WYKŁADY
Z ALGEBRY OGÓLNEJ
II

Ryszard R. Andruszkiewicz

WYKŁADY
Z ALGEBRY OGÓLNEJ
II

BIAŁYSTOK 2016

Opracowanie graficzne:
Maciej Kazuczyk

Redakcja:
Ryszard R. Andruszkiewicz

Korekta:
Karol Pryszczepko

Redakcja techniczna i skład:
Ryszard R. Andruszkiewicz

Wydanie publikacji sfinansowano ze środków
Wydziału Matematyki i Informatyki Uniwersytetu w Białymstoku

ISBN 978-83-7431-483- 1

Wydawnictwo Uniwersytetu w Białymstoku
15–097 Białystok, ul. M. Skłodowskiej-Curie 14, (85) 745 71 20
http://wydawnictwo.uwb.edu.pl
e-mail: ac-dw@uwb.edu.pl

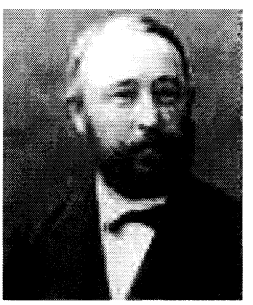
Druk i oprawa:
QUICK-DRUK, s.c., Łódź

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

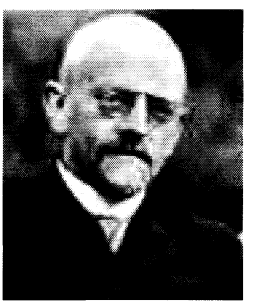
Spis treści

Henri Poincaré
1854-1912

Carl Gauss
1777-1855



Peter Sylow
1832-1918



David Hilbert
1862-1943

Évariste Galois
1811-1832

Emmy Noether
1882-1935

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Wstęp

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

grupy: grupy przekształceń, działanie grupy na zbiorze, twierdzenia Sylowa, grupy rozwiązalne, grupy proste, struktura skończenie generowanych grup abelowych;

pierścienie: pierścienie wielomianów wielu zmiennych, pierścienie noetherowskie, twierdzenie Hilberta o bazie, zbiory algebraiczne, pierścienie szeregów potęgowych;

ciała: ciała skończone, rozszerzenia algebraiczne, liczby algebraiczne i przestępne, ciało rozkładu wielomianu, równania rozwiązalne w pierwiastnikach, ciała algebraicznie domknięte, zasadnicze twierdzenie algebry, rozszerzenia konstruowalne, klasyczne konstrukcje geometryczne.

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

Materiał tu przedstawiony bazuje na znajomości kursowych wykładów z elementarnej teorii liczb, algebry liniowej i algebry I.

W podręczniku liczbami naturalnymi nazywamy dodatnie liczby całkowite, zaś sam zbiór wszystkich liczb naturalnych oznaczamy przez $\mathbb{N}$. Ponadto, $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ i $\mathbb{Z}$ oznacza pierścień liczb całkowitych. Koniec dowodu oznaczamy symbolem $\square$.

Autor dziękuje dr Karolowi Pryszczepko za pomoc w składzie komputerowym i korekcie tego podręcznika.

Rozdział 1

Działanie grupy na zbiorze

1.1 Określenie i własności działania grupy na zbiorze

Definicja 1.1. Niech A będzie niepustym zbiorem i niech $(G, \cdot, e)$ będzie grupą. Mówimy, że **grupa G działa na zbiorze** A, jeżeli istnieje odwzorowanie $\circ : G \times A \to A$ (przy czym dla $g \in G$, $a \in A$ zamiast $\circ((g, a))$ będziemy pisali $g \circ a$), spełniające następujące warunki:

1° $\forall_{a \in A} \quad e \circ a = a$,

2° $\forall_{g,h \in G} \quad \forall_{a \in A} \quad g \circ (h \circ a) = (g \cdot h) \circ a$.

Stwierdzenie 1.2. *Załóżmy, że grupa G działa za pomocą $\circ$ na zbiorze A. Wówczas dla każdego $g \in G$ odwzorowanie $l_g \colon A \to A$ dane wzorem $l_g(a) = g \circ a$ dla $a \in A$ jest bijekcją. Ponadto odwzorowanie $F_\circ \colon G \to S(A)$ dane wzorem $F_\circ(g) = l_g$ dla $g \in G$ jest homomorfizmem grup.*

Na odwrót, jeżeli $F \colon G \to S(A)$ jest homomorfizmem grup, to $\circ_F \colon G \times A \to A$ dane wzorem $g \circ_F a = (F(g))(a)$ dla $g \in G$, $a \in A$ jest działaniem grupy G na zbiorze A.

Ponadto przy tych oznaczeniach: $\circ_{F_\circ} = \circ$ i $F_{\circ_F} = F$.

Dowód. Załóżmy, że grupa G działa za pomocą $\circ$ na zbiorze A i niech $g \in G$. Weźmy dowolne $a \in A$. Wtedy $l_g(g^{-1} \circ a) = g \circ (g^{-1} \circ a) =$

$(gg^{-1})\circ a = e\circ a = a$, czyli funkcja l_g jest "na". Weźmy dowolne $a, b \in A$ takie, że $l_g(a) = l_g(b)$. Wtedy $g\circ a = g\circ b$, skąd $g^{-1}\circ(g\circ a) = g^{-1}\circ(g\circ b)$, czyli $(g^{-1}g)\circ a = (g^{-1}g)\circ b$, a więc $e\circ a = e\circ b$, co daje $a = b$. Zatem funkcja l_g jest "1-1". Wobec tego l_g jest bijekcją i $l_g \in S(A)$. Weźmy dowolne $g, h \in G$. Wówczas dla dowolnego $a \in A$ mamy, że $(F_\circ(gh))(a) = l_{gh}(a) = (gh)\circ a = g\circ(h\circ a)$ oraz $(F_\circ(g)\circ F_\circ(h))(a) = (F_\circ(g))((F_\circ(h))(a)) = (F_\circ(g))(l_h(a)) = (F_\circ(g))(h\circ a) = l_g(h\circ a) = g\circ(h\circ a)$. Stąd $F_\circ(gh) = F_\circ(g)\circ F_\circ(h)$ i $F_\circ$ jest homomorfizmem grup.

Na odwrót, załóżmy, że $F\colon G \to S(A)$ jest homomorfizmem grup i niech odwzorowanie $\circ_F\colon G\times A \to A$ będzie dane wzorem $g\circ_F a = (F(g))(a)$ dla $g \in G$, $a \in A$. Wtedy $F(e) = id_A$, więc $e\circ_F a = (F(e))(a) = id_A(a) = a$ dla każdego $a \in A$. Ponadto dla dowolnych $g, h \in G$, $F(gh) = F(g)\circ F(h)$, więc $g\circ_F(h\circ_F a) = g\circ_F((F(h))(a)) = (F(g))((F(h))(a)) = (F(g)\circ F(h))(a) = (F(gh))(a) = (gh)\circ_F a$ dla każdego $a \in A$. Wobec tego grupa G działa za pomocą $\circ_F$ na zbiorze A.

Weźmy dowolne $a \in A$ i $g \in G$. Wtedy, $g\circ_{F_\circ}$
$g\circ a$, skąd $\circ_{F_\circ}$
skąd wobec dowolności a, $F_{\circ_F}(g) = F(g)$ i dalej, wobec dowolności g, $F_{\circ_F} = F$. □

Załóżmy (aż do odwołania), że grupa $(G, \cdot, e)$ działa na zbiorze A za pomocą $\circ$. W zbiorze A określamy relację $\sim$, przyjmując dla dowolnych $a, b \in A$:

$$a \sim b \Leftrightarrow \exists_{g\in G}\, b = g\circ a. \tag{1.1}$$

Stwierdzenie 1.3. *Relacja $\sim$ określona wzorem* (1.1) *jest relacją równoważności w zbiorze A.*

Dowód. Weźmy dowolne $a \in A$. Wtedy z 1°, $a = e\circ a$, więc $a \sim a$ i relacja $\sim$ jest zwrotna.

Weźmy dowolne $a, b \in A$ takie, że $a \sim b$. Wtedy istnieje $g \in G$ takie, że $b = g\circ a$, skąd na mocy 2° i 1°, $g^{-1}\circ b = g^{-1}\circ(g\circ a) = (g^{-1}\cdot g)\circ a = e\circ a = a$, czyli $b \sim a$ i relacja $\sim$ jest symetryczna.

Weźmy dowolne $a, b, c \in A$ takie, że $a \sim b$ i $b \sim c$. Wtedy istnieją $g, h \in G$ takie, że $b = g\circ a$ i $c = h\circ b$, więc na mocy 2°, $c = h\circ(g\circ a) = (h\cdot g)\circ a$, skąd $a \sim c$ i relacja $\sim$ jest przechodnia. □

Klasę abstrakcji $Orb(a)$ relacji $\sim$ o reprezentancie $a \in A$ nazywamy **orbitą elementu** a. Z (1.1) wynika, że:

$$Orb(a) = \{g \circ a : g \in G\}. \tag{1.2}$$

Ponadto z własności klas abstrakcji relacji równoważności mamy od razu, że dla dowolnych $a, b \in A$:

$$Orb(a) = Orb(b) \text{ albo } Orb(a) \cap Orb(b) = \emptyset. \tag{1.3}$$

Z zasady abstrakcji wynika też następujące

Stwierdzenie 1.4 (Wzór orbit)**.** *Jeżeli grupa G działa na skończonym zbiorze A, to istnieją $a_1, a_2, \ldots, a_s \in A$ takie, że orbity $Orb(a_1)$, $Orb(a_2), \ldots, Orb(a_s)$ są parami rozłączne oraz $A = \bigcup_{i=1}^{s} Orb(a_i)$.*

Dla dowolnego elementu $a \in A$ zbiór:

$$Stab(a) = \{g \in G : g \circ a = a\} \tag{1.4}$$

nazywamy **stabilizatorem elementu** a. Oznaczmy $G^\circ = \bigcap_{a \in A} Stab(a)$.

Stwierdzenie 1.5. *Stabilizator $Stab(a)$ dowolnego elementu $a \in A$ jest podgrupą grupy G. Ponadto $G^\circ = KerF_\circ$, więc G° jest dzielnikiem normalnym grupy G. W szczególności, grupa G/G° zanurza się w grupę symetryczną $S(A)$.*

Dowód. Z 1° wynika od razu, że $e \in Stab(a)$. Niech $g, h \in Stab(a)$. Wtedy $g \circ a = h \circ a = a$, więc na mocy 2°, $(g \cdot h) \circ a = g \circ (h \circ a) = g \circ a = a$, skąd $g \cdot h \in Stab(a)$. Ponadto z 2° oraz z 1°, $g^{-1} \circ a = g^{-1} \circ (g \circ a) = (g^{-1} \cdot g) \circ a = e \circ a = a$, więc $g^{-1} \in Stab(a)$. Zatem $Stab(a)$ jest podgrupą grupy G.

Niech $g \in KerF_\circ$. Wtedy $l_g = id_A$, więc dla każdego $a \in A$: $g \circ a = a$, skąd $g \in Stab(a)$ i wobec tego $g \in G^\circ$. Na odwrót, niech $g \in G^\circ$. Wtedy dla każdego $a \in A$: $g \in Stab(a)$, skąd $g \circ a = a$, więc wobec dowolności a, $l_g = id_A$, a zatem $g \in KerF_\circ$. Wobec tego $G^\circ = KerF_\circ \lhd G$. Z twierdzenia o izomorfizmie $G/KerF_\circ \cong F_\circ(A) \leqslant S(A)$, więc grupa G/G° zanurza się w grupę symetryczną $S(A)$. □

Twierdzenie 1.6. *Dla każdego $a \in A$ moc orbity elementu a jest równa indeksowi stabilizatora tego elementu, tzn.*

$$|Orb(a)| = (G : Stab(a)). \tag{1.5}$$

Dowód. Niech $\mathcal{X}$ będzie zbiorem wszystkich warstw lewostronnych grupy G względem podgrupy $Stab(a)$, czyli $\mathcal{X} = \{gStab(a) : g \in G\}$. Określamy odwzorowanie $\phi\colon \mathcal{X} \to Orb(a)$ przy pomocy wzoru:

$$\phi(gStab(a)) = g \circ a \text{ dla } g \in G.$$

Dla dowolnych $g_1, g_2 \in G$ mamy, że $g_1Stab(a) = g_2Stab(a) \Leftrightarrow g_1^{-1}g_2 \in Stab(a) \Leftrightarrow (g_1^{-1}g_2) \circ a = a \Leftrightarrow g_1 \circ a = g_2 \circ a$, skąd wynika, że ϕ jest dobrze określone i ϕ jest różnowartościowe. Ponieważ dodatkowo ϕ jest 'na', więc ϕ jest bijekcją, czyli $|Orb(a)| = |\mathcal{X}| = (G : Stab(a))$. □

Z twierdzenia 1.6 i z twierdzenia Lagrange'a wynika od razu

Wniosek 1.7. *Jeżeli grupa G jest skończona, to dla każdego $a \in A$ liczba elementów orbity $Orb(a)$ jest dzielnikiem rzędu grupy G oraz $|Orb(a)| = \frac{|G|}{|Stab(a)|}$.*

1.2 Działanie grup na zbiorach - - przykłady i zastosowania

Przykład 1.8. Na mocy stwierdzenia 1.2 dla dowolnego niepustego zbioru A każda podgrupa G grupy symetrycznej $S(A)$ działa w naturalny sposób na zbiorze A za pomocą $\circ$ danego wzorem: $g \circ a = g(a)$ dla $g \in G$ oraz $a \in A$. W szczególności każda podgrupa G grupy $\mathbb{S}_n$ działa w naturalny sposób na zbiorze $\{1, 2, \ldots, n\}$.

Przykład 1.9. Dla dowolnego elementu a grupy $(G, \cdot, e)$ podzbiór $Z_G(a) = \{g \in G : ga = ag\}$ nazywamy **centralizatorem elementu** a, zaś podzbiór $C_G(a) = \{gag^{-1} : g \in G\}$ nazywamy **klasą elementów sprzężonych z elementem** a.

Pokażemy, że grupa G działa na zbiorze G za pomocą automorfizmów wewnętrznych. Mianowicie dla $g, a \in G$ określamy:

$$g \circ a = g \cdot a \cdot g^{-1}. \tag{1.6}$$

Wtedy dla dowolnych $g, h, a \in G$ mamy, że $e \circ a = e \cdot a \cdot e^{-1} = a$ oraz $g \circ (h \circ a) = g \circ (h \cdot a \cdot h^{-1}) = g \cdot h \cdot a \cdot h^{-1} \cdot g^{-1} = (g \cdot h) \cdot a \cdot (g \cdot h)^{-1} = (g \cdot h) \circ a$. Zatem grupa G działa na zbiorze G za pomocą $\circ$. Zauważmy, że dla dowolnego $a \in G$, $Stab(a) = \{g \in G : gag^{-1} = a\} = \{g \in G : ga = ag\} = Z_G(a)$ oraz $Orb(a) = \{gag^{-1} : g \in G\} = C_G(a)$.

Zatem ze stwierdzenia 1.5 oraz z twierdzenia 1.6 mamy od razu

Stwierdzenie 1.10. *Centralizator dowolnego elementu a grupy G jest jej podgrupą oraz moc klasy elementów sprzężonych z elementem a jest równa indeksowi centralizatora tego elementu w grupie G, czyli $|C_G(a)| = (G : Z_G(a))$.*

Definicja 1.11. Jeżeli rząd grupy skończonej G jest potęgą pewnej liczby pierwszej p o wykładniku naturalnym n, to mówimy, że G jest **p-grupą**.

Twierdzenie 1.12. *Każda skończona p-grupa ma nietrywialne centrum.*

Dowód. Niech G będzie skończoną p-grupą. Wtedy istnieje liczba naturalna n taka, że $|G| = p^n$ (p jest liczbą pierwszą!). Załóżmy, że centrum $Z(G)$ grupy G jest trywialne, tzn. $Z(G) = \{e\}$. Rozważmy działanie grupy G na siebie za pomocą automorfizmów wewnętrznych. Ze wzoru orbit istnieją $a_1, a_2, \ldots, a_s \in G$ takie, że $G = \bigcup_{i=1}^{s} Orb(a_i)$ oraz zbiory $Orb(a_1), Orb(a_2), \ldots, Orb(a_s)$ są parami rozłączne. Z pierwszości p oraz z wniosku 1.7 istnieją $k_1, \ldots, k_s \in \mathbb{N}_0$ takie, że $|Orb(a_i)| = p^{k_i}$ dla $i = 1, \ldots, s$. Ponadto z wniosku 1.7 mamy, że dla $a \in G$: $|Orb(a)| = 1 \Leftrightarrow |Stab(a)| = |G| \Leftrightarrow Stab(a) = G \Leftrightarrow a \in Z(G) \Leftrightarrow a = e$. Zatem dokładnie jedna orbita ma moc 1, a pozostałe orbity mają moc podzielną przez p. Ale $p^n = \sum_{i=1}^{s} p^{k_i}$, więc otrzymujemy sprzeczność. Zatem $Z(G) \neq \{e\}$. □

Lemat 1.13. *Jeżeli grupa G nie jest abelowa, to grupa $G/Z(G)$ nie jest cykliczna.*

Dowód. Załóżmy, że istnieje grupa nieabelowa G taka, że $G/Z(G)$ jest grupą cykliczną. Wtedy istnieje $a \in G$ takie, że $G/Z(G) = \langle aZ(G)\rangle$. Weźmy dowolne $x, y \in G$. Wtedy istnieją liczby całkowite k i l takie, że $xZ(G) = (aZ(G))^k = a^kZ(G)$ oraz $yZ(G) = (aZ(G))^l = a^lZ(G)$. Zatem $x = a^ku$ oraz $y = a^lv$ dla pewnych $u, v \in Z(G)$. Stąd $yx = a^lva^ku = a^la^kvu = a^ka^luv = (a^ku)(a^lv) = xy$, czyli grupa G jest abelowa, wbrew założeniu. □

Twierdzenie 1.14. *Jeżeli rząd grupy G jest kwadratem liczby pierwszej, to grupa G jest abelowa.*

Dowód. Z założenia istnieje liczba pierwsza p taka, że $|G| = p^2$. Ponadto z twierdzenia 1.12, $|Z(G)| > 1$. Zatem z twierdzenia Lagrange'a i z pierwszości p, $|Z(G)| = p$ lub $|Z(G)| = p^2$. Jeśli $|Z(G)| = p$, to grupa G nie jest abelowa oraz $|G/Z(G)| = p$, więc z pierwszości p grupa $G/Z(G)$ jest cykliczna, wbrew lematowi 1.13. Zatem $|Z(G)| = p^2$, skąd $Z(G) = G$ i grupa G jest abelowa. □

Przykład 1.15. Niech H będzie podgrupą grupy G. Wówczas dla każdego $g \in G$, $gHg^{-1} = \{ghg^{-1} : h \in H\}$ jest podgrupą grupy G jako obraz podgrupy H przy automorfizmie wewnętrznym $x \mapsto gxg^{-1}$, $x \in G$. Nazywamy ją **podgrupą sprzężoną** z podgrupą H.

Normalizatorem podgrupy H grupy G nazywamy podzbiór:

$$N_G(H) = \{g \in G : gHg^{-1} = H\}. \tag{1.7}$$

Oznaczmy przez $\mathcal{A}$ rodzinę wszystkich podgrup grupy G sprzężonych z podgrupą H. Wtedy $\mathcal{A} = \{gHg^{-1} : g \in G\}$. Rozważmy działanie grupy G na zbiorze $\mathcal{A}$ za pomocą automorfizmów wewnętrznych:

$$g \circ A = gAg^{-1} \text{ dla } g \in G,\ A \in \mathcal{A}.$$

Jeśli $A \in \mathcal{A}$, to istnieje $a \in G$ takie, że $A = aHa^{-1}$, więc dla $g \in G$, $g \circ A = g(aHa^{-1})g^{-1} = (ga)H(ga)^{-1} \in \mathcal{A}$. Ponadto dla $A \in \mathcal{A}$ oraz dla

$g, h \in G$ mamy, że $e \circ A = eAe^{-1} = A$ oraz $g \circ (h \circ A) = g \circ (hAh^{-1}) = ghAh^{-1}g^{-1} = (gh)A(gh)^{-1} = (gh) \circ A$. Zatem $\circ$ jest działaniem grupy G na zbiorze $\mathcal{A}$.

Dalej, $H = eHe^{-1} \in \mathcal{A}$ oraz $Stab(H) = \{g \in G : gHg^{-1} = H\} = N_G(H)$ oraz $Orb(H) = \mathcal{A}$. Zatem ze stwierdzenia 1.5 mamy, że $N_G(H)$ jest podgrupą grupy G. Ponadto dla $h \in H$ jest $hHh^{-1} = \{hxh^{-1} : x \in H\} = H$, więc $H \subseteq N_G(H)$. Zatem z określenia $N_G(H)$ mamy, że $H \lhd N_G(H)$.

Z tych rozważań oraz z twierdzenia 1.6 wynika od razu

Twierdzenie 1.16. *Normalizator $N_G(H)$ podgrupy H w grupie G jest podgrupą grupy G. Ponadto $H \lhd N_G(H)$ oraz moc zbioru wszystkich podgrup grupy G sprzężonych z podgrupą H jest równa indeksowi jej normalizatora w grupie G.*

Przykład 1.17. Niech A i B będą skończonymi podgrupami grupy G i niech

$$AB = \{ab : a \in A, b \in B\}.$$

Wówczas AB jest podzbiorem G, ale nie musi być podgrupą grupy G. Grupa $A \times B$ działa na zbiorze AB za pomocą $\circ$ zdefiniowanego następująco:

$$(a, b) \circ (xy) = axyb^{-1} \text{ dla } a, x \in A,\ b, y \in B.$$

Rzeczywiście, dla $x \in A$, $y \in B$ jest $(e, e) \circ (xy) = exye^{-1} = xy$ oraz dla $a_1, a_2, x \in A$ i $b_1, b_2, y \in B$: $[(a_1, b_1)(a_2, b_2)] \circ (xy) = (a_1a_2, b_1b_2) \circ (xy) = a_1a_2xy(b_1b_2)^{-1} = a_1a_2xyb_2^{-1}b_1^{-1} = a_1[(a_2, b_2) \circ (xy)]b_1^{-1} = (a_1, b_1) \circ [(a_2, b_2) \circ (xy)]$. Zauważmy, że $e = ee \in AB$, $Orb(e) = \{ab^{-1} : a \in A, b \in B\} = AB$ oraz $Stab(e) = \{(a, b) \in A \times B : aeb^{-1} = e\} = \{(a, b) \in A \times B : a = b\} = \{(a, a) : a \in A \cap B\}$. Stąd $|Stab(e)| = |A \cap B|$ i $|Orb(e)| = |AB|$.

Z tych rozważań oraz z wniosku 1.7 wynika od razu

Twierdzenie 1.18. *Jeżeli A i B są skończonymi podgrupami grupy G, to $|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$.*

Lemat 1.19 (Poincare)**.** *Niech H będzie podgrupą skończonego indeksu n w grupie G. Wówczas istnieje podgrupa normalna N grupy G taka, że $N \subseteq H$ i grupa G/N zanurza się w grupę $\mathbb{S}_n$, a więc w szczególności rząd grupy G/N dzieli liczbę $n!$.*

Dowód. Niech $\mathcal{M} = \{gH : g \in G\}$ będzie zbiorem wszystkich warstw lewostronnych grupy G względem podgrupy H. Dla $a, g \in G$ określamy $g \circ (aH) = (ga)H$. Jeżeli $a, b, g \in G$ i $aH = bH$, to $a^{-1}b \in H$ oraz $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b$, więc $(ga)H = (gb)H$. Ponadto, $e \circ (aH) = (ea)H = aH$ oraz dla $x, y \in G$: $x \circ (y \circ (aH)) = x \circ [(ya)H] = [x(ya)]H = [(xy)a]H = (xy) \circ (aH)$. Wobec tego grupa G działa na zbiorze $\mathcal{M}$.

Weźmy dowolne $a, g \in G$. Wówczas $g \in Stab(aH) \iff (ga)H = aH \iff a^{-1}ga \in H \iff g \in aHa^{-1}$, czyli $Stab(aH) = aHa^{-1}$. Stąd i na mocy stwierdzenia 1.5, $N = \bigcap_{a \in G} aHa^{-1}$ jest dzielnikiem normalnym grupy G i grupa G/N zanurza się w grupę $S(\mathcal{M})$. Ale $(G : H) = n$, więc $|\mathcal{M}| = n$ i z algebry I, $S(\mathcal{M}) \cong \mathbb{S}_n$. Zatem grupa G/N zanurza się w grupę $\mathbb{S}_n$ i w szczególności rząd grupy G/N dzieli liczbę $n!$. Ponadto $N \subseteq eHe^{-1} = H$, więc $N \subseteq H$. □

Rozdział 2

Twierdzenie Sylowa i jego zastosowania

2.1 Sformułowanie i dowód twierdzenia Sylowa

Lemat 2.1. *Dla dowolnych liczb naturalnych m i k oraz dla dowolnej liczby pierwszej p:*

$$\binom{p^k m}{p^k} \equiv m \pmod{p}.$$

Dowód. Z algebry I wiemy, że $\mathbb{Z}_p(x)$ jest ciałem charakterystyki p i $\mathbb{Z}_p[x]$ jest jego podpierścieniem oraz $(1+x)^{p^k} = 1 + x^{p^k}$. Stąd i ze wzoru dwumianowego Newtona $(1+x)^{p^k m} = [(1+x)^{p^k}]^m = (1+x^{p^k})^m = \sum_{i=0}^{m} \binom{m}{i} x^{p^k i}$, więc współczynnik przy x^{p^k} w wielomianie $f = (1+x)^{p^k m}$ jest równy $\binom{m}{1} \cdot 1 = m \cdot 1$. Ale ze wzoru Newtona mamy też, że $f = \sum_{j=0}^{p^k m} \binom{p^k m}{j} x^j$, więc ten współczynnik jest równy $\binom{p^k m}{p^k} \cdot 1$. Zatem w ciele $\mathbb{Z}_p$: $\binom{p^k m}{p^k} \cdot 1 = m \cdot 1$, skąd $\binom{p^k m}{p^k} \equiv m \pmod{p}$. □

Definicja 2.2. Niech p będzie liczbą pierwszą i niech G będzie grupą skończoną taką, że $|G| = p^k m$ dla pewnych $k, m \in \mathbb{N}$, $p \nmid m$. Każdą podgrupę H rzędu p^k grupy G nazywamy p-**podgrupą Sylowa** grupy G.

Twierdzenie 2.3 (Sylowa)**.** *Jeżeli liczba pierwsza p dzieli rząd grupy skończonej G, to:*

(i) grupa G zawiera p-podgrupę Sylowa,

(ii) liczba n_p, p-podgrup Sylowa grupy G przystaje do 1 modulo p i dzieli $|G|$,

(iii) każda p-podgrupa grupy G jest zawarta w pewnej p-podgrupie Sylowa grupy G,

(iv) każde dwie p-podgrupy Sylowa grupy G są sprzężone.

Dowód. Z założenia mamy, że istnieją $k, m \in \mathbb{N}$ takie, że $|G| = p^k m$ oraz $p \nmid m$. Niech $\mathcal{A}$ będzie zbiorem wszystkich p^k elementowych podzbiorów zbioru G. Wówczas grupa G działa na zbiorze $\mathcal{A}$ za pomocą przesunięć lewostronnych:

$$g \circ A = \{g \cdot a : a \in A\} \text{ dla } g \in G,\ A \in \mathcal{A}.$$

Rzeczywiście, dla dowolnych $g, h \in G$, $A \in \mathcal{A}$, $|g \circ A| = |\{g \cdot a : a \in A\}| = |A| = p^k$, $e \circ A = \{e \cdot a : a \in A\} = A$ i ponadto $g \circ (h \circ A) = g \circ \{h \cdot a : a \in A\} = \{g \cdot (h \cdot a) : a \in A\} = \{(g \cdot h) \cdot a : a \in A\} = (g \cdot h) \circ A$.

Zbiór $\mathcal{A}$ ma $\binom{p^k m}{p^k}$ elementów i na mocy lematu 2.1 liczba ta nie jest podzielna przez p. Ze wzoru orbit wynika zatem, że istnieje $X \in \mathcal{A}$, którego orbita $Orb(X)$ ma liczbę elementów s niepodzielną przez p. Z wniosku 1.7 mamy, że $p^k m = s \cdot |Stab(X)|$. Ale $p \nmid s$, więc stąd p^k dzieli $|Stab(X)|$, czyli $|Stab(X)| \geqslant p^k$. Ponadto dla $a \in X$ oraz $g \in Stab(X)$ mamy $g \cdot a \in X$, więc $Stab(X)a \subseteq X$, skąd $|Stab(X)| = |Stab(X)a| \leqslant |X| = p^k$. Zatem $|Stab(X)| = p^k$ oraz $Stab(X)a = X$ dla $a \in X$. Wobec tego na mocy stwierdzenia 1.5, $Stab(X)$ jest p-podgrupą Sylowa grupy G. Dla $a \in X$ mamy też, że $a^{-1}Stab(X)a = a^{-1}X \in Orb(X)$. Ale $a^{-1}Stab(X)a$ jest obrazem p-podgrupy Sylowa grupy G przy automorfizmie wewnętrznym, więc też jest p-podgrupą Sylowa grupy G. W ten sposób pokazaliśmy, że każda orbita o liczbie elementów niepodzielnej przez p, zawiera pewną p-podgrupę Sylowa grupy G.

Ponadto każda orbita $Orb(Y)$ dla $Y \in \mathcal{A}$ zawierająca p-podgrupę Sylowa H grupy G jest postaci $Orb(H) = \{aH : a \in G\}$, czyli składa się ze wszystkich warstw lewostronnych względem H, czyli ma dokładnie m elementów, na mocy twierdzenia Lagrange'a. Wobec tego liczba n_p, p-podgrup Sylowa grupy G jest równa liczbie orbit o liczbie elementów niepodzielnej przez p. Ponadto orbity takie są m elementowe. Stąd liczba elementów zbioru $\mathcal{A}$ należących do orbit o liczbie elementów niepodzielnej przez p jest równa $n_p \cdot m$. Wobec tego $n_p \cdot m \equiv |\mathcal{A}| \pmod{p}$, czyli na mocy lematu 2.1, $n_p \cdot m \equiv m \pmod{p}$. Ale $p \nmid m$, więc $n_p \equiv 1 \pmod{p}$. Kończy to dowód (i) oraz pierwszej części (ii).

Niech H będzie p-podgrupą grupy G. Wtedy istnieje liczba naturalna l taka, że $|H| = p^l$. Niech F będzie dowolną p-podgrupą Sylowa grupy G. Oznaczmy przez $\mathcal{B}$ zbiór warstw lewostronnych grupy G względem podgrupy F. Z twierdzenia Lagrange'a mamy, że $|\mathcal{B}| = m$. Grupa H działa na zbiorze $\mathcal{B}$ za pomocą przesunięć lewostronnych: $h \circ B = \{h \cdot b : b \in B\}$ dla $h \in H$ oraz $B \in \mathcal{B}$. Ponieważ $|\mathcal{B}| = m$ nie jest podzielne przez p, więc z pierwszości p oraz z twierdzenia 1.6 liczba elementów dowolnej orbity jest potęgą p, więc ze wzoru orbit wynika, że istnieje orbita jednoelementowa $Orb(gF) = \{gF\}$ dla pewnego $g \in G$. Stąd $hgF = gF$ dla każdego $h \in H$, czyli $Hg \subseteq gF$, skąd $H \subseteq gFg^{-1}$. Ponieważ gFg^{-1} jest p-podgrupą Sylowa grupy G jako obraz p-podgrupy Sylowa F przy automorfizmie wewnętrznym, więc otrzymujemy stąd (iii) oraz (iv). Ponadto na mocy twierdzenia 1.16 mamy, że $n_p = (G : N_G(H))$, więc n_p jest dzielnikiem $|G|$. Kończy to dowód drugiej części (ii) oraz naszego twierdzenia. □

Z dowodu twierdzenia Sylowa i z twierdzenia 1.16 wynika od razu następujące

Stwierdzenie 2.4. *Jeżeli H jest p-podgrupą Sylowa grupy G, to liczba n_p wszystkich p - podgrup Sylowa tej grupy wynosi*

$$n_p = (G : N_G(H)).$$

W szczególności $H \lhd G$ wtedy i tylko wtedy, gdy $n_p = 1$.

2.2 Pewne zastosowania twierdzenia Sylowa

Twierdzenie 2.5 (Cauchy'ego)**.** *Jeżeli liczba pierwsza p dzieli rząd grupy skończonej G, to w grupie G istnieje element rzędu p.*

Dowód. Z twierdzenia Sylowa taka grupa G posiada p-podgrupę Sylowa H oraz $|H| = p^k$ dla pewnego $k \in \mathbb{N}$, więc istnieje $h \in H \setminus \{e\}$. Z twierdzenia Lagrange'a $o(h) \mid p^k$ i $o(h) \neq 1$, bo $h \neq e$. Zatem $o(h) = p^l$ dla pewnego naturalnego $l \leqslant k$. Ale wówczas $o(h^{p^{l-1}}) = p$. □

Stwierdzenie 2.6. *Niech p będzie liczbą pierwszą i niech k, m będą liczbami naturalnymi takimi, że $p \nmid m$. Jeżeli liczba m nie posiada dzielnika $d > 1$ takiego, że $d \equiv 1 \pmod{p}$, to każda grupa G rzędu $p^k m$ posiada dzielnik normalny rzędu p^k.*

Dowód. Z twierdzenia Sylowa taka grupa G posiada podgrupę H rzędu p^k oraz liczba n_p, p-podgrup Sylowa grupy G dzieli liczbę $p^k m$ oraz $n_p \equiv 1 \pmod{p}$. Stąd $n_p \mid m$, więc na mocy założenia, $n_p = 1$. Zatem ze stwierdzenia 2.4, $H \lhd G$. □

Twierdzenie 2.7. *Jeżeli $p > q$ są liczbami pierwszymi, to każda grupa G rzędu $p^k q$, gdzie $k \in \mathbb{N}$, posiada dzielnik normalny rzędu p^k.*

Dowód. Ponieważ $p > q$ i $q > 1$ jako liczba pierwsza, więc $p \nmid q - 1$. Zatem ze stwierdzenia 2.6 grupa G posiada dzielnik normalny rzędu p^k. □

Twierdzenie 2.8. *Jeżeli $p > q$ są liczbami pierwszymi takimi, że q nie dzieli $p - 1$, to każda grupa G rzędu pq jest cykliczna.*

Dowód. Ze stwierdzenia 2.6 wynika, że w grupie G istnieją dzielniki normalne H i K takie, że $|H| = p$ i $|K| = q$. Zatem z twierdzenia Sylowa wynika, że H jest jedyną podgrupą rzędu p grupy G, zaś K jest jedyną podgrupą rzędu q grupy G. Załóżmy, że grupa G nie jest cykliczna. Wtedy z pierwszości liczb p i q oraz z twierdzenia Lagrange'a otrzymujemy, że każdy element $a \neq e$ grupy G ma rząd równy p lub

q. Ale jeśli $o(a) = p$, to $|\langle a\rangle| = p$, skąd $\langle a\rangle = H$ i każdy element $a \in H \setminus \{e\}$ ma rząd p, więc w grupie G istnieje dokładnie $p-1$ elementów rzędu p. Analogicznie, w grupie G istnieje dokładnie $q-1$ elementów rzędu q. Stąd $|G| = pq = 1 + (p-1) + (q-1)$, więc $(p-1)(q-1) = 0$ i mamy sprzeczność. Zatem grupa G jest cykliczna. □

Przykład 2.9. Niech p będzie liczbą pierwszą. Z algebry I wiemy, że zbiór wszystkich kwadratowych macierzy odwracalnych stopnia 2 nad ciałem $\mathbb{Z}_p$ tworzy grupę ze względu na mnożenie macierzy. Oznaczamy ją przez $GL_2(\mathbb{Z}_p)$. Zilustrujemy twierdzenie Sylowa na przykładzie tej grupy.

Rozpoczynamy od obliczenia jej rzędu. Z algebry liniowej wiadomo, że macierz $A \in M_2(\mathbb{Z}_p)$ jest odwracalna wtedy i tylko wtedy, gdy jej wiersze są liniowo niezależne. Pierwszy wiersz macierzy A jest zatem dowolnym niezerowym wektorem przestrzeni $\mathbb{Z}_p^2$, a więc można go wybrać na p^2-1 sposobów. Gdy pierwszy wiersz $[a, b]$ jest już wybrany, to drugi wiersz jest dowolnym wektorem ze zbioru $\mathbb{Z}_p^2 \setminus \{x \cdot [a, b] : x \in \mathbb{Z}_p\}$, a więc można go wybrać na dokładnie $p^2 - p$ sposobów. Zatem macierz A można wybrać na dokładnie $(p^2-1)(p^2-p)$ sposobów i wobec tego $|GL_2(\mathbb{Z}_p)| = p(p^2-1)(p-1)$.

Z twierdzenia Sylowa wynika zatem, że w grupie $GL_2(\mathbb{Z}_p)$ istnieje p-podgrupa Sylowa i ma ona dokładnie p elementów. Łatwo sprawdzić, że:

$$H = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{Z}_p \right\}$$

jest podgrupą grupy $GL_2(\mathbb{Z}_p)$. Ale $|H| = p$, więc H jest p-podgrupą Sylowa grupy $G = GL_2(\mathbb{Z}_p)$.

Wyznaczymy teraz liczbę n_p wszystkich p-podgrup Sylowa grupy G. Ze stwierdzenia 2.4 mamy, że $n_p = (G : N_G(H))$. Wystarczy zatem wyznaczyć $N_G(H)$. Niech $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in G$. Wtedy $\det(A) = ad - bc \neq 0$ oraz $A^{-1} = \frac{1}{ad-bc} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$. Ponadto $A \in N_G(H) \Leftrightarrow$

$B(x) = A \cdot \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} \cdot A^{-1} \in H$ dla każdego $x \in \mathbb{Z}_p$. Ale $B(x) = \begin{bmatrix} 1 - \frac{acx}{ad-bc} & \frac{a^2x}{ad-bc} \\ -\frac{c^2x}{ad-bc} & 1 + \frac{acx}{ad-bc} \end{bmatrix}$, więc skoro $B(1) \in H$, to $c = 0$.

Na odwrót, jeśli $c = 0$, to $B(x) \in H$ dla każdego $x \in \mathbb{Z}_p$. Zatem:

$$N_G(H) = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} : a, b, d \in \mathbb{Z}_p,\ a, d \neq 0 \right\}.$$

Stąd $|N_G(H)| = (p-1)^2 p$ oraz $(G : N_G(H)) = \frac{|G|}{|N_G(H)|} = \frac{p(p^2-1)(p-1)}{p(p-1)^2} = p + 1$, czyli $n_p = p + 1$.

Przykład 2.10. Niech $p > 2$ będzie liczbą pierwszą. Pokażemy, że dla każdej liczby naturalnej $d > 1$ dzielącej liczbę $p - 1$ istnieje nieabelowa grupa G rzędu pd. W szczególności wyniknie stąd, że jeżeli liczba pierwsza q dzieli $p - 1$, to istnieje nieabelowa grupa rzędu pq.

Ponieważ $|\mathbb{Z}_p^\star| = p - 1$ i z algebry I grupa $\mathbb{Z}_p^\star$ jest cykliczna, więc istnieje w niej podgrupa K rzędu d. Ale $d > 1$, więc istnieje $x \in K$ takie, że $x \neq 1$. Łatwo sprawdzić, że:

$$G = \left\{ \begin{bmatrix} k & a \\ 0 & 1 \end{bmatrix} : k \in K, a \in \mathbb{Z}_p \right\}$$

jest podgrupą grupy $GL_2(\mathbb{Z}_p)$. Ponadto $|G| = |\mathbb{Z}_p| \cdot |K| = pd$. Niech $A = \begin{bmatrix} x & 0 \\ 0 & 1 \end{bmatrix}$ oraz $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$. Wtedy $A, B \in G$ oraz $A \cdot B \neq B \cdot A$, bo $x \neq 1$. Zatem grupa G nie jest abelowa.

Twierdzenie 2.11. *Jeżeli $p > q > r$ są liczbami pierwszymi, to każda grupa G rzędu pqr posiada dzielnik normalny rzędu p lub q.*

Dowód. Załóżmy, że tak nie jest. Wtedy ze stwierdzenia 2.4 mamy, że $n_p > 1$ i $n_q > 1$. Ale z twierdzenia Sylowa $n_p | pqr$ oraz $n_p \equiv 1 \pmod{p}$, więc $n_p \mid qr$, skąd $n_p = q$ lub $n_p = r$ lub $n_p = qr$. Ale $p \nmid q - 1$ i $p \nmid r - 1$, bo $p > q > r$, więc $n_p = qr$. Wobec tego w grupie G istnieje dokładnie $qr(p-1)$ elementów rzędu p. Rozumując podobnie uzyskamy, że $n_q \geqslant p$. Zatem w grupie G istnieje co najmniej $p(q-1)$ elementów rzędu q. Stąd $|G| \geqslant qr(p-1) + p(q-1) + r > pqr + p(q-1) - qr > pqr$, bo $p > q$ i $q - 1 \geqslant r$. Ale $|G| = pqr$, więc mamy sprzeczność. □

Rozdział 3

Grupy rozwiązalne

3.1 Komutant grupy

Niech G będzie grupą. **Komutatorem** elementów $a, b \in G$ nazywamy element:

$$[a, b] = a^{-1}b^{-1}ab.$$

Komutantem grupy G nazywamy najmniejszą (w sensie inkluzji) podgrupę G' grupy G zawierającą wszystkie komutatory $[a, b]$, $a, b \in G$.

łatwo sprawdzić, że dla dowolnych elementów $a, b, g, x_1, \ldots, x_n \in G$ zachodzą następujące wzory:

$$ab = ba \Leftrightarrow [a, b] = e, \tag{3.1}$$

$$[a, b]^{-1} = [b, a], \tag{3.2}$$

$$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}], \tag{3.3}$$

$$g(x_1 \cdot \ldots \cdot x_n)g^{-1} = (gx_1g^{-1}) \cdot \ldots \cdot (gx_ng^{-1}). \tag{3.4}$$

Posługując się tymi wzorami bez trudu można wykazać, że komutant G' grupy G jest zbiorem wszystkich skończonych iloczynów wszystkich komutatorów utworzonych ze wszystkich elementów tej grupy, $G' \lhd G$ i grupa G/G' jest abelowa. Ponadto grupa G jest abelowa wtedy i tylko wtedy, gdy $G' = \{e\}$.

