$HK/K \sim H/(H \cap K).$$

Dowód: (i) Wobec Lematu 2.16 (ii) zbiór KH jest podgrupą G. Jeśli $k \in K, h \in H$, to $h_1 = khk^{-1} \in H$, więc $kh = h_1k \in HK$, co daje $KH \subset HK$. Przez symetrię założenia mamy także $HK \subset KH$, a więc $KH = HK$.

(ii) Jeśli $a \in H \cap K$ i $h \in H$, to $h^{-1}ah \in H$, a z uwagi na $K \lhd G$ mamy $h^{-1}ah \in K$, tj. $H \cap K \lhd H$. Druga część wynika z tego, że K jest dzielnikiem normalnym w G, a więc i w każdej podgrupie G, zawierającej K.

(iii) Jest jasne, że ϕ jest surjektywnym homomorfizmem grupy HK/K w $H/(H \cap K)$ i wystarczy wyznaczyć jego jądro:

$$\mathrm{Ker}\ \phi = \{hK:\ h(K \cap H) = K \cap H\} = \{hK:\ h \in K \cap H\} = \{eK\} = \{K\}. \qquad \square$$

4. Twierdzenie 2.18. (Drugie twierdzenie o izomorfizmach (najważniejsza część).) *Jeśli $K \lhd G$ i $K < H < G$ i oznaczymy $\overline{H} = H/K$ i $\overline{G} = G/K$, to*

(i) $\overline{H} < \overline{G}$,

(ii) $\overline{H} \lhd \overline{G}$ zachodzi wtedy i tylko wtedy, gdy $H \lhd G$. Mamy wówczas

$$G/H \sim \overline{G}/\overline{H}.$$

Dowód: (i) jest konsekwencją $H < G$.

(ii) Jeśli $H \lhd G$, to dla $g \in G, h \in H$ mamy

$$g^{-1}K \cdot hK \cdot gK = (g^{-1}hg)K = h_1K \in \overline{H},$$

gdzie $h_1 = g^{-1}hg \in H$. Zatem $\overline{H} \lhd \overline{G}$.

Jeżeli $\overline{H} \lhd \overline{G}$, to

$$g^{-1}K \cdot hK \cdot gK = h_1K \in \overline{H},$$

a zatem $g^{-1}hgK = h_1K$, co daje $g^{-1}hg = h_1k \in H$ z pewnym $k \in K$.

Jeśli warunek z (ii) jest spełniony i $\psi : G \longrightarrow \overline{G}$ jest kanonicznym homomorfizmem, to $\phi = \psi_{|H}$ jest kanonicznym homomorfizmem H na $\overline{H}$. Jeśli

$$\rho : \overline{G} \longrightarrow \overline{G}/\overline{H}$$

jest homomorfizmem kanonicznym, to złożenie

$$\alpha :\ G \xrightarrow{\psi} G/K = \overline{G} \xrightarrow{\rho} \overline{G}/\overline{H}$$

jest surjektywne. Pozostaje wyznaczyć $\mathrm{Ker}\,\alpha$:

$$g \in \mathrm{Ker}\ \alpha \iff \psi(g) \in \overline{H} \iff gK \in H/K \iff g \in H,$$

a więc $\mathrm{Ker}\ \alpha = H$. $\square$

5. Twierdzenie 2.19. *Przy ustalonym elemencie $g \in G$ odwzorowanie $\phi_g :\ G \longrightarrow G$ zadane przez*

$$\phi_g(x) = g^{-1}xg$$

jest automorfizmem.

Dowód: Dla $x, y \in G$ mamy

$$\phi_g(xy) = g^{-1}xyg = g^{-1}xgg^{-1}yg = \phi_g(x)\phi_g(y),$$

a więc ϕ_g jest endomorfizmem. Jeśli $x \in \mathrm{Ker}\,\phi_g$, to $g^{-1}xg = e$, a zatem

$$xg = gg^{-1}xg = ge = g$$

i widzimy, że $x = e$. Pozostaje wykazać surjektywność ϕ_g, a to wynika z równości

$$\phi(gxg^{-1}) = g^{-1}gxg^{-1}g = x \qquad (2.9.) \qquad \square$$

Automorfizm ϕ_g, występujący w tym twierdzeniu nazywa się *automorfizmem wewnętrznym grupy G, wyznaczonym przez g.* Zauważmy, że jeśli grupa G jest abelowa, to dla wszystkich $g, x \in G$ mamy $\phi_g(x) = x$, a więc jedynym automorfizmem wewnętrznym takiej grupy jest identyczność. Zbiór wszystkich automorfizmów wewnętrznych grupy G oznaczamy przez $I(G)$.

5. Zbiór wszystkich elementów $x \in G$ takich, że dla dowolnego $y \in G$ mamy $xy = yx$ nazywamy *centrum* grupy G i oznaczamy przez $Z(G)$. Poniższe twierdzenie pokazuje związek tego pojęcia z automorfizmami wewnętrznymi:

Twierdzenie 2.20. (i) *Zbiór $I(G)$ tworzy grupę ze względu na składanie.*

(ii) *Dla każdej grupy G mamy $Z(G) \triangleleft G$.*

(iii) *Grupa $I(G)$ jest izomorficzna z grupą ilorazową $G/Z(G)$.*

Dowód: (i) Z (2.9) wynika, że $\phi_{g^{-1}}$ jest automorfizmem wewnętrznym, odwrotnym do ϕ_g, tj. $\phi_g^{-1} = \phi_{g^{-1}}$, automorfizm ϕ_e jest elementem neutralnym i pozostaje zauważyć, że dla $g, h, x \in G$ mamy

$$(\phi_g \phi_h)(x) = (\phi_g(\phi_h(x)) = g^{-1}h^{-1}xhg = \phi_{hg}(x),$$

a więc

$$(\phi_g \phi_h)(x) = \phi_{hg}(x). \tag{2.10}$$

(ii) Jeśli $g \in G, h \in Z(G)$, to $ghg^{-1} = hgg^{-1} = h \in Z(G)$.

(iii) Rozpatrzmy odwzorowanie $\Psi : \ G \longrightarrow I(G)$ zadane przez $\Psi(g) = \phi_{g^{-1}}$. Podstawiając w (2.10) h^{-1} w miejsce h i g^{-1} w miejsce g otrzymujemy

$$\phi_{g^{-1}}\phi_{h^{-1}} = \phi_{h^{-1}g^{-1}} = \phi_{(gh)^{-1}},$$

a więc

$$\Psi(g)\Psi(h) = \Psi(gh)$$

i widzimy, że Ψ jest homomorfizmem. Ponieważ jądrem Ψ jest zbiór tych $g \in G$ dla których przy dowolnym $x \in G$ mamy

$$x = \phi_{g^{-1}}(x) = gxg^{-1},$$

tj. $xg = gx$, zatem $\operatorname{Ker} \Psi = Z(G)$ i możemy skorzystać z Twierdzenia 2.15. $\square$

Dla skrótu piszemy $\phi_g(x) = x^g$. Z dowodu części (i) Twierdzenia 2.20 i z (2.10) wynikają wzory

$$(x^h)^g = x^{hg}, \quad (x^g)^{-1} = (x^{-1})^g. \tag{2.11}$$

Jeśli M jest podzbiorem grupy G, to przez M^g oznaczamy obraz M przez automorfizm ϕ_g, tj.

$$M^g = \{x^g : \ x \in M\}.$$

Każdy ze zbiorów M^g nazywamy *zbiorem sprzężonym* M. Jeśli, w szczególności, $M = \{x\}$ jest zbiorem jednoelementowym, to elementy x^g $(g \in G)$ nazywamy *elementami sprzężonymi* z x. Zbiór

$$N_G(M) = \{g \in G : \ M^g = M\}$$

nazywamy *normalizatorem* zbioru M, a zbiór

$$C_G(M) = \{g \in G : \ mg = gm \text{ dla } m \in M\}$$

nazywamy *centralizatorem* M.

Twierdzenie 2.21. *Niech G będzie grupą.*

(i) *Dla każdego zbioru $M \subset G$ mamy $C_G(M) < N_G(M) < G$, a jeśli M jest jednoelementowy, to $C_G(M) = N_G(M)$.*

(ii) $Z(G) = C_G(G)$.

(iii) *Jeśli* $M \subset G$, *to ilość różnych zbiorów* M^g *jest równa indeksowi normalizatora, tj.* $[G : N_G(M)]$.

Dowód: Wprost z definicji otrzymujemy (i) i (ii), a by wykazać (iii) zauważmy, że jeśli $g = nh$ przy $n \in N_G(M)$, to

$$M^g = M^{nh} = (M^n)^h = M^h,$$

a jeśli $M^g = M^h$, to

$$M^{gh^{-1}} = (M^g)^{h^{-1}} = M,$$

wiec $n = gh^{-1} \in N_G(M)$. Zatem zbiory M^g są w odpowiedniości wzajemnie jednoznacznej z lewostronnymi warstwami względem normalizatora. $\square$

Wniosek 1. *Na to by klasa elementów sprzężonych z* $x \in G$ *była jednoelementowa potrzeba i wystarcza by* $x \in Z(G)$.

Dowód: Niech $M = \{x\}$. Jeśli x leży w centrum G, to z (i) wynika $N_G(M) = C_G(M) = G$, a teraz (iii) pokazuje, że klasa sprzężonych z x jest jednoelementowa.
Jeśli klasa sprzężonych z x jest jednoelementowa, to $C_G(M) = N_G(M) = G$, a więc $x \in Z(G)$. $\square$

Wniosek 2. *Jeśli* G *jest skończona, to ilość elementów sprzężonych z zadanym elementem* $x \in G$ *jest dzielnikiem* $\#G$.

Dowód: Stosujemy (iii) do zbioru $M = \{x\}$. $\square$

6. Niech p będzie liczbą pierwszą. Grupa G nazywa się *p-grupą*, jeśli rząd każdego elementu jest potęgą liczby p.

Fakt 2.22. *Jeśli* $\#G = p^n$, *to* G *jest p-grupą.*

Dowód: To wynika z twierdzenia Lagrange'a. $\square$

Dla grup skończonych twierdzenie odwrotne jest też prawdziwe, będzie ono udowodnione nieco później.

Twierdzenie 2.23. *Skończone p-grupy mają nietrywialne centrum.*

Dowód: Niech $\#G = p^r$ z $r \geq 1$ i przedstawmy G jako rozłączną sumę klas elementów sprzężonych:

$$G = K_1 \cup \cdots \cup K_m,$$

przy czym $K_1 = \{e\}$. Gdyby $Z(G) = \{e\}$, to z Wniosku 2 z Twierdzenia 2.22 wynikałoby, że ilość elementów w każdej z klas K_i $(i \neq 0)$ byłaby dzielnikiem p^r większym od 1, a więc dzieliłaby się przez p. Zatem $p^r = \#G \equiv 1 \pmod p$, co nie jest możliwe. $\square$

Wniosek: *Jeśli* $\#G = p^2$, *gdzie* p *jest liczbą pierwszą, to* G *jest abelowa.*

Dowód: Skorzystamy tu z uwagi, że jeśli p jest liczbą pierwszą, a $d \in \mathbb{N}$ dzieli p^2, to $d \in \{1, p, p^2\}$. W istocie, z Lematu 1.9 otrzymujemy, że jedynym dzielnikiem pierwszym takiej liczby d jest p, a więc d jest potęgą liczby p, nie przekraczającą p^2.

Załóżmy, że G nie jest abelowa. Niech h będzie nietrywialnym elementem $Z(G)$ i niech H będzie grupą cykliczną, generowaną przez h. Ponieważ H jest abelowa, zatem $H \neq G$, a ponieważ $\#H$ dzieli $\#G = p^2$, przeto H ma p elementów. Niech $g \in G \setminus H$ i niech K będzie grupą, generowaną przez g i h. Wówczas $H < K < G$, zatem $p = \#H < \#K \leq p^2$ i z twierdzenia Lagrange'a otrzymamy $\#K = p^2$, a więc $K = G$. Pozostaje zauważyć, że z uwagi na $gh = hg$ grupa K jest abelowa. $\square$

2.4. Produkty grup, sumy proste grup abelowych.

1. Jeśli A, B są grupami, to w zbiorze par $A \times B = \{(a, b) : \ a \in A, b \in B\}$ wprowadzamy działanie wzorem

$$(a, b) \cdot (c, d) = (ac, bd).$$

Twierdzenie 2.24. (i) *Z tak określonym działaniem $A \times B$ staje się grupą.*

(ii) *Grupa $A \times B$ zawiera podgrupy A_1, B_1, spełniające następujące warunki*:

(α) $A_1 \sim A$, $B_1 \sim B$,

(β) $A_1 \cap B_1 = \{e\}$,

(γ) *Każdy element $g \in G$ zapisuje się na jeden sposób w postaci $g = ab$ przy $a \in A_1$, $b \in B_1$,*

(δ) *Dla $x \in A_1$, $y \in B_1$ mamy $xy = yx$.*

Dowód: (i) Łączność działania jest konsekwencją łączności w grupach A, B. Jeśli e_A, e_B są jednościami grup A,B i przyjmiemy $e = (e_A, e_B)$, to

$$e \cdot (a, b) = (a, b) \cdot e = (a, b),$$

więc e jest elementem neutralnym w $A \times B$. Pozostaje zauważyć, że

$$(a, b)(a^{-1}, b^{-1}) = (a^{-1}, b^{-1})(a, b) = e.$$

(ii) Niech $A_1 = \{(a, e_B) : \ a \in A\}$, $B_1 = \{(e_A, b) : \ b \in B\}$. Łatwo sprawdzić, że odwzorowania $a \mapsto (a, e_B)$ i $b \mapsto (e_A, b)$ są izomorfizmami, co prowadzi do (α). Warunek (β) jest oczywisty, (γ) i (δ) wynikają z równości

$$(a, b) = (e_A, b)(a, e_B),$$

a by sprawdzić (δ) zauważmy, że jeśli $x = (a, e_B)$, $y = (e_A, b)$, to $xy = (a, b) = yx$. ☐

Wniosek: *Grupy A_1, B_1, pojawiające się w twierdzeniu są dzielnikami normalnymi grupy $A \times B$, a przy tym mamy*

$$(A \times B)/A_1 \sim B, \quad (A \times B)/B_1 \sim A.$$

Dowód: Pierwsza część jest konsekwencją warunku (δ). By udowodnić pierwszy izomorfizm z części drugiej wystarczy zauważyć, że odwzorowanie $(a, b) \mapsto b$ jest epimorfizmem $A \times B \longrightarrow B$, którego jądro jest równe A_1. Drugi izomorfizm dowodzi się podobnie. ☐

Następujący wynik pozwala na stwierdzenie, czy dana grupa jest produktem:

Twierdzenie 2.25. *Niech A, B będą podgrupami grupy G. Jeśli spełnione są następujące warunki:*

(i) $A \cap B = \{e\}$,

(ii) Dla $a \in A$, $b \in B$ mamy $ab = ba$,

(iii) $AB = G$, tj. każdy element G da się przedstawić w postaci ab, gdzie $a \in A$, $b \in B$,

to grupa G jest izomorficzna z produktem $A \times B$.

Dowód: Rozpatrzmy odwzorowanie $\Phi : \ A \times B \longrightarrow G$, zadane przez $(a, b) \mapsto ab$. Jest to homomorfizm, gdyż korzystając z (ii) mamy

$$\Phi((a, b)(c, d)) = \Phi((ac, bd)) = acbd = abcd = \Phi((a, b))\Phi((c, d)).$$

Surjektywność Φ jest konsekwencją (iii), a by wykazać injektywność zauważmy, że jeśli $(a, b) \in \operatorname{Ker}\Phi$, to $ab = e$, a zatem $b = a^{-1} \in A$ i widzimy, że $b \in A \cap B = \{e\}$, tj. $b = e$, co z uwagi na $a = b^{-1}$ daje $a = e$. ☐

2. Produkt grup definiuje się także dla większej liczby czynników. Jeśli $A_1, A_2, \ldots, A_n$ są grupami, to ich produktem

$$\prod_{i=1}^{n} A_i$$

nazywamy grupę, której elementami są ciągi $(a_1, a_2, \ldots, a_n)$ z $a_i \in A_i$, a mnożenie jest zdefiniowane przez

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n). \tag{2.12}$$

Zachodzi tu analogon Twierdzenia 2.24:

Twierdzenie 2.24a. (i) *Z działaniem określonym przez* (2.12) *produkt* $P = \prod_{i=1}^{n} A_i$ *staje się grupą.*

(ii) *Grupa* P *zawiera podgrupy* $B_1, \ldots, B_n$, *spełniające następujące warunki*:

(α) $A_i \sim B_i$ dla $i = 1, 2, \ldots, n$,

(β) Dla każdego j przekrój grupy B_j i grupy generowanej przez wszystkie pozostałe grupy B_i jest równy $\{e\}$,

(γ) *Każdy element* $g \in G$ *zapisuje się na jeden sposób w postaci* $g = b_1 \cdots b_n$ *przy* $b_i \in B_1$,

(δ) *Dla* $i \neq j$ *i* $x \in B_i$, $y \in B_j$ *mamy* $xy = yx$.

Nietrudny dowód indukcyjny pozostawiam do samodzielnego opracowania, podobnie jak sformułowanie analogonu Twierdzenia 2.25.

Zupełnie podobnie definiuje się produkt nieskończonej ilości grup:

Jeśli T jest dowolnym zbiorem indeksów, a dla każdego $\tau \in T$ jest zadana grupa A_τ, to produkt

$$\prod_{\tau \in T} A_\tau$$

jest grupą, której elementy są elementami (a_τ) produktu mnogościowego grup A_τ, a mnożenie jest zdefiniowane przez

$$(a_\tau) \cdot (b_\tau) = (a_\tau b_\tau).$$

Definiuje się także *produkt ograniczony* grup A_τ, którego elementami są te elementy produktu $(a_\tau) \in \prod_{\tau \in T} A_\tau$, dla których a_τ jest różne od jedności jedynie dla skończenie wielu τ. W przypadku, gdy zbiór T jest skończony, rozróżnienie pomiędzy produktem a produktem ograniczonym jest nieistotne.