Twierdzenie 3.1. *Niech H będzie podgrupą normalną grupy G. Wówczas:*

(i) $H' \lhd G$,

(ii) grupa G/H jest abelowa $\Leftrightarrow G' \subseteq H$.

Dowód. (i). Niech $h \in H'$ wtedy istnieją $a_1, \ldots, a_s, b_1, \ldots, b_s \in H$ takie, że $h = [a_1, b_1] \cdot \ldots \cdot [a_s, b_s]$. Stąd na mocy (3.4) i (3.3) dla dowolnego $g \in G$, $ghg^{-1} = [ga_1g^{-1}, gb_1g^{-1}] \cdot \ldots \cdot [ga_sg^{-1}, gb_sg^{-1}] \in H'$, bo $ga_ig^{-1}, gb_ig^{-1} \in H$ dla $i = 1, \ldots, s$. Zatem $H' \lhd G$.

(ii). Załóżmy, że grupa G/H jest abelowa. Wtedy dla dowolnych $a, b \in G$ mamy, że $(aH)(bH) = (bH)(aH)$, skąd $(ab)H = (ba)H$, czyli $(ba)^{-1}(ab) \in H$, skąd $[a, b] \in H$. Zatem $G' \subseteq H$. Na odwrót, załóżmy, że $G' \subseteq H$. Wtedy dla dowolnych $a, b \in G$ jest $[a, b] \in H$, czyli $a^{-1}b^{-1}ab \in H$, skąd $(ba)^{-1}(ab) \in H$. Zatem $(ab)H = (ba)H$, czyli $(aH)(bH) = (bH)(aH)$ i grupa G/H jest abelowa. □

Przykład 3.2. Niech G będzie grupą z przykładu 2.10 i niech H będzie takie jak w przykładzie 2.9. Pokażemy, że $G' = H$. Niech $A = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}$ oraz $B = \begin{bmatrix} r & s \\ 0 & 1 \end{bmatrix}$, gdzie $a, r \in K$ oraz $b, s \in \mathbb{Z}_p$. Łatwo sprawdzić, że wówczas $[A, B] = \begin{bmatrix} 1 & \frac{s(a-1)+b(1-r)}{ar} \\ 0 & 1 \end{bmatrix}$. Stąd $[A, B] \in H$ dla dowolnych $A, B \in G$. Zatem $G' \subseteq H$. Podstawiając $a = x$ (gdzie $x \neq 1$), $b = 0$, $r = x^{-1}$, $s = \frac{\alpha}{x-1}$ (gdzie α jest dowolnym elementem ciała $\mathbb{Z}_p$), uzyskamy, że $[A, B] = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$, skąd wynika, że $H \subseteq G'$. Zatem ostatecznie $G' = H$.

Stwierdzenie 3.3. *Jeżeli $f\colon G \to H$ jest homomorfizmem grupy G na grupę H, to $H' = f(G')$.*

Dowód. Niech $a, b \in G$. Wtedy

$$f([a, b]) = f(a^{-1}b^{-1}ab) = f(a)^{-1}f(b)^{-1}f(a)f(b) = [f(a), f(b)] \in H'.$$

Stąd z definicji komutanta grupy $f(G') \subseteq H'$.

Weźmy dowolne $h \in H'$. Wtedy istnieją $h_i, k_i \in H$ dla $i = 1, \ldots, s$ takie, że $h = [h_1, k_1] \cdot \ldots \cdot [h_s, k_s]$. Ponadto f jest 'na', więc istnieją $a_i, b_i \in G$ takie, że $h_i = f(a_i)$ oraz $k_i = f(b_i)$ dla $i = 1, \ldots, s$. Zatem $h = [f(a_1), f(b_1)] \cdot \ldots \cdot [f(a_s), f(b_s)] = f([a_1, b_1]) \cdot \ldots \cdot f([a_s, b_s]) = f([a_1, b_1] \cdot \ldots \cdot [a_s, b_s]) \in f(G')$, czyli $H' \subseteq f(G')$ i ostatecznie $H' = f(G')$. □

3.2 Określenie i charakteryzacja grupy rozwiązalnej

Definicja 3.4. Ciągiem komutantów grupy G nazywamy nierosnący ciąg jej podgrup

$$G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \ldots,$$

taki, że $G^{(0)} = G$ oraz $G^{(k+1)} = [G^{(k)}]'$ dla $k = 0, 1, 2, \ldots$.

Grupę G nazywamy **rozwiązalną**, jeśli $G^{(n)} = \{e\}$ dla pewnego n. Najmniejszą wartość n, dla której $G^{(n)} = \{e\}$ nazywamy **stopniem rozwiązalności** rozwiązalnej grupy G.

Przykład 3.5. Grupy trywialne są jedynymi grupami rozwiązalnymi stopnia 0, zaś nietrywialne grupy abelowe są jedynymi grupami rozwiązalnymi stopnia 1.

Przykład 3.6. Przy oznaczeniach z przykładu 3.2 mamy, że $G^{(1)} = G' = H \neq \{e\}$ oraz $H' = \{e\}$, bo $H \cong \mathbb{Z}_p^+$ (czyli H jest grupą abelową). Zatem $G^{(2)} = \{e\}$ oraz $G^{(1)} \neq \{e\}$, czyli G jest grupą rozwiązalną stopnia 2.

Uwaga 3.7. Z twierdzenia 3.1 przez prostą indukcję uzyskujemy, że dla dowolnej grupy G, $G^{(k)} \lhd G$ dla każdego $k = 0, 1, 2, \ldots$.

Uwaga 3.8. Z określenia komutanta grupy wynika od razu, że dla dowolnych podgrup A, B grupy G takich, że $A \subseteq B$ jest $A' \subseteq B'$. Przez prostą indukcję uzyskujemy stąd, że $A^{(k)} \subseteq B^{(k)}$ dla każdego $k = 1, 2, \ldots$.

Uwaga 3.9. Niech $f\colon G \to H$ będzie homomorfizmem grupy G na grupę H. Wtedy ze stwierdzenia 3.3 mamy, że $H' = f(G')$. Jeżeli dla pewnego naturalnego k zachodzi $H^{(k)} = f(G^{(k)})$, to ze stwierdzenia 3.3, $H^{(k+1)} = [H^{(k)}]' = [f(G^{(k)})]' = f([G^{(k)}]') = f(G^{(k+1)})$. Zatem $H^{(n)} = f(G^{(n)})$ dla każdego naturalnego n.

Z uwag 3.8 i 3.9 od razu wynika następujące

Stwierdzenie 3.10. *Dowolna podgrupa i dowolny obraz homomorficzny grupy rozwiązalnej są grupami rozwiązalnymi.*

Twierdzenie 3.11. *Niech H będzie dzielnikiem normalnym grupy G. Jeżeli grupy H i G/H są rozwiązalne, to grupa G też jest rozwiązalna.*

Dowód. Z założenia istnieją liczby naturalne m i n takie, że $H^{(n)} = \{e\}$ oraz $(G/H)^{(m)} = \{H\}$. Niech $f\colon G \to G/H$ będzie homomorfizmem naturalnym, tzn. $f(x) = xH$ dla $x \in G$. Wtedy z uwagi 3.9 uzyskamy, że $\{H\} = (G/H)^{(m)} = f(G^{(m)}) = [G^{(m)}H]/H$, skąd $G^{(m)} \subseteq H$. Zatem z uwagi 3.8, $(G^{(m)})^{(n)} \subseteq H^{(n)} = \{e\}$. Ale z określenia $G^{(s)}$ wynika, że $(G^{(m)})^{(n)} = G^{(m+n)}$, więc $G^{(m+n)} = \{e\}$, czyli grupa G jest rozwiązalna. □

Twierdzenie 3.12. *Grupa G jest rozwiązalna wtedy i tylko wtedy, gdy istnieją w niej podgrupy $G_1 = G, G_2, \ldots, G_{n+1} = \{e\}$ takie, że $G_{i+1} \lhd G_i$ oraz grupa G_i/G_{i+1} jest abelowa dla wszystkich $i = 1, \ldots, n$.*

Dowód. Jeżeli grupa G jest rozwiązalna, to ciąg (G_i) zdefiniowany wzorem $G_i = G^{(i-1)}$ dla $i = 1, \ldots, n+1$, spełnia warunki sformułowane w twierdzeniu, na mocy twierdzenia 3.1.

Na odwrót, załóżmy, że ciąg podgrup G_i dla $i = 1, 2, \ldots, n+1$ spełnia te warunki. Pokażemy, że $G^{(i)} \subseteq G_{i+1}$ dla $i = 0, 1, \ldots, n$. Dla $i = 0$ jest to oczywiste, bo $G^{(0)} = G = G_1$. Załóżmy, że dla pewnego $i < n$ jest $G^{(i)} \subseteq G_{i+1}$. Ponieważ grupa G_{i+1}/G_{i+2} jest abelowa, więc z twierdzenia 3.1, $G'_{i+1} \subseteq G_{i+2}$, skąd $G^{(i+1)} = [G^{(i)}]' \subseteq G'_{i+1} \subseteq G_{i+2}$. Zatem na mocy indukcji $G^{(n)} \subseteq G_{n+1} = \{e\}$, czyli $G^{(n)} = \{e\}$ i grupa G jest rozwiązalna. □

3.3 Przykłady grup rozwiązalnych

Przykład 3.13. Każda grupa G rzędu 12 jest rozwiązalna. Rzeczywiście, na mocy twierdzenia Sylowa w takiej grupie istnieje podgrupa H rzędu 4 i istnieje podgrupa K rzędu 3. Jeśli $K \lhd G$, to z twierdzenia Lagrange'a $|G/K| = \frac{|G|}{|K|} = \frac{12}{3} = 4$, więc na mocy twierdzenia 1.14 grupa G/K jest abelowa. Ale grupa K też jest abelowa, gdyż $|K| = 3$, więc z twierdzenia 3.11, grupa G jest rozwiązalna.

Załóżmy dalej, że podgrupa K nie jest normalna w grupie G. Wówczas z twierdzenia Sylowa liczba n_3 wszystkich 3-podgrup Sylowa spełnia warunki: $n_3 \equiv 1 \pmod 3$ oraz $n_3 \mid 12$ i $n_3 > 1$ na mocy stwierdzenia 2.4. Stąd $n_3 = 4$. Zatem w grupie G jest dokładnie $4 \cdot 2 = 8$ elementów rzędu 3, a ponieważ $|G| = 12$, więc istnieje dokładnie jedna 2-podgrupa Sylowa grupy G. Stąd ze stwierdzenia 2.4, $H \lhd G$. Zatem z twierdzenia Lagrange'a, $|G/H| = \frac{|G|}{|H|} = \frac{12}{4} = 3$, skąd grupa G/H jest abelowa. Ponadto $|H| = 4 = 2^2$, więc z twierdzenia 1.14 grupa H też jest abelowa. Zatem z twierdzenia 3.11 grupa G jest rozwiązalna.

Twierdzenie 3.14. *Każda skończona p-grupa jest grupą rozwiązalną.*

Dowód. Niech G będzie skończoną p-grupą. Wtedy istnieje liczba naturalna n taka, że $|G| = p^n$ (i oczywiście p jest liczbą pierwszą). Zastosujemy indukcję względem n. Dla $n = 1$, $|G| = p$, więc z algebry I grupa G jest cykliczna, czyli jest abelowa, a więc grupa G jest rozwiązalna. Załóżmy, że teza zachodzi dla wszystkich liczb naturalnych $k \leqslant n$ i niech G będzie grupą rzędu p^{n+1}. Z twierdzenia 1.12 i z pierwszości p wynika, że $|Z(G)| = p^k$ dla pewnej liczby naturalnej $k \leqslant n+1$. Jeżeli $k = n+1$, to $Z(G) = G$ i grupa G jest abelowa, czyli jest rozwiązalna. Jeśli zaś $k < n+1$, to z twierdzenia Lagrange'a $|G/Z(G)| = p^{n+1-k}$, więc z założenia indukcyjnego grupa $G/Z(G)$ jest rozwiązalna. Ale grupa $Z(G)$ jest abelowa, więc z twierdzenia 3.11 grupa G jest rozwiązalna. □

Z twierdzeń 3.11, 3.14 i 2.7 wynika od razu następujące

Twierdzenie 3.15. *Niech $p > q$ będą liczbami pierwszymi i niech $\alpha \in \mathbb{N}$. Wówczas każda grupa G rzędu $p^\alpha q$ jest rozwiązalna.*

Przykład 3.16. Pokażemy, że dla $n = 1, 2, 3, 4$ grupa permutacji $\mathbb{S}_n$ jest rozwiązalna. Ponieważ $|\mathbb{S}_1| = 1$ i $|\mathbb{S}_2| = 2$, więc grupy $\mathbb{S}_1$ i $\mathbb{S}_2$ są abelowe, a więc są rozwiązalne. Następnie, $\mathbb{A}_3 \lhd \mathbb{S}_3$ oraz $(\mathbb{S}_3 : \mathbb{A}_3) = 2$, więc $\mathbb{S}_3/\mathbb{A}_3$ jest grupą abelową oraz $|\mathbb{A}_3| = \frac{3!}{2} = 3$, czyli grupa $\mathbb{A}_3$ jest abelowa. Zatem z twierdzenia 3.11 grupa $\mathbb{S}_3$ jest rozwiązalna. W końcu, $(\mathbb{S}_4 : \mathbb{A}_4) = 2$, więc $|\mathbb{S}_4/\mathbb{A}_4| = 2$, czyli grupa $\mathbb{S}_4/\mathbb{A}_4$ jest abelowa i $|\mathbb{A}_4| = \frac{4!}{2} = 12$, więc z przykładu 3.13 grupa $\mathbb{A}_4$ jest rozwiązalna. Zatem z twierdzenia 3.11 grupa $\mathbb{S}_4$ jest rozwiązalna.

Twierdzenie 3.17. *Jeżeli $p > q$ są liczbami pierwszymi, to dla dowolnego naturalnego α każda grupa G rzędu $p^\alpha q^2$ jest rozwiązalna.*

Dowód. Z twierdzenia Sylowa mamy, że istnieje p-podgrupa Sylowa H grupy G. Jeśli liczba n_p, p-podgrup Sylowa grupy G jest równa 1, to ze stwierdzenia 2.4, $H \lhd G$. Wtedy $|G/H| = \frac{p^\alpha q^2}{p^\alpha} = q^2$, więc z twierdzenia 3.14 grupy H i G/H są rozwiązalne. Zatem z twierdzenia 3.11 grupa G jest rozwiązalna. Jeżeli zaś $n_p > 1$, to z twierdzenia Sylowa $n_p \mid p^\alpha q^2$ oraz $n_p \equiv 1 \pmod{p}$, skąd z pierwszości q i tego, że $p > q$ jest $n_p = q^2$. Zatem $p \mid q^2 - 1 = (q-1)(q+1)$, więc $p \mid q+1$. Ale $q + 1 \leqslant p$, więc $q + 1 = p$. Stąd z pierwszości p i q wynika, że $q = 2$ i $p = 3$. Ale wtedy $(G : H) = 2^2 = 4$, więc z lematu Poincare istnieje podgrupa normalna N grupy G taka, że $N \subseteq H$ oraz grupa G/N zanurza się w grupę $\mathbb{S}_4$. Zatem z przykładu 3.16 i ze stwierdzenia 3.10 grupa G/N jest rozwiązalna. Ponadto ze stwierdzenia 3.10 i z twierdzenia 3.14 grupa N też jest rozwiązalna. Stąd na mocy twierdzenia 3.11 grupa G jest rozwiązalna. □

Z twierdzeń 3.14, 3.15 i 3.17 wynika od razu następujący

Wniosek 3.18. *Jeżeli p i q są liczbami pierwszymi oraz $k, l = 1, 2$, to każda grupa rzędu $p^k q^l$ jest rozwiązalna.*

Twierdzenie 3.19. *Dla dowolnych liczb pierwszych p, q, r każda grupa G rzędu pqr jest rozwiązalna.*

Dowód. Na mocy wniosku 3.18 wystarczy ograniczyć się do przypadku, gdy $p > q > r$. Ale wtedy z twierdzenia 2.11 grupa G posiada dzielnik

normalny H rzędu p lub q. Zatem $|G/H| = \frac{pqr}{p} = qr$ lub $|G/H| = \frac{pqr}{q} = pr$, więc z wniosku 3.18 grupa G/H jest rozwiązalna. Ponadto grupa H jest abelowa, bo $|H| = p$. Zatem z twierdzenia 3.11 grupa G jest rozwiązalna. □

Twierdzenie 3.20. *Dla dowolnej liczby naturalnej α każda grupa G rzędu $3 \cdot 2^\alpha$ jest rozwiązalna.*

Dowód. Z twierdzenia Sylowa wynika, że istnieje w G podgrupa H rzędu 2^α. Ponadto z lematu Poincare istnieje w G podgrupa normalna $N \subseteq H$ taka, że grupa G/N zanurza się w grupę $\mathbb{S}_3$, bo $(G : H) = \frac{2^\alpha \cdot 3}{2^\alpha} = 3$. Zatem z przykładu 3.16 i ze stwierdzenia 3.10 grupa G/N jest rozwiązalna. Ponadto z twierdzenia 3.14 i ze stwierdzenia 3.10 grupa N jest rozwiązalna, więc z twierdzenia 3.11 grupa G jest rozwiązalna. □

Twierdzenie 3.21. *Dla dowolnej liczby pierwszej p każda grupa G rzędu $8p$ jest rozwiązalna.*

Dowód. Dla $p = 2$ teza wynika z twierdzenia 3.14, zaś dla $p = 3$ teza wynika z twierdzenia 3.20. Natomiast dla $p \neq 2, 3, 7$ teza wynika ze stwierdzenia 2.6 i z twierdzeń 3.14 i 3.11. Niech dalej $p = 7$. Jeśli $n_p = 1$, to rozumując jak wyżej uzyskamy, że grupa G jest rozwiązalna. Niech zatem $n_p > 1$. Wtedy z twierdzenia Sylowa $n_p = 8$, więc w grupie G istnieje dokładnie $8(p-1)$ elementów rzędu p. Ponadto z twierdzenia Sylowa istnieje w G podgrupa K rzędu 8, więc ponieważ $|G| = 8p$, to $n_2 = 1$ i ze stwierdzenia 2.4, $K \lhd G$. Ale wtedy grupy K i G/K są rozwiązalne, więc z twierdzenia 3.11 grupa G też jest rozwiązalna. □

Z twierdzeń 3.14, 3.15, 3.17, 3.19, 3.20 i 3.21 wynika w prosty sposób następujące

Twierdzenie 3.22. *Każda grupa rzędu mniejszego niż 60 jest rozwiązalna.*

Udowodnione przez nas twierdzenia są szczególnymi przypadkami słynnego twierdzenia Burnside'a:

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Twierdzenie 3.23 (Burnside'a)**.** *Jeżeli p i q są liczbami pierwszymi oraz α i β są liczbami naturalnymi, to każda grupa rzędu $p^\alpha q^\beta$ jest rozwiązalna.*

Dowód tego twierdzenia w pełnej ogólności wymaga skorzystania z teorii charakterów grup skończonych, albo sięgnięcia do bardzo zaawansowanych technik tzw. lokalnej metody badania grup skończonych.

Twierdzenie 3.24 (Feita, Thompsona)**.** *Każda grupa skończona nieparzystego rzędu jest rozwiązalna.*

Dowód tego twierdzenia jest bardzo trudny. Pierwszy oryginalny dowód opublikowany w 1963 roku zajął cały numer czasopisma Pacific Journal of Mathematics o objętości 257 stron!

Rozdział 4

Grupy proste

4.1 Grupy permutacji

Niech A będzie niepustym zbiorem oraz niech $a_1, a_2, \ldots, a_r$ $(r \geqslant 2)$ będą różnymi elementami zbioru A. Wówczas permutację postaci:

$$\begin{pmatrix} a_1 & a_2 & \ldots & a_{r-1} & a_r \\ a_2 & a_3 & \ldots & a_r & a_1 \end{pmatrix} \tag{4.1}$$

nazywamy **cyklem**, a liczbę r-jego długością. Cykl (4.1) zapisujemy prościej jako $(a_1, a_2, \ldots, a_r)$. Cykle długości 2 nazywamy **transpozycjami**.

Z algebry I wiemy, że każda permutacja nietożsamościowa dowolnego niepustego skończonego zbioru A jest iloczynem skończonej liczby cykli rozłącznych, zaś każdy cykl długości r jest iloczynem $r-1$ transpozycji. Duże znaczenie w rachunkach na permutacjach mają następujące wzory:

$$f \circ (a_1, a_2, \ldots, a_r) \circ f^{-1} = (f(a_1), f(a_2), \ldots, f(a_r)), \tag{4.2}$$

$$(a_1, a_2, \ldots, a_r)^{-1} = (a_r, \ldots, a_2, a_1) \tag{4.3}$$

zachodzące dla dowolnej permutacji f zbioru A i dla dowolnych różnych elementów $a_1, a_2, \ldots, a_r \in A$.

Lemat 4.1. *Każdy z następujących zbiorów generuje grupę* $\mathbb{S}_n$*:*
(i) zbiór transpozycji $(1, j)$*, gdzie* $j = 2, 3, \ldots, n$*,*
(ii) zbiór transpozycji $(k, k+1)$*, gdzie* $k = 1, 2, \ldots, n-1$*,*
(iii) zbiór złożony z transpozycji $(1, 2)$ *i cyklu* $(1, 2, \ldots, n)$*,*
(iv) zbiór złożony z transpozycji (a_1, a_2) *i cyklu* $(a_1, a_2, \ldots, a_n)$*, gdzie* $a_1, a_2, \ldots, a_n$ *są parami różnymi elementami zbioru* $\{1, 2, \ldots, n\}$*.*

Dowód. Z algebry I wiemy, że każda permutacja z $\mathbb{S}_n$ jest iloczynem skończonej liczby transpozycji. Jeżeli $1 < i < j \leqslant n$, to $(i, j) = (1, i)(1, j)(1, i)$. Zatem zbiór transpozycji $(1, j)$, gdzie $j = 2, 3, \ldots, n$ generuje grupę $\mathbb{S}_n$. Ponadto, jeśli $i < j$, $i, j = 1, 2, \ldots, n$, to $(i, j) = (i, i+1)(i+1, i+2)\ldots(j-2, j-1)(j-1, j)(j-2, j-1)\ldots(i+1, i+2)(i, i+1)$, więc zbiór transpozycji $(k, k+1)$, gdzie $k = 1, 2, \ldots, n-1$ generuje $\mathbb{S}_n$. Niech $\sigma = (1, 2)$ i $\tau = (1, 2, \ldots, n)$. Wtedy ze wzoru (4.2) $\tau\sigma\tau^{-1} = (\tau(1), \tau(2)) = (2, 3)$, $\tau(2, 3)\tau^{-1} = (\tau(2), \tau(3)) = (3, 4)$, itd. w końcu $\tau(n-2, n-1)\tau^{-1} = (\tau(n-2), \tau(n-1)) = (n-1, n)$. Zatem zbiór złożony z transpozycji $(1, 2)$ i cyklu $(1, 2, \ldots, n)$ generuje grupę $\mathbb{S}_n$.

Niech $a_1, a_2, \ldots, a_n$ będą różnymi elementami zbioru $\{1, 2, \ldots, n\}$. Wtedy $f = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix} \in \mathbb{S}_n$. Ponadto przekształcenie $\rho \mapsto f \circ \rho \circ f^{-1}$ jest automorfizmem grupy $\mathbb{S}_n$. Zatem z (iii) oraz ze wzoru (4.2) elementy (a_1, a_2) i $(a_1, a_2, \ldots, a_n)$ generują grupę $\mathbb{S}_n$. □

Wniosek 4.2. *Jeżeli liczba pierwsza* p *jest dzielnikiem rzędu podgrupy* G *grupy* $\mathbb{S}_p$ *i* G *zawiera pewną transpozycję, to* $G = \mathbb{S}_p$*.*

Dowód. Z twierdzenia Cauchy'ego istnieje w G element ρ rzędu p. Jedynymi elementami rzędu p w grupie $\mathbb{S}_p$ są cykle długości p. Niech więc $\rho = (a_1, a_2, \ldots, a_p)$. Bez zmniejszania ogólności można przyjąć, że transpozycja należąca do grupy G ma postać $\sigma = (a_1, a_k)$, gdzie $1 < k \leqslant p$. Wtedy z pierwszości p element $\tau = \rho^{k-1}$ też ma rząd p; jest więc cyklem długości p. Ponieważ $\rho^{k-1}(a_1) = a_k$, więc $\tau = (a_1, a_k, \ldots)$. Wobec tego teza wniosku wynika z lematu 4.1 (iv). □

Definicja 4.3. *Niech grupa* G *działa na zbiorze* A *za pomocą* $\circ$*. Mówimy, że to działanie jest* **przechodnie** *(lub, że* G *jest przechodnią*

grupą przekształceń zbioru A), jeżeli dla dowolnych $a, b \in A$ istnieje $g \in G$ takie, że $b = g \circ a$.

Przykład 4.4. Zauważmy, że grupa $\mathbb{S}_n$ jest przechodnią grupą przekształceń zbioru $\{1, 2, \ldots, n\}$ przy jej naturalnym działaniu na tym zbiorze (tzn. $g \circ a = g(a)$ dla $g \in \mathbb{S}_n$ i $a \in \{1, 2, \ldots, n\}$), gdyż dla dowolnych różnych $a, b \in \{1, 2, \ldots, n\}$ mamy, że $b = g(a)$ dla transpozycji $g = (a, b)$ oraz $a = e(a)$, gdzie $e = id_{\{1,2,\ldots,n\}}$.

Lemat 4.5. *Jeżeli G jest przechodnią grupą przekształceń zbioru A i $H \lhd G$, to każde dwie orbity zbioru A ze względu na działanie grupy H są równoliczne.*

Dowód. Niech a, b będą ustalonymi elemantami zbioru A. Ponieważ G jest przechodnią grupą przekształceń zbioru A, więc istnieje $g \in G$ takie, że $g \circ a = b$. Stąd $g^{-1} \circ b = a$.

Jak wiemy, odwzorowanie $l_g \colon A \to A$ określone wzorem $l_g(x) = g \circ x$ dla $x \in A$ jest wzajemnie jednoznaczne. Wykażemy, że przekształca ono orbitę $Orb(a) = \{h \circ a : h \in H\}$ na orbitę $Orb(b) = \{h \circ b : h \in H\}$. Dla $h \in H$ mamy $l_g(h \circ a) = g \circ (h \circ a) = (gh) \circ a = (gh) \circ (g^{-1} \circ b) = (ghg^{-1}) \circ b \in Orb(b)$, bo $ghg^{-1} \in H$. Zatem $l_g(Orb(a)) \subseteq Orb(b)$. Na odwrót, dla $h \in H$ mamy $h \circ b = h \circ (g \circ a) = g \circ [(g^{-1}hg) \circ a] = l_g((g^{-1}hg) \circ a) \in l_g(Orb(a))$, bo $g^{-1}hg \in H$. Zatem $Orb(b) \subseteq l_g(Orb(a))$ i ostatecznie $l_g(Orb(a)) = Orb(b)$. □

Wniosek 4.6. *Jeżeli G jest przechodnią grupą przekształceń zbioru A, liczba elementów zbioru A jest liczbą pierwszą i $H \lhd G$, to H jest przechodnią grupą przekształceń zbioru A lub $h \circ a = a$ dla dowolnych $h \in H$ i $a \in A$.*

Dowód. Z lematu 4.5 wynika, że liczba r elementów dowolnej orbity zbioru A ze względu na działanie grupy H jest dzielnikiem liczby p elementów zbioru A. Ponieważ p jest liczbą pierwszą, więc $r = p$ lub $r = 1$.

Jeżeli $r = p$, to jest tylko jedna orbita, tzn. H jest przechodnią grupą przekształceń zbioru A. Jeżeli $r = 1$, to $h \circ a = a$ dla dowolnych $h \in H$ i $a \in A$. □

Lemat 4.7. *Jeżeli $n \geqslant 2$ i G jest przechodnią i cykliczną podgrupą grupy $\mathbb{S}_n$, to generatorem G jest pewien cykl długości n.*

Dowód. Niech σ będzie generatorem grupy G. Niech k będzie najmniejszą liczbą naturalną taką, że $\sigma^k(1) = 1$. Jeżeli dla pewnych naturalnych liczby i, j takich, że $i < j < k$ byłoby $\sigma^i(1) = \sigma^j(1)$, to $\sigma^{j-i}(1) = 1$ wbrew minimalności k. Stąd elementy $1, \sigma(1), \ldots, \sigma^{k-1}(1)$ są parami różne. Ponadto z przechodniości grupy G dla $s \in \{1, 2, \ldots, n\}$ mamy $s = g(1)$ dla pewnego $g \in G$. Ale $G = \langle\sigma\rangle$, więc $\{1, 2, \ldots, n\} = \{1, \sigma(1), \ldots, \sigma^{k-1}(1)\}$, skąd $k = n$. Zatem $\sigma = (1, \sigma(1), \ldots, \sigma^{n-1}(1))$. □

Twierdzenie 4.8. *Jeżeli p jest liczbą pierwszą, a G - podgrupą przechodnią i rozwiązalną grupy $\mathbb{S}_p$, to każdy element grupy G różny od e ma co najwyżej jeden punkt stały.*

Dowód. Ponieważ grupa G jest rozwiązalna, więc istnieje taki ciąg $G = G_0 \rhd G_1 \rhd \ldots \rhd G_r \rhd G_{r+1} = \{e\}$, że grupa G_i/G_{i+1} jest abelowa, dla $i = 0, 1, \ldots, r$. Bez zmniejszania ogólności można założyć, że grupa G_r jest cykliczna i różna od $\{e\}$. Można bowiem na końcu rozważanego ciągu zamiast $G_r \rhd G_{r+1} = \{e\}$ napisać $G_r \rhd H \rhd G_{r+1} = \{e\}$, gdzie H jest dowolną podgrupą cykliczną grupy G_r różną od $\{e\}$.

Stosując wniosek 4.6 kolejno do grup $G_0, G_1, ..., G_r$ stwierdzamy, że każda z nich jest przechodnią grupą permutacji zbioru p-elementowego. Na mocy lematu 4.7 grupa G_r jest generowana przez cykl σ długości p. Stąd $|G_r| = p$.

Pokażemy, że każdy element $\tau \in G \setminus G_r$ ma rząd różny od p. Jeśli $\tau \in G \setminus G_r$, to $\tau \in G_i \setminus G_{i+1}$ dla pewnego $i \leqslant r - 1$. Jeżeli $\circ(\tau) = p$, to rząd warstwy τG_{i+1} w grupie G_i/G_{i+1}, który jest różny od 1, byłby równy p. Wtedy $p \mid (G_i : G_{i+1})$, a ponieważ $G_r \subseteq G_{i+1} \subseteq G_i \subseteq \mathbb{S}_p$, więc $(G_i : G_{i+1}) \mid (\mathbb{S}_p : G_r) = \frac{|\mathbb{S}_p|}{|G_r|} = \frac{p!}{p} = (p-1)!$. Stąd wynika, że $p \mid (p-1)!$, co jest niemożliwe. Uzyskana sprzeczność dowodzi, że każdy element rzędu p grupy G należy też do grupy G_r. Element taki ma więc postać σ^k, gdzie $k = 1, 2, \ldots, p-1$. Wynika stąd, że grupa G_r jest dzielnikiem normalnym grupy G, ponieważ żaden automorfizm wewnętrzny nie zmienia rzędu elementu.

Załóżmy, że pewien element $\tau \in G$ ma co najmniej dwa punkty stałe. Udowodnimy, że $\tau = e$. Niech punktami tymi będą 1 i 2, czyli $\tau(1) = 1, \tau(2) = 2$. Ponieważ $G_r = \langle\sigma\rangle$ jest przechodnią grupą przekształceń, więc istnieje taka liczba naturalna s, że $1 \leqslant s < p$ i $\sigma^s(1) = 2$. Permutacja σ^s jest więc cyklem długości p. Bez zmniejszania ogólności można przyjąć, że $\sigma^s = (1, 2, \ldots, p)$. Wtedy element $\pi = \sigma^{-s}\tau\sigma^s\tau^{-1}$ spełnia $\pi(1) = \sigma^{-s}\tau\sigma^s\tau^{-1}(1) = \sigma^{-s}\tau\sigma^s(1) = \sigma^{-s}\tau(2) = \sigma^{-s}(2) = 1$. Ponieważ $\sigma^s \in G_r$ i jak wykazaliśmy, $G_r \lhd G$, więc $\tau\sigma^s\tau^{-1} \in G_r$. Stąd $\pi \in G_r$. Zatem element π jest cyklem długości p lub $\pi = e$. Z $\pi(1) = 1$ wynika, że π nie jest cyklem długości p, a więc $\pi = e$. Wobec tego $\tau\sigma^s\tau^{-1} = \sigma^s$. Stąd na mocy tego, że $\sigma^s = (1, 2, \ldots, p)$ i wzoru (4.2) mamy $(\tau(1), \tau(2), \ldots, \tau(p)) = (1, 2, \ldots, p)$. Ponieważ $\tau(1) = 1$, więc stąd wynika, że $\tau(k) = k$ dla $k = 1, 2, \ldots, p$. Zatem $\tau = e$. □

Przykład 4.9. Udowodnimy, że jeśli a, b, c są różnymi elementami zbioru A, to zachodzi wzór:

$$[(a, c), (a, b, c)] = (a, b) \circ (a, c) = (a, c, b). \tag{4.4}$$

Rzeczywiście, ze wzorów (4.2) i (4.3) mamy, że $[(a, c), (a, b, c)] = (a, c)^{-1} \circ (a, b, c)^{-1} \circ (a, c) \circ (a, b, c) = [(a, c) \circ (c, b, a) \circ (a, c)^{-1}] \circ (a, b, c) = (a, b, c) \circ (a, b, c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} = (a, c, b)$ oraz $(a, b) \circ (a, c) = (a, c, b)$.

Przykład 4.10. Udowodnimy, że jeśli a, b, c, d są różnymi elementami zbioru A, to zachodzi wzór:

$$[(b, c, d), (d, c, a)] = (a, b) \circ (c, d). \tag{4.5}$$

Rzeczywiście, ze wzorów (4.2) i (4.3) mamy, że $[(b, c, d), (d, c, a)] = (b, d, c)^{-1} \circ (d, c, a)^{-1} \circ (b, d, c) \circ (d, c, a) = [(c, d, b) \circ (a, c, d) \circ (c, d, b)^{-1}] \circ (d, c, a) = (a, d, b) \circ (d, c, a) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} = (a, b) \circ (c, d)$.

Przykład 4.11. Udowodnimy, że jeśli a, b, c, d, e są różnymi elementami zbioru A, to zachodzi wzór:

$$[(a, b, c), (c, d, e)] = (b, e, c). \tag{4.6}$$

Rzeczywiście, $[(a,b,c),(c,d,e)] = (a,b,c)^{-1} \circ (c,d,e)^{-1} \circ (a,b,c) \circ (c,d,e)$
$= (c,b,a) \circ (e,d,c) \circ (a,b,c) \circ (c,d,e) = \begin{pmatrix} a & b & c & d & e \\ a & e & b & d & c \end{pmatrix} = (b,e,c).$

Przypomnijmy, że permutacja $f \in \mathbb{S}_n$ będąca iloczynem parzystej liczby transpozycji nazywa się **permutacją parzystą**. Zbiór wszystkich permutacji parzystych należących do $\mathbb{S}_n$ tworzy podgrupę, którą oznaczamy przez $\mathbb{A}_n$ i nazywamy n-tą **grupą alternującą**. Z algebry I wiemy też, że dla $n \geqslant 2$, $(\mathbb{S}_n : \mathbb{A}_n) = 2$, więc $\mathbb{A}_n \lhd \mathbb{S}_n$ oraz $|\mathbb{A}_n| = \frac{n!}{2}$. Ponadto cykl jest permutacją parzystą wtedy i tylko wtedy, gdy jego długość jest liczbą nieparzystą. Zatem ze wzoru (4.5) otrzymujemy, że **dla każdego naturalnego** $n \geqslant 4$ **grupa** $\mathbb{A}_n$ **nie jest abelowa**.

Twierdzenie 4.12. *Dla każdego naturalnego* $n \geqslant 2$*:* $\mathbb{S}_n' = \mathbb{A}_n$.

Dowód. Ponieważ grupa $\mathbb{S}_n/\mathbb{A}_n$ jest abelowa (bo ma rząd 2), więc z twierdzenia 3.1, $\mathbb{S}_n' \subseteq \mathbb{A}_n$. Pozostaje zatem wykazać tylko inkluzję odwrotną. Dla $n = 2$ jest ona oczywista, bo $\mathbb{A}_2 = \{e\}$. Dla $n = 3$ mamy, że $\mathbb{A}_3 = \{e, (1,2,3), (1,3,2)\}$, więc z przykładu 4.9, $\mathbb{A}_3 \subseteq \mathbb{S}_3'$. Niech teraz $n \geqslant 4$. Wtedy każdy element z $\mathbb{A}_n$ jest iloczynem parzystej liczby transpozycji. Wystarczy zatem wykazać, że iloczyn dowolnych dwóch transpozycji należy do $\mathbb{S}_n'$. Jeśli te transpozycje są rozłączne, to teza wynika z przykładu 4.10. W przeciwnym przypadku zaś teza wynika z przykładu 4.9. □

Twierdzenie 4.13. *Dla każdego naturalnego* $n \geqslant 5$*:* $\mathbb{A}_n' = \mathbb{A}_n$.

Dowód. Wystarczy wykazać, że dla $n \geqslant 5$ iloczyn dowolnych dwóch transpozycji należy do $\mathbb{A}_n'$. Jeśli te transpozycje są rozłączne, to teza wynika z przykładu 4.10. W przeciwnym przypadku iloczyn tych dwóch transpozycji jest postaci $(a,b)(a,c)$ dla pewnych różnych liczb $a, b, c \in \{1, 2, \ldots, n\}$. Ale $n \geqslant 5$, więc istnieją różne liczby $d, e \in \{1, 2, \ldots, n\} \setminus \{a, b, c\}$ i wówczas $(a,b) \circ (a,c) = [(a,b) \circ (d,e)] \circ [(d,e) \circ (a,c)] \in \mathbb{A}_n'$, na mocy przykładu 4.10. □

Z twierdzeń 4.12 i 4.13 oraz z definicji grupy rozwiązalnej uzyskujemy od razu następujące

Twierdzenie 4.14. *Dla każdego naturalnego $n \geqslant 5$ grupy $\mathbb{S}_n$ i $\mathbb{A}_n$ nie są rozwiązalne.*

Twierdzenie 4.15. *Jeżeli G jest podgrupą grupy $\mathbb{S}_n$, gdzie $n \geqslant 5$ i do G należą pewne dwa cykle długości 3 mające dokładnie jeden element wspólny, to grupa G nie jest rozwiązalna.*

Dowód. Przypuśćmy, że przy tych założeniach grupa G jest rozwiązalna. Wtedy z twierdzeń 3.12 i 3.1 istnieją w niej podgrupy $G_1 = G, G_2, \ldots, G_{k+1} = \{e\}$ takie, że $G_{i+1} \lhd G_i$ oraz $G_i' \subseteq G_{i+1}$ dla wszystkich $i = 1, \ldots, k$.

Z założenia istnieją różne liczby $a, b, c, d, e \in \{1, 2, \ldots, n\}$ takie, że $(a, b, c), (c, d, e) \in G$. Wtedy z przykładu 4.11 mamy, że $(b, e, c) = [(a, b, c), (c, d, e)] \in G'$.

Ponadto $(c, b, a) = (a, b, c)^{-1}, (e, d, c) = (c, d, e)^{-1} \in G$, więc z przykładu 4.11, $(a, d, c) = [(b, a, c), (c, e, d)] = [(c, b, a), (e, d, c)] \in G'$. Ale $G' = G_1' \subseteq G_2$, więc $(b, e, c), (c, a, d) = (a, d, c) \in G_2$. Zatem do G_2 należą dwa cykle długości 3 o dokładnie jednym wspólnym elemencie. Stąd przez prostą indukcję w podobny sposób uzyskamy, że dla każdego $i = 1, 2, \ldots, k + 1$ do podgrupy G_i należą dwa cykle długości 3 o dokładnie jednym wspólnym elemencie. Ale $|G_{k+1}| = 1$, więc otrzymujemy sprzeczność. □

Twierdzenie 4.16. *Jeżeli 2-podgrupa Sylowa skończonej grupy G jest grupą cykliczną, to G posiada dzielnik normalny indeksu 2.*

Dowód. Niech $L\colon G \to S(G)$ będzie zanurzeniem grupy G w grupę permutacji zbioru G, które każdemu elementowi $g \in G$ przypisuje lewostronne mnożenie l_g. Z założenia $|G| = 2^k m$, dla pewnych liczb naturalnych k i m, przy czym m jest nieparzyste oraz istnieje element $x \in G$ rzędu 2^k. Niech $x_1 = e, x_2, \ldots, x_m$ będą reprezentantami wszystkich parami rozłącznych warstw prawostronnych grupy G względem podgrupy $\langle x \rangle$. Wówczas G jest sumą parami rozłącznych podzbiorów 2^k-elementowych $X_i = \{x_i, xx_i, \ldots, x^{2^k-1}x_i\}$ dla $i = 1, \ldots, m$. Stąd $l_x = c_1 \circ c_2 \circ \ldots \circ c_m$, gdzie $c_i = (x_i, xx_i, \ldots, x^{2^k-1}x_i)$ jest cyklem 2^k-elementowym dla $i = 1, \ldots . m$. Ale m jest nieparzyste, więc permutacja l_x jest nieparzysta. Oznaczmy przez $A(G)$ podgrupę wszystkich

permutacji parzystych grupy $L(G)$. Wtedy $L(G) = A(G) \cup l_x A(G)$, $A(G) \cap l_x A(G) = \emptyset$, więc $A(G)$ jest podgrupą indeksu 2 w grupie $L(G)$. Ponadto grupy $L(G)$ i G są izomorficzne, więc grupa G posiada podgrupę H indeksu 2. Z algebry I wiemy, że wtedy $H \lhd G$. □

Z twierdzeń 3.24 i 4.16 oraz 3.11 wynika od razu, że **każda grupa skończona rzędu** $4k+2$ **jest rozwiązalna.**

4.2 Grupy proste

Definicja 4.17. Powiemy, że grupa G jest **grupą prostą**, jeżeli $G \neq \{e\}$ oraz jedynymi dzielnikami normalnymi grupy G są $\{e\}$ i G.

Lemat 4.18. *Jeżeli H jest podgrupą normalną grupy $\mathbb{A}_n$ oraz $n \geqslant 5$ i do H należy iloczyn dwóch rozłącznych transpozycji, to $H = \mathbb{A}_n$.*

Dowód. Bez zmniejszania ogólności rozważań możemy zakładać, że $(1,2)(3,4) \in H$. Niech i, j, k, l będą różnymi elementami zbioru $\{1,2,\ldots,n\}$. Ponieważ zbiory $X = \{1,2,\ldots,n\} \setminus \{1,2,3,4\}$ i $Y = \{1,2,\ldots,n\} \setminus \{i,j,k,l\}$ mają tyle samo elementów, więc istnieje bijekcja $g\colon X \to Y$. Zatem:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \ldots & n \\ i & j & k & l & g(5) & \ldots & g(n) \end{pmatrix} \in \mathbb{S}_n.$$

Zatem ze wzoru (4.2) mamy, że $(i,j)(k,l) = f \circ (1,2)(3,4) \circ f^{-1}$. Stąd dla $h = (i,j) \circ f$ mamy, że $(i,j)(k,l) = h \circ (1,2)(3,4) \circ h^{-1}$. Ponadto $f \in \mathbb{A}_n$ albo $h \in \mathbb{A}_n$, bo $sgn(h) = sgn\,((i,j)) \cdot sgn(f) = -sgn(f)$ i $H \lhd \mathbb{A}_n$, więc $(i,j)(k,l) \in H$. W ten sposób pokazaliśmy, że do H należy iloczyn dowolnych dwóch rozłącznych transpozycji. Niech teraz i, j, k będą różnymi elementami zbioru $\{1,2,\ldots,n\}$. Ponieważ $n \geqslant 5$, więc istnieją różne elementy $r, s \in \{1,2,\ldots,n\} \setminus \{i,j,k\}$ i wtedy $(i,j)(i,k) = [(i,j)(r,s)][(r,s)(i,k)] \in H$. Zatem do H należy iloczyn dowolnych dwóch transpozycji. Ale $\mathbb{A}_n$ składa się z permutacji, które są iloczynami parzystej liczby transpozycji, więc $\mathbb{A}_n \subseteq H$ i ostatecznie $H = \mathbb{A}_n$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Twierdzenie 4.19 (Galois)**.** *Dla każdego naturalnego $n \geqslant 5$, $\mathbb{A}_n$ jest nieabelową grupą prostą.*

Dowód. Jak wiemy dla $n \geqslant 5$ grupa $\mathbb{A}_n$ jest nieabelowa. Załóżmy, że H jest dzielnikiem normalnym grupy $\mathbb{A}_n$ różnym od $\{e\}$. Wtedy istnieje w H element f, który jest iloczynem parami rozłącznych cykli jednej z następujących postaci:

a) f jest cyklem długości co najmniej 4 lub iloczynem takiego cyklu przez inne cykle,

b) f jest iloczynem cyklu długości 3 przez inne cykle,

c) f jest cyklem długości 3,

d) f jest iloczynem parzystej liczby rozłącznych cykli długości 2.

W każdym z tych przypadków dla dowolnego cyklu g długości 3 mamy, że $g \in \mathbb{A}_n$, skąd $f \circ g \circ f^{-1} \circ g^{-1} \in H$, bo $H \lhd \mathbb{A}_n$.

W przypadku a) $f = (a, b, c, d, \ldots)(\ldots)\ldots$. Zatem dla $g = (a, b, c)$ na mocy wzorów (4.2) i (4.3): $f \circ g \circ f^{-1} = (f(a), f(b), f(c)) = (b, c, d)$, więc $f \circ g \circ f^{-1} \circ g^{-1} = (b, c, d) \circ (a, b, c)^{-1} = (b, c, d) \circ (c, b, a) = \begin{pmatrix} a & b & c & d \\ d & a & c & b \end{pmatrix} = (a, d, b)$.

W przypadku b) $f = (a, b, c)(d, e, \ldots)\ldots$. Zatem dla $g = (a, b, d)$ na mocy wzorów (4.2) i (4.3) uzyskamy, że $f \circ g \circ f^{-1} = (f(a), f(b), f(d)) = (b, c, e)$, więc $f \circ g \circ f^{-1} \circ g^{-1} = (b, c, e) \circ (d, b, a) = \begin{pmatrix} a & b & c & d & e \\ d & a & e & c & b \end{pmatrix} = (a, d, c, e, b)$.

W przypadku c) $f = (a, b, c)$. Zatem istnieje $d \in \{1, 2, \ldots, n\} \setminus \{a, b, c\}$ i dla $g = (a, b, d)$ na mocy wzorów (4.2) i (4.3) uzyskamy, że $f \circ g \circ f^{-1} = (f(a), f(b), f(d)) = (b, c, d)$, więc $f \circ g \circ f^{-1} \circ g^{-1} = (b, c, d) \circ (d, b, a) = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix} = (a, b) \circ (c, d)$.

W przypadku d) $f = (a, b) \circ (c, d)\ldots$. Zatem dla $g = (a, b, c)$ na mocy wzorów (4.2) i (4.3) uzyskamy, że $f \circ g \circ f^{-1} = (f(a), f(b), f(c)) = (b, a, d)$, więc $f \circ g \circ f^{-1} \circ g^{-1} = (b, a, d) \circ (c, b, a) = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix} = (a, c) \circ (b, d)$.

Jeżeli f jest typu a), to pewien cykl długości 3 należy do H, więc z c) iloczyn dwóch rozłącznych transpozycji należy do H i z lematu 4.18,

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

$H = \mathbb{A}_n$. Jeżeli f jest typu b), to z rezultatów uzyskanych w b), a), c) i z lematu 4.18 otrzymamy, że $H = \mathbb{A}_n$. W końcu, jeżeli f jest typu c) lub d), to z rezultatów uzyskanych w c) i d) oraz z lematu 4.18 też otrzymamy, że $H = \mathbb{A}_n$. □

Twierdzenie 4.20. *Każda grupa G rzędu* 120 *nie jest prosta.*

Dowód. Załóżmy, że istnieje grupa prosta G rzędu 120. Z twierdzenia Sylowa istnieje w G podgrupa P rzędu 5, gdyż $120 = 2^3 \cdot 3 \cdot 5$. Ponadto $n_5 \mid 2^3 \cdot 3 \cdot 5$ i $n_5 \equiv 1 \ (mod\ 5)$. Ponieważ $n_5 > 1$, więc otrzymujemy stąd, że $n_5 = 6$. Stąd ze stwierdzenia 2.4, $(G : N_G(P)) = 6$. Z lematu Poincare istnieje zatem w G podgrupa normalna N zawarta w $N_G(P)$ taka, że grupa G/N zanurza się w grupę $\mathbb{S}_6$. Ale G jest grupą prostą i $N \subseteq N_G(P) \neq G$, więc $N = \{e\}$. Zatem grupa G zanurza się w grupę $\mathbb{S}_6$. Możemy zatem traktować G jako podgrupę grupy $\mathbb{S}_6$. Z twierdzenia Galois $\mathbb{A}_6$ jest grupą prostą i ma rząd równy $\frac{6!}{2} = 360$. Ale $\mathbb{A}_6 \cap G \lhd G$, więc z prostoty grupy G, $\mathbb{A}_6 \cap G = \{e\}$ lub $\mathbb{A}_6 \cap G = G$. W pierwszym przypadku na mocy twierdzenia 1.18, $|G\mathbb{A}_6| = |G| \cdot |\mathbb{A}_6| = 120 \cdot 360 > 2 \cdot 360 = |\mathbb{S}_6|$, co prowadzi do sprzeczności. Natomiast w drugim przypadku $G \subseteq \mathbb{A}_6$ i $(\mathbb{A}_6 : G) = \frac{360}{120} = 3$, więc z lematu Poincare istnieje $K \lhd \mathbb{A}_6$ takie, że $K \subseteq G \neq \mathbb{A}_6$ oraz $(\mathbb{A}_6 : K) \mid 3!$, co też prowadzi do sprzeczności, gdyż $\mathbb{A}_6$ jest grupą prostą. □

Z twierdzenia 4.16 wynika od razu następujące

Twierdzenie 4.21. *Jeżeli 2-podgrupa Sylowa skończonej grupy G jest grupą cykliczną i $|G| > 2$, to G nie jest grupą prostą.*

Można udowodnić, że jeżeli G jest nieabelową grupą prostą rzędu niewiększego niż 1000, to $|G| = 60, 168, 360, 504, 660$.

Pełna klasyfikacja skończonych grup prostych została zakończona na początku lat osiemdziesiątych XX wieku.

Rozdział 5

Iloczyn prosty grup

5.1 Określenie i własności iloczynu prostego grup

Niech $(G_i, \cdot_i, e_i)$ dla $i = 1, 2, \ldots, n$ będą dowolnymi grupami. W zbiorze $G = G_1 \times G_2 \times \ldots \times G_n$ określamy działanie $\cdot$ wzorem:

$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 \cdot_1 b_1, a_2 \cdot_2 b_2, \ldots, a_n \cdot_n b_n). \quad (5.1)$$

Z powyższego wzoru wynika bezpośrenio, że dla każdego $k \in \mathbb{Z}$:

$$(a_1, a_2, \ldots, a_n)^k = (a_1^k, a_2^k, \ldots, a_n^k). \quad (5.2)$$

Niech $e = (e_1, e_2, \ldots, e_n)$. Łatwo sprawdzić, że wówczas $(G, \cdot, e)$ jest grupą. Nazywamy ją **iloczynem prostym grup** $G_1, G_2, \ldots, G_n$ i oznaczamy przez $G_1 \times G_2 \times \ldots \times G_n$. Dla uproszczenia notacji w dalszej części wykładu będziemy pisali e zamiast e_i oraz $\cdot$ zamiast $\cdot_i$, dla $i = 1, \ldots, n$. Jeżeli $G_1 = \ldots = G_n = G$, to zamiast $G_1 \times \ldots \times G_n$ będziemy pisali G^n.

Niech dla $i = 1, \ldots, n$, $\pi_i \colon G_1 \times \ldots \times G_n \to G_i$ będzie przekształceniem danym wzorem $\pi_i(a_1, \ldots, a_n) = a_i$. Łatwo sprawdzić, że wówczas π_i jest homomorfizmem grupy $G_1 \times \ldots \times G_n$ na grupę G_i oraz $Ker(\pi_i) = G_1 \times \ldots \times G_{i-1} \times \{e\} \times G_{i+1} \times \ldots \times G_n$. Zatem $Ker(\pi_i)$

jest dzielnikiem normalnym grupy $G_1 \times \ldots \times G_n$ i z twierdzenia o izomorfizmie $(G_1 \times \ldots \times G_n)/Ker(\pi_i) \cong G_i$ dla $i = 1, \ldots, n$.

Ponadto przekształcenie $f_i \colon G_i \to G_1 \times \ldots \times G_n$ dane wzorem $f_i(x) = (\underbrace{e, \ldots, e}_{i-1}, x, \underbrace{e, \ldots, e}_{n-i})$ dla $x \in G_i$ jest zanurzeniem grup oraz $\overline{G_i} = f_i(G_i) = \underbrace{\{e\} \times \ldots \{e\}}_{i-1} \times G_i \times \underbrace{\{e\} \times \ldots \times \{e\}}_{n-i}$, więc $\overline{G_i}$ jest podgrupą grupy $G_1 \times \ldots \times G_n$ oraz $\overline{G_i} \cong G_i$ dla $i = 1, \ldots, n$. Ponadto łatwo sprawdzić, że $\overline{G_i} \lhd G_1 \times \ldots \times G_n$ dla $i = 1, \ldots, n$.

Stwierdzenie 5.1. *Dla dowolnych grup $G_1, \ldots, G_n$ i dla dowolnej permutacji $\sigma \in \mathbb{S}_n$:*

$$G_1 \times \ldots \times G_n \cong G_{\sigma(1)} \times \ldots \times G_{\sigma(n)}.$$

Dowód. Wystarczy zauważyć, że przekształcenie $f \colon G_1 \times \ldots \times G_n \to G_{\sigma(1)} \times \ldots \times G_{\sigma(n)}$ dane wzorem $f(a_1, \ldots, a_n) = (a_{\sigma(1)}, \ldots, a_{\sigma(n)})$ jest izomorfizmem grup. □

Stwierdzenie 5.2. *Niech $A_1, \ldots, A_n, B_1, \ldots, B_n$ będą grupami takimi, że $A_i \cong B_i$ dla $i = 1, \ldots, n$. Wówczas:*

$$A_1 \times \ldots \times A_n \cong B_1 \times \ldots \times B_n.$$

Dowód. Niech $f_i \colon A_i \to B_i$ będzie izomorfizmem grup dla $i = 1, \ldots, n$. Łatwo zauważyć, że wówczas $f \colon A_1 \times \ldots \times A_n \to B_1 \times \ldots \times B_n$ dane wzorem $f(a_1, \ldots, a_n) = (f_1(a_1), \ldots, f_n(a_n))$ jest izomorfizmem grup. □

Stwierdzenie 5.3. *Dla dowolnych grup $A_1, \ldots, A_n, B_1, \ldots, B_m$:* $(A_1 \times \ldots \times A_n) \times (B_1 \times \ldots \times B_m) \cong A_1 \times \ldots \times A_n \times B_1 \times \ldots \times B_m$.

Dowód. Wystarczy zauważyć, że przekształcenie $f \colon (A_1 \times \ldots \times A_n) \times (B_1 \times \ldots \times B_m) \to A_1 \times \ldots \times A_n \times B_1 \times \ldots \times B_m$ dane wzorem $f((a_1, \ldots, a_n), (b_1, \ldots, b_m)) = (a_1, \ldots, a_n, b_1, \ldots, b_m)$ jest izomorfizmem grup. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Definicja 5.4. Powiemy, że grupa G jest **torsyjna**, jeżeli każdy jej element ma skończony rząd, tzn. dla każdego $g \in G$ istnieje $n \in \mathbb{N}$ takie, że $g^n = e$.

Definicja 5.5. Powiemy, że grupa G jest **beztorsyjna**, jeżeli każdy element $g \neq e$ tej grupy ma nieskończony rząd.

Przykład 5.6. Każda grupa skończona jest torsyjna. Przykładem nieskończonej grupy torsyjnej jest zbiór $\mathbb{C}_\infty$ wszystkich liczb zespolonych z takich, że $z^n = 1$ dla pewnego naturalnego n ze zwykłym mnożeniem liczb zespolonych. Przykładem grupy beztorsyjnej jest $\mathbb{Z}^+$.

Twierdzenie 5.7. *Jeżeli A_1 i A_2 są grupami torsyjnymi, zaś B_1 i B_2 są grupami beztorsyjnymi, to:*

$$A_1 \times B_1 \cong A_2 \times B_2 \Longleftrightarrow [A_1 \cong A_2 \text{ i } B_1 \cong B_2].$$

Dowód. Niech $f\colon A_1 \times B_1 \to A_2 \times B_2$ będzie izomorfizmem grup oraz niech $a \in A_1$. Wtedy $f(a,e) = (x,y)$ dla pewnych $x \in A_2$ i $y \in B_2$. Ale $a^n = e$ dla pewnego $n \in \mathbb{N}$, więc $(x^n, y^n) = (x,y)^n = [f(a,e)]^n = f(a^n, e^n) = f(e,e) = (e,e)$. Stąd $x^n = e$ i $y^n = e$, więc $y = e$, bo grupa B_2 jest beztorsyjna. Zatem $f(A_1 \times \{e\}) \subseteq A_2 \times \{e\}$. Ale $f^{-1}\colon A_2 \times B_2 \to A_1 \times B_1$ też jest izomorfizmem grup, więc zamieniając f na f^{-1} w powyższym rozumowaniu uzyskamy, że $f^{-1}(A_2 \times \{e\}) \subseteq A_1 \times \{e\}$. Zatem $f(A_1 \times \{e\}) = A_2 \times \{e\}$, czyli $A_1 \times \{e\} \cong A_2 \times \{e\}$, skąd $A_1 \cong A_2$.

Łatwo zauważyć, że przekształcenie $F\colon B_1 \to (A_2 \times B_2)/\overline{A_2}$ dane wzorem $F(b) = f(e,b)\overline{A_2}$ dla $b \in B_1$ jest homomorfizmem grup. Jeśli $b \in Ker(F)$, to $f(e,b)\overline{A_2} = \overline{A_2}$, skąd $f(e,b) \in \overline{A_2} = f(A_1 \times \{e\})$. Zatem istnieje $a \in A_1$ takie, że $f(e,b) = f(a,e)$, czyli $(e,b) = (a,e)$, więc $b = e$ i wobec tego F jest zanurzeniem grup. Weźmy dowolne $x \in A_2 \times B_2$. Wtedy istnieją $a \in A_1$ oraz $b \in B_1$ takie, że $x = f(a,b)$, więc $x\overline{A_2} = f(a,b)\overline{A_2}$. Ale $f(a,b) = f((a,e)\cdot(e,b)) = f(a,e)\cdot f(e,b)$, więc $[f(e,b)]^{-1}\cdot f(a,e)\cdot f(e,b) \in \overline{A_2}$, bo $f(a,e) \in \overline{A_2}$ oraz $\overline{A_2} \lhd A_2 \times B_2$. Zatem $x\overline{A_2} = f(e,b)\overline{A_2} = F(b)$, czyli F jest 'na'. Zatem ostatecznie F jest izomorfizmem grup, czyli $B_1 \cong (A_2 \times B_2)/\overline{A_2}$. Ponadto, jak wiemy, $(A_2 \times B_2)/\overline{A_2} \cong B_2$, więc ostatecznie $B_1 \cong B_2$.

Implikacja odwrotna wynika od razu ze stwierdzenia 5.2. □

Stwierdzenie 5.8. *Dla dowolnych liczb naturalnych m i n:*

$$(\mathbb{Z}^+)^n \cong (\mathbb{Z}^+)^m \Leftrightarrow n = m.$$

Dowód. Załóżmy, że $(\mathbb{Z}^+)^n \cong (\mathbb{Z}^+)^m$. Wtedy istnieje izomorfizm grup $f\colon (\mathbb{Z}^+)^n \to (\mathbb{Z}^+)^m$. Z algebry liniowej wynika, że f można jednoznacznie rozszerzyć do przekształcenia liniowego $F\colon \mathbb{Q}^n \to \mathbb{Q}^m$. Ponadto wówczas F jest izomorfizmem liniowym, więc $\mathbb{Q}^n \cong \mathbb{Q}^m$, skąd z algebry liniowej $n = m$.

Implikacja odwrotna jest oczywista. □

Stwierdzenie 5.9. *Niech $A_1, A_2, \ldots, A_n$ będą dowolnymi nietrywialnymi grupami. Wówczas grupa $A = A_1 \times A_2 \times \ldots \times A_n$ jest cykliczna wtedy i tylko wtedy, gdy $A_1, A_2, \ldots, A_n$ są skończonymi grupami cyklicznymi o parami względnie pierwszych rzędach.*

Dowód. Załóżmy, że grupa A jest cykliczna. Ponieważ obraz homomorficzny grupy cyklicznej jest grupą cykliczną, więc grupy $A_1, A_2, \ldots, A_n$ są cykliczne. Jeżeli dla pewnego $i = 1, 2, \ldots, n$ grupa A_i jest nieskończona, to A jest grupą cykliczną nieskończoną, czyli $A \cong \mathbb{Z}^+$. Ale $\overline{A_1}$ i $\overline{A_2}$ są dwiema nietrywialnymi podgrupami grupy A oraz $\overline{A_1} \cap \overline{A_2} = \{e\}$, więc mamy sprzeczność, bo przecięcie dowolnych dwóch nietrywialnych podgrup grupy $\mathbb{Z}^+$ jest podgrupą nietrywialną. Zatem $A_1, A_2, \ldots, A_n$ są skończonymi grupami cyklicznymi. Jeżeli ich rzędy nie są parami względnie pierwsze, to istnieje liczba naturalna $d > 1$ taka, że d dzieli $|A_i|$ i d dzieli $|A_j|$ dla pewnych różnych liczb $i, j \in \{1, 2, \ldots, n\}$. Ale wtedy w grupie A_i istnieje podgrupa H rzędu d oraz w grupie A_j istnieje podgrupa K rzędu d. Zatem $\overline{H}$ i $\overline{K}$ są dwiema różnymi podgrupami tego samego rzędu d w skończonej grupie cyklicznej A i otrzymujemy sprzeczność. Stąd $A_1, A_2, \ldots, A_n$ są skończonymi grupami cyklicznymi o parami względnie pierwszych rzędach.

Na odwrót, załóżmy, że $A_1, A_2, \ldots, A_n$ są skończonymi grupami cyklicznymi o parami względnie pierwszych rzędach $k_1, k_2, \ldots, k_n$ odpowiednio. Niech a_i będzie generatorem grupy A_i dla $i = 1, 2, \ldots, n$ i niech $k = k_1 \cdot k_2 \cdot \ldots \cdot k_n$. Wtedy $a_i^k = e$ dla $i = 1, 2, \ldots, n$, więc $(a_1, a_2, \ldots, a_n)^k = (a_1^k, a_2^k, \ldots, a_n^k) = e$, skąd $s = o((a_1, a_2, \ldots, a_n)) \leqslant k$. Ponadto $e = (a_1, a_2, \ldots, a_n)^s = (a_1^s, a_2^s, \ldots, a_n^s)$, więc $a_i^s = e$, skąd

$k_i \mid s$ dla wszystkich $i = 1, 2, \ldots, n$. Ale liczby $k_1, k_2, \ldots, k_n$ są parami względnie pierwsze, więc $k \mid s$. Zatem $k \leqslant s$. Ale także $s \leqslant k$, więc $s = k$. Stąd $o((a_1, a_2, \ldots, a_n)) = k = |A|$, czyli grupa A jest cykliczna. □

Stwierdzenie 5.10. *Niech $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, gdzie $p_1, \ldots, p_s$ są różnymi liczbami pierwszymi oraz $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$. Wówczas $\mathbb{Z}_n^+ \cong \mathbb{Z}_{p_1^{\alpha_1}}^+ \times \ldots \times \mathbb{Z}_{p_s^{\alpha_s}}^+$.*

Dowód. Z naszych założeń oraz ze stwierdzenia 5.9 wynika, że grupa $\mathbb{Z}_{p_1^{\alpha_1}}^+ \times \ldots \times \mathbb{Z}_{p_s^{\alpha_s}}^+$ jest cykliczna i ma rząd n. Zatem z algebry I ta grupa jest izomorficzna z grupą $\mathbb{Z}_n^+$. □

5.2 Wewnętrzna suma prosta

Lemat 5.11. *Jeżeli A i B są podgrupami normalnymi grupy G takimi, że $A \cap B = \{e\}$, to $ab = ba$ dla dowolnych $a \in A$ oraz $b \in B$.*

Dowód. Dla $a \in A$ oraz $b \in B$ mamy, że $[a, b] = a^{-1}(b^{-1}ab) \in A$, bo $a^{-1} \in A$ oraz $b^{-1}ab \in A$, gdyż $A \lhd G$. Ponadto $[a, b] = (a^{-1}b^{-1}a)b \in B$, gdyż $a^{-1}b^{-1}a \in B$, bo $b^{-1} \in B$ i $B \lhd G$. Zatem $[a, b] \in A \cap B = \{e\}$, skąd $[a, b] = e$, czyli $ab = ba$. □

Lemat 5.12. *Niech A i B będą podgrupami normalnymi grupy G. Wówczas równoważne są warunki:*

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

(ii) Dla dowolnych $a \in A$ oraz $b \in B$: $ab = e \Longrightarrow a = b = e$.

Dowód. $(i) \Rightarrow (ii)$. Weźmy $a \in A$ oraz $b \in B$ takie, że $ab = e$. Wtedy $b = a^{-1} \in A$ oraz $b \in B$, więc $b \in A \cap B$, skąd $b = e$. Ale $ab = e$, więc $a = e$.

$(i) \Leftarrow (ii)$. Weźmy dowolne $x \in A \cap B$. Wtedy $x \in A$ oraz $x^{-1} \in B$ oraz $x \cdot x^{-1} = e$, więc $x = e$. Zatem $A \cap B = \{e\}$. □

Przypomnijmy, że jeżeli A jest podgrupą normalną grupy G oraz H jest podgrupą grupy G, to $AH = \{ah : a \in A, h \in H\}$ jest podgrupą

grupy G oraz $AH = HA$. Jeżeli A i B są podgrupami normalnymi grupy G, to AB też jest podgrupą normalną grupy G.

Niech $A_1, A_2, \ldots$ będzie ciągiem podgrup normalnych grupy G. Wtedy określamy:

$$A_1A_2 \ldots A_{n+1} = (A_1A_2 \ldots A_n)A_{n+1} \text{ dla } n = 1, 2, \ldots.$$

Przez prostą indukcję można wykazać, że wtedy $A_1A_2 \ldots A_n$ jest podgrupą normalną w grupie G oraz

$$A_1A_2 \ldots A_n = \{a_1a_2 \ldots a_n : a_i \in A_i \text{ dla } i = 1, \ldots, n\},\ n = 2, 3, \ldots.$$

Lemat 5.13. *Jeżeli A i B są podgrupami normalnymi grupy G takimi, że $A \cap B = \{e\}$, to $AB \cong A \times B$.*

Dowód. Z lematów 5.11 i 5.12 w prosty sposób wynika, że przekształcenie $f\colon A \times B \to AB$ dane wzorem $f(a, b) = ab$ dla $a \in A$, $b \in B$ jest izomorfizmem grup. □

Definicja 5.14. Powiemy, że grupa G jest **wewnętrzną sumą prostą** swoich podgrup normalnych $H_1, \ldots, H_n$, jeżeli $G = H_1 \ldots H_n$ oraz dla dowolnych $h_1 \in H_1, \ldots, h_n \in H_n$ z tego, że $h_1 \ldots h_n = e$ wynika, że $h_1 = \ldots = h_n = e$. Piszemy wtedy

$$G = H_1 \oplus \ldots \oplus H_n.$$

Z lematu 5.12 mamy od razu następujące

Stwierdzenie 5.15. *Grupa G jest wewnętrzną sumą prostą swoich podgrup normalnych H_1 i H_2 wtedy i tylko wtedy, gdy $G = H_1H_2$ oraz $H_1 \cap H_2 = \{e\}$.*

Stwierdzenie 5.16. *Jeżeli grupa G jest wewnętrzną sumą prostą swoich podgrup normalnych $H_1, \ldots, H_n$, to $G \cong H_1 \times \ldots \times H_n$.*

Dowód. Indukcja względem $n \geqslant 2$. Dla $n = 2$ teza wynika od razu z lematu 5.13. Załóżmy, że teza zachodzi dla pewnego $n \geqslant 2$ i niech $G = H_1 \ominus \ldots \oplus H_n \oplus H_{n+1}$. Wtedy $H_1 \ldots H_n = H_1 \oplus \ldots \oplus H_n$, więc z założenia indukcyjnego $H_1 \ldots H_n \cong H_1 \times \ldots \times H_n$. Ponadto $G = (H_1 \ldots H_n) \ominus H_{n+1}$, więc z lematu 5.13, $G \cong (H_1 \ldots H_n) \times H_{n+1}$. Zatem ze stwierdzeń 5.2 i 5.3 mamy, że $G \cong H_1 \times \ldots \times H_n \times H_{n+1}$. □

Stwierdzenie 5.17. *Niech $G, G_1, \ldots, G_n$ będą grupami takimi, że $G \cong G_1 \times G_2 \times \ldots \times G_n$. Wtedy w grupie G istnieją podgrupy normalne $H_i \cong G_i$ dla $i = 1, \ldots, n$ takie, że $G = H_1 \oplus H_2 \oplus \ldots \oplus H_n$.*

Dowód. Niech $f\colon G_1 \times G_2 \times \ldots \times G_n \to G$ będzie izomorfizmem grup. Ponieważ $\overline{G_i} \lhd G_1 \times \ldots \times G_n$, więc $H_i = f(\overline{G_i})$ jest podgrupą normalną grupy G dla każdego $i = 1, \ldots, n$. Z określenia podgrup $\overline{G_i}$ wynika, że $G_1 \times \ldots \times G_n = \overline{G_1} \oplus \ldots \oplus \overline{G_n}$. Stąd w prosty sposób uzyskujemy, że $G = H_1 \oplus \ldots \oplus H_n$. □

Stwierdzenie 5.18. *Jeżeli $H_1, \ldots, H_n$ ($n \geqslant 2$) są skończonymi podgrupami normalnymi grupy G o parami względnie pierwszych rzędach, to $H_1 H_2 \ldots H_n = H_1 \oplus H_2 \oplus \ldots \oplus H_n$ oraz $H_1 H_2 \ldots H_n \cong H_1 \times H_2 \times \ldots \times H_n$.*

Dowód. Stosujemy indukcję względem n. Dla $n = 2$ mamy, że $H_1 \cap H_2$ jest podgrupą grup H_1 i H_2, więc z twierdzenia Lagrange'a $|H_1 \cap H_2|$ jest dzielnikiem $|H_1|$ i $|H_2|$. Ale $(|H_1|, |H_2|) = 1$, więc $H_1 \cap H_2 = \{e\}$, więc $H_1 H_2 = H_1 \oplus H_2 \cong H_1 \times H_2$ na mocy lematu 5.13 i stwierdzenia 5.15.

Załóżmy, że teza zachodzi dla pewnej liczby naturalnej $n \geqslant 2$ i niech $H_1, \ldots, H_n, H_{n+1}$ będą skończonymi podgrupami normalnymi grupy G o parami względnie pierwszych rzędach. Wtedy z założenia indukcyjnego $H_1 \ldots H_n = H_1 \oplus \ldots \oplus H_n \cong H_1 \times \ldots \times H_n$. Zatem $|H_1 \ldots H_n| = |H_1| \cdot \ldots \cdot |H_n|$ oraz $H_1 \ldots H_n$ jest podgrupą normalną grupy G. Ponadto $(|H_{n+1}|, |H_i|) = 1$ dla $i = 1, \ldots, n$, więc $(|H_{n+1}|, |H_1| \cdot \ldots |H_n|) = 1$. Zatem z pierwszej części dowodu $(H_1 \ldots H_n) \cap H_{n+1} = \{e\}$. Niech $h_i \in H_i$ dla $i = 1, \ldots, n+1$ będą takie, że $h_1 h_2 \ldots h_n h_{n+1} = e$. Wtedy $h_1 \ldots h_n = h_{n+1}^{-1} \in H_{n+1}$ oraz $h_1 \ldots h_n \in H_1 \ldots H_n$, skąd $h_1 \ldots h_n = e$. Zatem z założenia indukcyjnego $h_1 = \ldots = h_n = e$, skąd $h_{n+1} = e$. Wynka stąd, że $H_1 \ldots H_n H_{n+1} = H_1 \oplus \ldots \oplus H_n \oplus H_{n+1}$. Ale $H_1 \ldots H_{n+1} \cong H_1 \times \ldots \times H_{n+1}$ na mocy stwierdzenia 5.16, więc teza zachodzi dla liczby $n+1$. □

Z twierdzenia Sylowa, stwierdzeń 2.4 i 5.18 wynika od razu następujące

Twierdzenie 5.19. *Jeżeli dla każdej liczby pierwszej p dzielącej rząd grupy skończonej G istnieje w grupie G dokładnie jedna p-podgrupa Sylowa H_p, to grupa G jest izomorficzna z iloczynem prostym wszystkich swoich p-podgrup Sylowa.*

Ponieważ każda podgrupa grupy abelowej jest jej dzielnikiem normalnym, więc z twierdzenia Sylowa oraz z twierdzenia 5.19 wynika od razu następujący

Wniosek 5.20. *Każda skończona nietrywialna grupa abelowa jest sumą prostą wszystkich swoich p-podgrup Sylowa.*

Stwierdzenie 5.21. *Niech $p_1, \ldots, p_r$ będą różnymi liczbami pierwszymi oraz niech G_i będzie skończoną p_i-grupą dla $i = 1, \ldots, r$. Wówczas $\overline{G_i}$ jest jedyną p_i-podgrupą Sylowa grupy $G_1 \times \ldots \times G_r$ oraz $\overline{G_1}, \ldots, \overline{G_r}$ są wszystkimi p-podgrupami Sylowa grupy $G_1 \times \ldots \times G_r$.*

Dowód. Z założenia wynika, że $|G_i| = p_i^{k_i}$, $k_i \in \mathbb{N}$, $i = 1, \ldots, r$. Stąd $|G_1 \times \ldots \times G_r| = |G_1| \cdot \ldots \cdot |G_r| = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$. Ale $\overline{G_i} \cong G_i$, więc $\overline{G_i}$ jest p_i-podgrupą Sylowa grupy $G_1 \times \ldots \times G_r$ dla $i = 1, \ldots, r$. Ponadto $\overline{G_i} \lhd G_1 \times \ldots \times G_r$, więc na mocy stwierdzenia 2.4, $\overline{G_i}$ jest jedyną p_i-podgrupą Sylowa grupy $G_1 \times \ldots \times G_r$ dla $i = 1, \ldots, r$. □

Stwierdzenie 5.22. *Niech $p_1 < \ldots < p_r$ i $q_1 < \ldots < q_s$ będą liczbami pierwszymi. Niech G_i będzie skończoną p_i-grupą dla $i = 1, \ldots, r$ i niech H_j będzie skończoną q_j-grupą dla $j = 1, \ldots, s$. Wówczas $G_1 \times \ldots \times G_r \cong H_1 \times \ldots \times H_s \Leftrightarrow (r = s,\ p_i = q_i,\ G_i \cong H_i$ dla $i = 1, \ldots, r)$.*

Dowód. Implikacja $\Leftarrow$ wynika od razu ze stwierdzenia 5.2.
$\Rightarrow$. Niech $f\colon G_1 \times \ldots \times G_r \to H_1 \times \ldots \times H_s$ będzie izomorfizmem grup. Wtedy $|G_1 \times \ldots \times G_r| = |H_1 \times \ldots \times H_s|$, czyli $|G_1| \cdot \ldots \cdot |G_r| = |H_1| \cdot \ldots \cdot |H_s|$. Ale $|G_i| = p_i^{\alpha_i}$, $\alpha_i \in \mathbb{N}$, $i = 1, \ldots, r$ oraz $|H_j| = q_j^{\beta_j}$, $\beta_j \in \mathbb{N}$, $j = 1, \ldots, s$, więc $p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} = q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s}$. Stąd z twierdzenia o jednoznaczności rozkładu dla liczb naturalnych mamy, że $r = s$, $p_i = q_i$ oraz $\alpha_i = \beta_i$ dla $i = 1, \ldots, r$. Ponadto ze stwierdzenia 5.21, $\overline{G_i}$ jest jedyną p_i-podgrupą Sylowa grupy $G_1 \times \ldots \times G_r$, więc $f(\overline{G_i})$ jest jedyną p_i-podgrupą Sylowa grupy $H_1 \times \ldots \times H_r$, czyli ze stwierdzenia 5.21, $f(\overline{G_i}) = \overline{H_i}$, skąd $\overline{G_i} \cong \overline{H_i}$, czyli $G_i \cong H_i$ dla $i = 1, \ldots, r$. □

Rozdział 6

Struktura skończenie generowanych grup abelowych

6.1 Struktura skończonych grup abelowych

Lemat 6.1. *Niech p będzie liczbą pierwszą i niech $(A, +, \theta)$ będzie grupą abelową rzędu p^α, gdzie $\alpha \in \mathbb{N}$. Niech $a \in A$ będzie elementem maksymalnego rzędu w A. Jeżeli $\langle a \rangle \neq A$, to istnieje $c \in A$, $c \neq \theta$, takie, że $\langle a \rangle \cap \langle c \rangle = \{\theta\}$.*

Dowód. Z założenia wynika, że $A/\langle a \rangle$ jest skończoną p-grupą abelową. Zatem z twierdzenia Cauchy'ego istnieje $b \in A$ takie, że $o(b + \langle a \rangle) = p$, czyli $b \notin \langle a \rangle$ i $pb \in \langle a \rangle$. Zatem $pb = ka$ dla pewnego $k \in \mathbb{Z}$. Jeśli p nie dzieli k, to $(o(a), k) = 1$, więc istnieją $x, y \in \mathbb{Z}$ takie, że $o(a)x + ky = 1$, więc $a = o(a)xa + kya = y(ka) = y(pb) = pyb$, czyli $a \in \langle b \rangle$. Zatem $\langle a \rangle \subseteq \langle b \rangle$, skąd $o(a) \leqslant o(b)$, więc z maksymalności $o(a)$ jest $o(a) = o(b)$ i $\langle a \rangle = \langle b \rangle$. Zatem $b \in \langle a \rangle$, sprzeczność.

Stąd $p \mid k$ i $k = pl$ dla pewnego $l \in \mathbb{Z}$ oraz $pb = pla$, czyli $p(b - la) = \theta$. Niech $c = b - la$. Wtedy $c \notin \langle a \rangle$, bo $b \notin \langle a \rangle$, skąd $c \neq \theta$. Ponadto $pc = \theta$. Ale $\langle a \rangle \cap \langle c \rangle$ jest podgrupą grupy p-elementowej $\langle c \rangle$ i $c \notin \langle a \rangle$,

więc $\langle a\rangle \cap \langle c\rangle = \{\theta\}$. □

Lemat 6.2. *Niech p będzie liczbą pierwszą i niech $(A, +, \theta)$ będzie grupą abelową rzędu p^α dla pewnego $\alpha \in \mathbb{N}$. Jeżeli $a \in A$ jest elementem maksymalnego rzędu w A, to istnieje podgrupa B grupy A taka, że $\langle a\rangle \oplus B = A$.*

Dowód. Zastosujemy indukcję względem α. Dla $\alpha = 1$ mamy, że $o(a) = p$, więc $\langle a\rangle = A$ i wystarczy wziąć $B = \{\theta\}$. Załóżmy więc dalej, że nasz lemat zachodzi dla p-grup rzędu mniejszego od p^α. Jeśli $\langle a\rangle = A$, to wystarczy wziąć $B = \{\theta\}$. Niech dalej $\langle a\rangle \neq A$. Niech B będzie maksymalną podgrupą w A taką, że $\langle a\rangle \cap B = \{\theta\}$. Z lematu 6.1 wynika, że $|B| > 1$. Niech $\pi\colon A \to A/B$ będzie epimorfizmem naturalnym. Niech $o(a) = p^r$, gdzie $r \in \mathbb{N}$ i $r < \alpha$. Wtedy $p^r\pi(a) = \pi(p^r a) = \pi(\theta) = B$ oraz jeśli $o(\pi(a)) = m$, to $m \cdot (a + B) = B$, skąd $m \cdot a \in B$, więc $m \cdot a \in \langle a\rangle \cap B = \{\theta\}$, czyli $m \cdot a = \theta$. Zatem $o(a) \mid m$, czyli $p^r \mid m$. Ale $o(\pi(a)) \leqslant p^r$, więc stąd $o(\pi(a)) = o(a) = p^r$. Dla $x \in A$ mamy, że $o(x + B) \mid o(x)$, więc $o(x + B) \leqslant o(x) \leqslant o(a)$. Zatem $a + B$ jest elementem maksymalnego rzędu w grupie A/B. Ponadto $|A/B| = \frac{|A|}{|B|} < |A|$, bo $|B| > 1$. Zatem z założenia indukcyjnego istnieje podgrupa H grupy A taka, że $B \subseteq H$ oraz $\langle a+B\rangle \oplus H/B = A/B$. Stąd $\langle a+B\rangle \cap H/B = \{B\}$, czyli $\langle a\rangle \cap H \subseteq B$, więc $\langle a\rangle \cap H \subseteq \langle a\rangle \cap B = \{\theta\}$, czyli $\langle a\rangle \cap H = \{\theta\}$. Ale $B \subseteq H$, więc z maksymalności B musi być $H = B$ i stąd $A/B = \langle a + B\rangle$. Jeżeli $x \in A$, to istnieje $k \in \mathbb{Z}$ takie, że $x + B = k \cdot (a + B)$, skąd $x - ka \in B$, więc $x \in \langle a\rangle + B$. Zatem $A = \langle a\rangle \oplus B$. □

Z lematu 6.2 i z wniosku 5.20 wynika w prosty sposób następujące

Twierdzenie 6.3. *Każda nietrywialna skończona grupa abelowa jest sumą prostą pewnych swoich p-podgrup cyklicznych.*

Z twierdzenia Lagrange'a i ze stwierdzenia 5.9 wynika, że jeśli A jest cykliczną p-grupą, to nie istnieją nietrywialne grupy B, C takie, że $A \cong B \times C$. W szczególności cykliczna p-grupa nie jest sumą prostą pewnych swoich właściwych podgrup.

Niech $(A, +, \theta)$ będzie grupą abelową i niech $n \in \mathbb{N}$. Oznaczmy $nA = \{na : a \in A\}$. Wtedy $\theta = n \cdot \theta \in nA$ oraz dla dowolnych $a, b \in A$, $na - nb = n(a - b) \in nA$. Zatem nA jest podgrupą grupy A.

Lemat 6.4. *Niech A i B będą izomorficznymi grupami abelowymi. Wówczas dla dowolnej liczby naturalnej n: $nA \cong nB$.*

Dowód. Niech $f\colon A \to B$ będzie izomorfizmem grup i niech $n \in \mathbb{N}$. Wtedy dla $a \in A$ mamy, że $f(na) = nf(a) \in nB$, skąd $f(nA) \subseteq nB$. Niech $b \in B$. Wtedy istnieje $a \in A$ takie, że $b = f(a)$, skąd $nb = nf(a) = f(na)$, czyli $nB \subseteq f(nA)$ i ostatecznie $nB = f(nA)$. Zatem $nA \cong nB$. □

Stwierdzenie 6.5. *Niech p będzie liczbą pierwszą i niech $A_1, \ldots, A_n, B_1, \ldots, B_m$ będą nietrywialnymi p-grupami cyklicznymi oraz niech $|A_i| = p^{\alpha_i}$ dla $i = 1, \ldots, n$, gdzie $1 \leqslant \alpha_1 \leqslant \ldots \leqslant \alpha_n$ oraz $|B_j| = p^{\beta_j}$ dla $j = 1, \ldots, m$, gdzie $1 \leqslant \beta_1 \leqslant \ldots \leqslant \beta_m$. Jeżeli $A_1 \times \ldots \times A_n \cong B_1 \times \ldots \times B_m$, to $n = m$ oraz $\alpha_i = \beta_i$ dla $i = 1, \ldots, n$.*

Dowód. Zastosujemy indukcję ze względu na $\alpha_1 + \ldots + \alpha_n$. Jeśli $\alpha_1 + \ldots + \alpha_n = 1$, to $|A_1 \times \ldots \times A_n| = p^{\alpha_1 + \ldots + \alpha_n} = p$ i $p^{\beta_1 + \ldots + \beta_m} = |B_1 \times \ldots \times B_m| = |A_1 \times \ldots \times A_n| = p$, więc $\alpha_1 + \ldots + \alpha_n = 1 = \beta_1 + \ldots + \beta_m$, skąd $n = m = 1$ i $\alpha_1 = \beta_1 = 1$.