W przypadku, gdy grupy A_τ są abelowe ich produkt ograniczony nazywamy *sumą prostą* i oznaczamy przez $A_1 \oplus \cdots \oplus A_n$ gdy mamy do czynienia z kilkoma grupami, a przez $\bigoplus_\tau A_\tau$ w ogólnym przypadku. Stosuje się to zasadniczo wówczas, gdy działanie oznaczone jest symbolem " + ".

2.5. Grupy przekształceń.

1. Niech X będzie niepustym zbiorem, a G grupą. Mówimy, że *grupa* G *działa na* X, jeśli z każdym elementem $g \in G$ związana jest pewna permutacja ϕ_g zbioru X, przy czym spełniony jest warunek $\phi_{gh} = \phi_g \circ \phi_h$, a więc odwzorowanie $g \mapsto \phi_g$ jest homomorfizmem G w grupę $S(X)$ permutacji zbioru X. *Orbitą punktu* $x \in X$ nazywamy zbiór $O(x) = \{\phi_g(x) : \ g \in G\}$.

Przykłady: 1. Jeśli $X = \mathbb{R}^{\mathbb{N}}$ jest N-wymiarową przestrzenią liniową z ustaloną bazą $\omega_1, \ldots, \omega_N$, to działanie grupy liniowej $GL_N(\mathbb{R})$ na $\mathbb{R}^{\mathbb{N}}$ może być zadane w następujący sposób: jeśli $\mathfrak{A}$ jest przekształceniem liniowym o macierzy $M \in GL_N(\mathbb{R})$, a v jest wektorem w $\mathbb{R}^{\mathbb{N}}$, to kładziemy $\phi_M(v) = \mathfrak{A}v^T$, przy czym v^T jest wektorem transponowanym do v.

2. Zbiór wszystkich izometrii płaszczyzny (lub ogólniej, dowolnej przestrzeni euklidesowej) jest grupą, która w sposób naturalny działa na płaszczyźnie (lub przestrzeni euklidesowej).

Stabilizatorem $S_G(x)$ punktu x nazywamy zbiór $\{g \in G : \ \phi_g(x) = x\}$.

Twierdzenie 2.26. (i) Stabilizator $S_G(x)$ *jest podgrupą* G, *której indeks jest równy ilości elementów w orbicie* $O(x)$.

(ii) Jeśli elementy x, y *leżą w tej samej orbicie, to ich stabilizatory są sprzężone.*

Dowód: (i) Pierwsza własność jest trywialna. Jeśli $\phi_g(x) = \phi_h(x)$, to

$$\phi_{h^{-1}g}(x) = \phi_{h^{-1}}(\phi_g(x)) = \phi_{h^{-1}}(\phi_h(x)) = x,$$

tj. $h^{-1}g \in S_G(x)$, tj. $gS_G(x) = hS_G(x)$ i naodwrót. Zatem elementy orbity x odpowiadają warstwom względem stabilizatora.

(ii) Jeśli x, y leżą w tej samej orbicie, to istnieje $h \in G$ z $y = \phi_h(x)$. Zatem

$$\begin{aligned} S_G(y) = \ & S_G(\phi_h(x)) = \{g : \ \phi_g(\phi_h(x)) = \phi_h(x)\} \\ = \ & \{g : \ \phi_{h^{-1}gh}(x) = x\} = \{g : \ h^{-1}gh \in S_G(x)\} \\ & = \{g : \ g = hS_G(x)h^{-1}\} = S_G^{h^{-1}}(x). \end{aligned}$$

Wniosek: *Jeśli skończona p-grupa działa na zbiorze X, a p nie dzieli $\#X$, to istnieje $x \in X$ taki, że dla $g \in G$ mamy $\phi_g(x) = x$, tj. $S_G(x) = G$.*

Dowód: Zapiszmy X jako sumę rozłącznych orbit:

$$X = O_1 \cup O_2 \cup \cdots \cup O_m.$$

Z twierdzenia wynika, że dla $j = 1, 2, \ldots, m$ mamy $O_j = p^{c_j}$ z pewnymi $c_j \geq 0$. Zatem

$$\#X = \sum_{j=1}^{m} p^{c_j},$$

a ponieważ lewa strona tej równości nie dzieli się przez p, zatem po prawej stronie któryś z wykładników c_j musi być równy zeru. $\square$

2. Twierdzenia Sylowa.

Twierdzenie 2.27. (Pierwsze twierdzenie Sylowa.) *Jeśli p jest liczbą pierwszą , a G jest grupą skończoną, $\#G = N = p^k m$, przy czym $k \geq 1$ i $p \nmid m$, to istnieje podgrupa H grupy G, mająca p^k elementów.*

(Taka grupa nazywa się *podgrupą Sylowa*.)

Dowód: Oznaczmy $q = p^k$ i niech X będzie rodziną wszystkich q-elementowych podzbiorów grupy G. Określimy działanie grupy G na zbiorze X następująco:

Jeśli $\xi = \{h_1, \ldots, h_q\} \in X$, a $g \in G$, to

$$\phi_g(\xi) = \{gh_1, \ldots, gh_q\}.$$

1 krok: $p \nmid \#X$.

Mamy

$$\#X = \binom{N}{q} = \binom{p^k m}{p^k}$$
$$= \frac{(p^k m)(p^k m - 1) \cdots (p^k(m-1) + 1)}{p^k!} = \prod_{j=1}^{p^k} \frac{p^k(m-1) + j}{j},$$

ale, z uwagi na $j \leq p^k$, liczby $p^k(m-1) + j$ oraz j dzielą się przez tę samą potęgę liczby p.

Wniosek: *Istnieje orbita O, spełniająca $p \nmid \#O$.*

Bo X jest sumą orbit rozłącznych.

2 krok: Jeśli O jest orbitą, dla której $p \nmid \#O$ oraz $\xi \in O$, to p^k dzieli $\#S_G(\xi)$, a więc $p^k \leq \#S_G(\xi)$.

Wiemy, że $[G : S_G(\xi)] = \#O$ nie dzieli się przez p i pozostaje zauważyć, że z

$$p^k | p^k m = \#G = \#O \cdot \#S_G(a)$$

wynika $p^k | \#S_G(\xi)$.

Ostatni krok: Jeśli $\xi = \{h_1, \dots, h_q\} \in O$, gdzie O jest takie jak w kroku 2, to $S_G(\xi) = \xi$, tj. dla $g \in S_G(\xi)$ mamy $gh_i = h_j$ z pewnym j, a więc $gh_i \in \xi$, co możemy zapisać w postaci $S_G(\xi)h_i \subset \xi$. Porównując ilości elementów otrzymujemy teraz, korzystając z kroku 2:

$$p^k = q \leq \#S_G(\xi) = \#(S_G(\xi)g_i) \leq \#\xi = q,$$

a więc $S_G(\xi) = p^k$. □

Wniosek 1: (Twierdzenie Cauchy'ego.) *Jeśli liczba pierwsza p dzieli rząd grupy G, to G zawiera element rzędu p.*

Dowód: Niech H będzie podgrupą Sylowa grupy G, odpowiadającą liczbie p. Jeśli $a \neq e$ jest jej elementem, to jego rząd jest postaci p^r. Wówczas element $a^{p^{r-1}}$ ma rząd p. □

Wniosek 2. *Jeśli G jest skończoną p-grupą, to jej rząd jest potęgą p.*

Dowód: Gdyby istniała liczba pierwsza $q \neq p$ dzieląca rząd G, to wobec poprzedniego wniosku istniałby w G element rzędu q, wbrew założeniu. □

Twierdzenie 2.28. (Drugie twierdzenie Sylowa.) (i) *Każda p-podgrupa grupy G jest podgrupą pewnej podgrupy Sylowa.*

(ii) Wszystkie p-podgrupy Sylowa są sprzężone.

Dowód: (i) Niech H będzie p-podgrupą G. Orbita O, występującą w dowodzie poprzedniego twierdzenia, spełnia $p \nmid \#O$, a przy tym stabilizator $S_G(\xi)$ elementu $\xi \in O$ jest podgrupą Sylowa. Grupa H działa na O, a więc istnieje element $\eta \in O$, niezmienniczy względem tego działania, tj. $\phi_h(\eta) = \eta$ zachodzi dla wszystkich $h \in H$. To pokazuje, że $H < S_G(\eta)$, a $S_G(\eta)$ jest podgrupą Sylowa.

(ii) Niech U będzie dowolną p-podgrupą Sylowa grupy G. Stosując poprzednie rozumowanie widzimy, że $U = S_G(\eta)$ dla pewnego η z orbity O. Pozostaje przypomnieć, że wobec Twierdzenia 2.26 (ii) stabilizatory elementów tej samej orbity są sprzężone. □

Z twierdzeń Sylowa wyprowadzimy teraz pewien rezultat o grupie A_5, który pozwala na rozstrzygnięcie pytania o istnienie wzorów na rozwiązanie równań stopnia ≥ 5. Mówimy, że grupa G jest *grupą prostą*, gdy nie zawiera nietrywialnych (tj. różnych od G i $\{e\}$) dzielników normalnych. Takimi grupami są np. grupy C_p dla pierwszych p.

Wniosek. *Grupa A_5 jest prosta.*

Dowód: Grupa A_5 ma $5!/2 = 60 = 2^2 \cdot 3 \cdot 5$ elementów. Jej elementy różne od jedności mają następujące postacie:

$$(abcde) \text{ rzędu } 5, \ (abc) \text{ rzędu } 3 \text{ i } (ab)(cd) \text{ rzędu } 2,$$

przy czym liczby a, b, c, d, e tu występujące są różne.

Wynika stąd, że grupa A_5 zawiera 15 elementów rzędu 2, $\frac{5 \cdot 4 \cdot 3}{3} = 20$ elementów rzędu 3 i $5!/5 = 24$ elementy rzędu 5.

Załóżmy, że $\{1\} \neq N \triangleleft A_5$, ale $N \neq A_5$. Zatem $1 < \#N \leq 30$. Ponieważ p-podgrupy Sylowa są sprzężone, a N, jako dzielnik normalny, jest zamknięta na sprzężenia, zatem jeśli $p | \#N$, to N zawiera wszystkie te p-podgrupy, a zatem, wobec Twierdzenia 2.28 (i), zawiera wszystkie elementy rzędu p.

Tak więc jeśli $3 | \#N$, to N zawiera wszystkie elementy rzędu 3, a jest ich 20, co pokazuje, że $\#N \geq 21$, co jest możliwe jedynie gdy $\#N = 30$.

Jeśli zaś $5 | \#N$, to podobnie otrzymujemy $\#N \geq 25$ i $\#N = 30$.

Jeśli więc $\#N$ dzieli się przez 3 lub 5, to $\#N = 30$. Ponieważ 30 dzieli się zarówno przez 3 jak i przez 5, zatem poprzednie rozumowanie pokazuje, że N zawiera wszystkie elementy A_5 o rzędach 3 i 5, a zatem $30 = \#N \geq 20 + 24 + 1 = 46$, sprzeczność.

Pozostaje przypadek, gdy $\#N$ nie dzieli się ani przez 3, ani przez 5. Ponieważ $\#N$ dzieli 60, zatem $\#N \in \{2, 4\}$. Gdyby $\#N = 2$, to $N = \{1, (ab)(cd)\}$, ale

$$(abc)(ab)(cd)(cba) = (ad)bc) \notin N,$$

sprzeczność.

Jeśli $\#N = 4$, to N jest 2-podgrupą Sylowa grupy A_5. Ponieważ wobec Twierdzenia 2.28 (ii) wszystkie inne 2-podgrupy Sylowa są z nią sprzężone, to z normalności N wynika, że jest to jedyna 2-podgrupa Sylowa grupy A_n. To nie jest możliwe, bo musiałaby ona zawierać wszystkie elementy rzędu 2, a jest ich $15 > 4$. □

Wydaje się, że znamy wszystkie skończone grupy proste. Dowód tego faktu, zawarty w kilkuset pracach napisanych w ciągu 120 lat jest obecnie sprawdzany.

Znamy 17 serii nieskończonych (np. A_n $(n \geq 5)$, $PSL_n(F_q)$ $(n \geq 3,\ q \neq 2, 3)$,...,) oraz 26 grup prostych, nie należących do żadnej z serii. Są to tzw. *sporadyczne grupy proste*. Największe z nich to grupy nazwane *Monster* i *Baby-Monster*, znalezione dopiero w 1980 r. Są to grupy bardzo duże, np. Monster ma

$$2^{46}3^{20}5^{9}7^{6}11^{2}13^{3} \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

elementów. Grupa ta jest grupą obrotów w przestrzeni euklidesowej wymiaru 196 883.

Najwcześniej znaleziona grupa sporadyczna, to grupa Mathieu M_{11} odkryta w 1860 roku. Jest to podgrupa grupy S_{11}, generowana przez permutacje

$$(1, 2, \ldots, 11), \quad (5, 6, 4, 10)(11, 8, 3, 7)$$

.

2.6. Struktura skończonych grup abelowych

Twierdzenie 2.29. *Jeśli A jest skończoną grupą abelową, to jest ona bądź p-grupą, bądź też sumą prostą swoich Sylowskich p-podgrup.*

Dowód: Oznaczmy przez $p(G)$ największą liczbę pierwszą, dzielącą rząd grupy G. Zastosujemy indukcję względem $p(A)$. Jeśli $p(A) = 2$, to A jest 2-grupą i teza jest oczywista. Załóżmy, że teza jest słuszna dla grup G z $p(G) < p$ i niech $p(A) = p$ i $\#A = p^m Q$, przy czym p nie dzieli Q.

Jeśli $Q = 1$, to A jest p-grupą i nie ma czego dowodzić. Załóżmy przeto, że $Q > 1$. Niech A_p będzie p-podgrupą Sylowa grupy A. Ponieważ A jest abelowa, grupa A_p jest jedyną p-podgrupą Sylowa, a zatem zawiera wszystkie elementy A, których rząd jest potęga p. Wynika to z uwagi, że w grupie abelowej rząd iloczynu dzieli iloczyn rzędów czynników i z Twierdzenia 2.28 (i).

Zauważmy teraz, że

$$A'_p = \{a \in A : \ p \nmid o(a)\}$$

jest podgrupą A. Ponadto dla każdej liczby pierwszej $q \neq p$, dzielącej $\#A$ grupa A'_p zawiera q-podgrupę Sylowa grupy A, jako swoją q-podgrupę Sylowa. Z założenia indukcyjnego wynika, iż A'_p jest sumą prostą q-podgrup Sylowa grupy A, a zatem $\#A'_p = Q$. Ponieważ $A_p \cap A'_p = \{e\}$, zatem A zawiera sumę prostą $A_p \oplus A'_p$. Suma ta ma $p^m Q = \#A$ elementów, a więc pokrywa się z A. □

Twierdzenie 2.30. *Każda niecykliczna skończona grupa abelowa jest sumą prostą grup cyklicznych.*

Dowód: (McCluer) Z poprzedniego twierdzenia wynika, że wystarczy udowodnić twierdzenie dla skończonych p-grup abelowych. Jest też oczywiste, że wystarczy udowodnić następujące stwierdzenie, gdyż z niego wynika, iż jedynymi skończonymi p-grupami abelowymi, nierozkładalnymi na nietrywialne sumy proste są grupy cykliczne.

Jeśli A jest skończoną niecykliczną p-grupą abelową, a H jest jej największą podgrupą cykliczną, to istnieje grupa $H' < A$ taka, że $A \sim H \oplus H'$.

Załóżmy, że stwierdzenie to jest słuszne dla wszystkich p-grup abelowych, mających mniej niż p^m elementów i niech A będzie niecykliczną grupą o p^m elementach, z działaniem zapisanym addytywnie. Oznaczmy przez H największą podgrupą cykliczną A i niech $\#H = p^r$ $(r < m)$.

Pokażemy najpierw, że **istnieje element** $a \in A \setminus H$**, mający rząd** p. Ponieważ grupa A/H jest nietrywialną p-grupą, zatem z Wniosku 1 z Twierdzenia 2.27 wynika istnienie warstwy $x + H \in A/H$, mającej rząd p. Wówczas x^p leży w H. Jeśli g jest generatorem H, to istnieje $1 \leq j < p^r$, takie, że $x^p = g^j$.

Pokażemy, że p dzieli j. W istocie, gdyby p nie dzieliłoby j, to istniałaby liczba k taka, że $kj \equiv 1 \pmod{p^r}$ (to wynika z uwagi, że jeśli $NWD(A, N) = 1$, to kongruencja $Ax \equiv B \pmod N$ ma rozwiązanie), a jeśli p^m jest rzędem x, to

$$e = x^{p^m} = (x^p)^{p^{m-1}} = g^{jp^{m-1}},$$

a zatem $p^r = o(g)|jp^{m-1}$, co wobec $p \nmid j$ daje $p^r|p^{m-1}$, tj. $m \leq r \leq m-1 < m$, co niemożliwe. Zatem p dzieli j i możemy napisać $j = pt$ z pewnym całkowitym t. Jeśli teraz $h = g^{p^r - pt}$, to $h \in H$, zatem $a = xh \in A \setminus H$, a przy tym

$$a^p = x^p h^p = g^p t \cdot g^{p^r - pt} = g^0 = e,$$

a więc $o(a) = p$.