Niech k będzie taką liczbą naturalną, że teza zachodzi dla wszystkich $\alpha_1 + \ldots + \alpha_n < k$. Załóżmy, że $\alpha_1 + \ldots + \alpha_n = k$. Niech $A = A_1 \times \ldots \times A_n$ i $B = B_1 \times \ldots \times B_m$ oraz $A \cong B$. Wtedy $|A| = |B|$, skąd $\alpha_1 + \ldots + \alpha_n = \beta_1 + \ldots + \beta_m$ oraz z lematu 6.4 $pA \cong pB$, więc $|pA| = |pB|$. Ponadto pA_i jest grupą cykliczną rzędu $p^{\alpha_i - 1}$ dla $i = 1, \ldots, n$, więc $pA_i = \{\theta\} \iff \alpha_i = 1$ i podobnie pB_j jest grupą cykliczną rzędu $p^{\beta_j - 1}$ dla $j = 1, \ldots, m$. Dalej, $pA = pA_1 \times \ldots \times pA_n$ oraz $pB = pB_1 \times \ldots \times pB_m$. Ponadto $|pA| = p^{(\alpha_1 - 1) + \ldots + (\alpha_n - 1)} = p^{\alpha_1 + \ldots + \alpha_n - n}$ oraz analogicznie $|pB| = p^{\beta_1 + \ldots + \beta_m - m}$. Ale $|pA| = |pB|$, więc $\alpha_1 + \ldots + \alpha_n - n = \beta_1 + \ldots + \beta_m - m$, skąd $n = m$.

Jeżeli $|pA| = 1$, to $|pB| = 1$ i $(\alpha_1 - 1) + \ldots + (\alpha_n - 1) = 0$ oraz $(\beta_1 - 1) + \ldots + (\beta_m - 1) = 0$, czyli $\alpha_i = \beta_i = 1$ dla $i = 1, \ldots, n$. Załóżmy dalej, że $|pA| > 1$. Wtedy $\alpha_i - 1 > 0$ dla pewnego najmniejszego i oraz istnieje najmniejsze j takie, że $\beta_j - 1 > 0$. Zatem $\alpha_1 = \ldots = \alpha_{i-1} = 1$,

$\beta_1 = \ldots = \beta_{j-1} = 1$ oraz $pA \cong pA_i \times \ldots \times pA_n$, $pB \cong pB_j \times \ldots \times pB_m$, więc z założeia indukcyjnego $n-(i-1) = m-(j-1)$ oraz $\alpha_k - 1 = \beta_k - 1$ dla $k = i, \ldots, n$. Ponadto $n = m$, więc $i = j$. Zatem $\alpha_k = \beta_k$ dla wszystkich $k = 1, \ldots, i, \ldots, n$. □

Z twierdzenia 6.3 oraz ze stwierdzeń 5.1, 5.2 i 6.5 wynika od razu następujące **twierdzenie klasyfikacyjne dla skończonych p-grup abelowych**.

Twierdzenie 6.6. *Niech p będzie liczbą pierwszą i niech $k \in \mathbb{N}$. Oznaczmy przez Σ_k zbiór wszystkich ciągów $\sigma = (\alpha_1, \ldots, \alpha_n)$ liczb naturalnych $\alpha_1 \leqslant \ldots \leqslant \alpha_n$ takich, że $\alpha_1 + \ldots + \alpha_n = k$. Wówczas wszystkimi z dokładnością do izomorfizmu grupami abelowymi rzędu p^k są grupy $A_{p,\sigma} = \mathbb{Z}^+_{p^{\alpha_1}} \times \ldots \times \mathbb{Z}^+_{p^{\alpha_n}}$ dla $\sigma \in \Sigma_k$.*

Z twierdzeń 6.3 i 6.6 oraz ze stwierdzeń 5.1, 5.2, 5.16, 5.17, 5.22 i 6.5 wynika od razu następujące **twierdzenie klasyfikacyjne dla skończonych grup abelowych**.

Twierdzenie 6.7. *Niech $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, gdzie $p_1 < \ldots < p_s$ są liczbami pierwszymi oraz $\alpha_1, \ldots, \alpha_s \in \mathbb{N}$. Wówczas wszystkimi z dokładnością do izomorfizmu grupami abelowymi rzędu n są grupy A_n postaci $A_n = A_{p_1,\sigma_1} \times \ldots \times A_{p_s,\sigma_s}$, gdzie $\sigma_i \in \Sigma_{\alpha_i}$ dla $i = 1, \ldots, s$.*

6.2 Struktura skończenie generowanych abelowych grup beztorsyjnych

Definicja 6.8. Powiemy, że grupa abelowa $(A, +, \theta)$ jest **skończenie generowana**, jeżeli istnieją $a_1, \ldots, a_n \in A$ takie, że $A = \langle a_1, \ldots, a_n \rangle$, tzn. $A = \{k_1 \cdot a_1 + \ldots + k_n \cdot a_n : k_1, \ldots, k_n \in \mathbb{Z}\}$.

Definicja 6.9. Niech $(A, +, \theta)$ będzie grupą abelową beztorsyjną. Powiemy, że elementy $a_1, \ldots, a_n \in A$ są **liniowo niezależne**, jeżeli dla dowolnych $k_1, \ldots, k_n \in \mathbb{Z}$ z tego, że $k_1 \cdot a_1 + \ldots + k_n \cdot a_n = \theta$ wynika, że $k_1 = \ldots = k_n = 0$. Powiemy, że podzbiór $\{a_1, \ldots, a_n\} \subseteq A$ jest **bazą** grupy A, jeżeli $A = \langle a_1, \ldots, a_n \rangle$ oraz zbiór $\{a_1, \ldots, a_n\}$ jest liniowo niezależny.

Przykład 6.10. Łatwo zauważyć, że dla dowolnej liczby naturalnej n bazą grupy $(\mathbb{Z}^+)^n$ jest zbiór $\{\varepsilon_1, \ldots, \varepsilon_n\}$, gdzie $\varepsilon_1 = (1, 0, \ldots, 0), \varepsilon_2 = (0, 1, \ldots, 0), \ldots, \varepsilon_n = (0, 0, \ldots, 1)$.

Twierdzenie 6.11. *Każda skończenie generowana beztorsyjna grupa abelowa posiada skończoną bazę.*

Dowód. Niech A będzie skończenie generowaną beztorsyjną grupą abelową i niech n będzie minimalną liczbą generatorów grupy A. Jeśli $n = 1$, to $A = \langle a \rangle$ dla pewnego $a \in A$ oraz $o(a) = \infty$. Stąd $\{a\}$ jest bazą A. Niech dalej $n > 1$. Wtedy grupa A posiada n generatorów, ale nie posiada $n-1$ generatorów. Załóżmy, że A nie posiada skończonej bazy. Wówczas dla dowolnych $a_1, \ldots, a_n \in A$ takich, że $A = \langle a_1, \ldots, a_n \rangle$ istnieją $k_1, \ldots, k_n \in \mathbb{Z}$ nie wszystkie równe 0 i takie, że $k_1 \cdot a_1 + \ldots + k_n \cdot a_n = \theta$. Niech k będzie najmniejszą liczbą naturalną taką, że istnieją $b_1, \ldots, b_n \in A$ takie, że $A = \langle b_1, \ldots, b_n \rangle$ oraz dla pewnych $l_1, \ldots, l_n \in \mathbb{Z}$ jest $l_1 \cdot b_1 + \ldots + l_n \cdot b_n = \theta$ oraz $l_i = \pm k$ dla pewnego $i = 1, \ldots, n$. Jeżeli $k \mid l_j$ dla wszystkich $j = 1, \ldots, n$, to $l_j = kt_j$, $t_j \in \mathbb{Z}$ dla $j = 1, \ldots, n$ oraz $(kt_1)b_1 + \ldots + (kt_n)b_n = \theta$, więc $k(t_1b_1 + \ldots + t_nb_n) = \theta$, skąd z beztorsyjności grupy A, $t_1b_1 + \ldots + t_nb_n = \theta$. Ale $l_i = \pm k$, więc $t_i = \pm 1$, skąd $b_i \in \langle b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n \rangle$, więc $A = \langle b_1, \ldots, b_{i-1}, b_{i+1}, \ldots, b_n \rangle$, czyli grupa A posiada $n-1$ generatorów, wbrew założeniu. Zatem dla pewnego $j = 1, \ldots, n$ mamy, że k nie dzieli l_j. Oczywiście $j \neq i$, gdyż $l_i = \pm k$. Bez zmniejszania ogólności rozumowania możemy zakładać, że $i = n$ oraz $j = n-1$. Wtedy $l_{n-1} = ql_n + r$ dla pewnych $q, r \in \mathbb{Z}$, $0 < r < k$, więc $\theta = l_1b_1 + \ldots + l_{n-2}b_{n-2} + (ql_n + r)b_{n-1} + l_nb_n = l_1b_1 + \ldots + l_{n-2}b_{n-2} + rb_{n-1} + l_n(b_n + qb_{n-1})$ oraz $A = \langle b_1, \ldots, b_n \rangle = \langle b_1, \ldots, b_{n-1}, b_n + qb_{n-1} \rangle$ oraz $r < k$ i $r \in \mathbb{N}$, więc mamy sprzeczność z minimalnością k. □

Lemat 6.12. *Jeżeli grupa abelowa beztorsyjna A posiada bazę n-elementową, to $A \cong (\mathbb{Z}^+)^n$.*

Dowód. Niech $\{a_1, \ldots, a_n\}$ będzie bazą grupy A. Łatwo zauważyć, że przekształcenie $f\colon (\mathbb{Z}^+)^n \to A$ dane wzorem

$$f((k_1, \ldots, k_n)) = k_1 \cdot a_1 + \ldots + k_n \cdot a_n$$

jest izomorfizmem grup. □

Z lematu 6.12, przykładu 6.10, twierdzenia 6.11 i ze stwierdzenia 5.8 wynika od razu następujące **twierdzenie klasyfikacyjne dla skończenie generowanych grup abelowych beztorsyjnych**.

Twierdzenie 6.13. *Wszystkimi z dokładnością do izomorfizmu skończenie generowanymi grupami abelowymi beztorsyjnymi są grupy postaci* $(\mathbb{Z}^+)^n$ *dla* $n = 1, 2, \ldots$.

6.3 Struktura skończenie generowanych grup abelowych

Lemat 6.14. *Niech* B *będzie podgrupą grupy abelowej* A. *Jeżeli grupa* B *jest generowana przez* n*-elementów, zaś grupa* A/B *jest generowana przez* m*-elementów, to grupa* A *jest generowana przez* $(n+m)$*-elementów.*

Dowód. Z założenia istnieją $b_1, \ldots, b_n \in B$ i $a_1, \ldots, a_m \in A$ takie, że $B = \langle b_1, \ldots, b_n \rangle$ i $A/B = \langle a_1 + B, \ldots, a_m + B \rangle$. Pokażemy, że $A = \langle b_1, \ldots, b_n, a_1, \ldots, a_m \rangle$. Weźmy dowolne $a \in A$. Wtedy istnieją $k_1, \ldots, k_m \in \mathbb{Z}$ takie, że $a + B = k_1(a_1 + B) + \ldots + k_m(a_m + B)$, skąd $a - (k_1a_1 + \ldots + k_ma_m) \in B$. Zatem istnieją $l_1, \ldots, l_n \in \mathbb{Z}$ takie, że $a - (k_1a_1 + \ldots + k_ma_m) = l_1b_1 + \ldots + l_nb_n$, czyli $a = l_1b_1 + \ldots + l_nb_n + k_1a_1 + \ldots + k_ma_m$, więc $a \in \langle b_1, \ldots, b_n, a_1, \ldots, a_m \rangle$. Zatem grupa A jest generowana przez $(n + m)$-elementów. □

Lemat 6.15. *Jeżeli grupa abelowa* A *jest generowana przez elementy* $a_1, \ldots, a_n$, *to dla dowolnej jej podgrupy* B *grupa* A/B *jest generowana przez elementy* $a_1 + B, \ldots, a_n + B$.

Dowód. Weźmy dowolne $a \in A$. Wtedy istnieją $k_1, \ldots, k_n \in \mathbb{Z}$ takie, że $a = k_1a_1 + \ldots + k_na_n$, więc $a + B = (k_1a_1 + \ldots + k_na_n) + B = k_1(a_1 + B) + \ldots + k_n(a_n + B)$, skąd $A/B = \langle a_1 + B, \ldots, a_n + B \rangle$. □

Stwierdzenie 6.16. *Jeżeli grupa abelowa* A *jest generowana przez* n *elementów, to każda jej podgrupa też jest generowana przez* n *elementów.*

Dowód. Zastosujemy indukcję względem n. Dla $n = 1$ teza wynika stąd, że każda podgrupa grupy cyklicznej jest grupą cykliczną. Załóżmy, że teza zachodzi dla pewnej liczby naturalnej n i niech A będzie grupą abelową o generatorach $a_1, \ldots, a_n, a_{n+1}$. Niech B będzie dowolną podgrupą grupy A. Wtedy $A/\langle a_{n+1}\rangle = \langle a_1 + \langle a_{n+1}\rangle, \ldots, a_n + \langle a_{n+1}\rangle\rangle$, więc z lematu 6.15 i założenia indukcyjnego grupa $(B + \langle a_{n+1}\rangle)/\langle a_{n+1}\rangle$ jest generowana przez n-elementów. Ponadto z II twierdzenia o izomorfizmie $(B+\langle a_{n+1}\rangle)/\langle a_{n+1}\rangle \cong B/(B\cap\langle a_{n+1}\rangle)$, więc grupa $B/(B\cap\langle a_{n+1}\rangle)$ jest generowana przez n-elementów. Ponadto grupa $B \cap \langle a_{n+1}\rangle$ jest cykliczna (jako podgrupa grupy cyklicznej $\langle a_{n+1}\rangle$), więc jest generowana przez jeden element. Stąd z lematu 6.14 grupa B jest generowana przez $(n + 1)$-elementów. □

Częścią torsyjną grupy abelowej $(A, +, \theta)$ nazywamy podzbiór

$$T(A) = \{a \in A : n \cdot a = \theta \text{ dla pewnego } n \in \mathbb{N}\}.$$

Lemat 6.17. *Jeżeli A jest grupą abelową, to $T(A)$ jest podgrupą grupy A oraz grupa $A/T(A)$ jest beztorsyjna.*

Dowód. Ponieważ $1 \cdot \theta = \theta$, więc $\theta \in T(A)$. Ponadto dla $a, b \in T(A)$ istnieją $m, n \in \mathbb{N}$ takie, że $n \cdot a = \theta$ i $m \cdot b = \theta$, skąd $(mn) \cdot (a - b) = \theta$, czyli $a - b \in T(A)$. Zatem $T(A)$ jest podgrupą grupy abelowej A. Niech $a \in A$ oraz $n \in \mathbb{N}$ będą takie, że $n \cdot (a + T(A)) = T(A)$. Wtedy $n \cdot a \in T(A)$, więc istnieje $m \in \mathbb{N}$ takie, że $m \cdot (n \cdot a) = \theta$, skąd $(mn) \cdot a = \theta$, czyli $a \in T(A)$. Zatem $a + T(A) = T(A)$ i grupa $A/T(A)$ jest beztorsyjna. □

Stwierdzenie 6.18. *Jeżeli A jest skończenie generowaną grupą abelową, to istnieje beztorsyjna podgrupa C grupy A taka, że $A = T(A) \oplus C$.*

Dowód. Jeżeli $A = T(A)$, to wystarczy wziąć $C = \{\theta\}$. Niech dalej $A \neq T(A)$. Wtedy z lematów 6.15 i 6.17 wynika, że $A/T(A)$ jest skończenie generowaną abelową grupą beztorsyjną, więc na mocy twierdzenia 6.11 istnieją $a_1. \ldots, a_n \in A$ takie, że bazą grupy $A/T(A)$ jest zbiór $\{a_1 + T(A), \ldots, a_n + T(A)\}$.

Niech $C = \langle a_1, \ldots, a_n \rangle$ i $a \in T(A) \cap C$. Wtedy istnieje $m \in \mathbb{N}$ i istnieją $k_1, \ldots, k_n \in \mathbb{Z}$ takie, że $m \cdot a = \theta$ oraz $a = k_1 a_1 + \ldots + k_n a_n$, skąd $(mk_1)a_1 + \ldots + (mk_n)a_n = \theta$. Zatem $(mk_1) \cdot (a_1 + T(A)) + \ldots + (mk_n) \cdot (a_n + T(A)) = T(A)$, skąd $mk_i = 0$, czyli $k_i = 0$ dla $i = 1, \ldots, n$. Zatem $a = \theta$. Stąd $T(A) \cap C = \{\theta\}$, więc w szczególności grupa C jest beztorsyjna. Weźmy dowolne $a \in A$. Wtedy istnieją $l_1, \ldots, l_n \in \mathbb{Z}$ takie, że $a + T(A) = l_1(a_1 + T(A)) + \ldots + l_n(a_n + T(A))$, skąd $a - (l_1 a_1 + \ldots + l_n a_n) \in T(A)$. Zatem $a \in C + T(A)$. Stąd $A = T(A) + C$ i ostatecznie $A = T(A) \oplus C$. □

Lemat 6.19. *Każda skończenie generowana torsyjna grupa abelowa A jest skończona.*

Dowód. Na mocy założenia istnieją $a_1, a_2, \ldots, a_n \in A$ takie, że $A = \langle a_1, \ldots, a_n \rangle$. Ponadto istnieją $t_i \in \mathbb{N}$ takie, że $t_i \cdot a_i = \theta$. Zatem $|\{k \cdot a_i : k \in \mathbb{Z}\}| \leqslant t_i$ dla $i = 1, \ldots, n$, skąd

$$|A| = |\{k_1 a_1 + \ldots + k_n a_n : k_1, \ldots, k_n \in \mathbb{Z}\}| \leqslant t_1 t_2 \ldots t_n.$$

Zatem grupa A jest skończona. □

Ze stwierdzeń 6.16 i 6.18, lematu 6.19, twierdzeń 6.7 i 6.13, twierdzenia 5.7 oraz stwierdzeń 5.1, 5.2, 5.3, 5.16 i 5.17 wynika w prosty sposób następujące **twierdzenie klasyfikacyjne dla skończenie generowanych grup abelowych.**

Twierdzenie 6.20. *Wszystkimi z dokładnością do izomorfizmu skończenie generowanymi grupami abelowymi są grupy A postaci $A = A_n \times (\mathbb{Z}^+)^k$, gdzie A_n jest grupą z twierdzenia 6.7 oraz $k, n \in \mathbb{N}_0$.*

Ponadto mamy stąd też następujący

Wniosek 6.21. *Każda skończenie generowana grupa abelowa jest sumą prostą pewnych swoich podgrup cyklicznych.*

Następne twierdzenie na algebrze I, ale teraz podamy jego inny dowód wykorzystujący poznane twierdzenia klasyfikacyjne.

Twierdzenie 6.22. *Każda skończona podgrupa grupy multiplikatywnej dowolnego ciała jest cykliczna.*

Dowód. Niech A będzie skończoną podgrupą grupy multiplikatywnej $K^\star$ ciała K. Jeśli $A = \{1\}$, to $A = \langle 1\rangle$, czyli grupa A jest cykliczna. Załóżmy dalej, że $|A| > 1$. Wtedy istnieją różne liczby pierwsze $p_1, \ldots, p_s$ oraz istnieją liczby naturalne $\alpha_1, \ldots, \alpha_s$ takie, że $|A| = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Z twierdzenia 6.7 wynika, że $A \cong A_{p_1,\sigma_1} \times \ldots \times A_{p_s,\sigma_s}$, gdzie $\sigma_i \in \Sigma_{\alpha_i}$, $i = 1, \ldots, s$. Jeśli dla pewnego i grupa A_{p_i,σ_i} nie jest cykliczna, to w grupie A istnieje podgrupa $B \cong \mathbb{Z}^+_{p_i} \times \mathbb{Z}^+_{p_i}$. Ale wtedy dla każdego $b \in B$ będziemy mieli, że $b^{p_i} = 1$ oraz $|B| = p_i^2$, więc wielomian $f = x^{p_i} - 1$ posiada w ciele K co najmniej $p_i^2 > p_i$ pierwiastków. Otrzymaliśmy zatem sprzeczność. Stąd każda z grup A_{p_i,α_i} jest cykliczna. Zatem ze stwierdzeń 5.10 i 5.2 grupa A jest cykliczna. □

Udowodnimy teraz twierdzenie odgrywające ważną rolę w teorii Galois.

Twierdzenie 6.23. *Każda skończona grupa rozwiązalna G posiada ciąg podgrup $G = G_0 \supseteq G_1 \supseteq \ldots \supseteq G_{r+1} = \{e\}$ taki, że $G_{i+1} \lhd G_i$ oraz grupa G_i/G_{i+1} jest cykliczna dla $i = 0, 1, \ldots, r$.*

Dowód. Niech A będzie skończoną grupą abelową. Wówczas z twierdzenia 6.3 istnieją w A cykliczne podgrupy $C_1, \ldots, C_{r+1}$ takie, że $A = C_1 \oplus \ldots \oplus C_{r+1}$. Niech $A_0 = C_1 \oplus \ldots \oplus C_{r+1}$, $A_1 = C_1 \oplus \ldots \oplus C_r, \ldots, A_r = C_1, A_{r+1} = \{e\}$. Wówczas $A_{i+1} \lhd A_i$ oraz grupa $A_i/A_{i+1} \cong C_{r+1-i}$ jest cykliczna dla $i = 0, 1, \ldots, r$. Zatem teza twierdzenia zachodzi dla dowolnej skończonej grupy abelowej.

Niech teraz G będzie nieabelową skończoną grupą rozwiązalną. Z twierdzenia 3.12 wynika, że w G istnieje skończony ciąg podgrup $G = G_0 \supseteq G_1 \supseteq G_2 \supseteq \ldots \supseteq G_{k+1} = \{e\}$ taki, że $G_{i+1} \lhd G_i$ oraz G_i/G_{i+1} jest skończoną grupą abelową dla każdego $i = 0, 1, \ldots, k-1$. Z opisu podgrup w grupie ilorazowej oraz z pierwszej części dowodu naszego twierdzenia mamy, że dla każdego $i = 0, 1, \ldots, k-1$ istnieją w G_i podgrupy $G_{i0} = G_i \supseteq G_{i1} \supseteq \ldots \supseteq G_{ik_i} = G_{i+1}$ takie, że $G_{i,j+1} \lhd G_{ij}$ oraz grupa $(G_{ij}/G_{i+1})/(G_{i,j+1}/G_{i+1})$ jest cykliczna dla wszystkich $j = 0, 1, \ldots, k_i - 1$. Ale na mocy III twierdzenia

o izomorfizmie $(G_{ij}/G_{i+1})/(G_{i,j+1}/G_{i+1}) \cong G_{ij}/G_{i,j+1}$ dla wszystkich $i = 0, 1, \ldots, k-1$, $j = 0, 1, \ldots, k_i - 1$, więc twierdzenie jest udowodnione. □

Rozdział 7

Wielomiany wielu zmiennych i pierścienie noetherowskie

7.1 Pierścienie wielomianów wielu zmiennych

Niech P będzie dowolnym pierścieniem (przemiennym z jedynką) i niech $x_1, x_2, \ldots$ będą zmiennymi. Określamy przez indukcję

$$P[x_1, \ldots, x_n, x_{n+1}] \stackrel{def}{=} (P[x_1, \ldots, x_n])[x_{n+1}] \text{ dla } n = 1, 2, \ldots$$

Otrzymujemy w ten sposób pierścień wielomianów n-zmiennych $P[x_1, \ldots, x_n]$ dla $n = 1, 2, \ldots$. Mamy stąd np., że $P[x, y] = (P[x])[y]$, więc każdy element $f \in P[x, y]$ może być zapisany w postaci $f = g_0 + g_1 y + \ldots + g_n y^n$ dla pewnego $n \in \mathbb{N}_0$ i dla pewnych wielomianów $g_0, g_1, \ldots, g_n \in P[x]$; zatem $f = \sum a_{ij} x^i y^j$ oraz suma ta jest skończona i $a_{ij} \in P$ dla wszystkich i, j. Wynika stąd, że $P[x, y] \cong (P[y])[x]$.

Rozumując analogicznie można wykazać przez prostą indukcję, że każdy niezerowy element $f \in P[x_1, \ldots, x_n]$ można jednoznacznie zapisać w postaci:

$$f = \sum a_{k_1 \ldots k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}, \tag{7.1}$$

gdzie $k_1, \ldots, k_n \in \mathbb{N}_0$ i $a_{k_1 \ldots k_n} \in P \setminus \{0\}$. **Stopniem** takiego f nazywamy maksymalną wartość $k_1 + \ldots + k_n$ i oznaczamy symbolem $st(f)$;

przyjmujemy też, że $st(0) = -\infty$.

Stwierdzenie 7.1. *Niech $\varphi\colon P \to A$ będzie homomorfizmem pierścieni oraz niech $a_1, a_2, \ldots, a_n \in A$. Wówczas istnieje dokładnie jeden homomorfizm pierścieni $\Phi\colon P[x_1, x_2, \ldots, x_n] \to A$ taki, że $\Phi(p) = \varphi(p)$ dla każdego $p \in P$ oraz $\Phi(x_i) = a_i$ dla każdego $i = 1, 2, \ldots, n$. Ponadto zachodzi wzór:*

$$\Phi\left(\sum a_{k_1\ldots k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}\right) = \sum \varphi(a_{k_1\ldots k_n}) \cdot a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}. \tag{7.2}$$

Dowód. Zauważmy, że jeżeli homomorfizm pierścieni $\Phi\colon P[x_1, x_2, \ldots, x_n] \to A$ jest taki, że $\Phi(p) = \varphi(p)$ dla każdego $p \in P$ oraz $\Phi(x_i) = a_i$ dla każdego $i = 1, 2, \ldots, n$, to jest spełniony wzór (7.2). Wobec tego pozostaje do wykazania, że przekształcenie Φ dane tym wzorem jest homomorfizmem pierścieni, bo $\Phi(p) = \varphi(p)$ dla każdego $p \in P$ oraz $\Phi(x_i) = a_i$ dla każdego $i = 1, 2, \ldots, n$.

Zastosujemy indukcję względem n. Dla $n = 1$ teza wynika z algebry I. Załóżmy, że $n \geqslant 2$ i teza zachodzi dla liczby $n - 1$. Wtedy istnieje homomorfizm pierścieni $F\colon P[x_1, \ldots, x_{n-1}] \to A$ taki, że $F(p) = \varphi(p)$ dla każdego $p \in P$ oraz $F(x_i) = a_i$ dla każdego $i = 1, \ldots, n-1$. Z algebry I istnieje homomorfizm pierścieni $\Phi\colon (P[x_1, \ldots, x_{n-1}])[x_n] \to A$ taki, że $\Phi(w) = F(w)$ dla każdego $w \in P[x_1, \ldots, x_{n-1}]$ oraz $\Phi(x_n) = a_n$. Ale $(P[x_1, \ldots, x_{n-1}])[x_n] = P[x_1, x_2, \ldots, x_n]$ i $\Phi(p) = p$ dla każdego $p \in P$ oraz $\Phi(x_i) = F(x_i) = a_i$ dla $i = 1, \ldots, n-1$, więc Φ spełnia wszystkie żądane warunki. □

Wartością wielomianu $f = \sum a_{k_1\ldots k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \in P[x_1, \ldots, x_n]$ w punkcie $t = (t_1, \ldots, t_n) \in P^n$ nazywamy element $f(t) \in P$ dany wzorem:

$$f(t) = \sum a_{k_1\ldots k_n} t_1^{k_1} \cdot \ldots \cdot t_n^{k_n}. \tag{7.3}$$

Ze stwierdzenia 7.1 otrzymujemy, że dla dowolnego $t \in P^n$ oraz dla dowolnych wielomianów $f, g \in P[x_1, \ldots, x_n]$ zachodzą wzory:

$$(f + g)(t) = f(t) + g(t) \text{ oraz } (fg)(t) = f(t) \cdot g(t), \tag{7.4}$$

gdyż przekształcenie $f \mapsto f(t)$ jest homomorfizmem pierścieni.

Grupę multiplikatywną $(P^*, \cdot, 1)$ pierścienia P będziemy oznaczali przez P^*. Przypomnijmy, że

$$P^* = \{a \in P : \text{istnieje } b \in P \text{ taki, że } a \cdot b = 1\}.$$

Z algebry I wiemy, że jeżeli P jest **dziedziną całkowitości** (tzn. $P \neq \{0\}$ oraz dla dowolnych $a, b \in P$ z tego, że $a \cdot b = 0$ wynika $a = 0$ lub $b = 0$), to $P[x]$ też jest dziedziną całkowitości oraz $(P[x])^* = P^*$. Stąd przez prostą indukcję uzyskujemy następujące

Twierdzenie 7.2. *Jeżeli P jest dziedziną całkowitości, to dla każdego naturalnego n pierścień $P[x_1, \ldots, x_n]$ też jest dziedziną całkowitości oraz $(P[x_1, \ldots, x_n])^* = P^*$.*

Przypomnijmy, że **ideałem** pierścienia P nazywamy taki niepusty podzbiór $I \subseteq P$, że

(i) $i - j \in I$ dla dowolnych $i, j \in I$ oraz

(ii) $a \cdot i \in I$ dla dowolnych $a \in P$, $i \in I$.

Piszemy wtedy $I \lhd P$.

Z określenia ideału pierścienia P wynika, że jest on zawsze podgrupą grupy addytywnej P^+ tego pierścienia.

Jeżeli I jest ideałem pierścienia P, to możemy utworzyć tzw. **pierścień ilorazowy** P/I. Przypomnijmy, że $P/I = \{a + I : a \in P\}$ oraz dla $a \in P$ zbiór $a + I = \{a + i : i \in I\}$ nazywamy **warstwą ideału** I o reprezentancie a. Dla dowolnych $a, b \in P$ mamy, że $a + I = b + I \iff a - b \in I$; ponadto $(a + I) + (b + I) \stackrel{def}{=} (a + b) + I$ oraz $(a + I) \cdot (b + I) \stackrel{def}{=} a \cdot b + I$.

Łatwo sprawdzić, że jeśli $a_1, \ldots, a_n \in P$, to

$$(a_1, \ldots, a_n) = \{a_1 b_1 + \ldots + a_n b_n : b_1, \ldots, b_n \in P\}$$

jest najmniejszym (w sensie inkluzji) ideałem pierścienia P zawierającym zbiór $\{a_1, \ldots, a_n\}$ i wówczas elementy $a_1, \ldots, a_n$ nazywamy jego **generatorami**. Ideał I pierścienia P nazywamy ideałem skończenie generowanym, jeżeli $I = (a_1, \ldots, a_n)$ dla pewnych $a_1, \ldots, a_n \in P$. Szczególnym przypadkiem ideału skończenie generowanego jest **ideał główny** $(a) = \{ax : x \in P\}$ o generatorze $a \in P$. Pierścienie,

w których każdy ideał jest główny nazywamy **pierścieniami ideałów głównych**. Z algebry I wiemy, że $\mathbb{Z}$ oraz $K[x]$ dla dowolnego ciała K są pierścieniami ideałów głównych.

Przykład 7.3. Załóżmy, że a jest niezerowym elementem nieodwracalnym dziedziny całkowitości P, czyli $a \neq 0$ oraz $ab \neq 1$ dla każdego $b \in P$. Pokażemy, że wtedy ideał $I = (a, x)$ pierścienia wielomianów $P[x]$ nie jest główny. Załóżmy, że tak nie jest. Wtedy istnieje wielomian $f \in P[x]$ taki, że $I = (f)$. Ale $a, x \in (f)$, więc istnieją $g, h \in P[x]$ takie, że $a = fg$ i $x = fh$. Ponadto P jest dziedziną całkowitości, więc $0 = st(a) = st(fg) = st(f) + st(g)$, skąd $st(f) = 0$, czyli $f \in P \setminus \{0\}$. Ale $1 = f(1)h(1) = f \cdot h(1)$, więc $1 \in (f)$, czyli $1 \in I$. Zatem istnieją $u, v \in P[x]$ takie, że $1 = au + xv$, skąd $1 = a \cdot u(0) + 0 \cdot v(0) = a \cdot u(0)$ i mamy sprzeczność.

W szczególności wynika stąd, że jeżeli P jest dziedziną całkowitości nie będącą ciałem, to $P[x]$ nie jest pierścieniem ideałów głównych, np. $\mathbb{Z}[x]$ nie jest pierścieniem ideałów głównych oraz dla dowolnego ciała K ideał (x, y) pierścienia $K[x, y]$ nie jest główny.

Innym ważnym rodzajem ideałów pierścienia są tzw. ideały pierwsze. Mianowicie, ideał I pierścienia P nazywamy **ideałem pierwszym**, jeśli

(i) $I \neq P$ oraz

(ii) dla dowolnych $a, b \in P$ z tego, że $a \cdot b \in I$ wynika $a \in I$ lub $b \in I$.

Powiemy, że ideał I pierścienia P jest **ideałem maksymalnym** pierścienia P, jeżeli

(i) $I \neq P$ oraz

(ii) dla dowolnego ideału J pierścienia P takiego, że $I \subseteq J$ jest $J = I$ lub $J = P$.

Z algebry I wiemy, że ideał I pierścienia P jest ideałem pierwszym (maksymalnym) pierścienia P wtedy i tylko wtedy, gdy pierścień ilorazowy P/I jest dziedziną całkowitości (ciałem).

7.2 Pierścienie noetherowskie

Twierdzenie 7.4. *Dla dowolnego pierścienia P następujące warunki są równoważne:*

(i) każdy ideał pierścienia P jest skończenie generowany;

(ii) każdy wstępujący ciąg ideałów pierścienia P stabilizuje się, tzn. jeśli $I_1 \subseteq I_2 \subseteq \ldots$ są ideałami pierścienia P, to istnieje indeks s taki, że $I_s = I_{s+1} = \ldots$;

(iii) w każdej niepustej rodzinie ideałów pierścienia P istnieje element maksymalny.

Dowód. (i)$\Rightarrow$ (ii). Niech $I_1 \subseteq I_2 \subseteq \ldots$ będzie dowolnym ciągiem wstępującym ideałów pierścienia P i niech $I = \bigcup_{n=1}^{\infty} I_n$. Wtedy $I_n \subseteq I$ dla każdego $n \in \mathbb{N}$, skąd $I \neq \emptyset$. Jeżeli $a \in P$, $i \in I$, to istnieje $n \in \mathbb{N}$ takie, że $i \in I_n$ i $I_n \lhd P$, więc $a \cdot i \in I_n$, czyli $a \cdot i \in I$. Jeżeli $i, j \in I$, to istnieją $n, m \in \mathbb{N}$ takie, że $i \in I_n$ oraz $j \in I_m$. Niech $k = \max\{n, m\}$. Wtedy $I_n \subseteq I_k$ oraz $I_m \subseteq I_k$, więc $i, j \in I_k$, więc $i - j \in I_k$, bo $I_k \lhd P$. Zatem $i - j \in I$. Stąd $I \lhd P$, więc z założenia istnieją $a_1, \ldots, a_n \in I$ takie, że $I = (a_1, \ldots, a_n)$. Ponadto istnieją indeksy $k_1, \ldots, k_n \in \mathbb{N}$ takie, że $a_i \in I_{k_i}$ dla $i = 1, \ldots, n$. Niech $s = \max\{k_1, \ldots, k_n\}$. Wtedy $a_1, \ldots, a_n \in I_s$, więc $I = (a_1, \ldots, a_n) \subseteq I_s \subseteq I_m \subseteq I$ dla wszystkich indeksów $m \geqslant s$, skąd $I_s = I_m$ dla $m \geqslant s$. Zatem ciąg $I_1 \subseteq I_2 \subseteq \ldots$ stabilizuje się.

(ii)$\Rightarrow$(iii). Załóżmy, że w pewnej niepustej rodzinie $\mathcal{R}$ ideałów pierścienia P nie istnieje element maksymalny. Oznacza to, że dla każdego $I \in \mathcal{R}$ istnieje $J \in \mathcal{R}$ takie, że $I \subsetneq J$. Ponieważ rodzina $\mathcal{R}$ jest niepusta, więc przez prostą indukcję uzyskujemy stąd istnienie wstępującego ciągu $I_1 \subsetneq I_2 \subsetneq \ldots$ ideałów rodziny $\mathcal{R}$, który nie stabilizuje się. Otrzymaliśmy zatem sprzeczność z naszym założeniem.

(iii)$\Rightarrow$(i). Niech I będzie dowolnym ideałem pierścienia P. Oznaczmy przez $\mathcal{S}$ rodzinę wszystkich skończenie generowanych ideałów pierścienia P zawartych w ideale I. Ponieważ $\{0\} \in \mathcal{S}$, skąd $\mathcal{S} \neq \emptyset$, więc w rodzinie $\mathcal{S}$ istnieje element maksymalny M. Jeśli $M \neq I$, to istnieje $a \in I \setminus M$ i wtedy $M \subsetneq M + (a) \subseteq I$. Ale $M = (a_1, \ldots, a_n)$ dla pewnych $a_1, \ldots, a_n \in I$, więc $M + (a) = (a_1, \ldots, a_n, a)$, skąd $M + (a) \in \mathcal{S}$

i mamy sprzeczność z maksymalnością M. Zatem $M = I$ i ideał I jest skończenie generowany. □

Definicja 7.5. Każdy pierścień P spełniający którykolwiek z równoważnych warunków (i)-(iii) twierdzenia 7.4 nazywamy **pierścieniem noetherowskim**.

Twierdzenie 7.6. *Obraz homomorficzny pierścienia noetherowskiego jest pierścieniem noetherowskim.*

Dowód. Niech pierścień A będzie obrazem homomorficznym pierścienia noetherowskiego P. Wtedy istnieje homomorfizm $f\colon P \to A$ pierścienia P na pierścień A. Niech J będzie dowolnym ideałem pierścienia A. Wtedy $I = f^{-1}(J) \lhd P$. Ale f jest 'na', więc $f(I) = J$. Ponadto pierścień P jest noetherowski, więc istnieją $a_1, \ldots, a_n \in I$ takie, że $I = (a_1, \ldots, a_n)$. Łatwo zauważyć, że $f((a_1, \ldots, a_n)) = (f(a_1), \ldots, f(a_n))$. Zatem $J = (f(a_1), \ldots, f(a_n))$ i pierścień A jest noetherowski. □

Wniosek 7.7. *Niech P będzie pierścieniem. Jeżeli pierścień wielomianów $P[x]$ jest noetherowski, to pierścień P też jest noetherowski.*

Dowód. Z algebry I wiemy, że przekształcenie $f\colon P[x] \to P$ dane wzorem $f(w) = w(0)$ dla $w \in P[x]$ jest homomorfizmem pierścienia $P[x]$ na pierścień P. Zatem na mocy twierdzenia 7.6 pierścień P jest noetherowski. □

Przykład 7.8. Podpierścień pierścienia noetherowskiego nie musi być pierścieniem noetherowskim. Mianowicie pierścień $P = \mathbb{Q}[x]$ jest noetherowski, bo każdy jego ideał jest generowany przez jeden element. Łatwo zauważyć, że $A = \mathbb{Z} + (x) = \{f \in P : f(0) \in \mathbb{Z}\}$ jest podpierścieniem pierścienia P. Jeśli S jest podgrupą grupy $\mathbb{Q}^+$, to $I(S) = Sx + (x^2) = \{sx + x^2 f : f \in P, s \in S\}$ jest ideałem pierścienia A. Jeśli S_1 i S_2 są podgrupami grupy $\mathbb{Q}^+$ takimi, że $S_1 \subsetneqq S_2$, to $I(S_1) \subsetneqq I(S_2)$, bo istnieje $s \in S_2 \setminus S_1$ i wtedy $sx \in I(S_2) \setminus I(S_1)$. W celu wykazania tego, że pierścień A nie jest noetherowski wystarczy zatem wskazać wstępujący ciąg $S_1 \subsetneqq S_2 \subsetneqq \ldots$ podgrup grupy $\mathbb{Q}^+$. Można to zrobić na wiele sposobów. My wybierzemy jeden z najprostrzych. Mianowicie niech $S_i = \{\frac{k}{2^i} : k \in \mathbb{Z}\}$ dla $i \in \mathbb{N}$. Wówczas S_i jest podgrupą

grupy $\mathbb{Q}^+$, $S_i \subseteq S_{i+1}$ oraz $\frac{1}{2^{i+1}} \in S_{i+1} \setminus S_i$ dla każdego $i \in \mathbb{N}$. Zatem pierścień A nie jest noetherowski, chociaż jest on podpierścieniem pierścienia noetherowskiego P.

7.3 Twierdzenie Hilberta o bazie

Twierdzenie 7.9 (Hilberta o bazie)**.** *Jeżeli pierścień P jest noetherowski, to pierścień $P[x]$ też jest noetherowski.*

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje pierścień noetherowski P taki, że pierścień $P[x]$ nie jest noetherowski. Zatem istnieje ideał J pierścienia $P[x]$, który nie jest skończenie generowany. W szczególności $J \neq \{0\}$, bo $\{0\} = (0)$. Wynika stąd, że w zbiorze $J_1 = J \setminus \{0\}$ istnieje wielomian niezerowy f_1 minimalnego stopnia $k_1 \in \mathbb{N}_0$. Ponieważ ideał J nie jest skończenie generowany, więc $(f_1) \subsetneqq J$ oraz w zbiorze $J_2 = J \setminus (f_1)$ istnieje wielomian niezerowy f_2 minimalnego stopnia k_2. Ponieważ $J_2 \subseteq J_1$, więc $k_2 \geqslant k_1$. Jeśli wybrane już zostały wielomiany $f_1, f_2, \ldots, f_n$ takie, że f_i jest wielomianem minimalnego stopnia w zbiorze $J_i = J \setminus (f_1, \ldots, f_{i-1})$ dla $i = 1, \ldots, n$, to $J_n \subseteq J_{n-1} \subseteq \ldots \subseteq J_2 \subseteq J_1$, skąd $k_n \geqslant k_{n-1} \geqslant \ldots \geqslant k_2 \geqslant k_1$, gdzie $k_i = st(f_i)$ dla $i = 2, \ldots, n$. Ponadto $(f_1, \ldots, f_n) \subsetneqq J$, więc istnieje wielomian niezerowy $f_{n+1} \in J_{n+1} = J \setminus (f_1, \ldots, f_n)$ minimalnego stopnia k_{n+1}. Ponadto $J_{n+1} \subseteq J_n$, więc $k_{n+1} \geqslant k_n$. Przez indukcję skonstruowaliśmy zatem ciąg (f_n) niezerowych wielomianów stopni $k_1 \leqslant k_2 \leqslant \ldots$ o najstarszych współczynnikach $a_1, a_2, \ldots$ i takich, że f_1 jest wielomianem minimalnego stopnia w zbiorze $J_1 = J \setminus \{0\}$ oraz f_n jest wielomianem minimalnego stopnia w zbiorze $J_n = J \setminus (f_1, \ldots, f_{n-1})$ dla każdego $n = 2, 3, \ldots$.