Jeśli teraz B jest grupą cykliczną, generowaną przez a, to $B \cap H = \{0\}$. To pokazuje, że obraz H_0 grupy H przez kanoniczny homomorfizm $\phi : A \longrightarrow A/B$ jest izomorficzny z H. Zauważmy, że H_0 jest największą podgrupą cykliczną grup A/B. Wynika to z uwagi, że obraz elementu x grupy przez homomorfizm nie może mieć rzędu większego od rzędu x. Z założenia indukcyjnego wynika istnienie grupy $C < A/B$, spełniającej $A/B \sim H_0 \oplus C$, gdyż H_0 jest maksymalną podgrupą cykliczną grupy A/B. Jeśli teraz przyjmiemy $H' = \phi^{-1}(C)$, to otrzymamy $A \sim H \oplus H'$. W istocie, jeśli h leży w $H \cap H'$, to

$$\phi(h) \in \phi(H) \cap \phi(H') = H_0 \cap C = \{0\},$$

a ponadto dla dowolnego $g \in A$ możemy napisać $\phi(g) = h_0 + c$ z $h_0 \in H_0$ i $c \in C$. Jeśli teraz $\phi(h) = h_0$ z $h \in H$ oraz $\phi(h') = c$ z $h' \in H'$, to $\phi(g - h - h') = 0$, więc $b = g - h - h'$ leży w B, ale $B < H'$ (gdyż $\phi(B) = \{0\} \subset C$) i wobec $g = h + (b + h')$ otrzymujemy $g \in H + H'$. □

Wniosek. *Jeśli A jest grupą abelową w której dla każdej liczby pierwszej dzielącej $\#A$ istnieje conajwyżej p elementów $a \in A$ spełniających $a^p = e$, to A jest grupą cykliczną.*

Dowód: Niech A będzie taką grupą i załóżmy, że nie jest to grupa cykliczna. Jeśli dla każdej liczby pierwszej dzielącej $\#A$ jej p-Sylowska podgrupa A_p jest cykliczna, to z uwagi na $A \sim \bigoplus A_p$ wynika cykliczność A. Zatem istnieje p takie, że A_p nie jest cykliczna. Na podstawie Twierdzenia 2.30 otrzymujemy

$$A_p \sim \bigoplus_{j=1}^{m} B_j,$$

przy czym $m \geq 2$, grupy $B_1, \ldots, B_m$ są cykliczne, a ich rzędy są potęgami liczby p. Każda z tych grup zawiera grupę cykliczną p-elementową, powiedzmy $C_i < B_i$, a każdy element $x \in C_i$ spełnia warunek $x^p = e$. Zatem A_p zawiera $p^m > p$ elementów x, spełniających $x^p = e$, wbrew założeniu. □

III. Pierścienie i ciała

3.1. Podstawowe pojęcia

1. Przypomnijmy, że pierścień nazywa się *pierścieniem przemiennym*, jeśli jego mnożenie jest działaniem przemiennym. Jeśli w pierścieniu istnieje element neutralny dla mnożenia, to mówimy, że jest to *pierścień z jednością*. W pierścieniach przemiennych wprowadza się w naturalny sposób pojęcie podzielności: mówimy, że element $a \in R$ dzieli $b \in R$, jeśli przy pewnym $c \in R$ mamy $ac = b$. Piszemy wówczas $a|b$, a jeśli a nie dzieli b, to piszemy $a \nmid b$. Nietrudno sprawdzić, że jeśli $a|b$ i $a|c$, to $a|b \pm c$, a jeśli $a|b$ i $b|c$, to $a|c$.

Może się zdarzyć, że iloczyn dwóch niezerowych elementów pierścienia jest zerem. Tak jest np. w pierścieniu macierzy 2×2 o współczynnikach całkowitych, gdzie mamy

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Sytuacja taka zdarza się także w pierścieniach przemiennych. Jeśli np. R jest pierścieniem złożonym z wszystkich funkcji o wartościach rzeczywistych, określonych na odcinku I, a funkcje f, g są funkcjami charakterystycznymi dwóch niepustych rozłącznych podzbiorów I, to $fg = 0$, mimo iż $f \neq 0$ i $g \neq 0$.

Mówimy, że niezerowy element a pierścienia R jest *dzielnikiem zera*, gdy w R istnieje $b \neq 0$, takie, że $ab = 0$. Pierścień R nazywa się *pierścieniem bez dzielników zera*, jeśli z $ab = 0$ wynika $a = 0$ lub $b = 0$. Przykładami takich pierścieni są ciała, bo jeśli w ciele iloczyn ab jest równy 0, ale $a \neq 0$, to otrzymujemy $b = a^{-1}ab = 0$. Innym przykładem może być pierścień $\mathbb{Z}$, lub też, ogólniej, dowolny pierścień zawarty w ciele liczb zespolonych.

Mówimy, że pierścień S jest *podpierścieniem* pierścienia R, jeśli $R \subset S$ i R spełnia warunki pierścienia z tymi samymi co w R działaniami.

Lemat 3.1. *Na to by podzbiór S pierścienia R był jego podpierścieniem potrzeba i wystarcza, by były spełnione następujące warunki:*

(i) Jeśli $a, b \in S$, to $a - b \in S$,

(ii) Jeśli $a, b \in S$, to $ab \in S$.

Dowód: Jeśli S jest podpierścieniem, to spełnienie tych warunków wynika z definicji pierścienia. Jeśli zaś $S \subset R$ spełnia te warunki, to z (i) wynika, że S jest grupą abelową ze względu na dodawanie. Warunek (ii) gwarantuje wykonalność mnożenia, a łączność mnożenia i rozdzielczość wynikają ze spełnienia tych warunków w R. $\square$

Uwaga: Podpierścień pierścienia z jednością może nie mieć jedności, o czym świadczy przykład pierścienia złożonego z wszystkich liczb parzystych, który jest podpierścieniem $\mathbb{Z}$.

2. Jeśli R, S są pierścieniami, to *homomorfizmem* R w S nazywamy każde odwzorowanie $f : R \longrightarrow S$, spełniające dla wszystkich $x, y \in R$ warunki

$$f(x + y) = f(x) + f(y), \quad f(xy) = f(x)f(y).$$

Podobnie jak w przypadku homomorfizmów grup zbiór $f(R)$ nazywamy obrazem f, a zbiór

$$\{x \in R : \ f(x) = 0\}$$

nazywamy *jądrem* f i oznaczamy przez $\operatorname{Ker} f$. Tak samo jak w przypadku grup możemy mówić o mono-, epi-, izo-, endo- i automorfizmach.

Lemat 3.2. *Jeśli $f : R \longrightarrow S$ jest homomorfizmem pierścieni, to* $\operatorname{Ker} f$ *jest podpierścieniem R, spełniającym warunek*

Jeśli $a \in \operatorname{Ker} f$ i $r \in R$, to $ar \in \operatorname{Ker} f$ oraz $ra \in \operatorname{Ker} f$.

Dowód: Jeśli $a, b \in \operatorname{Ker} f$, to $f(a-b) = f(a) - f(b) = 0$ i $f(ab) = f(a)f(b) = 0$, zatem z lematu 3.1 wynika, że $\operatorname{Ker} f$ jest podpierścieniem R. Jeśli $r \in R$, to $f(ar) = f(a)f(r) = 0$ oraz $f(ra) = f(r)f(a) = 0$, a więc ar i ra leżą w $\operatorname{Ker} f$. □

Podpierścień I pierścienia R nazywa się *ideałem prawostronnym* jeśli z $r \in R$ i $a \in I$ wynika $ar \in I$, a *ideałem lewostronnym* jeśli z $r \in R$ i $a \in I$ wynika $ra \in I$. Podpierścień będący zarówno ideałem prawostronnym jak i lewostronnym nazywa się *ideałem* pierścienia R. Tak więc Lemat 3.2 stwierdza, że jądro homomorfizmu jest ideałem. Można więc powiedzieć, że pojęcie ideału pierścienia jest pojęciem analogicznym do pojęcia dzielnika normalnego w grupie. Każdy pierścień jest swoim własnym ideałem, a nadto zbiór $\{0\}$ jest ideałem w każdym pierścieniu. Te dwa ideały nazywamy *ideałami trywialnymi*. Ciała nie mają innych ideałów. W istocie, jeśli $I \subset R$ jest nietrywialnym ideałem w ciele R, x jest niezerowym elementem I, a $y = x^{-1}$ jest elementem odwrotnym do x, to z definicji ideału wynika $1 = xy \in I$, a więc dla dowolnego $r \in R$ mamy $r = r \cdot 1 \in R$, tj. $I = R$ jest ideałem trywialnym.

Niech I będzie ideałem w R. Jego elementy tworzą podgrupę I^+ w grupie, złożonej z elementów R, z dodawaniem jako działaniem (tj. w *grupie addytywnej* R^+ *pierścienia* R), która jest dzielnikiem normalnm w R, gdyż dodawanie w pierścieniu jest przemienne. Możemy więc rozpatrywać warstwy względem I. Są one postaci $a + I$. Oznaczmy przez R/I zbiór wszystkich takich warstw. W zbiorze tym wprowadzamy działania dodawania i mnożenia wzorami

$$(a+I) + (b+I) = (a+b) + I, \quad (a+I) \cdot (b+I) = ab + I. \tag{3.1}$$

Twierdzenie 3.3. *(i) Jeśli I jest ideałem w pierścieniu R, to zbiór R/I warstw z działaniami określonymi przez* (3.1) *jest pierścieniem, a odwzorowanie $\phi : R \longrightarrow R/I$ zadane przez $\phi(a) = a+I$ jest epimorfizmem.*

(ii) Jeśli pierścień R jest przemienny, to pierścień R/I również jest przemienny.

(iii) Jeśli pierścień R posiada jedność 1*, to $1 + I$ jest jednością w R/I.*

Dowód: (i) Ponieważ ze względu na dodawanie zbiór R/I jest grupą na mocy Twierdzenia 2.14, należy zająć się mnożeniem. Wykażemy najpierw, że mnożenie warstw, zdefiniowane wzorem (3.1) jest dobrze określone, tj. jego wynik nie zależy od wyboru elementu wyznaczającego warstwę. Jeśli $a_1 + I = b_1 + I$ i $a_2 + I = b_2 + I$, to z Twierdzenia 2.10 (iv) wynika, że dla $i = 1, 2$ mamy $c_i = a_i - b_i \in I$, a więc $a_i = b_i + c_i$ i otrzymujemy $a_1a_2 = b_1b_2 + b_1c_2 + b_2c_1 + c_1c_2$. Ponieważ b_1c_2, b_2c_1 i c_1c_2 leżą w I widzimy, że $b_1c_2 + b_2c_1 + c_1c_2 \in I$, a więc $a_1a_2 + I = b_1b_2 + I$. Łączność mnożenia i rozdzielność w R/I wynikają z odpowiednich własności pierścienia R. Zatem R/I jest pierścieniem, a stwierdzenie, że ϕ jest homomorfizmem wynika natychmiast z (3.1). Jego surjektywność jest oczywista.

(ii) i (iii) są konsekwencjami (3.1). □

Twierdzenie 3.4. *Niech $f : R \longrightarrow S$ będzie epimorfizmem pierścieni i niech J będzie jego jądrem. Oznaczmy przez $\phi : R \longrightarrow R/J$ homomorfizm opisany w Twierdzeniu* 3.3*. Wówczas pierścienie R/J i S są izomorficzne i istnieje dokładnie jeden izomorfizm $\psi : R/J \longrightarrow S$, taki, że dla $a \in R$ mamy $f(a) = \psi(\phi(a))$, tj.*

$$f = \psi \circ \phi. \tag{3.2}$$

Dowód: Z dowodu Twierdzenia 2.15 zastosowanego do grup addytywnych pierścieni R i S wynika, że odwzorowanie $R/J \longrightarrow S$ zadane wzorem $\psi(a+J) = f(a)$ jest izomorfizmem grup addytywnych R/J i S. Pozostaje sprawdzić, że ψ zachowuje mnożenie, a to wynika z równości

$$\psi((a+J)(b+J)) = \psi(ab+J) = f(ab) = f(a)f(b) = \psi(a+J)\psi(b+J). \qquad \square$$

Przykłady. a) Niech N będzie liczbą naturalną i niech $f_N : \mathbb{Z} \longrightarrow \mathbb{Z}_N$ (gdzie $\mathbb{Z}_N$ jest pierścieniem reszt z dzielenia przez N) będzie odwzorowaniem przeprowadzającym liczby całkowite na ich reszty z dzielenia przez N. Jest to epimorfizm, którego jądrem jest zbiór $N\mathbb{Z}$ liczb podzielnych przez N. Z Lematu 3.2 wynika, że $N\mathbb{Z}$ jest ideałem, a twierdzenie 3.4 daje izomorfizm

$$\mathbb{Z}/N\mathbb{Z} \sim \mathbb{Z}_{\mathbb{N}}.$$

b) Niech R będzie pierścieniem złożonym z wszystkich funkcji ciągłych na pewnym przedziale I o wartościach w $\mathbb{R}$. Dla $x \in I$ niech $f_x : R \longrightarrow \mathbb{R}$ będzie odwzorowaniem zadanym przez $f \mapsto f(x)$. Jest to epimorfizm o jądrze $I_x = \{f \in R : f(x) = 0\}$ i z Twierdzenia 3.4 wynika izomorfizm

$$R/I_x \sim \mathbb{R}.$$

3. Ideał I pierścienia R nazywa się *ideałem maksymalnym*, jeśli nie jest zawarty w żadnym nietrywialnym ideale różnym od I.

Twierdzenie 3.5. *Jeśli R jest pierścieniem przemiennym z jednością, to jego ideał I jest maksymalny wtedy i tylko wtedy, gdy pierścień ilorazowy R/I jest ciałem.*

Dowód: Niech I będzie ideałem maksymalnym i niech $a + I$ będzie niezerowym elementem pierścienia ilorazowego R/I. Wówczas $a \notin I$ i z maksymalności I wynika, że najmniejszy ideał zawierający I oraz a jest równy R.

Lemat 3.6. *Jeśli R jest pierścieniem przemiennym, $a \in R$ i I jest ideałem w R, to najmniejszym ideałem zawierającym a i I jest*

$$J = \{ra + b : r \in R, b \in I\}.$$

Dowód: Z definicji ideału wynika, że każdy ideał zawierający a i I musi zawierać wszystkie elementy postaci $ra + b$ przy $r \in R$ i $b \in I$, pozostaje więc pokazać, że J jest ideałem. Jeśli $r_i a + b_i \in J$ ($r_i \in R, b_i \in I, i = 1, 2$), to

$$(r_1 a + b_1) - (r_2 a + b_2) = (r_1 - r_2)a + (b_1 - b_2) \in J,$$

a jeśli $x = ra + b \in J$ ($r \in R, b \in I$) i $s \in R$, to $sx = (sr)a + sb$, a ponieważ $sb \in I$, zatem $sx \in J$. $\square$

Korzystając z tego lematu otrzymujemy istnienie elementów $r \in R$, $b \in I$, spełniających

$$ra + b = 1,$$

a to prowadzi do $(r + I)(a + I) = 1 + I$, a zatem $a + I$ ma element odwrotny w R/I, co pokazuje, że R/I jest ciałem.

Teraz załóżmy, ze R/I jest ciałem, ale ideał I nie jest ideałem maksymalnym. Zatem istnieje ideał J, różny od I i R, spełniający $I \subset J \subset R$. Wybierzmy dowolny element $x \in J \setminus I$. Ponieważ $x \notin I$, zatem $x + I$ jest niezerowym elementem R/I, a więc ma element odwrotny $y + I$, a to daje

$$1 + I = (x + I)(y + I) = xy + I.$$

Zatem $z = xy - 1 \in I \subset J$, a ponieważ z $x \in J$ wynika $xy \in J$, więc $1 = xy - z \in J$, co jest możliwe jedynie w wypadku $J = R$, a ten przypadek został wykluczony. $\square$

Wniosek. *Jeśli p jest liczbą pierwszą, to zbiór $p\mathbb{Z}$ wszystkich wielokrotności p jest ideałem maksymalnym w pierścieniu $\mathbb{Z}$.*

Dowód: Wynika z Twierdzenia 3.5, przykładu a) po Twierdzeniu 3.4 i tego, że zbiór reszt z dzielenia przez p jest ciałem. $\square$

Innym przykładami ideałów maksymalnych są ideały I_x z przykładu b) po Twierdzeniu 3.4.

Ideał I w pierścieniu przemiennym R nazywa się *ideałem pierwszym* jeśli z $ab \in I$ wynika, że conajmniej jeden z czynników a, b leży w I.

Twierdzenie 3.7. *Jeśli R jest pierścieniem przemiennym, to ideał $I \subset R$ jest ideałem pierwszym wtedy i tylko wtedy, gdy pierścień R/I nie ma dzielników zera.*

Dowód: Jeśli I jest ideałem pierwszym, a $(a + I)(b + I) = 0$, to $ab + I = 0$, zatem $ab \in I$, a więc a lub b leży w I, co powoduje, że jedna z warstw $a + I, b + I$ jest warstwą zerową. Naodwrót, jeśli R/I nie ma dzielników zera i $ab \in I$, to

$$0 + I = ab + I = (a + I)(b + I),$$

a zatem jedna z warstw $a+I, b+I$ jest zerowa, tj. $a \in I$ lub $b \in I$. $\square$

Ideał I w pierścieniu przemiennym z jednością R nazywa się *ideałem głównym*, jeśli istnieje element $a \in R$ taki, że $I = \{ra : r \in R\} = rR$, tj. I jest najmniejszym ideałem zawierającym element r.