W pierścieniu noetherowskim P mamy zatem wstępujący ciąg ideałów:

$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots.$$

Zatem istnieje indeks s taki, że $(a_1, \ldots, a_s) = (a_1, \ldots, a_s, a_{s+1}) = \ldots$. W szczególności $a_{s+1} \in (a_1, \ldots, a_s)$. Zatem istnieją $b_1, \ldots, b_s \in P$ takie, że

$$a_{s+1} = a_1 b_1 + \ldots + a_s b_s.$$

Ale $k_{s+1} \geqslant k_i$ dla $i = 1, \ldots, s$, więc $k_{s+1} - k_i \in \mathbb{N}_0$ dla $i = 1, \ldots, s$. Stąd $x^{k_{s+1}-k_i} \in P[x]$ dla $i = 1, \ldots, s$. Niech

$$f = f_{s+1} - (b_1 x^{k_{s+1}-k_1} f_1 + \ldots + b_s x^{k_{s+1}-k_s} f_s).$$

Wtedy $f \in J$ oraz $f \notin (f_1, \ldots, f_s)$, bo inaczej $f_{s+1} \in (f_1, \ldots, f_s)$, wbrew naszej konstrukcji wielomianu f_{s+1}. Stąd $f \in J_{s+1}$ i $st(f) \geqslant st(f_{s+1}) = k_{s+1}$. Ale wielomiany $x^{k_{s+1}-k_1} f_1, \ldots, x^{k_{s+1}-k_s} f_s$ są stopnia k_{s+1}, więc najstarszy współczynnik wielomianu $g = b_1 x^{k_{s+1}-k_1} f_1 + \ldots + b_s x^{k_{s+1}-k_s} f_s$ wynosi $b_1 a_1 + \ldots + b_s a_s = a_{s+1}$, czyli $st(f) < k_{s+1}$ i mamy sprzeczność. □

Wniosek 7.10. *Jeżeli pierścień P jest noetherowski, to dla dowolnego $n \in \mathbb{N}$ pierścień $P[x_1, \ldots, x_n]$ też jest noetherowski. W szczególności pierścień $\mathbb{Z}[x_1, \ldots, x_n]$ jest noetherowski oraz dla dowolnego ciała K pierścień $K[x_1, \ldots, x_n]$ jest noetherowski.*

Dowód. Indukcja względem n. Dla $n = 1$ teza wynika od razu z twierdzenia Hilberta o bazie. Załóżmy, że teza zachodzi dla pewnego naturalnego n. Wtedy $P[x_1, \ldots, x_n, x_{n+1}] = (P[x_1, \ldots, x_n])[x_{n+1}]$ oraz z założenia indukcyjnego pierścień $P[x_1, \ldots, x_n]$ jest noetherowski, więc z twierdzenia Hilberta o bazie pierścień $(P[x_1, \ldots, x_n])[x_{n+1}]$ też jest noetherowski, czyli pierścień $P[x_1, \ldots, x_n, x_{n+1}]$ jest noetherowski. □

Twierdzenie 7.11. *Każdy pierścień skończenie generowany jest noetherowski.*

Dowód. Niech P będzie pierścieniem skończenie generowanym. Wtedy istnieją elementy $a_1, \ldots, a_n \in P$ takie, że każdy element pierścienia P jest skończoną sumą elementów postaci $(k \cdot 1) \cdot a_1^{k_1} \cdot a_2^{k_2} \cdot \ldots \cdot a_n^{k_n}$ dla pewnego $k \in \mathbb{Z}$ i dla pewnych $k_1, k_2, \ldots, k_n \in \mathbb{N}_0$. Przekształcenie $\varphi\colon \mathbb{Z} \to P$ dane wzorem $\varphi(k) = k \cdot 1$ jest homomorfizmem pierścieni. Zatem na mocy stwierdzenia 7.1 istnieje homomorfizm pierścieni $\Phi\colon \mathbb{Z}[x_1, \ldots, x_n] \to P$ taki, że $\Phi(k) = k \cdot 1$ dla $k \in \mathbb{Z}$ oraz $\Phi(x_i) = a_i$ dla $i = 1, 2, \ldots, n$. Wobec tego Φ jest "na" i z wniosku 7.10 oraz z twierdzenia 7.6 pierścień P jest noetherowski. □

Rozdział 8

Pierścienie szeregów formalnych

8.1 Konstrukcja i podstawowe własności pierścienia szeregów formalnych

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

$$f = (f_0, f_1, f_2, \ldots) \tag{8.1}$$

takich, że $f_i \in P$ dla wszystkich $i = 0, 1, \ldots$.

Elementy zbioru $P[[x]]$ nazywamy **szeregami formalnymi** zmiennej x o współczynnikach z pierścienia P. Przyjmujemy umowę, że jeśli szereg nazywa się g, to $g = (g_0, g_1, g_2, \ldots)$, czyli $g_0, g_1, g_2, \ldots$ są jego kolejnymi współczynnikami. Przy tych oznaczeniach dla szeregów $f, g \in P[[x]]$ mamy, że:

$$f = g \iff f_i = g_i \text{ dla każdego } i = 0, 1, 2, \ldots. \tag{8.2}$$

Szereg $0 = (0, 0, 0, \ldots)$ nazywamy **zerowym**, a szereg $1 = (1, 0, 0, \ldots)$ nazywamy **jedynkowym**. Jeżeli $0 = f_1 = f_2 = \ldots$, to szereg f nazywamy **stałym**. Jeżeli $f \neq 0$, to istnieje najmniejsze n takie, że $f_n \neq 0$ i wówczas n nazywamy **stopniem szeregu** f i piszemy

$st(f) = n$, zaś f_n nazywamy **najmłodszym współczynnikiem** tego szeregu. Ponadto przyjmujemy, że $st(0) = \infty$ oraz dla $n \in \mathbb{N}_0$: $\infty > n$, $\infty + n = \infty + \infty = \infty$.

Sumą szeregów $f, g \in P[[x]]$ nazywamy szereg:

$$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \ldots). \tag{8.3}$$

łatwo zauważyć, że dla dowolnych szeregów $f, g \in P[[x]]$:

$$st(f + g) \geqslant \min\{st(f), st(g)\}. \tag{8.4}$$

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

Z określenia dodawania szeregów łatwo wynika, że system algebraiczny $(P[[x]], +, 0)$ jest grupą abelową, przy czym **szeregiem przeciwnym** do szeregu f jest szereg $-f = (-f_0, -f_1, -f_2, \ldots)$.

Iloczynem szeregów $f, g \in P[[x]]$ nazywamy szereg:

$$f \cdot g = (f_0 g_0, f_0 g_1 + f_1 g_0, f_0 g_2 + f_1 g_1 + f_2 g_0, \ldots). \tag{8.5}$$

Zatem dla każdego $n \in \mathbb{N}_0$:

$$(f \cdot g)_n = \sum_{i=0}^{n} f_i g_{n-i} = \sum_{i+j=n} f_i g_j. \tag{8.6}$$

Jeżeli $f_i = 0$ dla $i = 1, 2, \ldots$, to ze wzoru (8.6) wynika, że:

$$(f_0, 0, 0, \ldots) \cdot (g_0, g_1, g_2, \ldots) = (f_0 g_0, f_0 g_1, f_0 g_2, \ldots). \tag{8.7}$$

Jeżeli zaś $f_1 = 1$ oraz $f_i = 0$ dla $i = 0, 2, 3, \ldots$, to ze wzoru (8.6) wynika, że:

$$(0, 1, 0, 0, \ldots) \cdot (g_0, g_1, g_2, \ldots) = (0, g_0, g_1, g_2, \ldots). \tag{8.8}$$

Niech teraz $f, g \in P[[x]] \setminus \{0\}$ i $n = st(f)$ oraz $m = st(g)$. Wtedy $(f \cdot g)_k = 0$ dla wszystkich $k < n + m$. Rzeczywiście, $(f \cdot g)_k = \sum_{i+j=k} f_i g_j$ oraz $f_i = 0$ dla $i < n$, zaś dla $i \geqslant n$ jest $j < m$, więc $g_j = 0$. Stąd i z (8.7) mamy, że dla dowolnych szeregów $f, g \in P[[x]]$:

$$st(f \cdot g) \geqslant st(f) + st(g). \tag{8.9}$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Stwierdzenie 8.1. *Niech $f, g \in P[[x]] \setminus \{0\}$ będą takie, że najmłodszy współczynnik szeregu f lub najmłodszy współczynnik szeregu g jest elementem regularnym pierścienia P. Wtedy $st(f \cdot g) = st(f) + st(g)$ oraz najmłodszy współczynnik szeregu $f \cdot g$ jest iloczynem najmłodszych współczynników szeregów f i g.*

Dowód. Oznaczmy $n = st(f)$, $m = st(g)$. Weźmy dowolne $i, j \in \mathbb{N}_0$ takie, że $i + j = n + m$. Jeśli $i < n$, to $f_i = 0$. Jeśli $i > n$, to $j < m$, skąd $g_j = 0$. Zatem ze wzoru (8.6) mamy, że $(f \cdot g)_{n+m} = f_n g_m \neq 0$, bo $f_n \neq 0$, $g_m \neq 0$ oraz f_n lub g_m jest elementem regularnym. Stąd ze wzoru (8.9) wynika teza naszego stwierdzenia. □

Wniosek 8.2. *Jeżeli P jest dziedziną całkowitości, to dla dowolnych $f, g \in P[[x]]$*

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

Ze wzorów (8.5) i (8.6) wynika od razu, że mnożenie szeregów jest przemienne. Natomiast ze wzoru (8.7) wynika od razu, że $1 = (1, 0, 0, \ldots)$ jest elementem neutralnym mnożenia szeregów.

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

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

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

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

Ponadto $((f \cdot g) \cdot h)_n = \sum_{i+j=n} (f \cdot g)_i h_j = \sum_{i+j=n} \sum_{s+t=i} (f_s g_t) h_j =$

$\sum_{s+t+j=n} (f_s g_t) h_j$ oraz $(f \cdot (g \cdot h))_n = \sum_{s+k=n} f_s (g \cdot h)_k = \sum_{s+k=n} \sum_{t+j=k} f_s (g_t h_j)$

$= \sum_{s+t+j=n} f_s (g_t h_j)$, więc $f \cdot (g \cdot h) = (f \cdot g) \cdot h$. W ten sposob udowodniliśmy następujące

Twierdzenie 8.3. *Dla dowolnego pierścienia P system algebraiczny $(P[[x]], +, \cdot, 0, 1)$ tworzy pierścień.*

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

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

Ze wzorów (8.3) i (8.7) wynika, że przekształcenie $\varphi\colon P \to P[[x]]$ dane wzorem:

$$\varphi(a) = (a, 0, 0, \ldots) \tag{8.10}$$

jest różnowartościowym homomorfizmem pierścieni. Z tego powodu można dokonać utożsamienia:

$$(a, 0, 0, \ldots) \equiv a \text{ dla } a \in P. \tag{8.11}$$

Przy takim utożsamieniu P jest podpierścieniem pierścienia $P[[x]]$, a nawet pierścień wielomianów $P[x]$ jest podpierścieniem pierścienia $P[[x]]$.

Wprowadźmy teraz oznaczenie:

$$x = (0, 1, 0, 0, \ldots). \tag{8.12}$$

Wówczas ze wzoru (8.8) przez prostą indukcję uzyskamy, że:

$$x^n = (0, 0, \ldots, 0, \overset{n}{1}, 0, \ldots) \text{ dla } n = 0, 1, \ldots. \tag{8.13}$$

Niech $f \in P[[x]]$. Ze wzorów (8.7) i (8.13) mamy, że $(f_k, 0, 0, \ldots) \cdot x^k = (0, \ldots, 0, \overset{k}{f_k}, 0, \ldots)$ dla $k = 1, 2, \ldots$, więc $f = (f_0, 0, 0, \ldots) + (0, f_1, 0, \ldots) + \ldots \equiv f_0 + f_1 x + f_2 x^2 + \ldots$. Zatem dla dowolnego szeregu $f \in P[[x]]$ mamy utożsamienie:

$$f \equiv \sum_{i=0}^{\infty} f_i x^i. \tag{8.14}$$

Otrzymujemy w ten sposób naturalną notację dla szeregów z pierścienia $P[[x]]$.

Z wniosku 8.2 i tego, że pierścień P jest podpierścieniem pierścienia $P[[x]]$ wynika od razu następujące

Stwierdzenie 8.4. *Pierścień $P[[x]]$ jest dziedziną całkowitości wtedy i tylko wtedy, gdy pierścień P jest dziedziną całkowitości.*

Stwierdzenie 8.5. *Niech P będzie dowolnym niezerowym pierścieniem. Szereg $f \in P[[x]]$ jest odwracalny wtedy i tylko wtedy, gdy f_0 jest elementem odwracalnym pierścienia P.*

Dowód. Załóżmy, że szereg f jest odwracalny. Wtedy istnieje szereg $g \in P[[x]]$ taki, że $f \cdot g = 1$. Stąd w szczególności $f_0 \cdot g_0 = 1$, czyli $f_0 \in P^*$.

Na odwrót, załóżmy, że $f_0 \in P^*$. Określamy rekurencyjnie ciąg $(g_0, g_1, \ldots)$ przyjmując, że $g_0 = f_0^{-1}$ oraz $g_n = f_0^{-1} \cdot (-f_1 g_{n-1} - \ldots - f_n g_0)$ dla wszystkich $n = 1, 2, \ldots$. Wówczas $f_0 g_n + f_1 g_{n-1} + \ldots + f_n g_0 = 0$ dla $n = 1, 2, \ldots$ oraz $g = (g_0, g_1, \ldots) \in P[[x]]$. Zatem $f \cdot g = (f_0 g_0, 0, 0, \ldots) = 1$, czyli szereg f jest odwracalny. □

Stwierdzenie 8.6. *Dla dowolnego ciała K pierścień $K[[x]]$ jest dziedziną ideałów głównych i jedynymi jego ideałami są:* (0) *oraz ideały postaci (x^k) dla $k = 0, 1, \ldots$.*

Dowód. Ze stwierdzenia 8.4 pierścień $K[[x]]$ jest dziedziną całkowitości. Niech I będzie ideałem w $K[[x]]$ różnym od (0). Wtedy I zawiera niezerowy szereg. Zauważmy, że jeżeli $f = \sum_{i=k}^{\infty} f_i x^i \in I$ oraz $f_k \neq 0$, to $f = x^k \cdot \sum_{i=k}^{\infty} f_i x^{i-k} = x^k \cdot \sum_{j=0}^{\infty} f_{j+k} x^j$. Ponadto ze stwierdzenia 8.5 szereg $g = \sum_{j=0}^{\infty} f_{j+k} x^j$ jest odwracalny, gdyż $f_k \neq 0$ i K jest ciałem. Stąd $x^k = (x^k \cdot g) \cdot g^{-1} \in I$, a więc $(x^k) \subseteq I$.

Z zasady minimum istnieje najmniejsza nieujemna liczba całkowita m taka, że $x^m \in I$. Wtedy $(x^m) \subseteq I$. Weźmy dowolne $h \in I$. Jeśli $h = 0$, to $h \in (x^m)$. Jeśli zaś $h \neq 0$, to z pierwszej części dowodu istnieją nieujemna liczba całkowita k oraz szereg odwracalny $w \in K[[x]]$ takie, że $h = x^k \cdot w$ oraz $x^k \in I$. Z minimalności m mamy więc, że $k \geqslant m$, skąd $x^{k-m} \in K[[x]]$. Ponadto $h = x^m \cdot (x^{k-m} \cdot w)$, czyli $h \in (x^m)$. Oznacza to, że $I = (x^m)$. □

8.2 Twierdzenie Hilberta o bazie dla szeregów formalnych

Niech $h_i = \sum_{i=0}^{\infty} h_{ij}x^i \in P[[x]]$ dla $i = 0, 1, \ldots$ będą takimi szeregami, że dla każdego $j = 0, 1, \ldots$: $h_{ij} = 0$ dla prawie wszystkich i. Wówczas suma $\sum_{i=0}^{\infty} h_{ij}$ ma sens, gdyż jedynie skończona liczba jej składników jest różna od zera. Określamy:

$$\sum_{i=0}^{\infty} h_i \stackrel{def}{=} \sum_{j=0}^{\infty} \left(\sum_{i=0}^{\infty} h_{ij} \right) x^j. \tag{8.15}$$

Lemat 8.7. *Niech $g \in P[[x]]$ oraz $h_i = \sum_{i=0}^{\infty} h_{ij}x^i \in P[[x]]$ dla $i = 0, 1, \ldots$ będą takimi szeregami, że $\operatorname{st}\left(g - \sum_{i=0}^{p} h_i\right) > n+p$ dla wszystkich $p = 0, 1, \ldots$. Wówczas $g = \sum_{i=0}^{\infty} h_i$.*

Dowód. Z założenia wynika, że dla wszystkich $p = 0, 1, \ldots$ oraz $j = 0, 1, \ldots, n + p$: $\left(g - \sum_{i=0}^{p} h_i\right)_j = 0$, czyli $g_j = \sum_{i=0}^{p} h_{ij}$. W szczególności, $g_j = \sum_{i=0}^{p+1} h_{ij}$, co daje, że $h_{p+1\,j} = 0$. Jeżeli zaś dla pewnego $s \in \mathbb{N}$ jest $h_{p+1\,j} = \ldots = h_{p+s\,j} = 0$, to $g_j = \sum_{i=0}^{p+s+1} h_{ij} = \sum_{i=0}^{p} h_{ij} + h_{p+s+1\,j}$ oraz $g_j = \sum_{i=0}^{p} h_{ij}$, skąd $h_{p+s+1\,j} = 0$. Zatem $0 = h_{p+1\,j} = h_{p+2\,j} = \ldots$ oraz $g_j = \sum_{i=0}^{\infty} h_{ij}$. Wobec wzoru (8.15) oznacza to, że $g = \sum_{i=0}^{\infty} h_i$. □

Twierdzenie 8.8. *Jeżeli pierścień P jest noetherowski, to pierścień $P[[x]]$ też jest noetherowski.*

Dowód. Niech $I \lhd P[[x]]$. Jeżeli $I = \{0\}$, to $I = (0)$. Niech dalej $I \neq \{0\}$. Udowodnimy najpierw, że istnieją szeregi niezerowe $f_1, \ldots, f_s \in I$ o najmłodszych współczynnikach $a_1, \ldots, a_s$ odpowiednio i takie, że $a_{i+1} \notin (a_1, \ldots, a_i)$ dla $i = 1, \ldots, s-1$ oraz f_1 jest szeregiem minimalnego stopnia wśród wszystkich szeregów z ideału I, zaś dla $i = 1, \ldots, s-1$, f_{i+1} jest szeregiem minimalnego stopnia wśród wszystkich szeregów z ideału I, których najmłodszy współczynnik $a \notin (a_1, \ldots, a_i)$, przy czym najmłodszy współczynnik każdego szeregu niezerowego $f \in I$ należy do ideału $(a_1, \ldots, a_s)$ pierścienia P.

Mianowicie oznaczmy przez f_1 szereg minimalnego stopnia wśród wszystkich niezerowych szeregów z ideału I. Niech a_1 będzie najmłodszym współczynnikiem szeregu f_1. Jeżeli najmłodszy współczynnik każdego niezerowego szeregu $f \in I$ należy do ideału (a_1), to $s = 1$ i konstrukcję kończymy. W przeciwnym przypadku istnieje szereg $f_2 \in I$ minimalnego stopnia, którego najmłodszy współczynnik $a_2 \notin (a_1)$. Jeżeli dla pewnego $i \in \mathbb{N}$ szeregi $f_1, \ldots, f_i$ są już skonstruowane i najmłodszy współczynnik każdego niezerowego szeregu $f \in I$ należy do ideału $(a_1, \ldots, a_i)$, to $s = i$ i konstrukcję kończymy. W przeciwnym przypadku istnieje szereg $f_{i+1} \in I$ minimalnego stopnia, którego najmłodszy współczynnik $a_{i+1} \notin (a_1, \ldots, a_i)$. W pierścieniu noetherowskim P otrzymujemy zatem ściśle rosnący ciąg ideałów: $(a_1) \subset (a_1, a_2) \subset \ldots \subset (a_1, \ldots, a_{i+1})$. Oznacza to, że istnieje $s \in \mathbb{N}$ o tej własności, że najmłodszy współczynnik każdego szeregu niezerowego $f \in I$ należy do ideału $(a_1, \ldots, a_s)$ pierścienia P.

Oznaczmy $n_i = st(f_i)$ dla $i = 1, \ldots, s$. Z określenia szeregów $f_1, \ldots, f_s$ wynika, że $n_1 \leqslant n_2 \leqslant \ldots \leqslant n_s$. Udowodnimy, że $I = (f_1, \ldots, f_s)$. Ponieważ $f_1, \ldots, f_s \in I$, więc $(f_1, \ldots, f_s) \subseteq I$. Ponieważ $0 \in (f_1, \ldots, f_s)$, więc wystarczy wykazać, że każdy niezerowy szereg $g \in I$ stopnia n o najmłodszym współczynniku a należy do ideału $(f_1, \ldots, f_s)$. Możliwe są dwa przypadki:

1) $n \geqslant n_s$. Wtedy istnieją $b_{1,0}, \ldots, b_{s,0} \in P$ takie, że $a = \sum_{i=1}^{s} a_i b_{i,0}$. Ponadto $n \geqslant n_i$ dla $i = 1, \ldots, s$, więc $x^{n-n_i} \in P[[x]]$ dla $i = 1, \ldots, s$, skąd $h_0 = \sum_{i=1}^{s} b_{i,0} x^{n-n_i} f_i \in (f_1, \ldots, f_s)$ oraz najmłodszym współczynni-

kiem szeregu h_0 jest a, więc $st(g-h_0) > n$. Jeżeli dla pewnego $p \in \mathbb{N}_0$ mamy już skonstruowane szeregi $h_0, \ldots, h_p \in (f_1, \ldots, f_s)$ o tej własności, że dla każdego $q = 0, \ldots, p$, $st(g - \sum_{i=0}^{q} h_i) > n+q$ oraz $g - \sum_{i=0}^{p} h_i = cx^{n+p+1} + \ldots$, to $c \in (a_1, \ldots, a_s)$, więc istnieją $b_{1,p+1}, \ldots, b_{s,p+1} \in P$ takie, że $c = \sum_{i=1}^{s} a_i b_{i,p+1}$ i niech $h_{p+1} = \sum_{i=1}^{s} b_{i,p+1} x^{n+p+1-n_i} f_i$. Wtedy $h_{p+1} \in (f_1, \ldots, f_s)$, zatem $h_{p+1} = cx^{n+p+1} + \ldots$ oraz $st(g - \sum_{i=1}^{p+1} h_i) > n+p+1$. Z lematu 8.7 mamy zatem, że $g = \sum_{j=0}^{\infty} h_j$. Ponadto $\sum_{j=0}^{\infty} h_j = \sum_{j=0}^{\infty} \sum_{i=1}^{s} b_{i,j} x^{n+j-n_i} f_i \sum_{i=1}^{s} f_i \left(\sum_{j=0}^{\infty} b_{i,j} x^{n+j-n_i} \right)$, więc $g \in (f_1, \ldots, f_s)$.

2) $n < n_s$. Wówczas istnieje minimalne $r \leqslant s$, że $a \in (a_1, \ldots, a_r)$. Z określenia f_i wynika, że $n \geqslant n_r$. Stąd istnieją elementy $c_{1,0}, \ldots, c_{r,0} \in P$ takie, że $a = \sum_{i=1}^{r} a_i c_{i,0}$. Niech $u_0 = \sum_{i=1}^{r} c_{i,0} x^{n-n_i} f_i$. Wtedy $st(g-u_0) > n$. Powtarzając najwyżej $n_s - n$ razy to postępowanie otrzymamy szereg stopnia $\geqslant n_s$, a więc sprowadziliśmy problem do przypadku 1). □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Rozdział 9

Zbiory algebraiczne

9.1 Radykał ideału

Definicja 9.1. Radykałem ideału I pierścienia P nazywamy zbiór

$$rad(I) = \{a \in P : a^n \in I \text{ dla pewnego } n \in \mathbb{N}\}.$$

Stwierdzenie 9.2. *Dla dowolnego ideału I pierścienia P mamy $rad(I) \lhd P$ oraz $I \subseteq rad(I)$.*

Dowód. Dla $a \in I$ jest $a^1 = a \in I$, więc $I \subseteq rad(I)$; w szczególności $rad(I) \neq \emptyset$. Jeżeli $a, b \in rad(I)$, $x \in P$, to istnieją $m, n \in \mathbb{N}$ takie, że $a^n, b^m \in I$. Stąd $(ax)^n = a^n \cdot x^n \in I$, więc $ax \in rad(I)$. Ponadto $(a-b)^{n+m-1} = \sum_{k=0}^{n+m-1} (-1)^k \binom{n+m-1}{k} a^{n+m-1-k} b^k$. Jeżeli $k \geqslant m$, to $b^k = b^m \cdot b^{k-m} \in I$, skąd $(-1)^k \binom{n+m-1}{k} a^{n+m-1-k} b^k \in I$. Natomiast dla $k < m$, $k \leqslant m-1$, więc $-k \geqslant -m+1$, skąd $n+m-1-k \geqslant n$, a zatem $a^{n+m-1-k} = a^n \cdot a^{m-1-k} \in I$ oraz $(-1)^k \binom{n+m-1}{k} a^{n+m-1-k} b^k \in I$. Stąd $(a-b)^{n+m-1} \in I$, czyli $a - b \in rad(I)$ i wobec tego $rad(I) \lhd P$. □

Stwierdzenie 9.3. *Dla dowolnych ideałów I, J pierścienia P:*
(i) jeśli $I \subseteq J$, to $rad(I) \subseteq rad(J)$,
(ii) $rad(rad(I)) = rad(I)$.

Dowód. (i). Weźmy dowolne $a \in rad(I)$. Wtedy istnieje $n \in \mathbb{N}$ takie, że $a^n \in I$. Ale $I \subseteq J$, więc $a^n \in J$, skąd $a \in rad(J)$. Zatem $rad(I) \subseteq rad(J)$.

(ii). Ze stwierdzenia 9.2, $I \subseteq rad(I)$, więc z (i) wynika, że $rad(I) \subseteq rad(rad(I))$. Weźmy dowolne $a \in rad(rad(I))$. Wtedy istnieje $n \in \mathbb{N}$ takie, że $a^n \in rad(I)$. Stąd istnieje $m \in \mathbb{N}$, dla którego $(a^n)^m \in I$. Zatem $a^{nm} \in I$, skąd $a \in rad(I)$, a więc $rad(rad(I)) \subseteq rad(I)$ i ostatecznie $rad(rad(I)) = rad(I)$. □

Stwierdzenie 9.4. *Dla dowolnych ideałów $I_1, \ldots, I_n$ pierścienia P:*

$$rad(I_1 \ldots I_n) = rad(I_1 \cap \ldots \cap I_n) = rad(I_1) \cap \ldots \cap rad(I_n).$$

Dowód. Ponieważ $I_1 \ldots I_n \subseteq I_1 \cap \ldots \cap I_n$, więc ze stwierdzenia 9.3 (i), $rad(I_1 \ldots I_n) \subseteq rad(I_1 \cap \ldots \cap I_n)$. Ponadto dla wszystkich $k = 1, \ldots, n$: $I_1 \cap \ldots \cap I_n \subseteq I_k$, więc ze stwierdzenia 9.3 (i), $rad(I_1 \cap \ldots \cap I_n) \subseteq rad(I_k)$, skąd $rad(I_1 \ldots I_n) \subseteq rad(I_1) \cap \ldots \cap rad(I_n)$. Weźmy dowolne $a \in rad(I_1) \cap \ldots \cap rad(I_n)$. Wtedy $a \in rad(I_k)$ dla wszystkich $k = 1, \ldots, n$. Zatem istnieją $l_1, \ldots, l_n \in \mathbb{N}$ takie, że $a^{l_k} \in I_k$ dla każdego $k = 1, \ldots, n$. Stąd $a^{l_1+\ldots+l_n} = a^{l_1} \cdot \ldots \cdot a^{l_n} \in I_1 \ldots I_n$, a więc $a \in rad(I_1 \ldots I_n)$. Zatem $rad(I_1) \cap \ldots \cap rad(I_n) \subseteq rad(I_1 \ldots I_n)$. Kończy to dowód naszego stwierdzenia. □

Definicja 9.5. Mówimy, że ideał I pierścienia P jest **ideałem radykalnym**, jeżeli $I = rad(I)$.

Stwierdzenie 9.6. *Dla dowolnego ideału I pierścienia P równoważne są warunki:*

(i) I jest ideałem radykalnym,

(ii) dla każdego $a \in P$: $a^2 \in I \Rightarrow a \in I$.

Dowód. $(i) \Rightarrow (ii)$. Ponieważ $a^2 \in I$, więc $a \in rad(I) = I$, czyli $a \in I$.

$(ii) \Rightarrow (i)$. Wobec stwierdzenia 9.3 (i) wystarczy wykazać inkluzję $rad(I) \subseteq I$. Weźmy dowolne $b \in rad(I)$. Wtedy istnieje najmniejsza liczba naturalna m taka, że $b^m \in I$. Jeśli $m > 1$, to $m - 1 \in \mathbb{N}$ oraz $a = b^{m-1} \notin I$. Ale $a^2 = b^{2m-2} = b^m \cdot b^{m-2} \in I$, więc $a \in I$ i mamy sprzeczność. Oznacza to, że $m = 1$, skąd $b \in I$ oraz $rad(I) \subseteq I$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Ze stwierdzenia 9.6 i z definicji ideału pierwszego wynika od razu następujący

Wniosek 9.7. *Każdy ideał pierwszy pierścienia P jest ideałem radykalnym tego pierścienia.*

Stwierdzenie 9.8. *Przecięcie dowolnej niepustej rodziny $\{I_t\}_{t\in T}$ ideałów radykalnych pierścienia P jest ideałem radykalnym.*

Dowód. Niech $I = \bigcap_{t\in T} I_t$. Na mocy stwierdzenia 9.2 wystarczy wykazać, że $rad(I) \subseteq I$. Weźmy dowolne $a \in rad(I)$. Wtedy istnieje $n \in \mathbb{N}$ takie, że $a^n \in I$, skąd $a^n \in I_t$ dla każdego $t \in T$. Zatem $a \in rad(I_t) = I_t$ dla każdego $t \in T$, czyli $a \in \bigcap_{t\in T} I_t$, a więc $a \in I$. □

Twierdzenie 9.9. *Właściwy ideał I pierścienia P jest radykalny wtedy i tylko wtedy, gdy jest częścią wspólną wszystkich ideałów pierwszych zawierających I.*

Dowód. Z wniosku 9.7 i ze stwierdzenia 9.8 wynika, że część wspólna dowolnej niepustej rodziny ideałów pierwszych pierścienia P jest ideałem radykalnym.

Na odwrót. Najpierw udowodnimy, że dla każdego $a \in P \setminus I$ istnieje ideał pierwszy I_a pierścienia P taki, że $a \notin I_a$ oraz $I \subseteq I_a$. W tym celu oznaczmy przez $\mathcal{M}$ rodzinę wszystkich ideałów J pierścienia P takich, że $I \subseteq J$ oraz $a^n \notin J$ dla każdego $n \in \mathbb{N}$. Rodzina $\mathcal{M}$ jest niepusta, bo $I \in \mathcal{M}$ na mocy tego, że I jest właściwym ideałem radykalnym pierścienia P. Niech $\mathcal{A}$ będzie łańcuchem w $\mathcal{M}$, tzn. dla dowolnych $A, B \in \mathcal{A}$ jest $A \subseteq B$ lub $B \subseteq A$. Wtedy $J = \bigcup_{A\in\mathcal{A}} A \neq P$, bo inaczej $1 \in J$, skąd $1 \in A$, a więc $A = P$ dla pewnego $A \in \mathcal{A}$, co prowadzi do sprzeczności. Ponadto $J \lhd P$, bo $J \neq \emptyset$, gdyż $A \subseteq J$ dla $A \in \mathcal{A}$ oraz dla $j_1, j_2 \in J$, $r \in P$ istnieją $A, B \in \mathcal{A}$ takie, że $j_1 \in A$, $j_2 \in B$, skąd $rj_1 \in A \subseteq J$, czyli $rj_1 \in J$, ale $A \subseteq B$ lub $B \subseteq A$, więc $j_1, j_2 \in A$ lub $j_1, j_2 \in B$, skąd $j_1 - j_2 \in A$ lub $j_1 - j_2 \in B$, więc $j_1 - j_2 \in J$. Jeżeli dla pewnego $n \in \mathbb{N}$ jest $a^n \in J$, to $a^n \in A$ dla pewnego $A \in \mathcal{A}$, co prowadzi do sprzeczności. Zatem $a^n \notin J$ dla każdego $n \in \mathbb{N}$. Wobec tego $J \in \mathcal{M}$, co oznacza, że w $\mathcal{M}$ każdy łańcuch ma ograniczenie górne. Wobec tego z Lematu Zorna w $\mathcal{M}$ istnieje element maksymalny M. Stąd $M \lhd P$, $I \subseteq M \neq P$ oraz $a^n \notin M$ dla każdego $n \in \mathbb{N}$.

Weźmy dowolne $x, y \in P$ takie, że $xy \in M$ i załóżmy, że $x \notin M$ i $y \notin M$. Wtedy $M + (x) \lhd P$ i $M + (y) \lhd P$ oraz $M \subsetneq M + (x)$ i $M \subsetneq M + (y)$. Z maksymalności M i tego, że $I \subseteq M + (x)$ oraz $I \subseteq M+(y)$ wynika, że $M+(x) \notin \mathcal{M}$ i $M+(y) \notin \mathcal{M}$. Stąd $a^n \in M+(x)$ i $a^m \in M + (y)$ dla pewnych $n, m \in \mathbb{N}$. Zatem $a^{n+m} = a^n \cdot a^m \in [M + (x)][M + (y)] \subseteq M + (x)(y) = M + (xy) \subseteq M$, bo $xy \in M$, więc $a^{n+m} \in M$ i mamy sprzeczność. Wobec tego $x \in M$ lub $y \in M$ co oznacza, że M jest ideałem pierwszym pierścienia P, bo dodatkowo $M \neq P$, gdyż $a \notin M$. Wystarczy więc przyjąć $I_a = M$.

Stąd $I \subseteq \bigcap_{a \in P \setminus I} I_a$. Jeśli $I \neq \bigcap_{a \in P \setminus I} I_a$, to istnieje $c \in \bigcap_{a \in P \setminus I} I_a$ takie, że $c \notin I$. Ale wtedy $c \notin I_c$, więc $c \notin \bigcap_{a \in P \setminus I} I_a$. Wobec tego $I = \bigcap_{a \in P \setminus I} I_a$.

Niech teraz $\mathcal{R}$ będzie rodziną wszystkich ideałów pierwszych pierścienia P zawierających I. Rodzina $\mathcal{R}$ jest niepusta na mocy pierwszej części dowodu. Ponadto $I \subseteq \bigcap_{J \in \mathcal{R}} J \subseteq \bigcap_{a \in P \setminus I} I_a = I$, więc $I = \bigcap_{J \in \mathcal{R}} J$, co kończy dowód. □

9.2 Określenie zbioru algebraicznego

Niech K będzie dowolnym ciałem. Oznaczmy przez K^n standardową przestrzeń afiniczną wymiaru n nad K.

Definicja 9.10. Zbiorem algebraicznym wyznaczonym przez wielomiany $f_1, f_2, \ldots, f_s \in K[x_1, x_2, \ldots, x_n]$ nazywamy zbiór wszystkich rozwiązań w K^n układu:

$$f_1(t_1, \ldots, t_n) = 0, \ldots, f_s(t_1, \ldots, t_n) = 0, \tag{9.1}$$

tzn. zbiór tych $t \in K^n$, dla których $f_i(t) = 0$, dla wszystkich $i = 1, \ldots, s$.

Ze wzorów (7.4) wynika, że punkt $t \in K^n$ jest rozwiązaniem układu (9.1) wtedy i tylko wtedy, gdy dla dowolnego $f \in (f_1, \ldots, f_s) = I$ mamy $f(t) = 0$. Wobec tego zbiór rozwiązań układu (9.1) zależy jedynie od ideału I. Wobec tego nie ma potrzeby rozpatrywać nieskończonego zbioru równań wielomianowych, ponieważ jak orzeka wniosek 7.10 każdy ideał pierścienia $K[x_1, x_2, \ldots, x_n]$ jest skończenie generowany.

Dla każdego ideału I pierścienia $K[x_1, \ldots, x_n]$ przyjmujemy oznaczenie:

$$V(I) = \{t \in K^n : f(t) = 0 \text{ dla wszystkich } f \in I\}. \tag{9.2}$$

Twierdzenie 9.11. *Odwzorowanie $I \mapsto V(I)$ prowadzące ze zbioru ideałów pierścienia $K[x_1, x_2, \ldots, x_n]$ do zbiorów algebraicznych w K^n ma następujące własności:*

(i) $V(\{0\}) = K^n$, $V(K[x_1, x_2, \ldots, x_n]) = \emptyset$,

(ii) jeśli $I \subseteq J$, *to* $V(I) \supseteq V(J)$,

(iii) $V\left(\sum_\alpha I_\alpha\right) = \bigcap_\alpha V(I_\alpha)$ *dla dowolnej rodziny ideałów* $\{I_\alpha\}$ *w* $K[x_1, x_2, \ldots, x_n]$,

(iv) $V(I \cap J) = V(IJ) = V(I) \cup V(J)$,

(v) $V(I) = V(rad(I))$.

Dowód. Dowody własności (i)-(iii) są oczywiste. Jeśli chodzi o (iv), to wobec $IJ \subseteq I \cap J$ mamy $V(IJ) \supseteq V(I \cap J) \supseteq V(I) \cup V(J)$ na podstawie (ii). Wystarczy więc wykazać, że $V(IJ) \subseteq V(I) \cup V(J)$ lub równoważnie, że $t \notin V(I) \cup V(J)$ implikuje $t \notin V(IJ)$. Z założenia $t \notin V(I) \cup V(J)$ wynika istnienie wielomianów $f \in I$, $g \in J$ takich, że $f(t) \neq 0$ i $g(t) \neq 0$; wówczas $fg \in IJ$ i $(fg)(t) = f(t) \cdot g(t) \neq 0$, czyli $t \notin V(IJ)$. Ze stwierdzenia 9.2, $I \subseteq rad(I)$, więc z (ii) $V(rad(I)) \subseteq V(I)$. Weźmy dowolne $t \in V(I)$ i niech $f \in rad(I)$. Wtedy $f^m \in I$ dla pewnego $m \in \mathbb{N}$, skąd $0 = (f^m)(t) = (f(t))^m$, czyli $f(t) = 0$. Zatem $t \in V(rad(I))$. Oznacza to, że $V(I) \subseteq V(rad(I))$, więc ostatecznie $V(I) = V(rad(I))$. □

Uwaga 9.12. Własności (i), (iii), (iv) pozwalają określić na K^n topologię, w której jedynymi zbiorami domkniętymi są zbiory algebraiczne. Jest to tzw. **topologia Zariskiego**. Dowolny zbiór algebraiczny w K^n może być traktowany jako przestrzeń topologiczna z indukowaną topologią Zariskiego.

Uwaga 9.13. Z twierdzenia 9.11 wynika, że część wspólna dowolnej niepustej rodziny zbiorów algebraicznych w K^n jest zbiorem algebraicznym. Ponadto suma dwóch zbiorów algebraicznych w K^n jest

zbiorem algebraicznym. Przez prostą indukcję otrzymujemy stąd, że suma skończonej liczby zbiorów algebraicznych w K^n jest zbiorem algebraicznym.

Przykład 9.14. (a). Dla każdego $t \in K^n$ zbiór $\{t\}$ jest algebraiczny, gdyż $t = (t_1, \ldots, t_n)$ dla pewnych $t_1, \ldots, t_n \in K$ oraz $\{t\} = V((x_1 - t_1, \ldots, x_n - t_n))$. Zatem z uwagi 9.13 każdy skończony podzbiór zbioru K^n jest zbiorem algebraicznym. Jeśli zatem ciało K jest skończone, to każdy podzbiór K^n jest zbiorem algebraicznym. Ponieważ niezerowy wielomian $f \in K[x]$ może mieć w ciele K jedynie skończoną liczbę pierwiastków, więc zbiorami algebraicznymi w K^1 są jedynie: K oraz wszystkie skończone podzbiory zbioru K. Wynika stąd, że przestrzeń K^1 z topologią Zariskiego nie jest przestrzenią Hausdorfa, jeśli ciało K jest nieskończone.

(b). Dla dowolnego wielomianu $f \in K[x_1, \ldots, x_n]$ zbiór algebraiczny $V(f) = V((f))$ nazywamy **hiperpowierzchnią**. W K^n **hiperpłaszczyzną afiniczną** nazywamy niepuste podzbiory postaci $H = \{(t_1, \ldots, t_n) \in K^n : a_1 t_1 + \ldots + a_n t_n = b\}$ dla ustalonych $a_1, \ldots, a_n, b \in K$. Zauważmy, że H jest hiperpowierzchnią, gdyż $H = V(f)$ dla $f = a_1 x_1 + \ldots + a_n x_n - b$. Ponieważ każda prosta afiniczna l w K^n jest częścią wspólną skończonej liczby hiperpłaszczyzn afinicznych, więc l jest zbiorem algebraicznym w K^n. Krzywe stożkowe (okrąg, elipsa, parabola, hiperbola) są przykładami hiperpowierzchni w $\mathbb{R}^2$. Zatem figury złożone ze skończonej liczby prostych i krzywych stożkowych są zbiorami algebraicznymi w $\mathbb{R}^2$.