Wniosek. *W pierścieniu przemiennym każdy ideał maksymalny jest ideałem pierwszym.*

Dowód: Wynika z twierdzeń 3.5 i 3.7. $\square$

Fakt 3.8. *W pierścieniu $\mathbb{Z}$ każdy ideał jest ideałem głównym, generowanym przez liczbę naturalną, a każda liczba pierwsza generuje ideał maksymalny.*

Dowód: Niech I będzie ideałem w $\mathbb{Z}$. Jeśli $I = \{0\}$, to jest to ideał główny generowany przez 0. Jeśli zaś I jest ideałem niezerowym, to niech n będzie najmniejszą liczbą naturalną zawartą w I. Pokażemy, że $I = n\mathbb{Z}$. Jeśli $m \in I$, to na podstawie Lematu 1.7 możemy napisać $m = qn + r$, gdzie $q \in \mathbb{Z}$ i $0 \leq r < n$. Ponieważ $qn \in I$ i $m \in I$, zatem $r \in I$, co jest możliwe jedynie gdy $r = 0$, tj. m dzieli się przez n. Zatem $m \in n\mathbb{Z}$, a więc $I \subset n\mathbb{Z}$. Ponieważ inkluzja $n\mathbb{Z} \subset \mathbb{I}$ jest oczywista, to daje $n\mathbb{Z} = I$.

Jeśli p jest liczbą pierwszą, a ideał $I = p\mathbb{Z}$ nie jest maksymalny, to istnieje ideał J, rożny od I i $\mathbb{Z}$, spełniający $I \subset J \subset \mathbb{Z}$. Ideał J jest ideałem głównym, zatem $I = a\mathbb{Z}$, gdzie a jest liczbą naturalną. Ponieważ $p \in J$, zatem a dzieli p, co jest możliwe jedynie gdy $a = 1$ lub $a = p$, ale te przypadki są wykluczone. $\square$

4. Do przykładów pierścieni, które poznaliśmy, dodamy teraz pewną bardzo ważną klasę. Wielomiany, traktowane jako funkcje postaci $a_nX^n + \cdots + a_0$ z liczbowymi współczynnikami pojawiają się już w szkole. Nietrudno sprawdzić, że zbiory $\mathbb{Z}[X]$, $\mathbb{R}[X]$, $\mathbb{Q}[X]$, $\mathbb{C}[X]$ wszystkich wielomianów o współczynnikach odpowiednio całkowitych, wymiernych, rzeczywistych i zespolonych są pierścieniami ze zwykłymi działaniami dodawania i mnożenia. Niestety, podobna definicja wielomianu zawodzi np. w przypadku, gdy chcemy rozpatrywać wielomiany o współczynnikach z ciała 2-elementowego. W istocie, chcielibyśmy aby, tak jak w przypadku liczbowym, wielomiany $f(X) = X$ i $g(X) = X^{20}$ były różnymi wielomianami, ale wyrażenia te traktowane jako funkcje nad $GF(2) = \{0, 1\}$ są równe, gdyż $f(0) = g(0) = 0$ i $f(1) = g(1) = 1$.

Aby wprowadzić pojęcie wielomianu o współczynnikach z dowolnego pierścienia przemiennego musimy zatem uczynić to bez użycia pojęcia funkcji.

Niech R będzie dowolnym pierścieniem przemiennym z jednością 1. *Wielomianem* o współczynnikach z R nazywać będziemy każdy nieskończony ciąg $(a_0, a_1, a_2, \ldots)$ elementów z R, w których jedynie skończenie wiele wyrazów jest różnych od zera. Zbiór wszystkich takich ciągów oznaczamy przez $R[X]$. W zbiorze tym zdefiniujemy działania dodawania i mnożenia następująco:

Jeśli $\alpha = (a_0, a_1, \ldots) \in R[X]$, $\beta = (b_0, b_1, \ldots) \in R[X]$, to kładziemy

$$\alpha + \beta = (c_0, c_1, \ldots), \quad \alpha \cdot \beta = (d_0, d_1, \ldots), \tag{3.3}$$

przy czym dla $j = 0, 1, \ldots$ mamy

$$c_j = a_j + b_j, \quad d_j = \sum_{k=0}^{j} a_k b_{j-k} = \sum_{k+l=j} a_k b_l.$$

Twierdzenie 3.9. *Z tak zdefiniowanymi działaniami zbiór $R[X]$ jest przemiennym pierścieniem z jednością $\mathbf{1} = (e_0, e_1, \ldots)$, gdzie*

$$e_j = \begin{cases} 1 & \text{gdy } j = 0, \\ 0 & \text{gdy } j > 0 \end{cases}$$

i zerem $\mathbf{0} = (0, 0, \ldots, 0, \ldots)$.

Dowód: Wykonalność działań, łączność dodawania oraz przemienność mnożenia i dodawania wynikają natychmiast z definicji, podobnie jak i to, że $\mathbf{0}$ jest elementem neutralnym dla dodawania, a element $(-a_0, -a_1, \ldots)$ jest elementem przeciwnym do $(a_0, a_1, \ldots)$. Tak więc $R[X]$ jest grupą przemienną względem dodawania. By sprawdzić łączność mnożenia napiszmy $\alpha = (a_0, a_1, \ldots) \in R[X]$, $\beta = (b_0, b_1, \ldots) \in R[X]$,$\gamma = (c_0, c_1, \ldots) \in R[X]$. Prosty rachunek pokazuje, że oba elementy $(\alpha\beta)\gamma$, $\alpha(\beta\gamma)$ są równe $(d_0, d_1, \ldots)$, gdzie

$$d_j = \sum_{k+l+m=j} a_k b_l c_m,$$

a to dowodzi łączności. Podobnie rozdzielczość wynika z równości

$$\sum_{k+l=j}(a_k+b_k)c_l=\sum_{k+l=j}a_kc_l+\sum_{k+l=j}b_kc_l,$$

a jeśli $\mathbf{1}\cdot\alpha=(r_1,r_2,\ldots)$, to otrzymujemy

$$r_j=\sum_{k+l=j}e_ka_l=a_j,$$

a więc $\mathbf{1}$ jest elementem neutralnym dla mnożenia. $\square$

Jeśli ciąg $A=(a_0,a_1,\ldots)\in R[X]$ nie składa się z samych zer, to istnieje największy indeks n, dla którego $a_n\neq 0$. Indeks ten oznaczamy $\deg A$ i nazywamy *stopniem wielomianu A*.

Dla uproszczenia zapisu oznaczmy przez X ciąg $(0,1,0,0,\ldots)$, a dla dowolnego $r\in R$ oznaczmy przez $\bar{r}$ ciąg $(r,0,0,\ldots)$. Użyteczność tych oznaczeń wyjaśnia się w poniższym wniosku:

Wniosek. *Niech R będzie przemiennym pierścieniem z jednością, a $R[X]$ pierścieniem z twierdzenia* 3.2. *Wówczas*

(i) Dla $m=1,2,\ldots$ mamy $X^m=(c_0,c_1,\ldots)$, gdzie

$$c_j=\begin{cases}1 & \text{gdy } j=m,\\ 0 & \text{gdy } j\neq m.\end{cases}\tag{3.4}$$

(ii) Jeśli $\alpha=(a_0,a_1,\ldots)\in R[X]$ i dla $j>n$ zachodzi równość $a_j=0$, to

$$\alpha=\sum_{j=0}^{n}\bar{a}_jX^j.$$

(iii) Zbiór $\{(a_0,0,0,0,\ldots)\in R[X]\}$ jest pierścieniem izomorficznym z R.

Dowód: (i) Stosujemy indukcję. Dla $m=1$ równość nasza wynika z definicji X, a jeśli równość ta zachodzi dla pewnego m, to stosując (3.4) i definicję X widzimy, że jeśli $X=(c_0,c_1,\ldots)$ i $X^{m+1}=(d_0,d_1,\ldots)$, to z uwagi na $X^{m+1}=X\cdot X^m$ otrzymamy $d_j=\sum_{k+l=j}c_kd_l$, ale c_k jest niezerowe jedynie dla $k=1$, zaś $d_l\neq 0$ zachodzi tylko dla $l=m$, a zatem d_j znika dla $j\neq 1+m$, a $d_{1+m}=1$.

(ii) Tu wystarczy zauważyć, że możemy napisać

$$(a_0,a_1,\ldots,a_n,0,0,\ldots)=(a_0,0,0,\ldots)+(0,a_1,0,\ldots)+\cdots+(0,0,\ldots,0,a_n,0,\ldots),$$

oraz

$$(0,0,\ldots,a_j,0,0,\ldots)=(a_j,0,0,\ldots)\cdot X^j.$$

(iii) Odwzorowanie $r\mapsto(r,0,0,0,\ldots)$ daje żądany izomorfizm. $\square$

Izomorfizm w trzeciej części wniosku pozwala utożsamiać wielomiany postaci $(r,0,0,\ldots)$ z elementami $r\in R$. Pozwala to na traktowanie wielomianów o współczynnikach z pierścienia R jak formalne wyrażenia postaci $\sum_{j=0}^{n}a_jX^j$ z działaniami takimi jak w przypadku wielomianów o współczynnikach liczbowych. Jeśli $f=\sum_{j=0}^{n}a_jX^j\in R[X]$ i $a_n\neq 0$, to stopień f jest równy n.

Z każdym wielomianem

$$W=\sum_{j=0}^{n}a_jX^j\in R[X]$$

jest związana funkcja $f_W:R\longrightarrow R$, zadana wzorem

$$f_W(r)=\sum_{j=0}^{n}a_jr^j.$$

Funkcja taka nazywa się *funkcją wielomianową*. Widzieliśmy wyżej, że w pewnych przypadkach różnym wielomianom może odpowiadać ta sama funkcja wielomianowa.

Pierścienie $R[X_1, \dots, X_N]$ wielomianów N zmiennych o współczynnika z pierścienia R definiujemy w sposób indukcyjny. W przypadku $N = 1$ takim pierścieniem jest $R[X]$, a jeśli mamy już zdefiniowany pierścień $S = R[X_1 \dots, X_N]$ wielomianów N zmiennych, to $R[X_1, \dots, X_{N+1}]$ definiujemy jako pierścień wielomianów 1 zmiennej o współczynnikach z S.

3.2. Pierścienie całkowite.

1. Pierścień R nazywa się *pierścieniem całkowitym*, gdy jest przemienny, ma jedność i nie ma dzielników zera. Każdy pierścień liczbowy, zawierający liczbę 1 jest pierścieniem całkowitym. Następujące twierdzenie pozwala na konstruowanie wielu pierścieni całkowitych:

Twierdzenie 3.10. *Jeśli R jest pierścieniem całkowitym, to $R[X]$ jest również pierścieniem całkowitym.*

Dowód: Teza twierdzenia jest natychmiastową konsekwencją poniższego lematu:

Lemat 3.11. *Jeśli R jest pierścieniem całkowitym, a $f, g \in R[X]$ są niezerowe, to*

$$\deg(fg) = deg(f) + \deg(g).$$

Dowód: Jeśli $f(X) = a_0 + a_1X + \dots + a_mX^m$, $g(X) = b_0 + b_1X + \dots + b_nX^n$, a $a_m, b_n \neq 0$, to $f(X)g(X) = a_0b_0 + \dots + a_mb_nX^{m+n}$, przy czym z całkowitości R wynika $a_mb_n \neq 0$. □

Pierścienie całkowite można też opisać jako te pierścienie z jednością, które są zawarte w jakimś ciele. Wynika to z następującego twierdzenia:

Twierdzenie 3.12. *(i) Jeśli R jest pierścieniem całkowitym, to istnieje ciało K, zawierające pierścień R, a przy tym każdy element tego ciała da się przedstawić jako iloraz 2 elementów R.*

(ii) Każde ciało zawierające pierścień R zawiera podciało, izomorficzne z ciałem K, występującym w (i).

Dowód: (i) Rozpatrzmy zbiór Ω złożony z wszystkich par (a, b), gdzie $a, b \in R$ i $b \neq 0$. W zbiorze tym wprowadzamy relację binarną ρ wzorem

$$(a, b)\rho(c, d) \Leftrightarrow ad = bc.$$

I krok: *Relacja ρ jest relacją typu równoważności.*

W istocie, jest oczywiste, że ρ jest relacją zwrotną i symetryczną, pozostaje zatem sprawdzić jej przechodniość. Niech więc $(a, b)\rho(c, d)$ i $(c, d)\rho(e, f)$, przy czym b, d, f są elementami niezerowymi. Zatem $ad = bc$ i $cf = de$ i należy sprawdzić, że $af = de$. Mamy

$$(ad)f = (bc)f = b(cf) = b(de),$$

co wobec przemienności mnożenia prowadzi do $(af)d = (be)d$, tj. $(af - be)d = 0$. Ponieważ R nie ma dzielników zera, a przy tym $d \neq 0$, zatem $af - be = 0$, więc $af = be$.

II krok. *Wprowadzimy działania mnożenia i dodawania w zbiorze klas równoważności $K = \Omega/\rho$.*

Jeśli $\alpha, \beta \in K$, to sumę $\alpha + \beta$ i iloczyn $\alpha \cdot \beta$ definiujemy następująco: wybieramy $(a, b) \in \alpha$ i $(c, d) \in \beta$ i definiujemy $\alpha + \beta$ jako klasę zawierającą element $(ad + bc, bd)$, zaś $\alpha \cdot \beta$ jest klasą zawierającą (ac, bd). Należy sprawdzić, że operacje te nie zależą od wyboru elementów w klasach α i β. Niech więc $(a', b') \in \alpha$, $(c', d') \in \beta$, tj.

$$ab' = a'b, \quad cd' = c'd. \tag{3.5}$$

Trzeba sprawdzić, że $(ad + bc, bd)\rho(a'd' + b'c', b'd')$ oraz $(ac, bd)\rho(a'c', b'd')$, tj.

$$(ad + bc)b'd' = (a'd' + b'c')bd, \text{ i } acb'd' = a'c'bd,$$

a to wynika z (3.5) dzięki

$$(ad+bc)b'd' = ab'dd' + cd'bb' = a'bdd' + c'dbb' = (a'd' + b'c')bd$$

oraz

$$ab'cd' = a'bcd' = a'bc'd.$$

III krok: *Zbiór K jest grupą przemienną względem dodawania.*

Bezpośrednie sprawdzenie pokazuje, że dodawanie w K jest łączne i przemienne, a klasa $\mathbf{0}$, zawierająca $(0,1)$ jest elementem neutralnym dla dodawania. Nietrudno też zauważyć, że $\mathbf{0} = \{(0,b): \ b \in R, b \neq 0\}$. Jeśli $\alpha \in K$ oraz $(a,b) \in \alpha$, to klasa β, zawierająca $(-a,b)$ spełnia $\alpha + \beta = \mathbf{0}$, ponieważ element $\gamma = (ab + (-a)b, b \cdot b) = (0, b \cdot b)$ spełnia $\gamma \rho \mathbf{0}$.

IV krok: *Zbiór $K \setminus \{\mathbf{0}\}$ jest grupą względem mnożenia.*

Łączność i przemienność wynikają natychmiast z definicji, zaś elementem neutralnym jest klasa $\mathbf{1}$, zawierająca parę $(1,1)$. Jęśli α jest niezerowym elementem K i $(a,b) \in \alpha$, to $a \neq 0$ i $b \neq 0$. Jeśli zatem β jest klasą zawierającą (b,a), to $\gamma = \alpha \cdot \beta$ zawiera (ab, ab) i z $(ab,ab)\rho(1,1)$ otrzymujemy $\gamma = \mathbf{1}$.

V krok: *Dla $\alpha, \beta, \gamma \in K$ zachodzi równość $(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma$.*

Jeśli $(a_1, a_2) \in \alpha$, $(b_1, b_2) \in \beta$ i $(c_1, c_2) \in \gamma$, to klasa $(\alpha+\beta)\gamma$ zawiera parę $A = ((a_1b_2 + a_2b_1)c_1, a_2b_2c_2)$, zaś klasa $\alpha\gamma + \beta\gamma$ zawiera parę $B = (a_1c_1b_2c_2 + a_2b_1c_1c_2, a_2b_2c_2c_2)$ i pozostaje zauważyć, że $A\rho B$.

Widzimy zatem, że K jest ciałem.

VI krok: *Pierścień R jest izomorficzny z pewnym pierścieniem R' zawartym w K.*

Dla $r \in R$ znaczmy przez k_r klasę zawierającą parę $(r,1)$ i niech R' będzie zbiorem wszystkich klas tej postaci. Zauważmy, że R' jest podpierścieniem ciała K, gdyż z definicji działań wynikają równości

$$k_r + k_s = k_{r+s}, \quad k_r - k_s = k_{r-s}, \quad k_r \cdot k_s = k_{rs}.$$

Z wzorów tych wynika, że odwzorowanie $\Phi : R \longrightarrow R'$ zdane przez $r \mapsto k_r$ jest homomorfizmem. Jego surjektywność jest oczywista, a jeśli elementy $a \neq b$ leżą w R, to klasy k_a, k_b są różne. Zatem Φ jest izomorfizmem. Możemy zatem utożsamić pierścienie R i R'.

Do dowodu (i) pozostaje zauważyć, że klasa k, zawierająca parę (a,b) da się zapisać w postaci

$$k = k_a \cdot k_b^{-1}.$$

(ii) Niech L będzie ciałem, zawierającym pierścień R i niech M będzie jego podzbiorem złożonym z wszystkich elementów postaci ab^{-1}, gdzie $a, b \in R$, $b \neq 0$. Ponieważ M jest zamknięte na cztery działania (z wyjątkiem dzielenia przez zero), zatem jest ciałem. Niech K będzie ciałem skonstruowanym w (i). Rozpatrzmy odwzorowanie $\Psi : M \longrightarrow K$, określone następująco:

Jeśli $\xi = ab^{-1}$ $(a, b \in R, b \neq 0)$ jest elementem M, to $\Psi(\xi)$ jest klasą, zawierającą parę (a,b). Zauważmy, że $\Psi(\xi)$ nie zależy od sposoby przedstawienia ξ w postaci ilorazu elementów R, bo jeśli $\xi = ab^{-1} = cd^{-1}$, to $ad = bc$, a więc $(a,b)\rho(c,d)$. Odwzorowanie to jest wzajemnie jednoznaczne, a bezpośredni rachunek pokazuje, że jest ono homomorfizmem. □

Ciało skonstruowane w tym twierdzeniu nazywamy *ciałem ułamków pierścienia R*. Podana tu konstrukcja zastosowana do pierścienia $\mathbb{Z}$ prowadzi do ciała liczb wymiernych.

2. Najważniejszym rodzajem pierścieni wielomianów są pierścienie wielomianów o współczynnikach z ciała. Zanim je omówimy, potrzebne nam będą proste fakty z teorii ciał.

Ciało K nazywamy *ciałem prostym*, jeśli nie zawiera żadnego ciała, różnego od K.

Twierdzenie 3.13. *(i) Ciało liczb wymiernych i ciała $GF(p)$ (p - liczba pierwsza) są ciałami prostymi.*

(ii) Jeśli K jest ciałem prostym, to jest jednym z ciał wymienionych w (i).

(iii) Każde ciało K zawiera dokładnie jedno ciało proste.

Dowód: (i). Jeśli $K \subset \mathbb{Q}$ jest ciałem, to zawiera 1, a stąd wynika $\mathbb{Z} \subset \mathbb{K}$ i następnie $\mathbb{Q} \subset \mathbb{K}$, tj. $K = \mathbb{Q}$.

W przypadku ciała $GF(p)$ wystarczy zauważyć, że grupa addytywna tego ciała jest p-elementowa, a więc nie zawiera nietrywialnych podgrup.

(ii) Niech K będzie ciałem prostym i niech $0, e$ będą jego elementami neutralnymi dla dodawania i mnożenia. Jeśli wszystkie elementy ciągu $e, 2e, 3e, \ldots$ są różne, to zbiór

$$\mathfrak{A} = \{0, \pm e, \pm 2e, \ldots\}$$

jest pierścieniem izomorficznym z $\mathbb{Z}$ i z twierdzenia 3.12 (ii) wynika, że K zawiera ciało liczb wymiernych, co daje $K = \mathbf{Q}$. Jeśli nie wszystkie elementy ciągu $e, 2e, 3e, \ldots$ są różne, powiedzmy $me = ne$ (przy $1 \leq m < n$), to dla $r = n - m$ mamy $re = 0$, tj. nasz ciąg redukuje się do ciągu skończonego $e, 2e, \ldots, (r-1)e, 0$. Możemy przyjąć, że r jest najmniejszą liczbą dodatnią dla której $re = 0$. Wówczas r musi być liczbą pierwszą, gdyż w przeciwnym wypadku mielibyśmy $r = ab$ z $a > 1$ i $b > 1$, a zatem byłoby $0 = re = (ab)e = (ae)(be)$, co nie jest możliwe, bo w ciele nie ma dzielników zera. Pozostaje spostrzec że zbiór $L = \{0, e, 2e, \ldots, (r-1)e\}$ jest ciałem izomorficznym z $GF(r)$, a izomorfizm $L \longrightarrow GF(r)$ jest zadany przez $ke \mapsto k \bmod r$.

(iii) Takim ciałem jest część wspólna wszystkich ciał zawartych w K. □

Jeśli ciało K zawiera ciało $GF(p)$, to mówimy, że K ma *charakterystykę* p, a jeśli K zawiera ciało liczb wymiernych, to mówimy, że ma *charakterystykę* 0.

Fakt 3.14. *Jeśli K jest ciałem charakterystyki $p > 0$, to dla $a \in K$ mamy $pa = 0$.*

Dowód: Bo

$$pa = \overbrace{a + a + \cdots + a}^{p \text{ razy}} = \overbrace{ea + ea + \cdots + ea}^{p \text{ razy}} = (\overbrace{e + e + \cdots + e}^{p \text{ razy}})a = 0.$$

Twierdzenie 3.15. *Jeśli p jest liczbą pierwszą, K jest ciałem charakterystyki p, to dla $a, b \in K$ i $n = 1, 2, \ldots$ mamy*

$$(a + b)^{p^n} = a^{p^n} + b^{p^n}.$$

Dowód: W przypadku $n = 1$ wystarczy pokazać, że dla $k = 1, 2, \ldots, p-1$ symbole Newtona $\binom{p}{k}$ dzielą się przez p. Mamy

$$\binom{p}{k} = \frac{p!}{k!(p-k)!},$$

a w ułamku po prawej stronie licznik dzieli się przez p, a mianownik nie, gdyż jest iloczynem liczb mniejszych od p. Dla $n > 1$ stosujemy banalną indukcję. □

3. Jeśli K jest ciałem skończonym, to jego charakterystyka musi być dodatnia, a więc musi ono zawierać jedno z ciał $GF(p)$. Okazuje się, że ilość elementów w takim ciele musi być potęgą liczby p:

Twierdzenie 3.16. *Jeśli K jest ciałem skończonym, to ilość jego elementów jest równa p^N przy pewnym $N \geq 1$, przy czym p jest charakterystyką K.*

Dowód: Jeśli $\mathrm{char}(K) = p$, to $GF(p) \subset K$. Możemy zatem traktować K jako przestrzeń liniową nad $GF(p)$, gdyż w K jest określone dodawanie i mnożenie, a więc w szczególności mnożenie przez skalary z ciała $GF(p)$. Jeśli wymiar tej przestrzeni jest N, a $\omega_1, \ldots, \omega_N$ jest jej bazą, to każdy element K zapisze się jednoznacznie w postaci

$$\sum_{j=1}^{N} c_j \omega_j,$$

gdzie $c_1, \ldots, c_N$ są elementami $GF(p)$. Wynika stąd, że K ma p^N elementów. □

Później zobaczymy, że do każdej potęgi q liczby pierwszej istnieje ciało mające q elementów, a teraz podamy jedynie konstrukcję ciała 4-elementowego, podpowiedzianą przez dowód poprzedniego twierdzenia:

Rozpatrzmy 2-wymiarową przestrzeń liniową V nad ciałem $GF(2) = \{0, 1\}$. Można ją zidentyfikować ze zbiorem $\{0, 1, X, 1 + X\}$ wielomianów stałych i liniowych o współczynnikach z ciała $k = GF(2)$. Dodawanie jest wyznaczone przez strukturę przestrzeni liniowej, należy więc odpowiednio zdefiniować mnożenie.

Mnożenie przez 0 i przez 1 jest oczywiste, musimy więc jedynie zdefiniować mnożenie przez pozostałe elementy. Uczynimy to w poniższej tabelce:

$$X \cdot X = 1 + X, \ (1 + X) \cdot (1 + X) = X, \ X \cdot (1 + X) = 1.$$

Z pewnym wysiłkiem można rachunkowo sprawdzić, że w ten sposób nasza przestrzeń otrzymuje strukturę ciała. Nieco mądrzejszy sposób polega na zauważeniu, że jeśli I jest ideałem głównym w $k[X]$, generowanym przez wielomian $f(X) = X^2 + X + 1$, to pierścień ilorazowy $S = k[X]/I$ ma cztery elementy, które są klasami reszt z dzielenia przez f. Są one reprezentowane przez wielomiany $0, 1, X$ i $1 + X$. By pokazać, że pierścień S jest ciałem, wystarczy zauważyć, że wielomian $X \cdot (1 + X) = X + X^2$ daje resztę 1 z dzielenia przez f, gdyż $X^2 + X = 1 + f(X)$ (pamiętajmy, że w ciele o charakterystyce równej 2 zachodzi równość $-1 = 1$). Bez trudu widać też, że działania wprowadzone w przestrzeni liniowej V pokrywają się z działaniami w S.

4. Ideał I pierścienia R nazywa się *ideałem skończenie generowalnym*, jeśli istnieje skończony zbiór $A = \{a_1, a_2, \ldots, a_m\} \subset I$ taki, że I jest najmniejszym ideałem zawierającym A. Bardzo ważną klasę pierścieni stanowią pierścienie, w których każdy ideał jest skończenie generowalny. Noszą one nazwę *pierścieni Noetherowskich*, od nazwiska Emmy Noether. W przypadku pierścieni z jednością można je scharakteryzować w inny sposób, który okaże się później przydatny:

Twierdzenie 3.17. *Jeśli R jest pierścieniem z jednością, to R jest pierścieniem noetherowskim wtedy i tylko wtedy, gdy każdy wstępujący ciąg ideałów jest skończony, tj. nie istnieje nieskończony ciąg różnych ideałów*

$$I_1 \subset I_2 \subset \ldots.$$

Dowód: Niech R będzie pierścieniem noetherowskim i załóżmy, że istnieje nieskończony ciąg wstępujący różnych ideałów $I_1 \subset I_2 \subset \ldots$. Wówczas zbiór

$$I = \bigcup_{j=1}^{\infty} I_j$$

jest ideałem. W istocie, jeśli $a, b \in I$, to przy pewnych m, n mamy $a \in I_m$, $b \in I_n$. Możemy przyjąć, że $m \leq n$, a więc $I_m \subset I_n$. Wówczas $a, b \in I_n$, a zatem $a - b \in I_n \subset I$, a jeśli $r \in R$, to $ra \in I_n \subset I$, co pokazuje, że I jest ideałem. Nie jest on równy R, gdyż żaden z ideałów I_j nie zawiera 1. Ponieważ R jest noetherowski, zatem istnieją elementy $a_1, a_2, \ldots, a_k \in I$, generujące I i jeśli $a_i \in I_{n_i}$ $(i = 1, 2, \ldots, k)$, to wszystkie elementy a_i leżą w I_N, gdzie N jest największą z liczb $n_1, n_2, \ldots, n_k$. Zatem $I \subset I_N \subset I_{N+1} \subset I$, a więc $I_N = I_{N+1}$, sprzeczność.

Naodwrót, jeśli R nie jest noetherowski, to istnieje ideał $I \subset R$, nie mający skończonego układu generatorów. Niech a_1 będzie dowolnym niezerowym elementem I, a jeśli już wybrane są elementy $a_1, a_2, \ldots, a_n$, to niech I_n będzie ideałem przez nie generowanym. Z założenia wynika $I_n \subset I$ i $I_n \neq I$, więc możemy wybrać $a_{n+1} \in I \setminus I_n$. W ten sposób otrzymamy wstępujący ciąg różnych ideałów $I_1 \subset I_2 \subset \ldots$. $\square$

Okazuje się, że jeśli R jest pierścieniem noetherowskim, to pierścień wielomianów $R[X]$ też ma tę własność. Jest to treścią sławnego twierdzenia Hilberta:

Twierdzenie 3.18. (Twierdzenie Hilberta o bazie) *Jeśli R jest pierścieniem noetherowskim, to pierścień wielomianów $R[X]$ też jest noetherowski.*

Dowód: Niech I będzie ideałem w $R[X]$, który nie ma skończonego układu generatorów. Niech f_1 będzie niezerowym wielomianem najniższego stopnia, zawartym w I. Jeśli $f_1, \ldots, f_n$ są już wybrane, to niech $f_{n+1} \in I$ będzie wielomianem najniższego stopnia, nie leżącym w ideale I_n, generowanym przez $f_1, \ldots, f_n$. Jeśli $f_i(X) = a_i X^{N_i} + \cdots$ $(a_i \neq 0)$, to połóżmy

$$J_k = \sum_{j=1}^{k} a_j R.$$

Wtedy $N_1 \leq N_2 \leq \cdots$ oraz $J_1 \subset J_2 \subset J_3 \subset \ldots$.

Gdyby $J_{k+1} = J_k$, to $a_{k+1} = c_1 a_1 + \cdots + c_k a_k$ z pewnymi elementami $c_j \in R$. Wielomian

$$g(X) = \sum_{j=1}^{k} c_j X^{n_{k+1} - n_j} f_j(X) = a_{k+1} X^{n_{k+1}} + \cdots$$

leży w $I_k \subset I$, ale $\deg(f_{k+1} - g) < n_{k+1} = \deg f_{k+1}$, więc $f_{k+1} - g \in I_k$, co prowadzi do $f_{k+1} \in I_k$, sprzeczność. □

Pierścień całkowity R nazywa się *pierścieniem ideałów głównych*, jeśli każdy ideał w R jest ideałem głównym. Mówimy wtedy, że R jest pierścieniem PID (*"principal ideal domain"*). Jest to najprostsza klasa pierścieni noetherowskich. W takim pierścieniu każdy ideał jest generowany przez jeden element.

Z Faktu 3.8 wynika, że $\mathbb{Z}$ jest pierścieniem PID. Natępny rezultat prowadzi do innych pierścieni tego typu:

Twierdzenie 3.19. *Niech R będzie pierścieniem całkowitym. Jeśli istnieje funkcja $\Phi : R \longrightarrow \mathbb{N} \cup \{0\}$, spełniająca następujące warunki:*

(i) $\Phi(x) = 0$ zachodzi wtedy i tylko wtedy, gdy $x = 0$,

(ii) Dla dowolnych a i $b \neq 0$ z R istnieją $q, r \in R$ takie, że $a = qb + r$ oraz $\Phi(r) < \Phi(b)$,

to R jest pierścieniem ideałów głównych.

Dowód: Niech I będzie niezerowym ideałem w R i niech x będzie niezerowym elementem I o najmniejszej wartości $\Phi(x)$. Jeśli $y \in I$, to korzystając z (ii) napiszmy $y = qx + r$, przy czym $q, r \in R$, $\Phi(r) < \Phi(x)$. Z wyboru x wynika $\Phi(r) = 0$ i z (i) otrzymujemy $r = 0$, a więc $y \in xR$. Zatem $I \subset xR$, a ponieważ $xR \subset I$ jest oczywiste, otrzymujemy $I = xR$, a więc I jest ideałem głównym. □

Pierścienie całkowite, spełniające warunki (i) oraz (ii) tego twierdzenia nazywamy *pierścieniami euklidesowymi*. Najprostszym przykładem takiego pierścienia jest pierścień liczb całkowitych. W tym wypadku możemy przyjąć $\Phi(x) = |x|$. Spełnienie warunku (i) jest tu oczywiste, a warunek (ii) jest konsekwencją Lematu 1.7. Istnieją także ciekawsze przykłady:

Przykłady: a) Pierścień Gaussa $\mathbb{Z}[i] = \{x+iy : x, y \in \mathbb{Z}\}$. Pokażemy, że funkcja $\Phi(x+yi) = |x+iy|^2 = x^2 + y^2$ spełnia warunki Twierdzenia 3.19. Niech $a = x + iy$, $b = t + iu \neq 0$ i niech $w + is = a/b$. Istnieją liczby całkowite A, B spełniające $|w - A| \leq 1/2$ i $|s - B| \leq 1/2$. Jeśli teraz $q = A + iB$, to $q \in \mathbb{Z}[i]$, a przy tym

$$\left| \frac{a}{b} - q \right|^2 = (w - A)^2 + (s - B)^2 \leq \frac{1}{2},$$

więc jeśli przyjmiemy $r = a - qb$, to $r \in \mathbb{Z}[i]$ a przy tym

$$\Phi(r) = |r|^2 = |b|^2 \left| \frac{a}{b} - q \right|^2 \leq \frac{|b|^2}{2} < |b|^2 = \Phi(b).$$

Warunek (i) jest w tym przypadku oczywisty. □

b) Pierścień $K[X]$ wielomianów o współczynnikach w ciele K. Tutaj przyjmiemy dla $W \in K[X]$

$$\Phi(W) = \begin{cases} 0 & \text{gdy } W = 0, \\ 2^{\deg W} & \text{gdy } W \neq 0. \end{cases}$$

Spełnienie warunku (ii) jest konsekwencją następującego lematu:

Lemat 3.20. *Jeśli $f, g \in K[X]$ i $g \neq 0$, to istnieją $q, r \in K[X]$ takie, że $f = qg + r$, gdzie $q, r \in K[X]$, a nadto* $\deg r < \deg g$ *lub $r = 0$.*

Dowód: Niech $f(X) = a_n X^n + \cdots + a_0$, $g(X) = b_m X^m + \cdots + b_0$, przy czym $a_n, b_m \neq 0$. Jeśli $m < n$, to możemy przyjąć $q(X) = 0$, $r(X) = f(X)$, możemy więc założyć, że $m \geq n$.