(c). Zbiory algebraiczne $V(I)$ mogą być puste nawet dla właściwych ideałów I pierścienia $K[x_1, \ldots, x_n]$; zależy to od ciała K. Gdy $K = \mathbb{R}$, to $V(x_1^2 + 1) = \emptyset \subset K^1$, a gdy $K = \mathbb{C}$, to $V(x_1^2 + 1) = \{i, -i\}$. Można wykazać, że jeśli ciało K jest algebraicznie domknięte, to $V(I) \neq \emptyset$ dla każdego właściwego ideału pierścienia $K[x_1, \ldots, x_n]$.

Dla dowolnego niepustego podzbioru E przestrzeni K^n przyjmujemy oznaczenie:

$$I(E) = \{f \in K[x_1, \ldots, x_n] : f(t) = 0 \text{ dla wszystkich } t \in E\}. \quad (9.3)$$

Ponadto określamy: $I(\emptyset) = K[x_1, \ldots, x_n]$.

Stwierdzenie 9.15. *Dla dowolnego podzbioru E przestrzeni K^n zbiór $I(E)$ jest ideałem radykalnym pierścienia $K[x_1, \ldots, x_n]$.*

Dowód. Jeśli $E = \emptyset$, to $I(E) = K[x_1, \ldots, x_n]$, a więc $I(E)$ jest ideałem radykalnym. Załóżmy dalej, że $E \neq \emptyset$. Wtedy ze wzoru (9.3) wynika, że wielomian zerowy $0 \in I(E)$. Weźmy dowolne $f, g \in I(E)$, $h \in K[x_1, \ldots, x_n]$. Wtedy dla dowolnego $t \in E$: $f(t) = g(t) = 0$, więc na mocy wzorów (7.4), $(f - g)(t) = f(t) - g(t) = 0 - 0 = 0$ oraz $(fh)(t) = f(t) \cdot h(t) = 0 \cdot h(t) = 0$, skąd $f - g, fh \in I(E)$. Zatem $I(E) \lhd K[x_1, \ldots, x_n]$. Weźmy dowolne $h \in K[x_1, \ldots, x_n]$ takie, że $h^2 \in I(E)$. Wtedy dla dowolnego $t \in E$, $0 = (h^2)(t) = (h(t))^2$, skąd $h(t) = 0$, a więc $h \in I(E)$. Ze stwierdzenia 9.6 wynika zatem, że $I(E)$ jest ideałem radykalnym. □

Stwierdzenie 9.16. *Dla dowolnych podzbiorów E_1, E_2 przestrzeni K^n:*

(i) jeśli $E_1 \subseteq E_2$, to $I(E_2) \subseteq I(E_1)$,

(ii) $I(E_1 \cup E_2) = I(E_1) \cap I(E_2)$.

Dowód. (i). Weźmy dowolne $f \in I(E_2)$. Wtedy dla każdego $t \in E_2$ jest $f(t) = 0$. Ale $E_1 \subseteq E_2$, więc $f(t) = 0$ dla każdego $t \in E_1$, a to oznacza, że $f \in I(E_1)$. Zatem $I(E_2) \subseteq I(E_1)$.

(ii). Ponieważ $E_1 \subseteq E_1 \cup E_2$ i $E_2 \subseteq E_1 \cup E_2$, więc z (i), $I(E_1 \cup E_2) \subseteq I(E_1)$ i $I(E_1 \cup E_2) \subseteq I(E_2)$. Stąd $I(E_1 \cup E_2) \subseteq I(E_1) \cap I(E_2)$. Weźmy dowolne $f \in I(E_1) \cap I(E_2)$. Wtedy $f \in I(E_1)$ i $f \in I(E_2)$. Zatem $f(t) = 0$ dla każdego $t \in E_1$ i $f(t) = 0$ dla każdego $t \in E_2$. Stąd $f(t) = 0$ dla każdego $t \in E_1 \cup E_2$, czyli $f \in I(E_1 \cup E_2)$. Zatem $I(E_1) \cap I(E_2) \subseteq I(E_1 \cup E_2)$ i ostatecznie $I(E_1 \cup E_2) = I(E_1) \cap I(E_2)$. □

Twierdzenie 9.17. *Niech K będzie dowolnym ciałem. Jeśli $W \subseteq K^n$ jest zbiorem algebraicznym, to $V(I(W)) = W$. Ponadto $E \mapsto I(E)$ jest różnowartościowym odwzorowaniem zbioru wszystkich zbiorów algebraicznych w K^n w zbiór wszystkich ideałów radykalnych pierścienia $K[x_1, \ldots, x_n]$.*

Dowód. Z (9.2) i (9.3) mamy, że $W \subseteq V(I(W)))$. Ponadto $W = V(J)$ dla pewnego ideału J pierścienia $K[x_1, \ldots, x_n]$, a więc $J \subseteq I(W)$ na

mocy (9.2) i (9.3). Z twierdzenia 9.11 (ii), $V(I(W)) \subseteq V(J)$, czyli $V(I(W)) \subseteq W$. Zatem $V(I(W)) = W$. Weźmy dowolne zbiory algebraiczne W_1, W_2 takie, że $I(W_1) = I(W_2)$. Wtedy $V(I(W_1)) = V(I(W_2))$, więc $W_1 = W_2$ na mocy pierwszej części dowodu. Zatem odwzorowanie $W \mapsto I(W)$ na zbiorze wszystkich zbiorów algebraicznych w K^n jest różnowartościowe. Ponadto ze stwierdzenia 9.15, $I(W)$ jest ideałem radykalnym pierścienia $K[x_1, \ldots, x_n]$ dla każdego zbioru algebraicznego W w K^n. □

Następne twierdzenie podamy bez dowodu. Jest ono równoważne słynnemu *Twierdzeniu Hilberta o zerach.*

Twierdzenie 9.18. *Niech K będzie ciałem algebraicznie domkniętym. Jeśli J jest ideałem pierścienia $K[x_1, x_2, \ldots, x_n]$, to $I(V(J)) = rad(J)$.*

Definicja 9.19. Zbiór algebraiczny W nazywamy **przywiedlnym**, jeśli można go przedstawić w postaci sumy mnogościowej dwóch zbiorów algebraicznych różnych od W. W przeciwnym wypadku W nazywamy **zbiorem algebraicznym nieprzywiedlnym** lub **rozmaitością algebraiczną**.

Twierdzenie 9.20. *Niepusty zbiór algebraiczny W jest nieprzywiedlny wtedy i tylko wtedy, gdy $I(W)$ jest ideałem pierwszym pierścienia $K[x_1, \ldots, x_n]$.*

Dowód. Ponieważ zbiór W jest niepusty, więc na mocy twierdzenia 9.17, $I(W) \neq K[x_1, \ldots, x_n]$. Niech zbiór algebraiczny W będzie nieprzywiedlny. Weźmy dowolne $f, g \in K[x_1, \ldots, x_n]$ takie, że $fg \in I(W)$. Z twierdzenia 9.11 $V(f) \cap W$ i $V(g) \cap W$ są zbiorami algebraicznymi. Ponadto $W = (V(f) \cap W) \cup (V(g) \cap W)$, gdyż $(V(f) \cap W) \cup (V(g) \cap W) \subseteq W$ oraz jeśli $t \in W$ i $t \notin V(f) \cap W$, to $t \notin V(f)$, a więc $f(t) \neq 0$. Ale $fg \in I(W)$, więc $0 = (fg)(t) = f(t) \cdot g(t)$, skąd $g(t) = 0$ i wobec tego $t \in V(g) \cap W$. Z nieprzywiedlności zbioru W mamy stąd, że $W = V(f) \cap W$ lub $W = V(g) \cap W$, czyli $W \subseteq V(f)$ lub $W \subseteq V(g)$, a to oznacza, że $f \in I(W)$ lub $g \in I(W)$. Zatem $I(W)$ jest ideałem pierwszym pierścienia $K[x_1, \ldots, x_n]$.

Na odwrót, załóżmy, że $I(W)$ jest ideałem pierwszym pierścienia $K[x_1, \ldots, x_n]$. Niech $W = W_1 \cup W_2$ będzie przedstawieniem W w postaci sumy dwóch zbiorów algebraicznych W_1, W_2. Ze stwierdzenia 9.16 (ii), $I(W) = I(W_1) \cap I(W_2)$. Stąd $I(W_1)I(W_2) \subseteq I(W)$, więc z pierwszości ideału $I(W)$ otrzymujemy, że $I(W_1) \subseteq I(W)$ lub $I(W_2) \subseteq I(W)$. Z twierdzeń 9.11 i 9.17 otrzymujemy więc, że $W \subseteq W_1$ lub $W \subseteq W_2$, skąd $W = W_1$ lub $W = W_2$. Oznacza to, że zbiór W jest nieprzywiedlny. □

Twierdzenie 9.21. *Dla dowolnego zbioru algebraicznego W w K^n istnieje przedstawienie w postaci sumy:*

$$W = W_1 \cup \ldots \cup W_p, \tag{9.4}$$

takiej, że:

(i) $W_1, \ldots, W_p$ są zbiorami algebraicznymi nieprzywiedlnymi,

(ii) $W_i \not\subseteq \bigcup_{j \neq i} W_j$ dla dowolnego $i = 1, \ldots, p$.

Zbiory $W_1, \ldots, W_p$ spełniające warunki (i), (ii) są wyznaczone jednoznacznie przez W (i nazywane składowymi nieprzywiedlnymi zbioru algebraicznego W).

Dowód. Przypuśćmy, że W nie ma przedstawienia w postaci (9.4). Wówczas W jest przywiedlny, tzn. istnieją zbiory algebraiczne W_1, W_2, $W_1 \neq W$, $W_2 \neq W$ takie, że $W = W_1 \cup W_2$. Stąd W_1 nie można przedstawić w postaci (9.4) lub W_2 nie można przedstawić w postaci (9.4). Bez zmniejszania ogólności możemy zakładać, że W_1 nie ma przedstawienia postaci (9.4). Zatem istnieją zbiory algebraiczne $W_{11} \neq W_1$, $W_{12} \neq W_1$ takie, że $W_1 = W_{11} \cup W_{12}$, przy czym W_{11} lub W_{12} nie ma przedstawienia postaci (9.4). Kontynuując ten proces otrzymamy ściśle malejący ciąg zbiorów algebraicznych $W \supset W_1 \supset \ldots$, który na podstawie stwierdzenia 9.16 i twierdzenia 9.17 indukuje ściśle rosnący ciąg ideałów $I(W) \subset I(W_1) \subset \ldots$ pierścienia $K[x_1, \ldots, x_n]$. Otrzymaliśmy zatem sprzeczność z wnioskiem 7.10. Pierwsza część twierdzenia jest zatem udowodniona.

Jeśli otrzymany rozkład postaci (9.4) nie spełnia warunku (ii), to usuwając kolejno składniki rozkładu zawarte w sumie pozostałych do-

chodzimy w końcu do rozkładu spełniającego warunek (ii); rozkład taki nazywamy nieskracalnym.

Przypuśćmy, że mamy dwa nieskracalne przedstawienia zbioru W, powiedzmy $W = W_1 \cup \ldots \cup W_p = V_1 \cup \ldots \cup V_q$. Wówczas $W_i = W_i \cap W = W_i \cap (V_1 \cup \ldots \cup V_q) = (W_i \cap V_1) \cup \ldots \cup (W_i \cap V_q)$. Ponieważ W_i jest nieprzywiedlnym zbiorem algebraicznym, więc dla pewnego j mamy $W_i = W_i \cap V_j$, czyli $W_i \subseteq V_j$. Stosując to samo rozumowanie do V_j wnioskujemy o istnieniu i' takiego, że $V_j \subseteq W_{i'}$. Wobec tego $W_i \subseteq V_j \subseteq W_{i'}$, więc na podstawie nieskracalności rozkładu $i' = i$ oraz $W_i = V_j$. Wynika stąd, że dla każdego $i \in \{1, \ldots, p\}$ istnieje dokładnie jedno $j \in \{1, \ldots, q\}$ takie, że $W_i = V_j$, innymi słowy otrzymujemy funkcję $i \mapsto j$ ze zbioru $\{1, \ldots, p\}$ w zbiór $\{1, \ldots, q\}$. Przez symetrię uzyskujemy stąd, że dla każdego $j = 1, \ldots, q$ istnieje dokładnie jedno $i \in \{1, \ldots, p\}$ takie, że $V_j = W_i$. Zatem funkcja $i \mapsto j$ jest bijekcją, a więc $p = q$ oraz z dokładnością do porządku składników $V_i = W_i$ dla wszystkich $i = 1, \ldots, p$. □

Rozdział 10

Największy wspólny dzielnik i najmniejsza wspólna wielokrotność

10.1 Największy wspólny dzielnik

Definicja 10.1. Niech P będzie dziedziną całkowitości. Powiemy, że $d \in P$ jest **największym wspólnym dzielnikiem** elementów $a_1, \ldots, a_n \in P$, jeżeli

(i) $d \mid a_i$ dla każdego $i = 1, \ldots, n$ oraz

(ii) dla dowolnego $x \in P$ z tego, że $x \mid a_i$ dla każdego $i = 1, \ldots, n$ wynika $x \mid d$.

Piszemy wtedy $d \sim NWD(a_1, \ldots, a_n)$.

Uwaga 10.2. W dziedzinie całkowitości P mamy, że $d \in P$ jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_n \in P$ wtedy i tylko wtedy, gdy d jest wspólnym dzielnikiem elementów $a_1, \ldots, a_n$ podzielnym przez każdy ich wspólny dzielnik. W szczególności **każde dwa największe wspólne dzielniki elementów** $a_1, \ldots, a_n$ **są stowarzyszone** w dziedzinie P. Zatem jeżeli $d \sim NWD(a_1, \ldots, a_n)$, to zbiorem wszystkich największych wspólnych dzielników elementów $a_1, \ldots, a_n$ jest $\{d \cdot u : u \in P^*\}$.

Twierdzenie 10.3. *Jeżeli w dziedzinie całkowitości P dla dowolnych elementów $a, b \in P$ istnieje $NWD(a, b)$, to dla każdego naturalnego n i dla dowolnych elementów $a_1, a_2, \ldots, a_n \in P$ istnieje $NWD(a_1, a_2, \ldots, a_n)$ oraz dla $n \geqslant 2$ zachodzi wzór:*

$$NWD(a_1, \ldots, a_{n-1}, a_n) \sim NWD(NWD(a_1, \ldots, a_{n-1}), a_n). \quad (10.1)$$

Dowód. Stosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista, bo wprost z definicji $NWD(a_1) \sim a_1$ dla każdego $a_1 \in P$. Załóżmy, że $n > 1$ jest taką liczbą naturalną, że teza zachodzi dla liczby $n - 1$ i niech $a_1, \ldots, a_{n-1}, a_n$ będą dowolnymi elementami dziedziny P. Z założenia indukcyjnego wynika, że istnieje $d \in P$ takie, że $d \sim NWD(a_1, \ldots, a_{n-1})$. Zatem z założenia twierdzenia istnieje $D \in P$ takie, że $D \sim NWD(d, a_n)$. Wtedy $D \mid a_n$ i $D \mid d$ oraz $d \mid a_i$ dla $i = 1, \ldots, n-1$, więc $D \mid a_i$ dla $i = 1, \ldots, n-1$ i $D \mid a_n$, czyli D jest wspólnym dzielnikiem elementów $a_1, \ldots, a_n$. Załóżmy, że $x \in P$ jest wspólnym dzielnikiem elementów $a_1, \ldots, a_{n-1}, a_n$. Wtedy $x \mid a_n$ oraz x jest wspólnym dzielnikiem elementów $a_1, \ldots, a_{n-1}$, więc z uwagi 10.2, $x \mid d$. Zatem $x \mid d$ i $x \mid a_n$, więc z uwagi 10.2, $x \mid D$, a więc D jest podzielne przez każdy wspólny dzielnik elementów $a_1, \ldots, a_n$. Stąd z uwagi 10.2 mamy wzór (10.1) oraz $D \sim NWD(a_1, \ldots, a_n)$. □

Twierdzenie 10.4. *Jeżeli $d, a_1, \ldots, a_n$ są takimi elementami dziedziny całkowitości P, że $(a_1, \ldots, a_n) = (d)$, to $d \sim NWD(a_1, \ldots, a_n)$. W szczególności dla dowolnych elementów $a_1, \ldots, a_n$ dziedziny ideałów głównych P istnieje $NWD(a_1, \ldots, a_n)$ oraz zachodzi wzór:*

$$(a_1, \ldots, a_n) = (NWD(a_1, \ldots, a_n)). \quad (10.2)$$

Dowód. Dla $i = 1, \ldots, n$ mamy, że $a_i \in (a_1, \ldots, a_n)$, więc $a_i \in (d)$, skąd $d \mid a_i$. Niech $x \in P$ będzie wspólnym dzielnikiem elementów $a_1, \ldots, a_n$. Wtedy $a_i \in (x)$ dla $i = 1, \ldots, n$, skąd $(a_1, \ldots, a_n) \subseteq (x)$, czyli $(d) \subseteq (x)$, skąd $x \mid d$. Zatem z uwagi 10.2, $d \sim NWD(a_1, \ldots, a_n)$. □

Twierdzenie 10.5. *Niech p będzie elementem nierozkładalnym dziedziny całkowitości P. Jeżeli istnieją elementy $a, b \in P$ takie, że $p \mid ab$, ale p nie dzieli a i p nie dzieli b, to w dziedzinie P nie istnieje $NWD(pa, ab)$ oraz ideał (p, a) nie jest główny. W szczególności, jeżeli w dziedzinie całkowitości P dla dowolnych elementów $a, b \in P$ istnieje $NWD(a, b)$, to każdy element nierozkładalny pierścienia P jest elementem pierwszym w P.*

Dowód. Załóżmy, że przy tych założeniach istnieje $d \in P$ takie, że $d \sim NWD(pa, ab)$. Wtedy $d \mid pa$ i $d \mid ab$. Ponadto $p \mid pa$ i $p \mid ab$, więc z uwagi 10.2, $p \mid d$. Ponadto $a \mid pa$ i $a \mid ab$, więc $a \mid d$. Zatem istnieją $x, y, k, l \in P$ takie, że $pa = dx$, $ab = dy$, $d = pk$ i $d = al$. Zatem $pa = alx$, skąd $p = lx$, gdyż $a \neq 0$, bo p nie dzieli a. Ale p jest elementem nierozkładalnym, więc $l \in P^*$ lub $x \in P^*$.

Jeśli $l \in P^*$, to $a = dl^{-1} = pkl^{-1}$, skąd $p \mid a$ i mamy sprzeczność. Jeśli zaś $x \in P^*$, to $d = pax^{-1}$, skąd $ab = pax^{-1}y$, czyli $b = px^{-1}y$, a więc $p \mid b$ i też mamy sprzeczność. Wynika stąd, że nie istnieje $NWD(pa, ab)$.

Załóżmy, że ideał (p, a) jest główny. Wtedy istnieje $D \in P$ takie, że $(p, a) = (D)$. Zatem z twierdzenia 10.4, $D \sim NWD(p, a)$. Ale p nie dzieli a i p jest elementem nierozkładalnym w pierścieniu P, więc z uwagi 10.2, $D \sim 1$, skąd $(D) = (1)$, a więc $1 \in (p, a)$. Zatem $1 = pr + as$ dla pewnych $r, s \in P$, skąd $b = prb + abs$. Ponadto $p \mid ab$, więc stąd $p \mid b$ i mamy sprzeczność. Zatem ideał (p, a) nie jest główny. □

Przykład 10.6. Łatwo zauważyć, że

$$P = \mathbb{Z} + (x^2) = \left\{a + x^2 \cdot f : a \in \mathbb{Z}, f \in \mathbb{Z}[x]\right\}$$

jest podpierścieniem dziedziny całkowitości $\mathbb{Z}[x]$. Z własności stopnia wielomianu oraz najstarszego współczynnika prosto wynika, że x^2 jest elementem nierozkładalnym dziedziny P. Ponadto $x^2 \mid x^3 \cdot x^3$, bo $x^3 \cdot x^3 = x^2 \cdot x^4$ oraz $x^4 \in P$. Ale x^2 nie dzieli x^3, gdyż $x \notin P$. Zatem na mocy twierdzenia 10.5 w dziedzinie P nie istnieje $NWD(x^5, x^6)$ i ideał (x^2, x^3) nie jest główny.

Przykład 10.7. Niech d będzie liczbą całkowitą, która nie jest kwadratem liczby całkowitej. Wówczas d nie jest kwadratem liczby wymiernej, skąd wynika, że dla dowolnych $a_1, a_2, b_1, b_2 \in \mathbb{Q}$:

$$a_1 + b_1\sqrt{d} = a_2 + b_2\sqrt{d} \iff [a_1 = a_2 \text{ oraz } b_1 = b_2].$$

łatwo zauważyć, że $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ jest podciałem ciała $\mathbb{C}$ oraz $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$ jest podpierścieniem ciała $\mathbb{Q}(\sqrt{d})$. Dla dowolnych $x, y \in \mathbb{Q}$ określamy:

$$||x + y\sqrt{d}||_d = |x^2 - dy^2|. \tag{10.3}$$

Wtedy z niewymierności $\sqrt{d}$ i wzoru (10.3) wynika, że:

$$||\alpha||_d = 0 \iff \alpha = 0 \text{ dla dowolnego } \alpha \in \mathbb{Q}(\sqrt{d}). \tag{10.4}$$

$$\begin{gathered} ||\alpha||_d \text{ jest dodatnią liczbą wymierną} \\ \text{dla każdego niezerowego } \alpha \in \mathbb{Q}(\sqrt{d}). \end{gathered} \tag{10.5}$$

$$||\alpha||_d \in \mathbb{N} \text{ dla każdego niezerowego } \alpha \in \mathbb{Z}[\sqrt{d}]. \tag{10.6}$$

$$||\alpha \cdot \beta||_d = ||\alpha||_d \cdot ||\beta||_d \text{ dla dowolnych } \alpha, \beta \in \mathbb{Q}(\sqrt{d}). \tag{10.7}$$

Rzeczywiście, $\alpha = x + y\sqrt{d}$, $\beta = r + s\sqrt{d}$ dla pewnych $x, y, r, s \in \mathbb{Q}$, więc $\alpha \cdot \beta = (xr + dys) + (xs + yr)\sqrt{d}$, czyli

$$\begin{aligned} ||\alpha \cdot \beta||_d &= |(xr + dys)^2 - d(xs + yr)^2| = \\ &= |x^2r^2 + 2xrdys + d^2y^2s^2 - dx^2s^2 - 2dxsyr - dy^2r^2| = \\ &= |r^2(x^2 - dy^2) - ds^2(x^2 - dy^2)| = \\ &= |x^2 - dy^2| \cdot |r^2 - ds^2| = \\ &= ||\alpha||_d \cdot ||\beta||_d. \end{aligned}$$

$$\alpha \in (\mathbb{Z}[\sqrt{d}])^* \iff ||\alpha||_d = 1. \tag{10.8}$$

Rzeczywiście, jeśli $\alpha \in (\mathbb{Z}[\sqrt{d}])^*$, to istnieje $\beta \in \mathbb{Z}[\sqrt{d}]$ takie, że $\alpha \cdot \beta = 1$, skąd na mocy (10.3) i (10.7), $||\alpha||_d \cdot ||\beta||_d = 1$. Zatem z (10.6), $||\alpha||_d = 1$.

Na odwrót, załóżmy, że $\alpha \in \mathbb{Z}[\sqrt{d}]$ spełnia warunek $||\alpha||_d = 1$. Wtedy $\alpha = a + b\sqrt{d}$ dla pewnych $a, b \in \mathbb{Z}$, więc $|a^2 - db^2| = 1$, czyli $a^2 - db^2 = \pm 1$, skąd $\alpha \cdot (a - b\sqrt{d}) = 1$ lub $\alpha \cdot (-a + b\sqrt{d}) = 1$, zatem $\alpha \in (\mathbb{Z}[\sqrt{d}])^*$.

$$\begin{gathered}[\alpha \in \mathbb{Z}[\sqrt{d}] \text{ oraz } ||\alpha||_d \text{ jest liczbą pierwszą}] \\ \Rightarrow [\alpha \text{ jest elementem nierozkładalnym w } \mathbb{Z}[\sqrt{d}]].\end{gathered} \tag{10.9}$$

Rzeczywiście, na mocy (10.4) i (10.8) mamy, że $\alpha \neq 0$ i α nie jest elementem odwracalnym pierścienia $\mathbb{Z}[\sqrt{d}]$. Ponadto dla dowolnych $\beta, \gamma \in \mathbb{Z}[\sqrt{d}]$ takich, że $\alpha = \beta \cdot \gamma$ na mocy (10.7) mamy, że $||\alpha||_d = ||\beta||_d \cdot ||\gamma||_d$, więc z (10.6) i z pierwszości liczby $||\alpha||_d$ otrzymujemy, że $||\beta||_d = 1$ lub $||\gamma||_d = 1$. Zatem na mocy (10.8), $\beta \in (\mathbb{Z}[\sqrt{d}])^*$ lub $\gamma \in (\mathbb{Z}[\sqrt{d}])^*$. Stąd α jest elementem nierozkładalnym pierścienia $\mathbb{Z}[\sqrt{d}]$.

Załóżmy teraz, że $d < -2$. Pokażemy, że wówczas 2 jest elementem nierozkładalnym, ale nie jest elementem pierwszym w pierścieniu $\mathbb{Z}[\sqrt{d}]$. Najpierw zauważmy, że nie istnieje $\alpha \in \mathbb{Z}[\sqrt{d}]$ takie, że $||\alpha||_d = 2$, gdyż inaczej dla pewnych $x, y \in \mathbb{Z}$ mielibyśmy, że $x^2 + (-d)y^2 = 2$. Ale $-d > 2$, więc $y = 0$ i $x^2 = 2$, co prowadzi do sprzeczności. Stosując argumenty podobne do zastosowanych w dowodzie (10.9) łatwo wykazujemy, że 2 jest elementem nierozkładalnym w pierścieniu $\mathbb{Z}[\sqrt{d}]$. Ponadto 2 nie dzieli $\sqrt{d}$, bo inaczej istnieją $a, b \in \mathbb{Z}$ takie, że $\sqrt{d} = 2 \cdot (a + b\sqrt{d})$, skąd $1 = 2b$ i mamy sprzeczność.

Jeżeli d jest liczbą parzystą, to $d = -2k$ dla pewnego $k = 2, 3, \ldots$. Wtedy $2 \mid \sqrt{d} \cdot \sqrt{d}$, ale 2 nie dzieli $\sqrt{d}$, więc 2 nie jest elementem pierwszym w pierścieniu $\mathbb{Z}[\sqrt{d}]$ oraz z twierdzenia 10.5 nie istnieje $NWD(2\sqrt{d}, d)$ oraz ideał $(2, \sqrt{d})$ nie jest główny.

Jeżeli d jest liczbą nieparzystą, to 2 nie dzieli $1 + \sqrt{d}$ i 2 nie dzieli $1 - \sqrt{d}$, ale $2 \mid (1 + \sqrt{d}) \cdot (1 - \sqrt{d}) = 1 - d$. Zatem 2 nie jest elementem pierwszym w pierścieniu $\mathbb{Z}[\sqrt{d}]$ i na mocy twierdzenia 10.5 nie istnieje $NWD(2 - 2\sqrt{d}, 1 - d)$ oraz ideał $(2, 1 + \sqrt{d})$ nie jest główny.

Przykład 10.8. Niech P będzie dowolną dziedziną całkowitości. Wówczas dla dowolnego $a \in P$ mamy, że $a \sim NWD(a, 0)$ na mocy uwagi 10.2. Ponadto dla $a \in P$ i $u \in P^*$ jest $1 \sim NWD(a, u)$, bo $1 \mid a$ i $1 \mid u$ oraz dla dowolnego $x \in P$ takiego, że $x \mid a$ i $x \mid u$ istnieje $t \in P$

takie, że $u = xt$, skąd $1 = xtu^{-1}$, czyli $x \mid 1$. Jeżeli $a, b \in P$ oraz $a \mid b$, to z uwagi 10.2, $a \sim NWD(a, b)$.

10.2 Najmniejsza wspólna wielokrotność

Definicja 10.9. Niech P będzie dziedziną całkowitości. Powiemy, że $a \in P$ jest **najmniejszą wspólną wielokrotnością** elementów $a_1, \ldots, a_n \in P$, jeżeli

(i) $a_i \mid a$ dla każdego $i = 1, \ldots, n$ oraz

(ii) dla dowolnego $x \in P$ z tego, że $a_i \mid x$ dla każdego $i = 1, \ldots, n$ wynika $a \mid x$.

Piszemy wtedy $a \sim NWW(a_1, \ldots, a_n)$.

Uwaga 10.10. W dziedzinie całkowitości P mamy, że $a \in P$ jest najmniejszą wspólną wielokrotnością elementów $a_1, \ldots, a_n \in P$ wtedy i tylko wtedy, gdy a jest wspólną wielokrotnością elementów $a_1, \ldots, a_n$ dzielącą każdą ich wspólną wielokrotność. W szczególności **każde dwie najmniejsze wspólne wielokrotności elementów** $a_1, \ldots, a_n$ **są stowarzyszone** w dziedzinie P. Zatem jeżeli $a \sim NWW(a_1, \ldots, a_n)$, to zbiorem wszystkich najmniejszych wspólnych wielokrotności elementów $a_1, \ldots, a_n$ jest $\{a \cdot u : u \in P^*\}$.

Twierdzenie 10.11. *Jeżeli w dziedzinie całkowitości P dla dowolnych elementów $a, b \in P$ istnieje $NWW(a, b)$, to dla każdej liczby naturalnej n i dla dowolnych elementów $a_1, a_2, \ldots, a_n \in P$ istnieje $NWW(a_1, a_2, \ldots, a_n)$ oraz dla $n \geqslant 2$ zachodzi wzór:*

$$NWW(a_1, \ldots, a_{n-1}, a_n) \sim NWW(NWW(a_1, \ldots, a_{n-1}), a_n). \quad (10.10)$$

Dowód. Stosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista, bo wprost z definicji $NWW(a_1) \sim a_1$ dla każdego $a_1 \in P$. Załóżmy, że $n > 1$ jest taką liczbą naturalną, że teza zachodzi dla liczby $n-1$ i niech $a_1, \ldots, a_{n-1}, a_n$ będą dowolnymi elementami dziedziny P. Z założenia indukcyjnego istnieje $a \in P$ takie, że $a \sim NWW(a_1, \ldots, a_{n-1})$. Zatem z założenia twierdzenia istnieje $A \in P$ takie, że $A \sim NWW(a, a_n)$. Wtedy $a_n \mid A$ i $a \mid A$ oraz $a_i \mid a$ dla $i = 1, \ldots, n-1$, więc $a_i \mid A$

dla $i = 1, \ldots, n-1$ i $a_n \mid A$, czyli A jest wspólną wielokrotnością elementów $a_1, \ldots, a_n$. Załóżmy, że $x \in P$ jest wspólną wielokrotnością elementów $a_1, \ldots, a_{n-1}, a_n$. Wtedy $a_n \mid x$ oraz x jest wspólną wielokrotnością elementów $a_1, \ldots, a_{n-1}$, więc z uwagi 10.10, $a \mid x$. Zatem $a \mid x$ i $a_n \mid x$, więc z uwagi 10.10, $A \mid x$, a więc A dzieli każdą wspólną wielokrotność elementów $a_1, \ldots, a_n$. Stąd z uwagi 10.10 mamy wzór (10.10) oraz $A \sim NWW(a_1, \ldots, a_n)$. □

Twierdzenie 10.12. *Niech $a, a_1, \ldots, a_n$ będą takimi elementami dziedziny całkowitości P, że $(a_1) \cap \ldots \cap (a_n) = (a)$. Wówczas $a \sim NWW(a_1, \ldots, a_n)$. W szczególności dla każdych elementów $a_1, \ldots, a_n$ dziedziny ideałów głównych P istnieje $NWW(a_1, \ldots, a_n)$ oraz zachodzi wzór:*

$$(a_1) \cap \ldots \cap (a_n) = (NWW(a_1, \ldots, a_n)). \tag{10.11}$$

Dowód. Ponieważ $a \in (a_1) \cap \ldots \cap (a_n)$, więc $a \in (a_i)$ dla $i = 1, \ldots, n$, skąd $a_i \mid a$ dla każdego $i = 1, \ldots, n$. Niech $x \in P$ będzie wspólną wielokrotnością elementów $a_1, \ldots, a_n$. Wtedy $x \in (a_i)$ dla każdego $i = 1, \ldots, n$, skąd $x \in (a_1) \cap \ldots \cap (a_n) = (a)$, czyli $x \in (a)$, a więc $a \mid x$. Zatem $a \sim NWW(a_1, \ldots, a_n)$. □

Twierdzenie 10.13. *Niech p będzie elementem nierozkładalnym dziedziny całkowitości P. Jeżeli istnieją elementy $a, b \in P$ takie, że $p \mid ab$, ale p nie dzieli a i p nie dzieli b, to w dziedzinie P nie istnieje $NWW(p, a)$. W szczególności, jeżeli w dziedzinie całkowitości P dla dowolnych elementów $a, b \in P$ istnieje $NWW(a, b)$, to każdy element nierozkładalny pierścienia P jest elementem pierwszym w P.*

Dowód. Załóżmy, że przy tych założeniach istnieje $A \in P$ takie, że $A \sim NWW(p, a)$. Wtedy $p \mid A$ i $a \mid A$. Ponadto $p \mid pa$ i $a \mid pa$, więc $A \mid pa$. Ale $p \mid ab$ i $a \mid ab$, więc też $A \mid ab$. Zatem istnieją $x, y, s \in P$ takie, że $A = ax$, $pa = Ay$ i $ab = As$. Stąd $pa = axy$, czyli $p = xy$, bo $a \neq 0$, gdyż p nie dzieli a. Ale p jest elementem nierozkładalnym pierścienia P, więc $x \in P^*$ lub $y \in P^*$. Jeżeli $x \in P^*$, to $a = Ax^{-1}$ i $p \mid A$, więc $p \mid a$ wbrew założeniu. Jeżeli zaś $y \in P^*$, to $A = pay^{-1}$, skąd $ab = pay^{-1}s$, czyli $b = py^{-1}s$, więc $p \mid b$ wbrew założeniu. □

Przykład 10.14. Przy oznaczeniach przykładu 10.6 w pierścieniu P nie istnieje na mocy twierdzenia 10.13, $NWW(x^2, x^3)$.

Przykład 10.15. Na mocy twierdzenia 10.13 i przykładu 10.7 dla parzystego $d < -2$ w pierścieniu $\mathbb{Z}[\sqrt{d}]$ nie istnieje $NWW(2, \sqrt{d})$ oraz dla nieparzystego $d < -2$ nie istnieje $NWW(2, 1 + \sqrt{d})$ w pierścieniu $\mathbb{Z}[\sqrt{d}]$.

Przykład 10.16. Niech P będzie dowolną dziedziną całkowitości. Wprost z definicji najmniejszej wspólnej wielokrotności otrzymujemy, że jeżeli $a, b \in P$ i $a \mid b$, to $b \sim NWW(a, b)$. W szczególności dla $a \in P$, $0 \sim NWW(a, 0)$. Jeżeli $u \in P^*$ i $a \in P$, to $u \mid a$, więc $a \sim NWW(a, u)$.

10.3 NWD i NWW w dziedzinach z jednoznacznością rozkładu

Twierdzenie 10.17. *Niech P będzie dziedziną z jednoznacznością rozkładu i niech $p_1, \ldots, p_s$ będą parami niestowarzyszonymi elementami pierwszymi pierścienia P. Niech $\alpha_1, \ldots, \alpha_s \in \mathbb{N}_0$ oraz $a = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Wówczas wszystkimi z dokładnością do stowarzyszenia dzielnikami elementu a są elementy postaci:*

$$d = p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}, \tag{10.12}$$

gdzie $\beta_i = 0, 1, \ldots, \alpha_i$ dla $i = 1, \ldots, s$.

Dowód. Ponieważ P jest dziedziną z jednoznacznością rozkładu, więc na mocy założeń twierdzenia elementy postaci (10.12) są parami niestowarzyszone. Ponadto $a = d \cdot c$ dla $c = p_1^{\alpha_1 - \beta_1} \cdot \ldots \cdot p_s^{\alpha_s - \beta_s}$ i $c \in P$, bo $\alpha_i - \beta_i \in \mathbb{N}_0$ dla $i = 1, \ldots, s$. Zatem $d \mid a$.

Na odwrót, niech $d \in P$ będzie dzielnikiem elementu a. Wtedy istnieje $b \in P$ takie, że $a = d \cdot b$. Ale $a \neq 0$, więc $d, b \neq 0$. Jeżeli p jest elementem pierwszym pierścienia P takim, że $p \mid d$ lub $p \mid b$, to $p \mid a$, więc $p \mid p_i$ dla pewnego $i = 1, \ldots, s$, skąd z pierwszości p_i, $p \sim p_i$. Zatem z jednoznaczności rozkładu pierścienia P istnieją nieujemne liczby całkowite β_i, γ_i dla $i = 1, \ldots, s$ oraz istnieją

$u, v \in P^*$ takie, że $d = u \cdot p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$ oraz $b = v \cdot p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$. Stąd $uvp_1^{\beta_1+\gamma_1} \cdot \ldots \cdot p_s^{\beta_s+\gamma_s} = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Zatem $\beta_i + \gamma_i = \alpha_i$, skąd $\beta_i = 0, 1, \ldots, \alpha_i$ oraz $d \sim p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$. □

Z twierdzenia 10.17 oraz z definicji NWD i NWW wynika od razu następujące

Twierdzenie 10.18. *Niech P będzie dziedziną z jednoznacznością rozkładu i niech $p_1, \ldots, p_s$ będą parami niestowarzyszonymi elementami pierwszymi w P. Niech $\alpha_i, \beta_i \in \mathbb{N}_0$ dla $i = 1, \ldots, s$ oraz niech $a \sim p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ i $b \sim p_1^{\beta_1} \cdot \ldots \cdot p_s^{\beta_s}$. Wtedy*
(i) $p_1^{\min(\alpha_1,\beta_1)} \cdot \ldots \cdot p_s^{\min(\alpha_s,\beta_s)} \sim NWD(a, b)$,
(ii) $p_1^{\max(\alpha_1,\beta_1)} \cdot \ldots \cdot p_s^{\max(\alpha_s,\beta_s)} \sim NWW(a, b)$.

Z twierdzeń 10.17, 10.11, 10.3 i przykładów 10.16 i 10.8 wynika od razu następujące

Twierdzenie 10.19. *Jeżeli P jest dziedziną z jednoznacznością rozkładu, to dla dowolnego naturalnego n i dla dowolnych elementów $a_1, \ldots, a_n \in P$ istnieją $NWD(a_1, \ldots, a_n)$ i $NWW(a_1, \ldots, a_n)$.*

Definicja 10.20. Powiemy, że elementy $a_1, \ldots, a_n$ dziedziny z jednoznacznością rozkładu P są **względnie pierwsze**, jeżeli zachodzi $1 \sim NWD(a_1, \ldots, a_n)$.

Stwierdzenie 10.21. *Niech $a_1, a_2, \ldots, a_n$, nie wszystkie równe 0, będą elementami dziedziny z jednoznacznością rozkładu P. Wtedy $1 \sim NWD\left(\frac{a_1}{NWD(a_1,\ldots,a_n)}, \ldots, \frac{a_n}{NWD(a_1,\ldots,a_n)}\right)$.*

Dowód. Z twierdzenia 10.19 wynika, że istnieje $a \in P$ takie, że $a \sim NWD(a_1, a_2, \ldots, a_n)$. Ponadto $a \neq 0$, bo $a_i \neq 0$ dla pewnego $i = 1, 2, \ldots, n$. Zatem $b_i = \frac{a_i}{a} \in P$ dla $i = 1, 2, \ldots, n$. Weźmy dowolne $x \in P$ takie, że $x \mid b_i$ dla wszystkich $i = 1, 2, \ldots, n$. Wtedy dla $i = 1, 2, \ldots, n$ istnieje $c_i \in P$ takie, że $b_i = x \cdot c_i$. Zatem $a_i = (ax)c_i$, skąd $ax \mid a_i$ dla $i = 1, 2, \ldots, n$. Z definicji największego wspólnego dzielnika wynika zatem, że $ax \mid a$, co wobec $a \neq 0$ daje $x \in P^*$. Wobec tego $x \sim 1$ i $1 \sim NWD(b_1, b_2, \ldots, b_n)$. □

Twierdzenie 10.22. *Niech a, b, c będą elementami dziedziny z jednoznacznością rozkładu P. Jeżeli elementy a i b są względnie pierwsze oraz $a \cdot b \sim c^n$ dla pewnego naturalnego n, to istnieją $c_1, c_2 \in P$ takie, że $a \sim c_1^n$ i $b \sim c_2^n$.*

Dowód. Jeżeli $a = 0$, to $b \sim NWD(a, b)$. Ale $1 \sim NWD(a, b)$, więc $b \sim 1$ i wystarczy wziąć $c_1 = 0$ oraz $c_2 = 1$. Analogicznie dla $b = 0$ wystarczy wziąć $c_1 = 1$ i $c_2 = 0$. Niech dalej $a \neq 0$ i $b \neq 0$. Jeżeli $a \in P^*$, to $b \sim ab$, więc $b \sim c^n$ i $a \sim 1^n$. Jeżeli $b \in P^*$, to podobnie $a \sim c^n$ i $b \sim 1^n$. Możemy zatem zakładać, że $a \notin P^*$ i $b \notin P^*$ oraz $a \neq 0$ i $b \neq 0$. Ponieważ P jest dziedziną z jednoznacznością rozkładu oraz elementy a i b są względnie pierwsze, więc istnieją parami niestowarzyszone elementy pierwsze $p_1, \ldots, p_s, q_1, \ldots, q_r$ oraz istnieją liczby naturalne $\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_r$ takie, że $a \sim p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ i $b \sim q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}$. Zatem $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r} \sim c^n$. Stąd na mocy twierdzenia 10.17 istnieją nieujemne liczby całkowite $\gamma_1, \ldots, \gamma_s, \delta_1, \ldots, \delta_r$ takie, że $c \sim p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s} \cdot q_1^{\delta_1} \cdot \ldots \cdot q_r^{\delta_r}$. Zatem $p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r} \sim p_1^{n\gamma_1} \cdot \ldots \cdot p_s^{n\gamma_s} \cdot q_1^{n\delta_1} \cdot \ldots \cdot q_r^{n\delta_r}$, skąd z jednoznaczności rozkładu w pierścieniu P, $\alpha_i = n\gamma_i$ dla $i = 1, \ldots, s$ oraz $\beta_j = n\delta_j$ dla $j = 1, \ldots, r$. Zatem $a \sim c_1^n$ dla $c_1 = p_1^{\gamma_1} \cdot \ldots \cdot p_s^{\gamma_s}$ oraz $b \sim c_2^n$ dla $c_2 = q_1^{\delta_1} \cdot \ldots \cdot q_r^{\delta_r}$. □

Rozdział 11

Pierścienie euklidesowe i ich zastosowania

11.1 Pierścienie euklidesowe

Definicja 11.1. Niezerowy pierścień P nazywamy **pierścieniem euklidesowym**, jeżeli istnieje funkcja $N\colon P \to \mathbb{N}_0$ zwana **normą** spełniająca następujące warunki:
(I) $\forall_{a\in P}\ N(a) = 0 \iff a = 0$,
(II) $\forall_{a,b\in P}\ N(a \cdot b) = N(a) \cdot N(b)$,
(III) $\forall_{b\in P\setminus\{0\}}\ \forall_{a\in P}\ \exists_{q,r\in P}\ a = q \cdot b + r$ oraz $N(r) < N(b)$.