Zastosujemy indukcję względem n. Jeśli $n = m$, to przyjmujemy $q(X) = a_n/b_m$. Wówczas teza będzie spełniona, jeśli

$$r(X) = f(X) - q(X)g(X) = (a_m X^m + a_{m-1}X^{m-1} + \ldots) - (\frac{a_m}{b_m})(b_m X^m + b_{m-1}X^{m-1} + \ldots).$$

Załózmy, że $n > m$, a teza jest prawdziwa dla wszystkich wielomianów stopnia mniejszego od n. Kładąc

$$h(X) = \frac{a_n}{b_m} X^{n-m}$$

oraz

$$\begin{aligned} W(X) = f(X) - h(X)g(X) &= (a_n X^n + a_{n-1}X^{n-1} + \ldots) - (\frac{a_n}{b_m} X^{n-m})(b_m X^m + b_{m-1}X^{m-1} + \ldots) \\ &= \left(a_{n-1} - \frac{a_n b_{m-1}}{b_m} X^{n-1}\right) + \ldots \end{aligned}$$

widzimy, że do pary W, g możemy zastosować przesłankę indukcyjną, gdyż mamy $\deg W < n$ lub $W = 0$. Możemy zatem napisać $W(X) = A(X)g(X) + B(X)$, przy czym $A, B \in K[X]$ i $\deg B < \deg g$ lub $B = 0$, a to prowadzi do

$$f(X) = h(X)g(X) + W(X) = (h(X) + A(X))g(X) + B(X)$$

i przyjmując $q = hg$ i $r = B$ otrzymujemy tezę. □

Jako wniosek otrzymamy teraz

Twierdzenie 3.21. *Jeśli K jest ciałem, to każdy ideał w $K[X]$ jest ideałem głównym.*

Dowód: Wynika z poprzedniego przykładu i Twierdzenia 3.19. □

5. Niech R będzie pierścieniem całkowitym. Element $u \in R$ nazywa się *elementem odwracalnym*, jeśli istnieje $v \in R$, takie, że $uv = 1$. Zbiór wszystkich elementów odwracalnych pierścienia R oznaczamy przez $U(R)$. Nietrudno zauważyć, że $U(\mathbb{Z}) = \{-1, 1\}$, a $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Twierdzenie 3.22. *Zbiór $U(R)$ jest grupą względem mnożenia.*

Dowód: Jeśli $u \in U(R)$, to istnieje $v \in R$ takie, że $uv = 1$, a wtedy $v \in U(R)$, tj. $U(R)$ jest zamknięty na elementy odwrotne. Jeśli $u_1, u_2 \in U(R)$, to istnieją $v_1, v_2 \in U(R)$, spełniające $u_i v_i = 1$ dla $i = 1, 2$, a stąd otrzymujemy $(u_1 u_2)(v_1 v_2) = 1$, tak więc $U(R)$ jest zamknięty na mnożenie. □

Przykład: Niech $R = \{x + y\sqrt{2} : \ x, y \in \mathbb{Z}\}$. Nietrudno sprawdzić, że R jest pierścieniem całkowitym. Równość

$$(1 + \sqrt{2})(-1 + \sqrt{2}) = 1$$

pokazuje, że liczba $\epsilon = 1 + \sqrt{2}$ jest odwracalna w R, tj. leży w $U(R)$. Zatem wszystkie potęgi ϵ też leżą w $U(R)$, a ponieważ $\epsilon > 1$ przeto liczby $\epsilon, \epsilon^2, \ldots$ są wszystkie różne. Można pokazać, korzystając z teorii liczb, że w tym przypadku grupa $U(R)$ jest izomorficzna z sumą prostą grupy cyklicznej nieskończonej i grupy C_2.

Niezerowy element $\pi \in R$ nazywa się *elementem nierozkładalnym*, gdy nie jest odwracalny, a z równości $\pi = ab$ z $a, b \in R$ wynika, że jeden z czynników a, b jest odwracalny. Wynika stąd, że jeśli π jest nierozkładalny, a c dzieli π, to $c \in U(R)$, lub też $c = \epsilon\pi$ przy pewnym $\epsilon \in U(R)$.

Przykład: *W przypadku $R = \mathbb{Z}$ elementy nierozkładalne, to liczby pierwsze i liczby do nich przeciwne.*

Mówimy, że pierścień całkowity R jest *pierścieniem z jednoznacznością rozkładu*, jeśli spełnione są następujące warunki:

(i) *Każdy niezerowy i nieodwracalny element $a \in R$ da się przedstawić w postaci*

$$a = \pi_1 \pi_2 \cdots \pi_r,$$

gdzie $r \geq 1$, a elementy $\pi_1, \ldots, \pi_r$ są nierozkładalne,

(ii) *Jeśli*

$$a = \pi_1 \pi_2 \cdots \pi_r = P_1 P_2 \cdots P_s$$

są dwoma rozkładami elementu a na elementy nierozkładalne, to $r = s$ i można tak przenumerować elementy $P_1, \ldots, P_r$, by zachodziły równości

$$P_i = \epsilon_i \pi_i \quad (i = 1, 2, \ldots, r).$$

Elementy $a, b \in R$ różniące się czynnikiem odwracalnym (tj. $a = \epsilon b$ z odwracalnym ϵ) nazywają się *stowarzyszone*. Łatwo zauważyć, że jeśli a i b są stowarzyszone, to $a|b$ i $b|a$, a nadto dla $c \in R$ warunki $c|a$ i $c|b$ są równoważne, podobnie jak i warunki $a|c$ i $b|c$. Nietrudno też spostrzec, że elementy a, b są stowarzyszone wtedy i tylko wtedy, gdy ideały główne, generowane przez a i b są równe, tj. $aR = bR$.

Pierścienie z jednoznacznością rozkładu nazywane są także *pierścieniami UFD*, od angielskiej nazwy "*unique factorization domain*".

Twierdzenie 3.23. *(i) Jeśli R jest noetherowskim pierścieniem całkowitym, to każdy nieodwracalny jego element $a \neq 0$ da się przedstawić w postaci iloczynu elementów nierozkładalnych.*

(ii) Jeśli R jest pierścieniem całkowitym, w którym każdy element niezerowy i nieodwracalny jest iloczynem elementów nierozkładalnych, to na to by R był pierścieniem z jednoznacznością rozkładu potrzeba i wystarcza, by dla każdego elementu nierozkładalnego π zachodziła implikacja: jeśli π dzieli iloczyn 2 elementów, to dzieli przynajmniej jeden z nich.

Dowód: (i) Najpierw pokażemy, że każdy niezerowy i nieodwracalny element R jest podzielny przez conajmniej jeden element nierozkładalny. Niech $a \in R$, $a \neq 0$, $a \notin U(R)$ i załóżmy, że a nie dzieli się przez żaden element nierozkładalny. W szczególności a nie jest nierozkładalny, zatem istnieją elementy $a_1, b_1 \in R \setminus U(R)$, takie, że $a = a_1 b_1$ i żaden z nich nie ma dzielnika nierozkładalnego. Kontynuując to postępowanie otrzymamy nieskończony ciąg niestowarzyszonych elementów $a_0 = a, a_1, a_2, \ldots$, spełniających warunek $a_{n+1}|a_n$ dla $n = 0, 1, 2, \ldots$. Niech $I_n = a_n R$ będzie ideałem głównym, generowanym przez a_n. Mamy wówczas

$$I_0 \subset I_1 \subset I_2 \subset I_n \subset \ldots,$$

przy czym wszystkie inkluzje są właściwe i żaden z ideałów I_n nie jest równy R, a więc nie zawiera 1. Twierdzenie 3.17 pokazuje, że sytuacja taka nie jest możliwa.

Teraz możemy pokazać, że każdy niezerowy element $a \in R \setminus U(R)$ jest iloczynem elementów nierozkładalnych. Przypuśćmy, że dla pewnego a nie jest to prawdą. Niech π_1 będzie nierozkładalnym dzielnikiem a i niech $a_1 = a/\pi_1$. Jeśli a_1 jest nierozkładalny, to $a = \pi_1 a_1$ jest iloczynem elementów nierozkładalnych, wbrew założeniu. Powtarzając to postępowanie otrzymamy nieskończony ciąg $a_0 = a, a_1, a_2, \ldots, a_n, \ldots$ elementów R i ciąg elementów nierozkładalnych $\pi_1, \pi_2, \ldots$, spełniających $a_n = a_{n+1}\pi_{n+1}$ dla $n = 1, 2, \ldots$. Wynika stąd, że ideały $I_n = a_n R$ tworzą ciąg wstępujący, co przeczy Twierdzeniu 3.17.

(ii) Załóżmy, że R jest UFD i niech π będzie elementem nierozkładalnym, dzielącym iloczyn ab. Zatem istnieje $c \in R$ takie, że $ab = c\pi$ i rozkładając c na czynniki nierozkładalne otrzymamy rozkład iloczynu ab, w którym π jest jednym z czynników. Jeśli π nie dzieli ani a ani b, to rozkłady tych elementów nie mogą zawierać czynnika stowarzyszonego z π, a to prowadzi do rozkładu ab, różnego od poprzedniego, sprzeczność.

Załóżmy teraz słuszność implikacji wymienionej w twierdzeniu. Zauważmy, że łatwą indukcją otrzymujemy, że z $\pi | \prod_{i=1}^n a_i$ wynika, iż π dzieli conajmniej jeden z elementów a_i.

Gdyby R nie był pierścieniem UFD, to istniałby element $a \in R$, mający dwa istotnie różne rozkłady na elementy nierozkładalne, powiedzmy

$$a = \prod_{i=1}^{r} \pi_i = \prod_{i=1}^{s} \rho_i. \tag{3.6}$$

Możemy założyć, że $r \leq s$, a element a jest tak dobrany, by r było najmniejsze.

Ponieważ π_1 dzieli $\rho_1 \cdots \rho_s$, zatem π_1 dzieli pewien element ρ_j, a zatem ρ_j i π_1 są stowarzyszone, tj. $\rho_j = \epsilon \pi_1$ z pewnym $\epsilon \in U(R)$. Dzieląc obie strony równości (3.6) przez π_1 widzimy, że a/π_i ma dwa różne rozkłady o długościach $s - 1 \geq r - 1$, co przeczy wyborowi a. $\square$

Wniosek 1: *Jeśli R jest noetherowskim pierścieniem całkowitym, to jest on pierścieniem z jednoznacznością rozkładu wtedy i tylko wtedy gdy implikacja $\pi|ab \Leftrightarrow \pi|a$ lub $\pi|b$ zachodzi dla każdego elementu nierozkładalnego $\pi \in R$* $\square$.

Wniosek 2. *Jeśli R jest noetherowskim pierścieniem całkowitym, to jest on pierścieniem z jednoznacznością rozkładu wtedy i tylko wtedy gdy ideały główne generowane przez elementy nierozkładalne są ideałami pierwszymi.* $\square$

Uwaga: W Twierdzeniu 3.23 warunku całkowitości pierścienia nie można opuścić, gdyż np. w pierścieniu reszt z dzielenia przez 15 niezerowymi elementami nieodwracalnymi są reszty $\{3, 5, 6, 9, 10, 12\}$, ale żaden z tych elementów nie jest nierozkładalny.

Następujący wynik jest uogólnieniem Lematu 1.8:

Twierdzenie 3.24. *Jeśli R jest pierścieniem ideałów głównych, $a, b \in R$ i nie istnieje nieodwracalny element $c \in R$, dzielący zarówno a jak i b, to istnieją elementy $x, y \in R$, spełniające*

$$ax + by = 1.$$

Dowód: Niech I będzie najmniejszym ideałem, zawierającym oba elementy a, b. Z lematu 3.6 zastosowanego do a i ideału bR wynika, że $I = \{ax + by : \ x, y \in R\}$. Ponieważ R jest pierścieniem PID, zatem istnieje element c, dla którego mamy $I = cR$. Ponieważ $a, b \in I$, przeto c dzieli zarówno a, jak i b. Ponieważ z założenia wynika, że c jest odwracalny, zatem z uwagi na $1 = c \cdot c^{-1}$ widzimy, że $1 \in cR = I$, a zatem $1 = ax + by$ przy odpowiednich $x, y \in R$. $\square$

Zastosujemy to twierdzenia do pokazania, że każdy pierścień PID jest UFD:

Twierdzenie 3.25. *Jeśli R jest pierścieniem ideałów głównych, to jest pierścieniem z jednoznacznością rozkładu.*

Dowód: Z Wniosku 1 z Twierdzenia 3.23 otrzymujemy, że wystarczy pokazać, iż z podzielności ab przez element nierozkładalny π wynika podzielność przez π jednego z elementów a, b. Niech zatem $\pi \in R$ będzie elementem nierozkładalnym i załóżmy, że $\pi|ab$, ale $\pi \nmid a$. Zastosujemy Twierdzenie 3.24 do elementów π i a. Możemy to uczynić, gdyż nie ma elementu nierozkładalnego dzielącego π i a. Zatem istnieją $x, y \in R$ spełniające $ax + \pi y = 1$, a więc

$$abx + \pi yb = b.$$

Ponieważ $\pi|ab$, zatem $\pi|b$. $\square$

Wniosek: *Każdy pierścień euklidesowy jest pierścieniem z jednoznacznym rozkładem. Dotyczy to w szczególności pierścieni $\mathbb{Z}$, $\mathbb{Z}[i]$ oraz $K[X]$, gdzie K jest dowolnym ciałem.* $\square$

6. Zajmiemy się teraz nieco bliżej pierścieniami z jednoznacznością rozkładu. Niech R będzie takim pierścieniem. Wygodnie jest wybrać jeden element z każdej klasy stowarzyszonych elementów nierozkładalnych. Niech P będzie zbiorem tak wybranych reprezentantów. W przypadku $R = \mathbb{Z}$ klasy te mają postać $\{-p, p\}$, gdzie p jest liczbą pierwszą i z każdej takiej klasy wybieramy liczbę dodatnią, a więc w tym wypadku P jest zbiorem liczb pierwszych.

Każdy niezerowy i nieodwracalny element $a \in R$ możemy przedstawić w postaci iloczynu elementów nierozkładalnych zasadniczo na jeden sposób. Jeśli w takim przedstawieniu pojawią się czynniki stowarzyszone z elementami z P, to zapisujemy je w postaci iloczynu elementu z P i elementu odwracalnego. Tak więc zawsze możemy napisać

$$a = \epsilon \prod_{j=1}^{k} \rho_j,$$

gdzie $\epsilon \in U(R), \rho_j \in P$. Łącząc razem powtarzające się czynniki możemy przekształcić ten rozkład do postaci

$$a = \epsilon \prod_{j=1}^{r} \pi_j^{\alpha_j},$$

przy czym $\epsilon \in U(R)$, elementy $\pi_j \in P$ są wszystkie różne, a $\alpha_j \geq 1$ są liczbami całkowitymi. Wygodnie jest dopuszczać także wykładniki zerowe, co pozwoli na napisanie

$$a = \epsilon \prod_{\pi \in P} \pi^{\alpha(p)},$$

prz czym wykładniki $\alpha(p) \geq 0$ są całkowite, ale jedynie skończenie wiele z nich jest różnych od zera. I tak np. zamiast pisać $80 = 2^4 \cdot 5$ piszemy

$$48 = 2^4 \cdot 3^0 \cdot 5 \cdot 7^0 \cdots .$$

Zapis ten możemy stosować także do elementów $a \in U(R)$. W tym wypadku wszystkie wykładniki $\alpha(p)$ są równe zeru. Wygoda tego dziwnego zapisu za chwilę się pojawi.

Jeśli $a, b \in R$ są niezerowe, to *największym wspólnym dzielnikiem* tych elementów nazywamy taki element c, który dzieli a i b, a na dodatek każdy element d, dzielący a i b jest dzielnikiem c. Taki element, o ile istnieje, oznaczamy przez $NWD(a, b)$.

Najmniejszą wspólną wielokrotnością a i b nazywamy taki element c, który dzieli się przez a i b, a na dodatek każdy element d, podzielny przez a i b jest podzielny przez c, tj. jest wielokrotnością c. Taki element, o ile istnieje, oznaczamy przez $NWW(a, b)$.

Twierdzenie 3.26. *(i) Jeśli R jest UFD, to każda para elementów $a, b \in R$ posiada $NWD(a, b)$ i $NWW(a, b)$.*

(ii) Jeśli

$$a = \epsilon \prod_{p \in P} p^{\alpha(p)}, \quad b = \eta \prod_{p \in P} p^{\beta(p)}, \tag{3.7}$$

gdzie $\epsilon, \eta \in U(R), \alpha(p) \geq 0, \beta(p) \geq 0$, to

$$NWD(a, b) = \prod_{p \in P} p^{\gamma(p)}, \quad NWW(a, b) = \prod_{p \in P} p^{\delta(p)},$$

gdzie $\gamma(p) = \min\{\alpha(p), \beta(p)\}$, $\delta(p) = \max\{\alpha(p), \beta(p)\}$

(iii) Elementy $NWD(a, b)$ i $NWW(a, b)$ są wyznaczone jedynie z dokładnością do odwracalnego czynnika.

(iv) Elementy ab i $NWD(a, b) \cdot NWW(a, b)$ są stowarzyszone.

Dowód: Rozpoczniemy od prostego lematu:

Lemat 3.27. *Jeśli R jest UFD oraz $a, b \in R$ są postaci* (3.7)*, to a dzieli b wtedy i tylko wtedy, gdy dla wszystkich $p \in P$ mamy $\alpha(p) \leq \beta(p)$.*

Dowód: Jeśli dla wszystkich $p \in P$ zachodzi nierówność $a(p) \leq \beta(p)$, to $n(p) = a(p) - \beta(p) \geq 0$, a więc

$$c = \prod_{p \in P} p^{n(p)} \in R$$

i $a \cdot (\eta\epsilon^{-1}c) = b$, co z uwagi na $\eta\epsilon^{-1} \in U(R)$ daje $a|b$. □

Jeśli teraz $A = \prod_{p \in P} p^{\gamma(p)}$, gdzie $\gamma(p) = \min\{\alpha(p), \beta(p)\}$, to z lematu wynika $A|a$ i $A|b$, a jeśli $B = u \prod_{p \in P} p^{\lambda(p)}$ (przy czym $u \in U(R)$ i $\lambda(p) \geq 0$) dzieli a i b, to z lematu wynika $\lambda(p) \leq \alpha(p)$ i $\lambda(p) \leq \beta(p)$. To prowadzi do $\lambda(p) \leq \gamma(p)$ i kolejne zastosowanie lematu daje $B|A$, tak więc $NWD(a, b)$. Dowiedliśmy w ten sposób pierwszych części (i) i (ii).

By udowodnić części drugie połóżmy $\mathfrak{A} = \prod_{p \in P} p^{\delta(p)}$, gdzie $\delta(p) = \max\{\alpha(p), \beta(p)\}$. Z lematu wynika podzielność $\mathfrak{A}$ przez a i b, a jeśli $\mathfrak{B} = v \prod_{p \in P} p^{\mu(p)}$ (przy czym $v \in U(R)$ i $\mu(p) \geq 0$) dzieli się zarówno przez a, jak i b, to z lematu wynika $\mu(p) \geq \alpha(p)$ i $\mu(p) \geq \beta(p)$, zatem $\mu(p) \geq \delta(p)$ i lemat daje podzielność $\mathfrak{B}$ przez $\mathfrak{A}$. W ten sposób udowodniliśmy (i) i (ii), a dowód (iii) wynika z uwagi, że jeśli a i a' są stowarzyszone, a także b i b' są stowarzyszone, to warunki $a|b$ i $a'|b'$ są równoważne. Warunek (iv) jest konsekwencją równości

$$x + y = \max\{x, y\} + \min\{x, y\},$$

słusznej dla dowolnych liczb rzeczywistych x, y. □

7. Znajdowanie $NWD(a,b)$ i $NWW(a,b)$ jest proste, gdy znamy rozkłady elementów a, b na czynniki nierozkładalne. I tak np. w pierścieniu $\mathbb{Z}$ dla liczb

$$a = 45\,394\,981\,632, \quad b = 1\,542\,206\,324\,736$$

bez trudu otrzymamy

$$NWD(a,b) = 1\,596\,672, \quad NWW(a,b) = 43\,846\,468\,018\,569\,216,$$

jeśli wiemy, że

$$a = 2^8 3^{11} 7 \cdot 11 \cdot 13, \quad b = 2^{16} 3^4 7^4 11^2.$$

W przypadku pierścieni euklidesowych istnieją lepsze metody znajdowania NWW. Podamy takie dwie metody w przypadku pierścienia liczb całkowitych. Pierwsza z nich została opisana w "*Elementach*" Euklidesa (ok. 2300 lat temu) i nosi nazwę *algorytmu Euklidesa*.

Twierdzenie 3.28. (Euklides) *Niech $a < b$ będą liczbami naturalnymi. Zdefiniujemy dwa ciągi $q_1, q_2, \ldots$ i $r_0, r_1, r_2, \ldots$ liczb całkowitych nieujemnych kładąc $r_{-1} = a, r_0 = b$, a jeśli już mamy wyznaczone liczby $r_{-1}, r_0, q_1, r_1, \ldots, q_m, r_m$, a przy tym $r_m > 0$, to q_{m+1}, r_{m+1} wyznaczamy na podstawie Lematu 1.7 z równości*

$$r_{m-1} = q_{m+1} r_m + r_{m+1} \quad (0 \leq r_{m+1} < r_m). \tag{3.8}$$

Ponieważ ciąg $r_0, r_1, r_2, \ldots$ jest malejący, zatem dla pewnego indeksu n mamy $r_n = 0$, a wtedy $NWD(a,b) = r_{n-1}$.

Dowód: Pokażemy przez indukcję, że r_{n-1} dzieli r_j dla $j = n, n-1, \ldots, 1, 0, -1$. W istocie, $r_{n-1}|0 = r_n$ i $r_{n-1}|r_{n-1}$, a jeśli r_{n-1} dzieli r_{k+1} i r_k, to wobec (3.8) dzieli także r_{k-1}. Prosta indukcja pokazuje, że r_{n-1} jest wspólnym dzielnikiem a i b, a więc $0 < r_{n-1} \leq NWD(a,b)$.

Teraz pokażemy, że $NWD(a,b)$ dzieli każdy wyraz ciągu r_k. W istocie $NWD(a,b)$ dzieli $r_{-1} = a$ i $r_0 = b$, a jeśli dzieli r_{k-1} i r_k, to wobec (3.8) dzieli także r_{k+1}. Zatem $NWD(a,b)$ dzieli r_{n-1}, co prowadzi do $NWD(a,b) \leq r_{n-1}$ i ostatecznie otrzymujemy $NWD(a,b) = r_{n-1}$. □

Podany tu algorytm ta daje się stosować z oczywistymi zmianami w dowolnych pierścieniach euklidesowych (stąd się bierze ich nazwa).

Wadą algorytmu Euklidesa jest konieczność wielokrotnego wykonywania dzielenia z resztą, co dla dużych liczb może być czasochłonne. Podamy teraz inny sposób znajdowania największego wspólnego dzielnika, zaproponowany w 1962 r. przez R.Silvera i J.Terziana, nie mający tej wady. Stosuje on jedynie odejmowanie i dzielenie przez 2, a w wielu przypadkach jest szybszy od algorytmu Euklidesa. Algorytm ten nazywa się *binarnym algorytmem znajdowania największego wspólnego dzielnika.*

Pomysł jest bardzo prosty: jeśli liczby a, b są obie parzyste, to zastępujemy a przez $a/2$ i b przez $b/2$, zapamiętując wspólny czynnik 2; jeżeli dokładnie jedna z tych liczb jest parzysta, to dzielimy ją przez 2, nie zmieniając drugiej. Jeśli wreszcie obie są nieparzyste i różne, to odejmujemy mniejszą od większej, a mniejszą zostawiamy bez zmiany. Następnie powtarzamy te czynności. Czytelnik sprawdzi bez trudu, że przy tej procedurze iloczyn $NWD(a,b)$ przez iloczyn zapamiętanych dwójek nie ulega zmianie, a ponieważ mniejsza z liczb stale się zmniejsza, więc po pewnym czasie algorytm musi doprowadzić do $a = b$ lub $\min\{a,b\} = 1$, co oczywiście wyznacza szukany największy wspólny dzielnik.

Procedurę tę można nieco przyśpieszyć, jeśli w przypadku nieparzystych a, b o dużej różnicy, zamiast brania różnicy wykonamy dzielenie z resztą. Obliczając tym sposobem, dla przykładu, największy wspólny dzielnik liczb 23 458 i 1235 otrzymujemy

$$\begin{array}{cc} 23458 & 1235 \\ 11729 & 1235 \end{array}$$

i tu, zamiast odejmowania, wykonujemy dzielenie z resztą, co prowadzi do pary

$$\begin{array}{cc} 1235 & 614 \end{array}$$

i dalej mamy:

$$\begin{array}{rl} 1235 & 307 \\ 928 & 307 \\ 464 & 307 \\ 232 & 307 \\ 116 & 307 \\ 58 & 307 \\ 29 & 307 \\ 29 & \;\;17 = 307 - 10 \cdot 29 \end{array}$$

a tu już widzimy, że $NWD(a, b) = 1$.

8. Pojęcie największego wspólnego dzielnika wykorzystamy do dowodu, że własność jednoznacznego rozkładu zachowuje się przy przejściu od pierścienia do pierścienia wielomian;ow.

Twierdzenie 3.29. *Jeśli R jest UFD, to $R[X]$ też.*

Dowód: Dla $f \in R[X]$ niech $V(f)$ będzie ideałem głównym generowanym przez największy wspólny dzielnik współczynników f (jest to tzw. *pojemność* wielomianu f). Jeśli $V(f) = R$, to mówimy, że f jest *wielomianem pierwotnym.*

Lemat 3.30. (Lemat Gaussa): *Jesli $V(f) = V(g) = R$, to $V(fg) = R$.*

Dowód: Niech $f(X) = a_nX^n + \cdots + a_0$, $g(X) = b_mX^m + \cdots + b_0$ i $f(X)g(X) = c_{n+m}X^{n+m} + \cdots + c_0$. Załóżmy, że $V(fg) = vR$, przy czym $v \notin U(R)$. Niech π będzie dowolnym elementem nierozkładalnym, dzielącym v. Wtedy $\pi|a_0b_0$, więc $\pi|a_0$ lub $\pi|b_0$. Załóżmy, że r, s są najmniejszymi indeksami, spełniającymi $\pi \nmid a_r$, $\pi \nmid b_s$.

Wobec

$$\pi|v|c_{rs} = a_rb_s + \sum_{\substack{i+j=rs \\ [i,j]\neq[r,s]}} a_ib_j$$

otrzymujemy sprzeczność. □

Wniosek: *Jeśli $V(f) = vR$, $V(g) = uR$, to $V(fg) = uvR$.*

Dowód: Mamy $f(X) = vF(X)$ i $g(X) = uG(X)$, przy czym F, G są pierwotne. Z lematu wynika, że FG jest wielomianem pierwotnym i pozostaje zauważyć, że

$$f(X)g(X) = uv(F(X)G(X)). \qquad \square$$

Lemat 3.31. *Jeśli $W \in R[X]$ jest nierozkładalny w R, to jest także nierozkładalny w ciele ułamków pierścienia R.*

Dowód: Niech W będzie wielomianem nierozkładalnym w R. Wtedy oczywiście $V(W) = R$. Przypuśćmy, że W jest rozkładalny w K, ciele ułamków R, np. $W(X) = f(X)g(X)$ z $f, g \in K[X]$, $\deg f, g \geq 1$. Możemy napisać

$$f(X) = \frac{a}{q_1}F(X), \quad g(X) = \frac{b}{q_2}G(X),$$

gdzie $a, b, q_1, q_2 \in R$, a wielomiany $F, G \in R[X]$ są pierwotne. Wówczas

$$q_1q_2W(X) = (aF(X))(bG(X))$$

i z wniosku otrzymujemy

$$q_1q_2R = V(q_1q_2W) = V(aF)V(bG) = abR,$$

co prowadzi do nietrywialnego rozkładu

$$W(X) = \epsilon F(X)G(X), \quad (\epsilon \in U(R)$$

gdyż $\deg F = \deg f \geq 1$ i $\deg G = \deg g \geq 1$. Otrzymana sprzeczność dowodzi prawdziwości lematu. $\square$

Teraz możemy udowodnić nasze twierdzenie. Elementy nierozkładalne w $R[X]$ to albo nierozkładalne wielomiany stopnia ≥ 1, albo też nierozkładalne elementy R, traktowane jako wielomiany stałe. Rozpatrzymy oba przypadki.

Najpierw niech $\pi(X) \in R[X]$ będzie wielomianem nierozkładalnym w R stopnia ≥ 1 i niech $\pi(X)$ dzieli iloczyn $f(X)g(X)$ $(f, g \in R[X])$. Z lematu 3.31 wynika nierozkładalność $\pi(X)$ w ciele K, a zatem π dzieli f lub g w K. Powiedzmy, że $\pi | f$ w K, a więc istnieje wielomian $h \in K[X]$ taki, że $f(X) = \pi(X)h(X)$. Możemy napisać

$$h(X) = \frac{a}{q} H(X),$$

$$f(X) = bF(X),$$

gdzie $F, H \in R[X]$ są wielomianami pierwotnymi, a $a, b, q \in R$. To prowadzi do

$$bqF(X) = aH(X)\pi(X),$$

ale $\pi(X)$ jest pierwotny, a więc $bq = a$ i otrzymujemy $F(X) = H(X)\pi(X)$, a zatem

$$\pi(X) | F(X) | bF(X) = f(X).$$

Teraz niech $\pi \in R$ będzie elementem nierozkładalnym w R i niech $\pi | f(X)g(X)$, gdzie $f, g \in R[X]$. Oznacza to, że π dzieli wszystkie współczynniki iloczynu fg, a zatem jeśli $V(fg) = aR$, to $\pi | a$. Jeśli $V(f) = bR$, $V(g) = cR$, to z uwagi na wniosek z Lematu 3.30 mamy $V(fg) = V(f)V(g)$, a więc $a = \epsilon bc$, gdzie ϵ jest elementem odwracalnym. Z podzielności a przez π wynika, że $\pi | b$ lub $\pi | c$, a więc $\pi | f$ lub $\pi | g$. $\square$

Uwaga 1. Jeśli R jest PID, to powtarzając rozumowanie podane w przypadku $R = \mathbb{Z}$ w dowodzie Faktu 3.8 otrzymujemy, że ideał generowany przez element nierozkładalny jest ideałem maksymalnym. Nie jest to prawdą w dowolnych pierścieniach całkowitych. Np. w pierścieniu $\mathbb{Z}[X]$ wielomian X jest nierozkładalny, ale ideał $I = X\mathbb{Z}[X]$ przezeń generowany nie jest maksymalny, bo łatwo pokazać, że pierścień ilorazowy $\mathbb{Z}[X]/I$ jest izomorficzny z $\mathbb{Z}$, a więc nie jest ciałem.

Uwaga 2. Wszystkie poznane dotąd przykłady pierścieni z jednoznacznym rozkładem były pierścieniami ideałów głównych. Twierdzenie 3.29 pozwala podać przykład pierścienia UFD, który nie jest PID. Rozpatrzmy pierścień $\mathbb{C}[X, Y]$ wielomianów 2 zmiennych o zespolonych współczynnikach. Z Twierdzenia 3.29 wynika, że jest to pierścień z jednoznacznością rozkładu. Połóżmy

$$I = \{W(X, Y)X + V(X, Y)Y : \; W, V \in \mathbb{C}[X, Y]\}.$$

Bez trudu sprawdzamy, że I jest ideałem w $\mathbb{C}[X, Y]$, zawierającym zarówno X jak i Y. Pokażemy, że nie jest to ideał główny. W istocie, gdyby dla pewnego wielomianu f 2 zmiennych mielibyśmy $I = f(X, Y)\mathbb{C}[X, Y]$, to oba wielomiany X i Y dzieliłyby się przez f, co jest możliwe tylko wtedy, gdy f jest wielomianem stałym, a więc $I = \mathbb{C}[X, Y]$. Ale wtedy $1 \in I$, a zatem istnieją wielomiany W i V, spełniające

$$W(X, Y)X + V(X, Y)Y = 1,$$

co nie jest możliwe, bo funkcja wielomianowa związana z wielomianem po lewej stronie tej równości przyjmuje w punkcie $(0, 0)$ wartość 0, a to prowadzi do równości $0 = 1$.

9. Twierdzenie 3.32 (Twierdzenie Bezout'a) *Jeśli K jest ciałem, a $W \in K[X]$, to $a \in K$ jest pierwiastkiem W wtedy i tylko wtedy, gdy wielomian W jest podzielny przez $X - a$.*

Dowód: Korzystając z Lematu 3.20 możemy napisać

$$W(X) = q(X)(X - a) + r(X),$$

gdzie $q, r \in K[X]$, a przy tym $r = 0$, lub też $\deg r < \deg(X - a) = 1$, tj. $r(X) = c$, przy pewnym $c \in K$. Traktując tę równość jako równość pomiędzy funkcjami wielomianowymi i podstawiając $X = a$, otrzymamy $W(a) = c$. Zatem a będzie zerem W wtedy i tylko wtedy, gdy $c = 0$, tj. $r = 0$, a więc $X - a$ dzieli W. $\square$

Jeśli a jest pierwiastkiem wielomianu $W \neq 0$, to mówimy, że ma on *krotność* r, jeśli $(X-a)^r | W(X)$, ale $(X-a)^{r+1} \nmid W(X)$, tj. mamy

$$W(X) = (X-a)^r V(X),$$

gdzie $V \in K[X]$ i $V(a) \neq 0$.

I tak np. liczba 1 jest dwukrotnym pierwiastkiem wielomianu $W(X) = X^3 + X^2 - 5X + 3$, a liczba -3 jest jego pierwiastkiem jednokrotnym, gdyż $W(X) = (X-1)^2(X+3)$.

Twierdzenie 3.33. *Jeśli K jest ciałem, a $W \in K[X]$ ma stopień n, to W może mieć conajwyżej n pierwiastków w K liczonych wraz z krotnościami.*

Dowód: Zastosujemy indukcję względem stopnia wielomianu W. Jeśli $\deg W = 1$, tj. $W(X) = aX + b$, to jedynym pierwiastkiem W jest element $-ba^{-1}$. Załóżmy prawdziwość tezy dla wielomianów stopni $< n$ i niech $\deg W = n$. Jeśli W nie ma pierwiastków w ciele K, to teza jest oczywiście prawdziwa. Jeśli zaś $a \in K$ jest pierwiastkiem W, to z twierdzenia wynika istnienie wielomianu $W_1 \in K[X]$, spełniającego $W(X) = (X-a)W_1(X)$, a ponieważ $\deg W_1 = n - 1 < n$, to możemy zastosować założenie indukcyjne do wielomianu W_1. □

Wniosek *Każda skończona podgrupa grupy multyplikatywnej ciała jest cykliczna.*

Dowód: Wynika z twierdzenia i z wniosku z Twierdzenia 2.30. □

Pochodną wielomianu $W(X) = \sum_{j=0}^{N} a_j X^j \in K[X]$ możemy zdefiniować bez pojęcia granicy wzorem

$$W'(X) = \sum_{j=1}^{N} j a_j X^{j-1}. \tag{3.9}$$

Bez trudu sprawdzamy, że znane z analizy wzory

$$(W+V)' = W' + V', \quad (WV)' =' V + WV' \tag{3.10}$$

są słuszne i w naszej sytuacji. Jednakże nie wszystkie własności pochodnej, znane a znalizy, przenoszą sią na nasz przypadek. Jeśli np. K jest ciałem 2-elementowym, a $W(X) = x^2$, to W' jest wielomianem zerowym, ale funkcja wielomianowa wyznaczona przez W nie jest stałą, gdyż $W(0) = 0 \neq 1 = W(1)$.

Twierdzenie 3.34. *Niech $K \subset L$ będą ciałami. Jeśli element $a \in L$ jest r-krotnym pierwiastkiem wielomianu $W \in K[X]$, a $r \geq 2$, to a jest pierwiastkiem $W'(X)$. Jeśli przy tym r nie dzieli się przez charakterystykę ciała K, to a jest $(r-1)$-krotnym pierwiastkiem $W'(X)$.*

Dowód: Z definicji krotności wynika równość

$$W(X) = (X-a)^r V(X),$$

przy czym $V(a) \neq 0$.

Korzystając z (3.10) otrzymujemy

$$W'(X) = r(X-a)^{r-1}V(X) + (X-a)^r V'(X) = (X-a)^{r-1}(rV(X) + (X-a)V'(X))$$

i z uwagi na $r \geq 2$ otrzymujemy $W'(a) = 0$. Gdyby element a był pierwiastkiem wielomianu

$$rV(X) + (X-a)V'(X),$$

to mielibyśmy $rV(a) = 0$, co wobec $V(a) \neq 0$ jest możliwe jedynie wówczas, gdy r dzieli się przez charakterystykę ciała K, gdyż ciała nie mają dzielników zera. □

Uwaga: Warunek w drugiej części Twierdzenia 3.34 jest istotny, bo np. w dowolnym ciele charakterystyki p element 1 jest p-krotnym pierwiastkiem wielomianu $W(X) = X^p - 1$ dzięki równości

$$X^p - 1 = (X-1)^p,$$

zaś pochodna $W'(X)$ jest wielomianem zerowym, a więc 1 nie jest jej $(p-1)$-krotnym pierwiastkiem.