Przykład 11.2. Każde ciało K jest pierścieniem euklidesowym z normą N daną wzorem $N(a) = 1$ dla $a \in K \setminus \{0\}$ oraz $N(0) = 0$.

Przykład 11.3. Pierścień liczb całkowitych $\mathbb{Z}$ jest pierścieniem euklidesowym z normą N daną wzorem $N(a) = |a|$ dla $a \in \mathbb{Z}$.

Przykład 11.4. Dla dowolnego ciała K pierścień $K[x]$ jest pierścieniem euklidesowym z normą N daną wzorem $N(w) = 2^{st(w)}$ dla $w \in K[x] \setminus \{0\}$ oraz $N(0) = 0$.

Przykład 11.5. Dla $d = -2, -1, 2, 3$ pierścień $\mathbb{Z}[\sqrt{d}]$ jest pierścieniem euklidesowym z normą N daną wzorem $N(\alpha) = ||\alpha||_d$ dla $\alpha \in \mathbb{Z}[\sqrt{d}]$, gdzie funkcja $||\cdot||_d$ określona została w przykładzie 10.7.

Rzeczywiście, warunki (I) oraz (II) były pokazane w przykładzie 10.7, pozostaje więc wykazać, że zachodzi warunek (III). W tym celu weźmy dowolne $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, $\beta \neq 0$. Wtedy α, β należą do ciała $\mathbb{Q}(\sqrt{d})$, więc istnieją liczby wymierne x, y takie, że $\frac{\alpha}{\beta} = x + y\sqrt{d}$. Niech x_0 będzie liczbą całkowitą najbliższą liczby x i niech y_0 będzie liczbą całkowitą najbiliższą liczby y. Wtedy $|x - x_0| \leqslant \frac{1}{2}$ i $|y - y_0| \leqslant \frac{1}{2}$. Określamy $\gamma = x_0 + y_0\sqrt{d}$ i $\rho = \alpha - \gamma \cdot \beta$. Wtedy $\gamma, \rho \in \mathbb{Z}[\sqrt{d}]$, $\alpha = \gamma \cdot \beta + \rho$ oraz $\rho = \alpha - \gamma \cdot \beta = \frac{\alpha}{\beta} \cdot \beta - \gamma \cdot \beta = \beta \cdot (\frac{\alpha}{\beta} - \gamma) = \beta \cdot [(x + y\sqrt{d}) - (x_0 + y_0\sqrt{d})] = \beta \cdot [(x - x_0) + (y - y_0)\sqrt{d}]$, czyli na mocy przykładu 10.7, $N(\rho) = ||\rho||_d = ||\beta||_d \cdot ||(x - x_0) + (y - y_0)\sqrt{d}||_d = ||\beta||_d \cdot |(x - x_0)^2 - d(y - y_0)^2|$. Wystarczy zatem wykazać, że dla dowolnych liczb wymiernych p, q takich, że $0 \leqslant p, q \leqslant \frac{1}{2}$ zachodzi nierówność:

$$|p^2 - dq^2| < 1. \tag{11.1}$$

Jeżeli $d = -2, -1, 2$, to $|p^2 - dq^2| \leqslant p^2 + |d|q^2 \leqslant \left(\frac{1}{2}\right)^2 + 2 \cdot \left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1$. Natomiast dla $d = 3$:
$|p^2 - dq^2| = |p^2 - 3q^2| = \begin{cases} p^2 - 3q^2 \leqslant \frac{1}{4} & \text{gdy } p^2 - 3q^2 \geqslant 0 \\ 3q^2 - p^2 \leqslant \frac{3}{4} & \text{gdy } p^2 - 3q^2 < 0 \end{cases}$. Zatem także $|p^2 - dq^2| < 1$.

Stwierdzenie 11.6. *Niech P będzie pierścieniem euklidesowym z normą N. Wówczas*
(i) $N(1) = 1$,
(ii) $\forall_{a \in P}\ a \in P^* \iff N(a) = 1$.

Dowód. (i) Weźmy $a \in P \setminus \{0\}$. Wtedy z (I), $N(a) \neq 0$. Zatem na mocy (II), $0 \neq N(a) = N(1 \cdot a) = N(1) \cdot N(a)$, więc po skróceniu $N(1) = 1$.

(ii) Niech $a \in P^*$. Wtedy istnieje $b \in P$ takie, że $a \cdot b = 1$. Zatem z (i) oraz (II), $1 = N(a) \cdot N(b)$, czyli $N(a) = 1$. Na odwrót, załóżmy, że $N(a) = 1$. Wtedy z (I) jest $a \neq 0$. Zatem z (III) istnieją $q, r \in P$ takie, że $1 = q \cdot a + r$ i $N(r) < N(a) = 1$. Ale $N(r) \in \mathbb{N}_0$, więc $N(r) = 0$, skąd na mocy (I), $r = 0$, czyli $1 = q \cdot a$. Zatem $a \in P^*$. □

Twierdzenie 11.7. *Każdy pierścień euklidesowy jest dziedziną ideałów głównych. W szczególności każdy pierścień euklidesowy jest dziedziną z jednoznacznością rozkładu.*

Dowód. Niech P będzie pierścieniem euklidesowym z normą N. Wtedy $P \neq \{0\}$. Weźmy dowolne $a, b \in P \setminus \{0\}$. Wtedy z (I), $N(a), N(b) \neq 0$, więc z (II) $N(a \cdot b) = N(a) \cdot N(b) \neq 0$, czyli z (I) $a \cdot b \neq 0$. Zatem P jest dziedziną całkowitości.

Niech I będzie dowolnym ideałem pierścienia P. Jeżeli $I = \{0\}$, to $I = (0)$, czyli I jest ideałem głównym. Załóżmy dalej, że $I \neq \{0\}$. Wtedy z (I) istnieje w zbiorze $I \setminus \{0\}$ element a o najmniejszej normie $N(a)$. Oczywiście $(a) \subseteq I$. Weźmy dowolne $i \in I$. Wtedy z (III) istnieją $q, r \in P$ takie, że $i = q \cdot a + r$ i $N(r) < N(a)$. Stąd $r = i - q \cdot a \in I$ oraz $N(r) < N(a)$, więc z wyboru a, $r \notin I \setminus \{0\}$, czyli $r = 0$. Zatem $i = q \cdot a \in (a)$, skąd $I \subseteq (a)$ i ostatecznie $I = (a)$. Zatem ideał I jest główny.

Ostatnia część twierdzenia wynika z algebry I. □

Stwierdzenie 11.8. *Niech P będzie pierścieniem euklidesowym z normą N i niech p będzie liczbą pierwszą.*

(i) Jeżeli $a \in P$ i $N(a) = p$, to a jest elementem pierwszym w P.

(ii) Jeżeli w pierścieniu P nie istnieje element o normie p oraz $N(b) = p^2$ dla pewnego $b \in P$, to b jest elementem pierwszym w P.

Dowód. (i). Ponieważ $p > 1$, więc z (I), $a \neq 0$ i ze stwierdzenia 11.6, $a \notin P^*$. Weźmy dowolne $b, c \in P$ takie, że $a = bc$. Wtedy z (II), $p = N(b) \cdot N(c)$, więc z pierwszości p i tego, że $N(b), N(c) \in \mathbb{N}_0$ otrzymujemy $N(b) = 1$ lub $N(c) = 1$, czyli wobec stwierdzenia 11.6, $b \in P^*$ lub $c \in P^*$. Zatem a jest elementem nierozkładalnym pierścienia P. Ale P jest dziedziną z jednoznacznością rozkładu na mocy twierdzenia 11.7, więc z algebry I, a jest elementem pierwszym w P.

(ii). Ponieważ $p^2 > 1$, więc z (I), $b \neq 0$ i ze stwierdzenia 11.6, $b \notin P^*$. Weźmy dowolne $x, y \in P$ takie, że $b = xy$. Wtedy z (II) $p^2 = N(x) \cdot N(y)$. Ponadto $N(x), N(y) \in \mathbb{N}_0$ i w P nie istnieje element o normie p oraz p jest liczbą pierwszą, więc $N(x) = 1$ lub $N(y) = 1$. Stąd na mocy stwierdzenia 11.6, $x \in P^*$ lub $y \in P^*$. Zatem b jest elementem nierozkładalnym pierścienia P. Ale P jest dziedziną z jednoznacznością rozkładu, więc b jest elementem pierwszym w P. □

Ponieważ każdy pierścień euklidesowy P jest dziedziną z jednoznacznością rozkładu, więc z twierdzenia 10.19 dla dowolnych $a, b \in P$

istnieje $NWD(a,b)$. Okazuje się, że $NWD(a,b)$ można wyznaczyć efektywnie przy pomocy **Algorytmu Euklidesa**.

Lemat 11.9. *Niech P będzie dziedziną z jednoznacznością rozkładu. Wówczas dla dowolnych $a,b,q \in P$:*

$$NWD(a,b) \sim NWD(a,b-q\cdot a).$$

Dowód. Oznaczmy $d \sim NWD(a,b)$, $D \sim NWD(a,b-q\cdot a)$. Wtedy $d \mid a$ i $d \mid b$, skąd $d \mid b-q\cdot a$, więc $d \mid D$. Ponadto $D \mid a$ i $D \mid b-q\cdot a$, więc $D \mid b$, skąd $D \mid d$. Zatem $d \sim D$. □

Niech teraz P będzie pierścieniem euklidesowym z normą N i niech $a,b \in P$. Jeśli $a=b=0$, to $NWD(a,b) \sim 0$. Jeśli $a=0$, to $NWD(a,b) \sim b$. Jeśli $b=0$, to $NWD(a,b) \sim a$. Możemy zatem dalej zakładać, że $a \neq 0$ i $b \neq 0$. Bez zmniejszania ogólności rozważań możemy dalej zakładać, że $N(a) \leqslant N(b)$. Z warunku (III) i lematu 11.9 istnieją $q_1, r_1 \in P$ takie, że

$$b = q_1\cdot a + r_1 \text{ i } N(r_1) < N(a) \text{ oraz } NWD(a,b) \sim NWD(r_1,a).$$

Jeśli $r_1 \neq 0$, to z warunku (III) i lematu 11.9 istnieją $q_2, r_2 \in P$ takie, że

$$a = q_2\cdot r_1 + r_2 \text{ i } N(r_2) < N(r_1) \text{ oraz } NWD(r_1,a) \sim NWD(r_2,r_1).$$

Ponieważ nie istnieje nieskończony malejący ciąg liczb naturalnych, więc otrzymujemy stąd, że istnieje liczba naturalna n oraz istnieją $q_i, r_i \in P$ dla $i=1,\ldots,n$ takie, że

$$r_{i-1} = q_{i+1}\cdot r_i + r_{i+1}, N(r_{i+1}) < N(r_i), NWD(r_i,r_{i-1}) \sim NWD(r_{i+1},r_i)$$

dla wszystkich $i=0,1,\ldots,n$, przy czym $r_{-1}=b$, $r_0=a$ oraz $r_{n+1}=0$. Stąd przez prostą indukcję

$$NWD(a,b) \sim r_n.$$

Ponadto możemy rekurencyjnie określić ciągi $(x_i)_{i=-1}^n$ oraz $(y_i)_{i=-1}^n$ elementów pierścienia P:

$$x_{-1}=0,\ y_{-1}=1,\ x_0=1,\ y_0=0,$$

$$x_i = x_{i-2} - q_i x_{i-1},\ y_i = y_{i-2} - q_i y_{i-1} \text{ dla } i = 1, \ldots, n$$

i wtedy

$$r_i = a \cdot x_i + b \cdot y_i \text{ dla } i = -1, 0, \ldots, n,$$

skąd w szczególności

$$NWD(a, b) \sim r_n = a \cdot x_n + b \cdot y_n.$$

11.2 Zastosowania pierścieni euklidesowych

Twierdzenie 11.10 (Fermata)**.** *Każda liczba pierwsza postaci* $4k + 1$ *jest sumą kwadratów dwóch liczb naturalnych.*

Dowód. Niech p będzie liczbą pierwszą oraz $p = 4k+1$ dla pewnego $k \in \mathbb{N}$. Z twierdzenia 6.22 grupa $\mathbb{Z}_p^*$ jest cykliczna, czyli istnieje $c \in \mathbb{Z}_p^*$ takie, że $c^{p-1} = 1$ oraz $c^m \neq 1$ dla wszystkich liczb naturalnych $m < p - 1$. W szczególności $c^{2k} \neq 1$. Ale $c^{4k} = 1$, więc $0 = c^{4k} - 1 = (c^{2k} - 1) \cdot (c^{2k} + 1)$, skąd $c^{2k} + 1 = 0$ w ciele $\mathbb{Z}_p$. Zatem w pierścieniu $\mathbb{Z}$, $p \mid c^{2k} + 1$, czyli $p \mid x^2 + 1$ dla $x = c^k$.

Z przykładu 11.5 wiemy, że pierścień $\mathbb{Z}[i]$ jest pierścieniem euklidesowym, a więc jest on dziedziną z jednoznacznością rozkładu. Ponadto $p \mid (x + i) \cdot (x - i)$ oraz p nie dzieli ± 1 w pierścieniu $\mathbb{Z}$, więc p nie jest elementem pierwszym w $\mathbb{Z}[i]$. Zatem p nie jest elementem nierozkładalnym w $\mathbb{Z}[i]$. Ponadto $p \neq 0$ i $p \notin (\mathbb{Z}[i])^*$, więc p jest elementem rozkładalnym w pierścieniu $\mathbb{Z}[i]$. Zatem istnieją niezerowe i nieodwracalne elementy $\alpha, \beta \in \mathbb{Z}[i]$ takie, że $p = \alpha \cdot \beta$, skąd $p^2 = ||\alpha||_{-1} \cdot ||\beta||_{-1}$. Ale $||\alpha||_{-1}, ||\beta||_{-1} > 1$, więc stąd $||\alpha||_{-1} = ||\beta||_{-1} = p$. Istnieją $a, b \in \mathbb{Z}$ takie, że $\alpha = a + bi$. Zatem $p = a^2 + b^2 = |a|^2 + |b|^2$. Ale liczba pierwsza nie jest kwadratem liczby całkowitej, więc $|a|, |b| \in \mathbb{N}$, czyli p jest sumą kwadratów dwóch liczb naturalnych. □

Lemat 11.11. *Niech* $m = 2t + 1$ *dla pewnej liczby naturalnej* t*. Jeżeli liczby naturalne* x *i* y *spełniają równanie:*

$$x^2 + 1 = y^m, \tag{11.2}$$

to istnieje parzysta liczba naturalna a taka, że:

$$\sum_{k=0}^{t}(-1)^k\binom{m}{2k}a^{2k}=1. \tag{11.3}$$

Dowód. Jeżeli x jest liczbą nieparzystą, to y musi być liczbą parzystą, skąd $4 \mid y^m$, bo $m>1$. Zatem $4 \mid x^2+1$. Ale $x^2 \equiv 1 \ (mod\ 4)$, więc mamy sprzeczność. Zatem x jest parzyste, zaś y jest nieparzyste.

W pierścieniu $\mathbb{Z}[i]$, który jak wiemy jest dziedziną z jednoznacznością rozkładu, mamy, że $(x+i)\cdot(x-i)=y^m$. Gdyby elementy $x+i$, $x-i$ nie były względnie pierwsze, to istniałby element pierwszy $\pi \in \mathbb{Z}[i]$ taki, że $\pi \mid x+i$ oraz $\pi \mid x-i$, skąd $\pi \mid (x+i)-(x-i)$, czyli $\pi \mid 2i$, skąd $\pi \mid 2$, gdyż $2i \sim 2$. Ale x jest liczbą parzystą, więc $\pi \mid x$. Ponadto $\pi \mid x+i$, więc stąd $\pi \mid i$. Lecz $i \in (\mathbb{Z}[i])^*$, więc $\pi \mid 1$, skąd $\pi \in (\mathbb{Z}[i])^*$ i mamy sprzeczność. Zatem elementy $x+i$ oraz $x-i$ są względnie pierwsze. Z twierdzenia 10.22 istnieje $\alpha \in \mathbb{Z}[i]$ takie, że $x+i \sim \alpha^m$. Istnieje więc $u \in (\mathbb{Z}[i])^* = \{1,-1,i,-i\}$ takie, że $x+i=u\cdot\alpha^m$. Ponadto m jest liczbą nieparzystą, zaś grupa $(\mathbb{Z}[i])^*$ jest cykliczna rzędu 4 o generatorze i, więc $\langle i^m\rangle = \langle i\rangle$, skąd $u=v^m$ dla pewnego $v \in (\mathbb{Z}[i])^*$. Zatem $x+i=(v\cdot\alpha)^m$. Ponadto $v\cdot\alpha = a+bi$ dla pewnych $a,b \in \mathbb{Z}$, więc $x+i=(a+bi)^m$. Stąd $|x+i|=|a+bi|^m$, czyli $x^2+1=(a^2+b^2)^m$. Ze wzoru Newtona

$$\begin{aligned}(a+bi)^m &= \sum_{k=0}^{m}\binom{m}{k}a^{m-k}b^k i^k = \\ &= \sum_{k=0}^{t}(-1)^k\binom{m}{2k}a^{m-2k}b^{2k} + i\cdot\sum_{k=0}^{t}(-1)^k\binom{m}{2k+1}a^{2(t-k)}b^{2k+1},\end{aligned}$$

skąd $1 = b\cdot\sum_{k=0}^{t}(-1)^k\binom{m}{2k+1}a^{2(t-k)}b^{2k}$, więc $b \mid 1$ w pierścieniu $\mathbb{Z}$, czyli $b=\pm1$, skąd $x^2+1=(a^2+1)^m$, więc a jest parzyste oraz mamy, że $\sum_{k=0}^{t}(-1)^k\binom{m}{2k+1}a^{2(t-k)} = \pm1$, więc $\sum_{j=0}^{t}(-1)^{t-j}\binom{m}{2j}a^{2j} = \pm1$. Zatem $\sum_{j=0}^{t}(-1)^j\binom{m}{2j}a^{2j} = \pm1$. Jeśli $a=0$, to $x^2+1=1$, skąd $x=0$ i mamy

sprzeczność. Zatem $a \neq 0$, więc bez zmniejszania ogólności rozważań możemy zakładać, że $a \in \mathbb{N}$. Ponieważ liczba a jest parzysta, więc $\sum_{j=0}^{t} (-1)^j \binom{m}{2j} a^{2j} = 1 + 4l$ dla pewnego $l \in \mathbb{Z}$. Stąd $1 + 4l = \pm 1$, więc ostatecznie $\sum_{k=0}^{t} (-1)^k \binom{m}{2k} a^{2k} = 1$. □

Twierdzenie 11.12 (Lebesgue'a)**.** *Jeżeli m i n są liczbami naturalnymi oraz $m > 1$, to równanie:*

$$x^m - y^{2n} = 1 \tag{11.4}$$

nie posiada rozwiązania w liczbach naturalnych x, y.

Dowód. Załóżmy, że przy tych założeniach równanie (11.4) posiada rozwiązanie w liczbach naturalnych x, y. Gdyby m było liczbą parzystą, to istniałyby liczby naturalne a i b takie, że $a^2 - b^2 = 1$. Wtedy $(a-b)(a+b) = 1$, skąd $a + b = 1$ i mamy sprzeczność. Zatem m jest liczbą nieparzystą i istnieją liczby naturalne x, y takie, że $x^2 + 1 = y^m$. Zatem z lematu 11.11 istnieje parzysta liczba naturalna a taka, że $\sum_{k=0}^{t} (-1)^k \binom{m}{2k} a^{2k} = 1$, gdzie $m = 2t + 1$ dla pewnego naturalnego t. Stąd $1 + (-1)^{\frac{m(m-1)}{2}} a^2 + \sum_{k=2}^{t} (-1)^k \binom{m}{2k} a^{2k} = 1$, czyli:

$$\frac{m(m-1)}{2} = \sum_{k=2}^{t} (-1)^k \binom{m}{2k} a^{2k-2}. \tag{11.5}$$

Niech s będzie największą nieujemną liczbą całkowitą taką, że $2^s \mid \frac{m(m-1)}{2}$. Wtedy $\frac{m(m-1)}{2} = 2^s l$ dla pewnej liczby nieparzystej l. Łatwo sprawdzić, że dla $k = 2, 3, \ldots, t$ zachodzi tożsamość:

$$\binom{m}{2k} a^{2k-2} = \frac{m(m-1)}{2} \cdot \binom{m-2}{2k-2} \cdot \frac{a^{2k-2}}{k(2k-1)}. \tag{11.6}$$

Dla $k \geqslant 2$ mamy, że $2^{2k-2} > k$, skąd 2^{2k-2} nie dzieli liczby $k(2k-1)$. Ponadto a jest parzyste, więc dla $k \geqslant 2$, $2^{2k-2} \mid a^{2k-2}$. Wynika stąd, że

istnieją względnie pierwsze liczby naturalne b, c takie, że $\frac{a^{2k-2}}{k(2k-1)} = \frac{2b}{c}$ oraz c jest liczbą nieparzystą. Stąd uzyskujemy, że

$$\binom{m}{2k} a^{2k-2} = 2^s l \binom{m-2}{2k-2} \cdot \frac{2b}{c} = 2^{s+1} l \binom{m-2}{2k-2} \cdot \frac{b}{c}.$$

Zatem $2^{s+1} \mid c \cdot \binom{m}{2k} a^{2k-2}$, skąd wobec nieparzystości c, $2^{s+1} \mid \binom{m}{2k} a^{2k-2}$ dla $k = 2, \ldots, t$. Zatem ze wzoru (11.5), $2^{s+1} \mid \frac{m(m-1)}{2}$ i mamy sprzeczność. □

Rozdział 12

Jednoznaczność rozkładu w pierścieniach wielomianów

12.1 Wielomiany pierwotne

W całym tym rozdziale zakładamy, że pierścień P jest dziedziną z jednoznacznością rozkładu.

Definicja 12.1. Wielomian $f = a_0 + a_1x + \ldots + a_nx^n \in P[x]$ nazywamy **pierwotnym**, jeżeli jego współczynniki są względnie pierwsze, tzn. $1 \sim NWD(a_0, a_1, \ldots, a_n)$.

Uwaga 12.2. Niech $a \in P$ oraz $g = b_0 + b_1x + \ldots + b_mx^m \in P[x]$. Zauważmy, że $a \mid g$ w pierścieniu $P[x]$ wtedy i tylko wtedy, gdy $a \mid b_i$ w pierścieniu P dla wszystkich $i = 0, 1, \ldots, m$. W szczególności wielomian $f \in P[x]$ jest pierwotny wtedy i tylko wtedy, gdy nie istnieje element pierwszy $p \in P$ dzielący f w pierścieniu $P[x]$ (równoważnie: nie istnieje element pierwszy pierścienia P dzielący wszystkie współczynniki wielomianu f).

Lemat 12.3. *Każdy niezerowy wielomian $f \in P[x]$ można przedstawić w postaci*

$$f = z(f) \cdot f^*,$$

gdzie $z(f) \in P$, zaś f^* jest wielomianem pierwotnym w $P[x]$. Przedstawienie to jest jednoznaczne z dokładnością do stowarzyszenia, tj.

jeśli $f = z_1 f_1^* = z_2 f_2^*$, *gdzie wielomiany* $f_1^*, f_2^* \in P[x]$ *są pierwotne, a* $z_1, z_2 \in P$, *to* $z_1 \sim z_2$ *w* P *i* $f_1^* \sim f_2^*$ *w* $P[x]$.

Dowód. Niech $f = a_0 + a_1 x + \ldots + a_n x^n$. Przyjmijmy $z(f) = NWD(a_0, a_1, \ldots, a_n)$. Wtedy dla $i = 0, 1, \ldots, n$: $a_i = z(f) \cdot b_i$ dla pewnego $b_i \in P$. Ze stwierdzenia 10.21 mamy, że $1 \sim NWD(b_0, b_1, \ldots, b_n)$, czyli wielomian $f^* = b_0 + b_1 x + \ldots + b_n x^n$ jest pierwotny. Ponadto $f = z(f) \cdot f^*$. Ponieważ $f = z_1 f_1^*$, więc z_1 dzieli wszystkie współczynniki wielomianu f. Zatem $z_1 \mid z(f)$, gdyż $z(f) = NWD(a_0, a_1, \ldots, a_n)$. Stąd $z(f) = a \cdot z_1$ dla pewnego $a \in P$ oraz $a z_1 f^* = z_1 f_1^*$. Ale wielomian f jest niezerowy, więc $z_1 \neq 0$, a zatem $a f^* = f_1^*$. Stąd a dzieli wszystkie współczynniki wielomianu pierwotnego f_1^*, czyli $a \in P^*$. Zatem $z_1 \sim z(f)$ w P i $f_1^* \sim f^*$ w $P[x]$. Rozumując analogicznie uzyskamy, że $z_2 \sim z(f)$ w P i $f_2^* \sim f^*$ w $P[x]$. Zatem $z_1 \sim z_2$ w P oraz $f_1^* \sim f_2^*$ w $P[x]$. □

Lemat 12.4. *Każdy element pierwszy* p *pierścienia* P *jest elementem pierwszym pierścienia* $P[x]$.

Dowód. Ponieważ $(P[x])^* = P^*$, więc p nie jest odwracalny w $P[x]$. Ponadto $p \neq 0$. Weźmy dowolne wielomiany $f, g \in P[x]$ takie, że $p \mid fg$ w $P[x]$. Oznaczmy przez I ideał główny pierścienia P generowany przez element p. Ponieważ p jest elementem pierwszym, więc I jest ideałem pierwszym, a więc pierścień ilorazowy P/I jest dziedziną całkowitości. Stąd pierścień wielomianów $(P/I)[x]$ jest dziedziną całkowitości. Oznaczmy przez π naturalny homomorfizm pierścienia P na pierścień P/I, tzn. $\pi(a) = a + I$ dla $a \in P$. Wtedy z algebry ogólnej I przekształcenie $\Pi\colon P[x] \to (P/I)[x]$ dane wzorem $\Pi(a_0 + a_1 x + \ldots + a_n x^n) = \pi(a_0) + \pi(a_1)x + \ldots + \pi(a_n)x^n$ jest homomorfizmem pierścienia $P[x]$ na pierścień $(P/I)[x]$. Ponieważ $p \mid fg$ w $P[x]$, więc $0 = \Pi(fg) = \Pi(f) \cdot \Pi(g)$. Ale $(P/I)[x]$ jest dziedziną całkowitości, więc $\Pi(f) = 0$ lub $\Pi(g) = 0$, co oznacza, że wszystkie współczynniki wielomianu f dzielą się przez p lub wszystkie współczynniki wielomianu g dzielą się przez p. Stąd $p \mid f$ lub $p \mid g$ w $P[x]$. □

Lemat 12.5 (Gaussa)**.** *Iloczyn skończonej liczby wielomianów pierwotnych w* $P[x]$ *jest wielomianem pierwotnym w* $P[x]$.

Dowód. Niech $f_1, \ldots, f_k \in P[x]$ będą wielomianami pierwotnymi. Załóżmy, że ich iloczyn $f_1 \ldots f_k$ nie jest wielomianem pierwotnym w $P[x]$. Wtedy istnieje element pierwszy $p \in P$ taki, że $p \mid f_1 \ldots f_k$ w $P[x]$. Ale z lematu 12.4, p jest elementem pierwszym w pierścieniu $P[x]$, więc $p \mid f_i$ dla pewnego $i = 1, \ldots, k$. Stąd wielomian f_i nie jest pierwotny i mamy sprzeczność. □

Lemat 12.6. *Jeżeli wielomian f pierwotny w $P[x]$ dzieli wielomian $g \in P[x]$ w pierścieniu $K[x]$, gdzie K jest ciałem ułamków dla pierścienia P, to $f \mid g$ w pierścieniu $P[x]$.*

Dowód. Z założenia istnieje wielomian $h \in K[x]$ taki, że $g = hf$. Ponieważ K jest ciałem ułamków pierścienia P, więc istnieje niezerowe $a \in P$ takie, że $ah = \varphi \in P[x]$. Zatem $ag = f\varphi$. Jeśli $g = 0$, to $g = 0 \cdot f$, a więc $f \mid g$ w $P[x]$. Załóżmy dalej, że $g \neq 0$. Wtedy z lematu 12.3 istnieją niezerowe elementy $z(g), z(\varphi) \in P$ oraz wielomiany g^*, φ^* pierwotne w $P[x]$ i takie, że $g = z(g)g^*$ oraz $\varphi = z(\varphi)\varphi^*$. Stąd $[az(g)]g^* = z(\varphi)(f\varphi^*)$. Ale z lematu 12.5 wielomian $f\varphi^*$ jest pierwotny w $P[x]$, więc z lematu 12.3 istnieje $u \in P^*$ takie, że $az(g)u = z(\varphi)$. Zatem $g^* = u(f\varphi^*)$, więc $g = f \cdot (z(g)u\varphi^*)$, czyli $f \mid g$ w $P[x]$. □

12.2 Twierdzenie Gaussa

Lemat 12.7. *Jeżeli wielomian $f \in P[x]$ dodatniego stopnia jest nierozkładalny w pierścieniu $P[x]$, to jest on również nierozkładalny w pierścieniu $K[x]$, gdzie K jest ciałem ułamków pierścienia P.*

Dowód. Z założenia mamy, że $f \neq 0$ i $f \notin (P[x])^*$ oraz wielomian f jest pierwotny w $P[x]$. Załóżmy, że wielomian f nie jest nierozkładalny w pierścieniu $K[x]$. Wtedy istnieją nieodwracalne w $K[x]$ wielomiany $g_1, h_1 \in K[x]$ takie, że $f = g_1h_1$. Stąd $st(f) = st(g_1) + st(h_1)$, a ponieważ $(K[x])^* = K \setminus \{0\}$, więc $st(g_1) > 0$ i $st(h_1) > 0$. Ale K jest ciałem ułamków pierścienia P, więc istnieją niezerowe $a, b \in P$ takie, że $g_2 = ag_1 \in P[x]$ i $h_2 = bh_1 \in P[x]$, przy czym $st(g_2) = st(g_1)$ i $st(h_2) = st(h_1)$. Stąd $abf = g_2h_2$. Z lematu 12.3 istnieją niezerowe

$z(g_2), z(h_2) \in P$ oraz wielomiany g_2^*, h_2^* pierwotne w $P[x]$, dla których $g_2 = z(g_2)g_2^*$ i $h_2 = z(h_2)h_2^*$. Zatem $(ab)f = (z(g_2)z(h_2))(g_2^*h_2^*)$. Ponadto z lematu 12.5 wielomian $g_2^*h_2^*$ jest pierwotny w $P[x]$, więc z lematu 12.3, $f \sim g_2^*h_2^*$ w $P[x]$. Zatem istnieje $u \in P^*$ takie, że $f = ug_2^*h_2^* = (ug_2^*)h_2^*$. Ale $st(ug_2^*) = st(g_2^*) = st(g_2) > 0$ i $st(h_2^*) = st(h_2) > 0$, więc wielomian f jest rozkładalny w $P[x]$ i mamy sprzeczność. □

Lemat 12.8. *Niech K będzie ciałem ułamków pierścienia P. Jeżeli wielomian pierwotny $f \in P[x]$ jest nierozkładalny w $K[x]$, to f jest nierozkładalny w $P[x]$.*

Dowód. Z założenia $f \neq 0$ i $f \notin K^*$. Zatem $f \notin (P[x])^* = P^*$. Weźmy dowolne $g_1, g_2 \in P[x]$ takie, że $f = g_1g_2$. Wtedy z nierozkładalności f w $K[x]$ mamy, że $g_1 \in (K[x])^* = K^*$ lub $g_2 \in K^*$. Można zakładać, że $g_1 \in K^*$. Stąd $g_1 \in P \setminus \{0\}$, bo $g_1 \in P[x]$. Jeśli $g_1 \notin P^*$, to istnieje element pierwszy $p \in P$ taki, że $p \mid g_1$, skąd $p \mid f$, co przeczy pierwotności wielomianu f. Zatem $g_1 \in P^*$ i wobec tego f jest nierozkładalny w $P[x]$. □

Lemat 12.9. *Każdy element nierozkładalny pierścienia P jest elementem nierozkładalnym w $P[x]$.*

Dowód. Niech $a \in P$ będzie elementem nierozkładalnym w P. Wtedy $a \neq 0$ i $a \notin P^*$. Ale $(P[x])^* = P^*$, więc $a \notin (P[x])^*$. Weźmy dowolne $f, g \in P[x]$ takie, że $a = fg$. Wtedy $0 = st(a) = st(f) + st(g)$, skąd $st(f) = st(g) = 0$, czyli $f, g \in P$. Zatem $f \in P^*$ lub $g \in P^*$, a więc $f \in (P[x])^*$ lub $g \in (P[x])^*$. Oznacza to, że a jest elementem nierozkładalnym w pierścieniu $P[x]$. □

Twierdzenie 12.10 (Gaussa)**.** *Jeżeli P jest dziedziną z jednoznacznością rozkładu, to $P[x]$ też jest dziedziną z jednoznacznością rozkładu.*

Dowód. Z algebry ogólnej I wynika, że wystarczy udowodnić, że każdy niezerowy element nieodwracalny $f \in P[x]$ jest iloczynem skończonej liczby wielomianów nierozkładalnych w $P[x]$ oraz, że każdy element nierozkładalny pierścienia $P[x]$ jest elementem pierwszym w $P[x]$.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Ponieważ P jest dziedziną całkowitości, więc $P[x]$ też jest dziedziną całkowitości i $(P[x])^* = P^*$. Niech $f \in P[x]$ będzie niezerowym elementem nieodwracalnym w $P[x]$. Wtedy $f \notin P^*$ i $f \neq 0$. Jeśli $st(f) = 0$, to f jest niezerowym elementem nieodwracalnym w dziedzinie z jednoznacznością rozkładu P, więc f jest iloczynem skończonej liczby elementów nierozkładalnych w pierścieniu P. Zatem z lematu 12.9, f jest iloczynem skończonej liczby elementów nierozkładalnych w $P[x]$. Załóżmy, że nie każdy niezerowy element nieodwracalny w $P[x]$ jest iloczynem skończonej liczby elementów nierozkładalnych w $P[x]$. Wówczas wśród wszystkich niezerowych wielomianów nieodwracalnych z $P[x]$, które nie są iloczynami skończonej liczby elementów nierozkładalnych w $P[x]$ istnieje wielomian f_0 najniższego stopnia n. Z pierwszej części dowodu $n > 0$. Ponadto z lematu 12.3, $f_0 = z(f_0)f_0^*$ dla pewnego niezerowego $z(f_0) \in P$ oraz dla pewnego wielomianu f_0^* pierwotnego w $P[x]$. Z pierwszej części dowodu wynika, że wielomian f_0^* nie jest iloczynem skończonej liczby wielomianów nierozkładalnych w $P[x]$. Ponadto $st(f_0^*) = n$ i f_0^* jest elementem rozkładalnym w $P[x]$. Zatem istnieją niezerowe wielomiany g, h nieodwracalne w $P[x]$ i takie, że $f_0^* = gh$. Ponieważ wielomian f_0^* jest pierwotny, więc $st(g) > 0$ i $st(h) > 0$. Ale $st(f_0^*) = st(g) + st(h)$, więc $st(g) < n$ i $st(h) < n$. Z minimalności n wynika, że $g = w_1 \dots w_s$ oraz $h = u_1 \dots u_r$ dla pewnych wielomianów $w_1, \dots, w_s, u_1, \dots, u_r$ nierozkładalnych w $P[x]$. Stąd $f_0^* = w_1 \dots w_s u_1 \dots u_r$ i mamy sprzeczność. Zatem każdy niezerowy element nieodwracalny pierścienia $P[x]$ jest iloczynem skończonej liczby elementów nierozkładalnych tego pierścienia.

Pozostaje wykazać, że każdy element f nierozkładalny w $P[x]$ jest elementem pierwszym tego pierścienia. Jeśli $st(f) = 0$, to $f \in P$ i z lematu 12.9, f jest elementem nierozkładalnym w P. Ale P jest dziedziną z jednoznacznością rozkładu, więc f jest elementem pierwszym w P. Zatem z lematu 12.4, f jest elementem pierwszym w $P[x]$. Niech dalej $st(f) > 0$. Wtedy f jest wielomianem pierwotnym w $P[x]$. Zatem z lematu 12.7, f jest elementem nierozkładalnym w pierścieniu $K[x]$, gdzie K jest ciałem ułamków pierścienia P. Ale z algebry ogólnej I wiemy, że $K[x]$ jest dziedziną z jednoznacznością rozkładu, więc f jest elementem pierwszym pierścienia $K[x]$. Weźmy dowolne $g, h \in P[x]$

takie, że $f \mid gh$ w $P[x]$. Wtedy $f \mid gh$ w $K[x]$, więc $f \mid g$ lub $f \mid h$ w $K[x]$. Z lematu 12.6 mamy zatem, że $f \mid g$ lub $f \mid h$ w $P[x]$. Stąd f jest elementem pierwszym w pierścieniu $P[x]$. □

Z twierdzenia 12.10 przez prostą indukcję uzyskujemy natychmiast następujący

Wniosek 12.11. *Jeżeli P jest dziedziną z jednoznacznością rozkładu, to dla każdego $n \in \mathbb{N}$ pierścień $P[x_1, \ldots, x_n]$ wielomianów n-zmiennych o współczynnikach z P jest dziedziną z jednoznacznością rozkładu.*

Ponieważ każde ciało jest dziedziną z jednoznacznością rozkładu, więc z wniosku 12.11 wynika od razu następujący

Wniosek 12.12. *Dla dowolnego ciała K i dla dowolnego $n \in \mathbb{N}$ pierścień $K[x_1, \ldots, x_n]$ wielomianów n-zmiennych o współczynnikach z ciała K jest dziedziną z jednoznacznością rozkładu.*

Z algebry ogólnej I wiemy, że $\mathbb{Z}$ jest dziedziną z jednoznacznością rozkładu. Zatem z wniosku 12.11 otrzymujemy też

Wniosek 12.13. *Dla dowolnego $n \in \mathbb{N}$ pierścień $\mathbb{Z}[x_1, \ldots, x_n]$ wielomianów n-zmiennych o współczynnikach całkowitych jest dziedziną z jednoznacznością rozkładu.*

12.3 Wielomiany nierozkładalne

Stwierdzenie 12.14. *Niech a będzie dowolnym elementem dziedziny całkowitości A. Wówczas wielomian $x + a$ jest elementem pierwszym w pierścieniu $A[x]$.*

Dowód. Oczywiście $x \neq 0$ oraz $x \notin A[x]^*$, gdyż $(A[x])^* = A^*$. Weźmy dowolne $f, g \in A[x]$ takie, że $(x + a) \mid fg$ w pierścieniu $A[x]$. Wtedy z twierdzenia Bezout, $(fg)(-a) = 0$, a więc $0 = f(-a) \cdot g(-a)$. Ale A jest dziedziną całkowitości, więc $f(-a) = 0$ lub $g(-a) = 0$ i wobec tego $(x + a) \mid f$ lub $(x + a) \mid g$. Zatem $x + a$ jest elementem pierwszym w pierścieniu $A[x]$. □

Twierdzenie 12.15 (Eisensteina)**.** *Niech P będzie dziedziną z jednoznacznością rozkładu, niech K będzie ciałem ułamków pierścienia P i niech*

$$f = a_0 + a_1 x + \ldots + a_n x^n \in P[x], \quad n \geqslant 1.$$

Jeśli istnieje taki element nierozkładalny $p \in P$, że $p \nmid a_n$, $p \mid a_i$ dla $i = 0, 1, \ldots, n-1$ oraz $p^2 \nmid a_0$, to wielomian f jest nierozkładalny w $K[x]$ (i w $P[x]$, o ile wielomian f jest pierwotny).

Dowód. Niech $a \sim NWD(a_0, a_1, \ldots, a_n)$. Wtedy $b_i = \frac{a_i}{a} \in P$ dla $i = 0, 1, \ldots, n$ oraz ze stwierdzenia 10.21, $1 \sim NWD(b_0, b_1, \ldots, b_n)$. Zatem $f = a \cdot f^*$, gdzie $f^* = b_0 + b_1 x + \ldots + b_n x^n$. Ale $p \nmid a_n$, więc $p \nmid a$ i wobec tego $p \mid b_i$ dla $i = 0, 1, \ldots, n-1$, $p \nmid b_n$ i $p^2 \nmid b_0$. Ponadto wielomian f^* jest pierwotny. Załóżmy, że wielomian f jest rozkładalny w $K[x]$. Wtedy wielomian f^* też jest rozkładalny w $K[x]$, więc z lematu 12.7 istnieją wielomiany $g_1, g_2 \in P[x]$ dodatnich stopni takie, że $f^* = g_1 \cdot g_2$. Ponieważ p jest elementem pierwszym w pierścieniu P, więc $L = P/(p)$ jest dziedziną całkowitości. Niech $\pi\colon P \to L$ będzie homomorfizmem naturalnym i niech $\Pi\colon P[x] \to L[x]$ będzie indukowanym homomorfizmem pierścienia $P[x]$ na pierścień $L[x]$. Ponieważ $p \mid b_i$ dla $i = 0, 1, \ldots, n-1$, więc $\Pi(f^*) = \pi(b_n)x^n$. Dalej, $\pi(b_n) \neq 0$, gdyż $p \nmid b_n$. Ponadto $\Pi(f^*) = \Pi(g_1) \cdot \Pi(g_2)$, przy czym $st(\Pi(g_i)) < n$ dla $i = 1, 2$, więc ze stwierdzenia 12.14 $x \mid \Pi(g_i)$ dla $i = 1, 2$ w pierścieniu $L[x]$. Stąd $(\Pi(g_i))(0) = 0$ dla $i = 1, 2$ i wobec tego $p \mid g_i(0)$ dla $i = 1, 2$. Zatem $p^2 \mid g_1(0) \cdot g_2(0)$. Ale $g_1(0) \cdot g_2(0) = f^*(0) = b_0$, więc $p^2 \mid b_0$ i mamy sprzeczność.