8. Zajmiemy się teraz istnieniem pierwiastków wielomianów.

Twierdzenie 3.35. *Jeśli K jest ciałem, a $W \in K[X]$ jest wielomianem nierozkładalnym dodatniego stopnia, to istnieje ciało L, zawierające K, w którym W ma pierwiastek. Przy tym L, traktowane jako przestrzeń liniowa nad K ma wymiar skończony, równy* $\deg W$.

Dowód: Z uwagi po Twierdzeniu 3.29 wynika, że ideał I, generowany przez W jest ideałem maksymalnym, a Twierdzenie 3.5 pokazuje teraz, że pierścień ilorazowy $L = K[X]/I$ jest ciałem. Jeśli $\phi : K[X] \longrightarrow K[X]/I$ jest kanonicznym homomorfizmem, to jego obcięcie do K jest monomorfizmem, a więc obraz $\phi(K)$ jest podciałem L, izomorficznym z K, możemy więc utożsamić K z tym obrazem, co daje $\phi(a) = a$ dla $a \in K$. Niech

$$\theta = \phi(X) = X + I.$$

Jeśli $W(t) = \sum_{j=0}^{N} a_j t^j$, to

$$W(\theta) \sum_{j=0}^{N} a_j (X+I)^j = (\sum_{j=0}^{N} a_j X^j) + I = W + I = I,$$

ale I jest zerem w $K[X]/I$.

Druga część tezy wynika z uwagi, że jeśli $\deg W = N$, to ciało ilorazowe $K[X]/I$ jest pierścieniem reszt z dzielenia przez W, a więc bazą tego ciała, traktowanego jako przestrzeń liniowa nad K są reszty wielomianów $1, X, \ldots, X^{N-1}$. □

Wniosek 1. *Jeśli K jest ciałem, a $W \in K[X]$ jest dowolnym wielomianem dodatniego stopnia, to istnieje ciało L, zawierające K, w którym W jest iloczynem wielomianów liniowych. Przy tym ciało L, traktowane jako przestrzeń liniowa nad K, ma wymiar skończony..*

Dowód: Jeśli mamy dwa ciała $A \subset B$, to możemy traktować B jako przestrzeń liniową nad A. Wymiar tej przestrzeni nazywa się *stopniem ciała B nad A* i oznacza $[B : A]$.

Lemat 3.36. *(i) Jeśli $A \subset B \subset C$ są ciałami, a przy tym stopnie $[C : B]$ i $[B : A]$ są skończone, to*

$$[C : A] = [C : B][B : A].$$

(ii) Jeśli $A_1 \subset A_2 \subset \ldots \subset A_r$ są ciałami i wszystkie stopnie $[A_{i+1} : A_i]$ są skończone, to

$$[A_r : A_1] = \prod_{j=1}^{r-1} [A_{j+1} : A_j].$$

Dowód: (i) Niech $m = [B : A]$ i $n = [C : B]$ i niech $a_1, \ldots, a_m$ będzie bazą B nad A, zaś $b_1, \ldots, b_n$ bazą C nad B. Wystarczy pokazać, że zbiór

$$\{a_i b_j : \ 1 \le i \le m, 1 \le j \le n\}$$

jest bazą C nad A.

Jeśli $x \in C$, to $x = \sum_{j=1}^{n} \beta_j b_j$ z $\beta_j \in B$. Ponadto dla $j = 1, 2, \ldots, n$ możemy napisać $\beta_j = \sum_{i=1}^{m} \alpha_{ji} a_i$ z $\alpha_{ji} \in A$, a to prowadzi do

$$x = \sum_{j=1}^{n} \sum_{i=1}^{m} \alpha_{ji} a_i b_j,$$

pokazując, że elementy $a_i b_j$ są układem generatorów przestrzeni C nad ciałem A. By pokazać, że są one liniowo niezależne przypuśćmy, że z pewnymi $\alpha_{ij} \in A$ mamy równość

$$\sum_{i,j} \alpha_{ij} a_i b_j = 0.$$

Pisząc ją w postaci

$$\sum_{j=1}^{n}(\sum_{i=1}^{m}\alpha_{ij}a_i)b_j = 0$$

i korzystając z liniowej niezależności elementów b_j nad ciałem B otrzymujemy $\sum_{i=1}^{m}\alpha_{ij}a_i = 0$ dla $j = 1, 2, \ldots, n$, co jest możliwe jedynie gdy wszystkie α_{ij} znikają.

Część (ii) wynika teraz przez nietrudną indukcję. □

Zastosujemy indukcję względem stopnia wielomianu W. Jeśli $\deg W = 1$, to nie ma czego dowodzić. Załóżmy zatem, że wniosek jest słuszny dla wszystkich ciał K i dla wszystkich wielomianów z $K[X]$ o stopniu $< n$, gdzie $n \geq 2$. Niech $f \in K[X]$ będzie wielomianem stopnia n. Stosujemy Twierdzenie 3.35, by znaleźć ciało $K_1 \supset K$, w którym f ma pierwiastek ξ i które spełnia $m = [K_1 : K] < \infty$. Z Twierdzenia 3.32 wynika, że wielomian $g(X) = f(X)/(X-\xi)$ leży w $K_1[X]$, a ponieważ $\deg g = n-1 < n$ przeto z założenia indukcyjnego wynika istnienie ciała $K_2 \supset K_1$, w którym g jest iloczynem wielomianów liniowych oraz $r = [K_2 : K_1] < \infty$. Zatem w K_2 wielomian f jest iloczynem wielomianów liniowych, a z Lematu 3.36 wynika

$$[K_2 : K] = mr < \infty. \qquad \square$$

Wniosek 2. *Jeśli $q = p^n$, gdzie p jest liczbą pierwszą, to istnieje ciało mające q elementów. Ciało to ma stopień n nad ciałem p-elementowym, a jego grupa multyplikatywna jest cykliczna.*

Dowód: Niech k będzie ciałem p-elementowym. Z poprzedniego wniosku wynika istnienie ciała K, zawierającego k, w którym wielomian $F(X) = X^q - X \in k[X]$ jest iloczynem czynników liniowych. Z Twierdzenia 3.34 wynika, że F nie ma pierwiastków wielokrotnych, gdyż jego pochodna $F'(X) = -1$ nie ma pierwiastków. Zatem w ciele K wielomian F ma q różnych pierwiastków. Oznaczmy przez Ω zbiór tych pierwiastków. Pokażemy, że Ω jest ciałem. Dla $a \in \Omega$ mamy $a^q = a$, a więc dla $a \neq 0$ zachodzą równości

$$a^{q-1} = 1,\ a^{-1} = a^{q-2},\ (a^{-1})^q = a^{q(q-2)} = a^{q-2} = a^{-1},$$

z których wynika $a^{-1} \in \Omega$, a jeśli $a, b \in \Omega$, $b \neq 0$, to $(ab)^q = a^q b^q = ab$, a z Twierdzenia 3.15 otrzymujemy

$$(a+b)^q = a^q + b^q,\ (a-b)^q = a^q - b^q,$$

co daje $ab \in \Omega$ i $a \pm b \in \Omega$.

Cykliczność grupy multyplikatywnej wynika z Wniosku z Twierdzenia 3.33. □

Można pokazać, używając teorii rozszerzeń ciał, że każde dwa ciała mające q elementów są izomorficzne.

Ciało K nazywamy *ciałem algebraicznie domkniętym*, jeśli każdy wielomian z $K[X]$ o dodatnim stopniu ma w K pierwiastek.

Twierdzenie 3.37. *Następujące warunki spełnione przez ciało K są równoważne:*

(i) Jedynymi wielomianami nierozkładalnymi w $K[X]$ są wielomiany pierwszego stopnia,

(ii) Każdy wielomian $f \in K[X]$ mający stopień dodatni rozkłada się w $K[X]$ na czynniki liniowe,

(iii) K jest ciałem algebraicznie domkniętym.

Dowód: Implikacja (i) $\Rightarrow$ (ii) wynika z tego, że pierścień $K[X]$ jest UFD (Wniosek z Twierdzenia 3.25), a implikacja (ii) $\Rightarrow$ (iii) jest trywialna. Pozostaje pokazać, że z (iii) wynika (i). Jeśli K jest ciałem algebraicznie domkniętym to każdy wielomian $f \in K[X]$ stopnia dodatniego ma w K pierwiastek, powiedzmy ξ, a wtedy z Twierdzenia 3.32 wynika, że $X - \xi$ dzieli f, a więc f może być nierozkładalny jedynie gdy $\deg f = 1$. □

Przykładem ciała algebraicznie domkniętego jest, jak udowodnił C.F.Gauss, ciało liczb zespolonych. Dowód tego twierdzenia opiera się na następującym twierdzeniu, którego dowód podaje się zazwyczaj na wykładzie funkcji analitycznych:

Twierdzenie Liouville'a. *Jeśli $f(z)$ jest funkcją o wartościach zespolonych określoną na płaszczyźnie zespolonej, która w każdym punkcie $z \in \mathbb{C}$ ma pochodną*

$$f'(z) = lim_{w \to z} \frac{f(w) - f(z)}{w - z},$$

a przy tym jest ograniczona, tj. istnieje stała M taka, że dla $z \in \mathbb{C}$ mamy $|f(z)| \leq M$, to f jest funkcją stałą.

Wniosek 1. Tzw. "Zasadnicze Twierdzenie Algebry". *Ciało $\mathbb{C}$ jest algebraicznie domknięte.*

Dowód: Jeśli $f(z) = a_n z^n + \cdots + a_0$ ma stopień dodatni i nie ma pierwiastków, to funkcja $g(z) = 1/f(z)$ jest określona na całej płaszczyźnie i, jak łatwo obliczyć, ma tam pochodną równą

$$g'(z) = -\frac{f'(z)}{f^2(z)}.$$

Jeśli $A = \max\{|a_i| : \ i = 0, 1, 2, \ldots, n-1\}$, to dla ostatecznie dużych $|z|$ mamy

$$|f(z)| \geq |a_n||z|^n - Mn|z|^{n-1} > B|z|^n,$$

z odpowiednią stałą $B > 0$, a więc funkcja g jest ograniczona. Z twierdzenia Liouville'a wynika, że g jest funkcją stałą, a zatem $\deg f = 0$, wbrew założeniu. □

Wniosek 2. *Jedyne nierozkładalne wielomiany w $\mathbb{C}[X]$ to wielomiany liniowe.*

Dowód: Wynika natychmiast z Wniosku 1 i Twierdzenia 3.37. □

Wniosek 3. *Nierozkładalne wielomiany w $\mathbb{R}[X]$ to wielomiany liniowe oraz wielomiany kwadratowe $aX^2 + bX + c$ o ujemnym wyróżniku $\Delta - b^2 - 4ac$.*

Dowód: Nierozkładalność wielomianów liniowych jest oczywista. Jeśli zaś $f \in \mathbb{R}[X]$ ma stopień ≥ 2, to korzystając z Wniosku 1 i z uwagi, że jeśli $f(z) = 0$, to $f(\bar{z}) = 0$, możemy napisać

$$f(X) = A \prod_{i=1}^{r} (X - x_i) \prod_{j=1}^{s} (X - z_i)(X - \bar{z}_i),$$

gdzie $x_1, \ldots, x_r$ są rzeczywistymi pierwiastkami f, zaś $z_1, \bar{z}_1, \ldots, z_s, \bar{z}_s$ są sprzężonymi parami nierzeczywistych pierwiastków f. Ponieważ liczby $z_i + \bar{z}_i$ i $z_i \bar{z}_i$ są rzeczywiste, zatem wielomian kwadratowy

$$(X - z_i)(X - \bar{z}_i)$$

ma rzeczywiste współczynniki. Jeśli więc f jest nierozkładalny w $\mathbb{R}[X]$, to musimy mieć $r = 0$ i $s = 1$ i pozostaje zauważyć, że wyróżnik wielomianu $(X - z_i)(X - \bar{z}_i)$ jest ujemny, gdyż inaczej ten wielomian miałby pierwiastek rzeczywisty. □

Znacznie trudniej jest sprawdzić czy dany wielomian o współczynnikach wymiernych jest nierozkładalny. Podamy tu kilka przykładowych twierdzeń na ten temat. Pierwsze z nich dotyczy wielomianów o współczynnikach w dowolnym ciele K:

Twierdzenie 3.37. *Na to by wielomian $f \in K[X]$ stopnia 2 lub 3 był nierozkładalny w K potrzeba i wystarcza by nie miał on pierwiastka w K.*

Dowód: Wystarczy zauważyć, że rozkładalny wielomian stopnia ≤ 3 musi mieć czynnik pierwszego stopnia. □

Z lematu Gaussa wynika, że badanie nierozkładalności wielomianów o wymiernych współczynnikach sprowadza się do badania nierozkładalności wielomianów w $\mathbb{Z}[X]$.

Twierdzenie 3.38. Kryterium Eisensteina. *Jeśli* $f(X) = \sum_{j=0}^{N} a_j X^j \in \mathbb{Z}[X]$ *i istnieje liczba pierwsza* p *dzieląca* $a_0, a_1, \ldots, a_{N-1}$*, nie dzieląca* a_N*, a ponadto* $p^2 \nmid a_0$*, to* f *jest nierozkładalny w* $\mathbb{Z}[X]$ *i* $\mathbb{Q}[X]$.

Dowód: Przypuśćmy, że wielomian f spełniający założenia jest rozkładalny, powiedzmy $f = gh$, przy czym $g(X) = \sum_{j=0}^{m} b_j X^j$, $h(X) = \sum_{j=0}^{n} c_j X^j$ i $1 \leq m, n < N$, $m + n = N$. Ponieważ $p|a_0 = b_0 c_0$ i $p^2 \nmid a_0$, zatem dokładnie jedna z liczb b_0, c_0 dzieli się przez p. Powiedzmy, że $p|b_0$, $p \nmid c_0$. Nie wszystkie wspólczzniki b_i są podzielne przez p, gdyż inaczej liczba $a_N = b_m c_n$ dzieliłaby się przez p, wbrew założeniu. Niech $k \geq 1$ będzie najmniejszym indeksem dla którego $p \nmid b_k$. Ponieważ $k < n$, zatem

$$p|a_k = b_k c_0 + \sum_{\substack{i+j=k \\ i<k}} b_i c_j,$$

co prowadzi do sprzeczności, gdyż $p \nmid b_k c_0$ i $p| \sum_{\substack{i+j=k \\ i<k}} b_i c_j$. □

9. Można udowodnić czysto algebraicznie, że każde ciało jest podciałem pewnego ciała algebraicznie domkniętego. Podamy teraz taki dowód w przypadku ciał conajwyżej przeliczalnych. W ogólnym przypadku idea dowodu jest ta sama, należy wszakże zamiast zwykłej indukcji użyć tzw. indukcji pozaskończonej.

Twierdzenie 3.39. *Jeśli* K *jest ciałem skończonym lub przeliczalnym, to istnieje algebraicznie domknięte ciało* $\hat{K}$*, zawierające* K.

Dowód: Zbiór $K[X]$ jest w naszym przypadku przeliczalny, ustawmy zatem wszystkie wielomiany dodatniego stopnia o współczynnikach z K w ciąg: $f_1, f_2, \ldots$. Niech $K_0 = K$ i dla $i = 1, 2, \ldots$ niech K_i oznacza ciało zawierające K_{i-1}, w którym wielomian f_i jest iloczynem wielomianów liniowych, a przy tym $[K_i : K_{i-1}] < \infty$. Istnienie takiego ciała wynika z Wniosku z Twierdzenia 3.32. Połóżmy $\hat{K} = \bigcup_{i=0}^{\infty} K_i$ i zauważmy, że $\hat{K}$ jest ciałem. Z konstrukcji wynika, że każdy z wielomianów f_i jest w $\hat{K}$ iloczynem wielomianów liniowych. Pokażemy, że to samo zachodzi dla każdego wielomianu $f \in \hat{K}[X]$ o stopniu dodatnim. Jeśli $f(X) = \sum_{j=0}^{n} a_j X^j$ $(a_j \in \hat{K})$, to istnieje N takie, że wszystkie współczynniki a_j leżą w K_N, a więc $f \in K_N[X]$. Stosując ponownie Wniosek z Twierdzenia 3.32 otrzymujemy ciało M zawierające K_N, w którym f rozkłada się na czynniki liniowe, a przy tym $[M : K_N] < \infty$. Z wniosku z Lematu 3.33 zastosowanego do ciągu

$$K = K_0 \subset K_1 \subset \ldots \subset K_N \subset M$$

otrzymujemy $T = [M : K] < \infty$. Niech teraz $\xi \in M$ będzie dowolnym pierwiastkiem f. Ponieważ $\dim_K M = T < \infty$, zatem elementy $1, \xi, \xi^2, \ldots, \xi^T$ są zależne liniowo nad K, a zatem istnieją $c_0, c_1, \ldots, c_T \in K$, nie wszystkie równe zeru, spełniające $c_0 + c_1\xi + \ldots + c_T\xi^T = 0$. Zatem ξ jest pierwiastkiem niezerowego wielomianu $\sum_{j=0}^{T} c_j X^j \in K[X]$. Wielomian ten jest równy któremuś z wielomianów f_j, którego pierwiastki leżą w $\hat{K}$, a zatem $\xi \in \hat{K}$, jak twierdziliśmy. To pokazuje, że $\hat{K}$ jest ciałem algebraicznie domkniętym. □