Stąd wielomian f jest nierozkładalny w pierścieniu $K[x]$. Jeśli dodatkowo wielomian f jest pierwotny, to ze stwierdzenia 12.8 f jest nierozkładalny także w pierścieniu $P[x]$. □

Przykład 12.16. Pokażemy, że dla dowolnej liczby pierwszej p i dla dowolnej nieujemnej liczby całkowitej k wielomian $f_k = x^{p^k(p-1)} + x^{p^k(p-2)} + \ldots + x^{p^k} + 1$ jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$. Niech $f = x^{p-1} + x^{p-2} + \ldots + x + 1$. Wtedy $f_k = f(x^{p^k})$ dla $k \in \mathbb{N}_0$. Z algebry I wiemy, że dla dowolnego ustalonego wielomianu $h \in \mathbb{Q}[x]$ przekształcenie $w \mapsto w(h)$ jest endomorfizmem pierścienia $\mathbb{Q}[x]$. Ponadto przekształcenia $w \mapsto w(x+1)$ i $w \mapsto w(x-1)$ są wzajemnie

odwrotne, więc są one automorfizmami tego pierścienia. Ponieważ automorfizm pierścieni zachowuje własność bycia elementem nierozkładalnym, więc wystarczy wykazać, że $g_k = f_k(x+1)$ jest wielomianem nierozkładalnym w $\mathbb{Q}[x]$ dla dowolnego $k \in \mathbb{N}_0$. Ale $f = \frac{x^p-1}{x-1}$, więc $f(x+1) = \frac{(x+1)^p-1}{x} = x^{p-1} + \sum_{i=1}^{p-2} \binom{p}{i} x^{p-1-i} + p$. Z elementarnej teorii liczb wiemy, że $p \mid \binom{p}{i}$ dla każdego $i = 1, \ldots, p-1$. Zatem z kryterium Eisensteina wielomian $f(x+1)$ jest nierozkładalny w $\mathbb{Q}[x]$. Stąd wielomian $f = f_0$ jest nierozkładalny w $\mathbb{Q}[x]$. Niech dalej $k \geqslant 1$. Z dowodu lematu 2.1 wynika, że $(x+1)^{p^k} = x^{p^k} + p\varphi + 1$ dla pewnego wielomianu $\varphi \in \mathbb{Z}[x]$ stopnia $< p^k$ takiego, że $\varphi(0) = 0$. Zatem $g_k = f_k(x+1) = f((x+1)^{p^k}) = f(x^{p^k} + p\varphi + 1) = (x^{p^k} + p\varphi)^{p-1} + \sum_{i=1}^{p-2} \binom{p}{i} (x^{p^k} + p\varphi)^{p-1-i} + p$. Stąd wszystkie współczynniki wielomianu g_k są całkowite i jego najstarszy współczynnik jest równy 1, zaś wyraz wolny jest równy p. Ponadto wszystkie współczynniki tego wielomianu za wyjątkiem najstarszego są podzielne przez p. Zatem z kryterium Eisensteina wielomian $g_k = f_k(x+1)$ jest nierozkładalny w $\mathbb{Q}[x]$. Stąd zaś wynika, że wielomian f_k jest nierozkładalny w $\mathbb{Q}[x]$.

Rozdział 13

Rozszerzenia ciał

13.1 Pochodna wielomianu

Podstawowe pojęcia i własności związane z ciałami i rozszerzeniami algebraicznymi ciał zostały podane w kursie algebry I.

Definicja 13.1. Niech K będzie ciałem oraz $f = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in K[x]$. Wtedy $f' = a_1 + 2a_2x + ... + na_nx^{n-1}$ nazywamy **pochodną wielomianu** f.

Lemat 13.2. *Niech K będzie ciałem i $f, f_1, \ldots, f_n, g \in K[x]$ oraz $c \in K$. Wtedy:*
(i) $(f_1 + \ldots + f_n)' = f_1' + \ldots + f_n'$,
(ii) $(cf)' = cf'$,
(iii) $(fg)' = f'g + fg'$,
(iv) $(f^n)' = nf^{n-1} \cdot f'$, *dla* $n = 1, 2, \ldots$,
(v) $(f \circ g)' = (f' \circ g) \cdot g'$.

Dowód. (i). Niech $f = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ i $g = b_0 + b_1x + b_2x^2 + \ldots + b_mx^m$. Bez zmniejszenia ogólności można przyjąć, że $m \geqslant n$. Wtedy $(f + g)' = (a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + b_0 + b_1x + b_2x^2 + \ldots + b_mx^m)' = (a_0 + b_0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \ldots + b_mx^m)' = a_1 + b_1 + 2(a_2 + b_2)x + \ldots + n(a_n + b_n)x^{n-1} + (n + 1)b_{n+1}x^n + \ldots + mb_mx^{m-1} = (a_1 + 2a_2x + \ldots + na_nx^{n-1}) + (b_1 + 2b_2x + \ldots + mb_mx^{m-1}) = f' + g'$.

Załóżmy teraz, że dla dowolnych $f_1, \ldots, f_n \in K[x]$ zachodzi wzór $(f_1 + \ldots + f_n)' = f_1' + \ldots + f_n'$. Weźmy dowolne $f_1, \ldots, f_n, f_{n+1} \in K[x]$. Wówczas z założenia oraz z pierwszej części dowodu mamy $(f_1 + \ldots + f_n + f_{n+1})' = ((f_1 + \ldots + f_n) + f_{n+1})' = (f_1 + \ldots + f_n)' + f_{n+1}' = f_1' + \ldots + f_n' + f_{n+1}'$.

(ii). Niech $f = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n$. Wówczas $(cf)' = (ca_0 + ca_1 x + ca_2 x^2 + ... + ca_n x^n)' = ca_1 + c2a_2 x + ... + cna_n x^{n-1} = c(a_1 + 2a_2 x + ... + na_n x^{n-1}) = cf'$.

(iii). Niech $f = \sum_{i=0}^{r} a_i x^i$, $g = \sum_{j=0}^{s} b_j x^j$. Wtedy $fg = \sum_{i=0}^{r} \sum_{j=0}^{s} a_i b_j x^{i+j}$. Korzystając z podpunktu (i)

$$(fg)' = \sum_{i=0}^{r} \sum_{j=0}^{s} (a_i b_j x^{i+j})' = \sum_{i=0}^{r} \sum_{j=0}^{s} (i+j) a_i b_j x^{i+j-1}$$
$$= \sum_{i=0}^{r} i a_i x^{i-1} \sum_{j=0}^{s} b_j x^j + \sum_{i=0}^{r} a_i x^i \sum_{j=0}^{s} j b_j x^{j-1} = f'g + fg'.$$

(iv). Zastosujemy indukcję ze względu na n. Dla $n = 1$ wzór jest prawdziwy. Załóżmy prawdziwość wzoru dla liczby naturalnej $n - 1$. Wówczas wykorzystując wzór (iii) oraz założenie mamy $(f^n)' = (f^{n-1} \cdot f)' = (f^{n-1})' \cdot f + f^{n-1} \cdot f' = (n-1) f^{n-2} \cdot f' \cdot f + f^{n-1} \cdot f' = (n-1) f^{n-1} \cdot f' + f^{n-1} \cdot f' = n f^{n-1} \cdot f'$.

(v). Zastosujemy indukcję ze względu na stopień wielomianu f. Jeżeli $f = c$ jest stały, to $f \circ g$ jest stały i obie strony wzoru (v) są równe 0. Niech zatem $n = st(f) > 0$ i załóżmy, że wzór jest prawdziwy dla wielomianów stopni mniejszych niż n. Otrzymujemy więc $f = a_n x^n + f_1$, gdzie $st(f_1) < n$. Stąd $f' = n a_n x^{n-1} + f_1'$. Wobec tego $f \circ g = a_n g^n + f_1 \circ g$ oraz $f' \circ g = n a_n g^{n-1} + f_1' \circ g$. Zatem na mocy wzorów $(i), (ii), (iv)$ i założenia indukcyjnego otrzymujemy: $(f \circ g)' = (a_n g^n + f_1 \circ g)' = a_n (g^n)' + (f_1 \circ g)' = n a_n g^{n-1} \cdot g' + (f_1' \circ g) \cdot g' = (n a_n g^{n-1} + f_1' \circ g) \cdot g' = (f' \circ g) \cdot g'$. □

Stwierdzenie 13.3. *Jeżeli $f \in K[x]$ oraz wielomiany f i f' są względnie pierwsze, to wielomian f nie posiada pierwiastków wielokrotnych w żadnym rozszerzeniu ciała K.*

Dowód. Załóżmy, że w pewnym rozszerzeniu L ciała K wielomian f posiada pierwiastek wielokrotny a. Wtedy istnieje $h \in L[x]$ taki, że $f = (x-a)^2 h$. Zatem z lematu 13.2, $f' = 2(x-a)h + (x-a)^2 h'$, skąd $f'(a) = 0$. Ale wielomiany f i f' są względnie pierwsze, więc istnieją $u, v \in K[x]$ takie, że $uf + vf' = 1$. Zatem $1 = u(a)f(a) + v(a)f'(a) = 0$ i mamy sprzeczność. □

Wniosek 13.4. *Jeżeli K jest ciałem charakterystyki zero i wielomian $f \in K[x]$ jest nierozkładalny, to f nie posiada pierwiastków wielokrotnych w żadnym rozszerzeniu ciała K.*

Dowód. Niech $n = st(f)$ i niech a będzie najstarszym współczynnikiem f. Wtedy $a \neq 0$ i $ch(K) = 0$, więc $na \neq 0$. Zatem na jest najstarszym współczynnikiem wielomianu f' i wobec tego $f' \neq 0$ oraz $st(f') = n - 1 < st(f)$. Ponadto wielomian f jest nierokładalny, więc wielomiany f i f' są względnie pierwsze. Zatem na mocy stwierdzenia 13.3 wielomian f nie posiada pierwiastków wielokrotnych. □

Przykład 13.5. Niech K będzie ciałem charakterystyki zero i niech L będzie dowolnym rozszerzeniem ciała K. Udowodnimy, że dla każdego $n \in \mathbb{N}$ i dla dowolnego $0 \neq a \in K$ wielomian $f = x^n - a$ nie posiada pierwiastków wielokrotnych w ciele L. Zauważmy, że $f' = nx^{n-1}$ oraz $\frac{1}{n} \in K$, gdyż $ch(K) = 0$. Ponadto $\frac{1}{n} x f' - f = a$ i $a \neq 0$, więc wielomiany f i f' są względnie pierwsze. Zatem ze stwierdzenia 13.3 wielomian f nie posiada pierwiastków wielokrotnych w L.

13.2 Twierdzenie Abela

Lemat 13.6. *Jeżeli ciało L jest rozszerzeniem nieskończonego ciała K i wielomiany $F, G \in L[x]$ są takie, że $F(0) \neq 0$, $G \neq 0$, to istnieje element $d \in K^*$ taki, że wielomiany F i $G(dx)$ są względnie pierwsze w $L[x]$.*

Dowód. Jeżeli $st(G) = 0$ lub $st(F) = 0$, to F lub G jest odwracalny i wystarczy przyjąć $d = 1$. Załóżmy więc, że $st(G) \geqslant 1$ i $st(F) \geqslant 1$. Bez zmniejszenia ogólności można przyjąć, że wielomiany F i G są

unormowane. Z algebry I wynika, że istnieją nierozkładalne wielomiany unormowane $F_1, F_2, \ldots, F_t, G_1, G_2, \ldots, G_u \in L[x]$ takie, że $F = F_1 \cdot F_2 \cdot \ldots \cdot F_t$ i $G = G_1 \cdot G_2 \cdot \ldots \cdot G_u$. Mamy więc:

$$F_i(x) = a_{i0} + a_{i1}x + \ldots + x^{r_i} \quad \text{dla} \quad i = 1, 2, \ldots, t,$$

$$G_j(x) = b_{j0} + b_{j1}x + \ldots + x^{s_j} \quad \text{dla} \quad j = 1, 2, \ldots, u,$$

gdzie $r_i, s_j \in \mathbb{N}$. Ponieważ $F(0) \neq 0$, więc $0 \neq F_1(0) \ldots F_t(0) = a_{10} \ldots a_{t0}$ i stąd $a_{i0} \neq 0$ dla $i = 1, 2, \ldots, t$.

Aby wielomiany F i G były względnie pierwsze wystarczy tak dobrać element $d \in K$ by żadne dwa wielomiany F_i i $G_j(dx)$ nie były stowarzyszone. Gdyby F_i i $G_j(dx)$ były stowarzyszone, to dla pewnego niezerowego $\alpha \in L$: $a_{i0} + a_{i1}x + \ldots + x^{r_i} = \alpha(b_{j0} + b_{j1}dx + \ldots + (dx)^{s_j})$, skąd $r_i = s_j$, $1 = \alpha \cdot d^{s_j}$ oraz $a_{i0} = \alpha \cdot b_{j0}$, więc $\frac{b_{j0}}{a_{i0}} = d^{s_j}$. Ponieważ ciało K jest nieskończone i wielomiany $x^{s_j} - \frac{b_{j0}}{a_{i0}}$ dla $i = 1, \ldots, t$, $j = 1, \ldots, u$ mają w ciele L skończenie wiele wszystkich pierwiastków, więc można tak dobrać $d \in K^*$ by dla żadnej pary indeksów i, j, których jest skończona ilość, nie zachodziła równość $\frac{b_{j0}}{a_{i0}} = d^{s_j}$. Wtedy wielomiany F_i i $G_j(dx)$ nie będą stowarzyszone, a więc wielomiany F i $G(dx)$ będą względnie pierwsze. □

Twierdzenie 13.7 (Abel)**.** *Niech elementy a, b rozszerzenia L ciała K charakterystyki zero, będą algebraiczne względem K. Wtedy istnieje element $c \in L$ algebraiczny względem K taki, że $K(a, b) = K(c)$.*

Dowód. Z założenia mamy, że K jest ciałem nieskończonym. Niech $f, g \in K[x]$ będą wielomianami minimalnymi odpowiednio dla elementów a i b. Z wniosku 13.4 wiadomo, że element a jest pierwiastkiem jednokrotnym wielomianu f. Wtedy $f = (x-a)f_1$, gdzie $f_1 \in K(a)[x]$ oraz $f_1(a) \neq 0$. Niech $F = f_1(x + a)$, $G = g(x + b)$, gdzie $F, G \in K(a, b)[x]$ oraz $F(0) = f_1(a) \neq 0$ i $G \neq 0$. Spełnione są zatem założenia lematu 13.6. Istnieje więc element $d \in K^*$ taki, że wielomiany F i $G(dx)$ są względnie pierwsze. Zatem istnieją wielomiany $w, v \in K(a, b)[x]$ dla których:

$$wF + vG(dx) = 1,$$

i wracając do podstawień mamy:

$$wf_1(x+a) + vg(dx+b) = 1. \tag{13.1}$$

Podstawiając w równaniu (13.1) w miejsce x dwumian $x-a$ i oznaczając $h = g(dx - da + b) \in K(a,b)[x]$, otrzymujemy:

$$w(x-a)f_1 + v(x-a)h = 1. \tag{13.2}$$

Ponieważ $h(a) = g(da-da+b) = g(b) = 0$, więc h jest podzielny w pierścieniu $K(a,b)[x]$ przez $x-a$. Ze wzoru (13.2) wynika, że w pierścieniu $K(a,b)[x]$: $1 \sim NWD(f_1, h)$. Ponadto $f = (x-a)f_1$, więc w pierścieniu $K(a,b)[x]$: $x - a \sim NWD(f,h)$.

Weźmy element $c = -da+b$. Oczywiście $c \in K(a,b)$, a stąd $K(c) \subseteq K(a,b)$. Ponadto $h = g(dx+c) \in K(c)[x]$ oraz $f \in K[x] \subseteq K(c)[x]$ i istnieje wielomian unormowany $\varphi \in K(c)[x]$ taki, że $\varphi \sim NWD(f,h)$ w pierścieniu $K(c)[x]$, więc $\varphi \mid x-a$ w pierścieniu $K(a,b)[x]$. Stąd $\varphi = 1$ lub $\varphi \sim (x-a)$. Jednak w pierwszym przypadku otrzymamy sprzeczność z tym, że $x - a \sim NWD(f,h)$ w pierścieniu $K(a,b)[x]$, więc $\varphi = \alpha(x-a)$ dla pewnego $\alpha \in K(a,b)$. Ale wielomian φ jest unormowany, więc $\alpha = 1$ i $\varphi = x - a \in K(c)[x]$, skąd $a \in K(c)$. Zatem $b = da + c \in K(c)$ i wobec tego $K(a,b) \subseteq K(c)$. Stąd ostatecznie otrzymujemy $K(a,b) = K(c)$. □

Twierdzenie 13.8. *Niech elementy $a_1, ..., a_n$ rozszerzenia L ciała K charakterystyki zero będą algebraiczne względem K. Wtedy istnieje element $c \in L$ algebraiczny względem K i taki, że $K(c) = K(a_1, ..., a_n)$.*

Dowód. Zastosujemy indukcję względem n. Dla $n = 1$ twierdzenie jest prawdziwe. Załóżmy prawdziwość twierdzenia dla liczb naturalnych mniejszych od n. Na mocy założenia indukcyjnego istnieje taki element $a \in K(a_1, ..., a_{n-1})$ algebraiczny względem ciała K, że $K(a_1, ..., a_{n-1}) = K(a)$. Wtedy $K(a_1, ..., a_n) = K(a, a_n)$. Z twierdzenia 13.7 wynika, że istnieje element $c \in K(a_1, ..., a_n)$ algebraiczny względem ciała K taki, że $K(a, a_n) = K(c)$. Stąd ostatecznie otrzymujemy, że $K(a_1, ..., a_n) = K(c)$. □

13.3 Ciało rozkładu wielomianu

Definicja 13.9. *Niech K będzie podciałem ciała L i niech K_1 będzie podciałem ciała L_1. Niech $f\colon K \to K_1$ i $F\colon L \to L_1$ będą izomorfizmami ciał. Mówimy, że F jest* **przedłużeniem izomorfizmu** *f, jeżeli $F(a) = f(a)$ dla każdego $a \in K$.*

Lemat 13.10. *Niech $f\colon K \to K_1$ będzie izomorfizmem ciał i niech K będzie podciałem ciała L. Wówczas istnieje ciało L_1 izomorficzne z L i będące rozszerzeniem ciała K_1 oraz istnieje izomorfizm $F\colon L \to L_1$ będący przedłużeniem izomorfizmu f.*

Dowód. Jeśli $K = L$, to wystarczy przyjąć $L_1 = K_1$ i $F = f$. Niech dalej $K \neq L$. Wtedy $M = L \setminus K \neq \emptyset$. Z teorii mnogości wiadomo, że istnieje wówczas zbiór M_1 rozłączny z K_1 przy czym zbiór M_1 jest równoliczny ze zbiorem M. Niech $g\colon M \to M_1$ będzie bijekcją zbioru M na zbiór M_1. Określamy odwzorowanie $F\colon L \to K_1 \cup M_1$ w ten sposób, że $F(x) = f(x)$ dla $x \in K$ oraz $F(x) = g(x)$ dla $x \in M$. Wówczas F jest bijekcją. W zbiorze $L_1 = K_1 \cup M_1$ wprowadzamy teraz dodawanie i mnożenie wzorami:

$$F(x) + F(y) = F(x + y), \qquad F(x) \cdot F(y) = F(x \cdot y). \tag{13.3}$$

Proste sprawdzenie pokazuje, że L_1 z tymi działaniami tworzy ciało oraz $F\colon L \to L_1$ jest izomorfizmem ciał, przy czym dla $a \in K$ mamy $F(a) = f(a)$. Zatem $K_1 = F(K)$ jest podciałem w L_1 oraz F jest przedłużeniem izomorfizmu f. □

Lemat 13.11. *Niech K będzie ciałem. Wówczas dla każdego wielomianu nierozkładalnego $w \in K[x]$ istnieje ciało L zawierające K jako podciało i takie, że wielomian w ma pierwiastek w ciele L.*

Dowód. Ponieważ $K[x]$ jest dziedziną ideałów głównych i wielomian w jest nierozkładalny w $K[x]$, więc z algebry I, $I = (w)$ jest ideałem maksymalnym pierścienia $K[x]$. Zatem pierścień ilorazowy $L_1 = K[x]/I$ jest ciałem i każdy jego element można zapisać jednoznacznie w postaci $(c_0 + c_1x + \ldots + c_{n-1}x^{n-1}) + I$, gdzie $n = st(w)$ oraz $c_0, c_1, \ldots, c_{n-1} \in K$.

Stąd odwzorowanie $h\colon K \to L$ dane wzorem $h(a) = a + I$ jest zanurzeniem pierścieni i wobec tego $h(K) = \{a + I : a \in K\} = K_1$ jest podciałem ciała L_1, przy czym $f\colon K_1 \to K$ dane wzorem $f(a+I) = a$ dla $a \in K$ jest izomorfizmem ciał. Z lematu 13.10 istnieje ciało L zawierające K jako podciało oraz istnieje izomorfizm ciał $F\colon L_1 \to L$ będący przedłużeniem izomorfizmu f. Ponadto $w = a_0 + a_1x + \ldots + a_nx^n$ dla pewnych $a_0, a_1, \ldots, a_n \in K$. Oznaczmy $\alpha = F(x + I)$. Wtedy $\alpha \in L$ oraz $w(\alpha) = a_0 + a_1F(x+I) + \ldots + a_n[F(x+I)]^n = F(a_0+I) + F(a_1 + I)F(x+I) + \ldots + F(a_n+I)F(x^n+I) = F((a_0 + a_1x + \ldots + a_nx^n) + I)$. Ale $a_0 + a_1x + \ldots + a_nx^n = w \in I = (w)$, więc $(a_0 + a_1x + \ldots + a_nx^n) + I$ jest zerem pierścienia ilorazowego $K[x]/I$ i wobec tego $F((a_0 + a_1x + \ldots + a_nx^n) + I) = 0$. Zatem $w(\alpha) = 0$. □

Twierdzenie 13.12. *Niech K będzie dowolnym ciałem. Wówczas dla dowolnego wielomianu $w \in K[x]$ dodatniego stopnia n o najstarszym współczynniku a istnieje ciało L zawierające K jako podciało oraz istnieją $a_1, a_2, \ldots, a_n \in L$ takie, że $w = a(x - a_1)(x - a_2)\ldots(x - a_n)$.*

Dowód. Stosujemy indukcję względem n. Dla $n = 1$ teza jest oczywista, bo wtedy $w = ax + b = a(x + \frac{b}{a})$ i wystarczy przyjąć $L = K$ oraz $a_1 = -\frac{b}{a}$. Załóżmy, że teza zachodzi dla dowolnego ciała i dla wielomianów dodatnich stopni mniejszych od n, gdzie $n > 1$ jest ustaloną liczbą naturalną. Niech $w \in K[x]$ będzie dowolnym wielomianem stopnia n. Wówczas z algebry I wiemy, że istnieje wielomian nierozkładalny $u \in K[x]$ taki, że $u \mid w$. Zatem $w = uh$ dla pewnego $h \in K[x]$. Z lematu 13.11 istnieje ciało L zawierające ciało K jako podciało oraz istnieje $\alpha \in L$ takie, że $u(\alpha) = 0$. Stąd $w(\alpha) = u(\alpha)\cdot h(\alpha) = 0 \cdot h(\alpha) = 0$. Zatem z twierdzenia Bezout istnieje $w_1 \in L[x]$ taki, że $w = (x - \alpha)w_1$. Stąd $st(w_1) = n - 1$ i z założenia indukcyjnego istnieje ciało M zawierające L jako podciało oraz istnieją $a_1, \ldots, a_{n-1} \in M$ takie, że $w_1 = a(x - a_1)\cdot \ldots \cdot (x - a_{n-1})$, gdzie a jest najstarszym współczynnikiem wielomianu w_1. Ale $w = (x - \alpha)w_1$, więc a jest najstarszym współczynnikiem wielomianu w oraz K jest podciałem ciała M i $w = a(x - a_1) \cdot \ldots \cdot (x - a_{n-1}) \cdot (x - a_n)$ dla $a_n = \alpha$. □

Definicja 13.13. Niech K będzie ciałem i $f \in K[x]$ dowolnym wielomianem dodatniego stopnia. Jeżeli L jest rozszerzeniem ciała K, w którym wielomian f rozkłada się na czynniki liniowe:

$$f = a(x - a_1)(x - a_2)...(x - a_n),$$

to ciało $K(a_1, a_2, ..., a_n) \subseteq L$ nazywamy **ciałem rozkładu wielomianu** $f \in K[x]$.

Stwierdzenie 13.14. *Jeżeli L jest ciałem rozkładu wielomianu $f = x^n - 1 \in K[x]$ i $ch(K) = 0$, to grupa $U_n = \{a \in L : a^n = 1\}$ jest cykliczna i ma dokładnie n - elementów. Jeśli ε jest generatorem tej grupy, to $L = K(\varepsilon)$.*

Dowód. Z algebry I wiemy, że wielomian $f = x^n - 1$ może mieć co najwyżej n pierwiastków. Zatem grupa U_n jest skończona i na mocy twierdzenia 6.22 jest cykliczna. Ponadto z przykładu 13.5 wielomian f nie posiada pierwiastków wielokrotnych, więc ten wielomian ma w L dokładnie n różnych pierwiastków. Stąd $|U_n| = n$ i $U_n = \{1, \varepsilon, \ldots, \varepsilon^{n-1}\}$. Wobec tego $L = K(\varepsilon)$. □

Stwierdzenie 13.15. *Jeżeli L jest ciałem rozkładu wielomianu $f = x^n - a \in K[x]$, $a \neq 0$ i $ch(K) = 0$, to w grupie L^* istnieje element ε rzędu n. Ponadto $K(\varepsilon)$ jest ciałem rozkładu wielomianu $x^n - 1 \in K[x]$ i $L = (K(\varepsilon))(b)$ dla dowolnego $b \in L$ takiego, że $b^n = a$ oraz $(L : K(\varepsilon)) \leqslant n$.*

Dowód. Z przykładu 13.5 wielomian $f = x^n - a$ nie posiada pierwiastków wielokrotnych, więc ten wielomian ma w L dokładnie n różnych pierwiastków $b = b_1, b_2, \ldots, b_n \in L$. Ale $a \neq 0$, więc $b \neq 0$ i wobec tego $\frac{b_1}{b}, \frac{b_2}{b}, \ldots, \frac{b_n}{b} \in L$ są parami różnymi elementami grupy $U_n = \{c \in L : c^n = 1\}$. Ale na mocy twierdzenia 6.22 grupa U_n jest cykliczna i $|U_n| = n$, więc istnieje w niej element ε rzędu n oraz $K(\varepsilon)$ jest ciałem rozkładu wielomianu $x^n - 1 \in K[x]$. Stąd wszystkimi pierwiastkami wielomianu $x^n - a \in K[x]$ w ciele L są: $b, b\varepsilon, \ldots, b\varepsilon^{n-1}$. Zatem $L = (K(\varepsilon))(b)$ i wobec tego $(L : K(\varepsilon)) \leqslant n$. □

Przykład 13.16. Niech L będzie ciałem rozkładu wielomianu $f = x^4 - 2$ nad ciałem $\mathbb{Q}$. Pierwiastkami wielomianu f są liczby: $\pm\sqrt[4]{2}$, $\pm\sqrt[4]{2}i$. Zatem L ma postać $L = \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i) = \mathbb{Q}(\sqrt[4]{2}, i)$. Istotnie, $\pm\sqrt[4]{2}i, \pm\sqrt[4]{2} \in \mathbb{Q}(\sqrt[4]{2}, i)$, oraz $i = (\sqrt[4]{2})^3 \cdot \frac{\sqrt[4]{2}i}{2}$, $\sqrt[4]{2} \in \mathbb{Q}(\pm\sqrt[4]{2}, \pm\sqrt[4]{2}i)$. Ponieważ $\sqrt[4]{2}$ oraz i są liczbami algebraicznymi, więc wzorując się na dowodach twierdzenia 13.7 i lematu 13.6 poszukamy liczby c algebraicznej względem ciała $\mathbb{Q}$ takiej, że $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(c)$. Wielomianami minimalnymi elementów $\sqrt[4]{2}$ oraz i są odpowiednio $f = x^4 - 2$, $g = x^2 + 1$. Ale $f = (x^2 - \sqrt{2})(x^2 + \sqrt{2}) = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$ i $g = (x + i)(x - i)$, więc $f_1 = (x + \sqrt[4]{2})(x - \sqrt[4]{2}i)(x + \sqrt[4]{2}i)$, skąd $F = f_1(x + \sqrt[4]{2}) = (x + 2\sqrt[4]{2})(x + \sqrt[4]{2} - \sqrt[4]{2}i)(x + \sqrt[4]{2} + \sqrt[4]{2}i)$ oraz $G = g(x + i) = (x + 2i)x$. Stąd widać, że dla dowolnej niezerowej liczby wymiernej d wielomiany dx i $x + 2\sqrt[4]{2}$, dx i $x + \sqrt[4]{2} - \sqrt[4]{2}i$, dx i $x + \sqrt[4]{2} + \sqrt[4]{2}i$ oraz $dx + 2i$ i $x + 2\sqrt[4]{2}$, $dx + 2i$ i $x + \sqrt[4]{2} - \sqrt[4]{2}i$, $dx + 2i$ i $x + \sqrt[4]{2} + \sqrt[4]{2}i$ są względnie pierwsze. Na mocy dowodu twierdzenia 13.7 mamy zatem, że $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2} \cdot q + i)$ dla każdego $q \in \mathbb{Q} \setminus \{0\}$ i w szczególności dla $q = 1$, $\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2} + i)$.

Jeśli $\varphi : K \to L$ jest izomorfizmem ciał oraz $f = a_0 + a_1x + ... + a_nx^n \in K[x]$, to przez $\varphi(f)$ będziemy oznaczali wielomian $\varphi(f) = \varphi(a_0) + \varphi(a_1)x + ... + \varphi(a_n)x^n \in L[x]$. Z algebry I wiemy, że przekształcenie $w \mapsto \varphi(w)$ dla $w \in K[x]$, jest izomorfizmem pierścienia $K[x]$ na pierścień $L[x]$.

Twierdzenie 13.17. *Jeżeli $\varphi : K \to L$ jest izomorfizmem ciał, element a jest pierwiastkiem nierozkładalnego wielomianu $f \in K[x]$ oraz b jest pierwiastkiem wielomianu $\varphi(f) \in L[x]$, to φ można rozszerzyć do izomorfizmu $\psi : K(a) \to L(b)$ takiego, że $\psi(a) = b$.*

Dowód. Na algebry I wiemy, że każdy element $c \in K(a)$ można jednoznacznie przedstawić w postaci $c = a_0 + a_1a + ... + a_{n-1}a^{n-1}$ oraz element $d \in L(b)$ w postaci $d = b_0 + b_1b + ... + b_{n-1}b^{n-1}$, gdzie $a_0, a_1, ..., a_{n-1} \in K$, $b_0, b_1, ..., b_{n-1} \in L$ i $n = st(f)$. Określmy odwzorowanie $\psi : K(a) \to L(b)$ wzorem:

$$\psi(a_0 + a_1a + ... + a_{n-1}a^{n-1}) = \varphi(a_0) + \varphi(a_1)b + ... + \varphi(a_{n-1})b^{n-1}.$$

Z określenia odwzorowania ψ wynika, że $\psi(a) = b$, $\psi(K(a)) = L(b)$ oraz ψ jest różnowartościowe. Ponadto $\psi|_K = \varphi$ oraz $\psi(\alpha + \beta) = \psi(\alpha) + \psi(\beta)$ dla wszystkich $\alpha, \beta \in K(a)$.

Weźmy dowolne $\alpha, \beta \in K(a)$. Wtedy $\alpha = a_0 + a_1 a + \ldots a_{n-1}a^{n-1}$ oraz $\beta = b_0 + b_1 a + \ldots + b_{n-1}a^{n-1}$ dla pewnych $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in K$. Niech $g = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$ i $h = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$. Niech r będzie resztą z dzielenia wielomianu gh przez f. Wtedy istnieje $u \in K[x]$ taki, że $gh = fu + r$, gdzie $st(r) < n$. Otrzymujemy wówczas $\varphi(g)\varphi(h) = \varphi(f)\varphi(u) + \varphi(r)$. Ponieważ $f(a) = (\varphi(f))(b) = 0$, więc $g(a)h(a) = r(a)$ oraz $(\varphi(g))(b)(\varphi(h)(b) = (\varphi(r))(b)$. Stąd

$$\psi(\alpha\beta) = \psi(g(a)h(a)) = \psi(r(a)) = (\varphi(r))(b) = (\varphi(g))(b)(\varphi(h)(b) =$$

$$= \psi(g(a))\psi(h(a)) = \psi(\alpha)\psi(\beta).$$

Wobec tego odwzorowanie ψ jest izomorfizmem ciał. □

Jeżeli L i M są rozszerzeniami ciała K i izomorfizm $f\colon L \to M$ jest stały na K (tzn. $f(a) = a$ dla każdego $a \in K$), to mówimy, że f jest K-**izomorfizmem**. Z twierdzenia 13.17 wynika następujący

Wniosek 13.18. *Niech L będzie rozszerzeniem ciała K. Jeżeli $f \in K[x]$ jest wielomianem nierozkładalnym nad ciałem K, $a, b \in L$ są jego pierwiastkami, to istnieje K-izomorfizm $\varphi : K(a) \to K(b)$ spełniający warunek $\varphi(a) = b$.*

Twierdzenie 13.19. *Jeżeli $\varphi : K \to L$ jest izomorfizmem ciał, K_1 jest ciałem rozkładu wielomianu $f \in K[x]$, L_1 jest ciałem rozkładu wielomianu $\varphi(f) \in L[x]$, to istnieje taki izomorfizm $\tau : K_1 \to L_1$, który jest rozszerzeniem izomorfizmu φ.*

Dowód. Zastosujemy indukcję ze względu na stopień wielomianu f. Jeżeli $st(f) = 0$, to $st(\varphi(f)) = 0$ i $K = K_1$, $L = L_1$. Wtedy za τ wystarczy wziąć izomorfizm φ.

Niech zatem $st(f) = n > 0$ i załóżmy, że twierdzenie jest prawdziwe dla wielomianów stopni mniejszych od n należących do $K[x]$. Niech $f = a(x - a_1)(x - a_2)...(x - a_n)$ oraz $\varphi(f) = b(x - b_1)(x - b_2)...(x - b_n)$, wtedy $K_1 = K(a_1, a_2, ..., a_n)$ i $L_1 = L(b_1, b_2, ..., b_n)$. Niech $g \in K[x]$

będzie czynnikiem nierozkładalnym wielomianu f takim, że $g(a_1) = 0$. Wówczas wielomian $\varphi(g)$ jest czynnikiem nierozkładalnym wielomianu $\varphi(f)$. Przyjmijmy, że b_1 jest pierwiastkiem wielomianu $\varphi(g)$. Na mocy twierdzenia 13.17 istnieje izomorfizm $\varphi_1 : K(a_1) \to L(b_1)$ będący rozszerzeniem φ i taki, że $\varphi_1(a_1) = b_1$. Mamy

$$f = (x - a_1)h_1 \quad \text{i} \quad \varphi(f) = (x - b_1)h_2,$$

gdzie $h_1 \in K(a_1)[x]$, $h_2 \in L(b_1)[x]$. Ponieważ $\varphi_1(f) = \varphi(f)$ i $\varphi_1(x - a_1) = x - \varphi_1(a_1) = x - b_1$, więc $\varphi_1(h_1) = h_2$.

Ale $h_1 = a(x - a_2)...(x - a_n)$, więc ciało $K_1 = K(a_1, a_2, ..., a_n) = (K(a_1))(a_2, ..., a_n)$ jest ciałem rozkładu wielomianu $h_1 \in K(a_1)[x]$. Podobnie ciało $L_1 = L(b_1, b_2, ..., b_n) = (L(b_1))(b_2, ..., b_n)$ jest ciałem rozkładu $h_2 \in L(b_1)[x]$. Ponieważ $st(h_1) = st(f) - 1$, więc z założenia indukcyjnego wiemy, że istnieje izomorfizm $\tau : K_1 \to L_1$ będący rozszerzeniem izomorfizmu $\varphi_1 : K(a_1) \to L(b_1)$. □

Przyjmując w twierdzeniu 13.19 $L = K$ oraz za φ odwzorowanie tożsamościowe otrzymujemy

Wniosek 13.20. *Każde dwa ciała rozkładu wielomianu $f \in K[x]$ są K- izomorficzne.*

Wniosek 13.21. *Niech L będzie ciałem rozkładu wielomianu nierozkładalnego $f \in K[x]$. Jeżeli $a, b \in L$ są pierwiastkami f, to istnieje K-automorfizm σ ciała L taki, że $\sigma(a) = b$.*

Dowód. Z wniosku 13.18 istnieje K-izomorfizm ciał $\tau\colon K(a) \to K(b)$ taki, że $\tau(a) = b$. Zauważmy, że L jest ciałem rozkładu wielomianu f nad ciałami $K(a)$ i $K(b)$. Wobec tego z twierdzenia 13.19 istnieje izomorfizm ciał $\sigma\colon L \to L$ będący rozszerzeniem τ. Zatem σ jest automorfizmem ciała L stałym na K i takim, że $\sigma(a) = b$. □

Pokażemy teraz zastosowanie ciała rozkładu wielomianu dla ciał skończonych. Z algebry I wiemy, że jeżeli ciało K jest skończone, to $ch(K) = p \neq 0$ dla pewnej liczby pierwszej p oraz $|K| = p^n$ dla pewnego $n \in \mathbb{N}$. Okazuje się, że zachodzi następujące

Twierdzenie 13.22. *Dla dowolnej liczby pierwszej p i dla dowolnej liczby naturalnej n jedynym z (z dokładnością do izomorfizmu) ciałem p^n-elementowym jest ciało rozkładu wielomianu $x^{p^n} - x \in \mathbb{Z}_p[x]$.*

Dowód. Niech L będzie ciałem rozkładu wielomianu $f = x^{p^n} - x \in \mathbb{Z}_p[x]$. Wówczas $ch(L) = p$ i wobec tego $f' = -1$. Zatem ze stwierdzenia 13.3 wielomian f nie ma pierwiastków wielokrotnych. Stąd zbiór $L_f \subseteq L$ wszystkich pierwiastków wielomianu f w ciele L ma dokładnie p^n elementów. Z małego twierdzenia Fermata wynika, że $\mathbb{Z}_p \subseteq L_f$. Ponadto dla dowolnych $a, b \in L_f$, $(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b$, więc $a - b \in L_f$ oraz dla dowolnego $0 \neq a \in L_f$, $(\frac{1}{a})^{p^n} - \frac{1}{a} = \frac{a - a^{p^n}}{a^{p^n} a} = 0$, więc $\frac{1}{a} \in L_f$. Zatem L_f jest podciałem p^n-elementowym ciała L i L_f zawiera $\mathbb{Z}_p$ oraz wszystkie pierwiastki wielomianu f. Stąd $L_f = L$, czyli $|L| = p^n$.

Na odwrót, niech K będzie dowolnym ciałem p^n-elementowym. Z algebry I wiemy, że wówczas w K istnieje podciało M izomorficzne z ciałem $\mathbb{Z}_p$. Z twierdzenia Lagrange'a $a^{p^n - 1} = 1$ dla każdego $0 \neq a \in K$. Zatem każdy element ciała K jest pierwiastkiem wielomianu $x^{p^n} - x \in M[x]$. Z drugiej strony wielomian ten nie może mieć więcej niż p^n pierwiastków. Wobec tego K jest ciałem rozkładu wielomianu $f \in M[x]$. Ponadto z wniosku 13.20 każde dwa ciała rozkładu wielomianu $x^{p^n} - x \in \mathbb{Z}_p[x]$ są izomorficzne. □

13.4 Domknięcie algebraiczne ciała

W niniejszym punkcie będziemy badali takie ciała K, że w $K[x]$ każdy wielomian dodatniego stopnia jest iloczynem wielomianów liniowych należących do $K[x]$. Są to tzw. **ciała algebraicznie domknięte**. Udowodnimy, że każde ciało można zanurzyć w ciele algebraicznie domkniętym. Rozpoczynamy od prostej charakteryzacji ciał algebraicznie domkniętych.

Twierdzenie 13.23. *Dla dowolnego ciała K następujące warunki są równoważne:*
(i) jeżeli L jest algebraicznym rozszerzeniem ciała K, to $L = K$,

(ii) jeżeli L jest skończonym rozszerzeniem ciała K, to $L = K$,
(iii) każdy wielomian nierozkładalny w $K[x]$ jest liniowy,
(iv) ciało K jest algebraicznie domknięte,
(v) każdy wielomian stopnia dodatniego należący do $K[x]$ ma pierwiastek w K.

Dowód. Implikacja $(i) \Rightarrow (ii)$ jest oczywista, ponieważ każde rozszerzenie skończone jest algebraiczne.

$(ii) \Rightarrow (iii)$. Jeżeli $f \in K[x]$ jest wielomianem nierozkładalnym, to istnieje takie rozszerzenie L ciała K, w którym f ma pierwiastek. Niech $a \in L$ i $f(a) = 0$. Wtedy $st(f) = (K(a) : K) = 1$, ponieważ na mocy (ii) mamy $K(a) = K$.

$(iii) \Rightarrow (iv)$. Jeżeli $f \in K[x]$ i $st(f) > 0$, to f jest iloczynem skończonej liczby wielomianów nierozkładalnych w $K[x]$, a więc na mocy (iii) f jest iloczynem wielomianów liniowych należących do $K[x]$.

$(iv) \Rightarrow (v)$. Oczywiste.

$(v) \Rightarrow (i)$. Niech L będzie rozszerzeniem algebraicznym ciała K. Weźmy dowolne $a \in L$. Wówczas istnieje wielomian nierozkładalny $f \in K[x]$ taki, że $f(a) = 0$. Ale z założenia f ma pierwiastek w ciele K, więc $st(f) = 1$ i wobec tego $a \in K$. Zatem $L = K$. □

Twierdzenie 13.24. *Każde ciało algebraicznie domknięte jest nieskończone.*

Dowód. Jeżeli ciało K jest skończone, $K = \{a_1, a_2, \ldots, a_n\}$, to wielomian $f = (x - a_1)(x - a_2) \ldots (x - a_n) + 1 \in K[x]$ i f nie ma pierwiastka w K. Zatem z twierdzenia 13.23 ciało K nie jest algebraicznie domknięte. □

Twierdzenie 13.25. *Jeżeli K jest podciałem algebraicznie domkniętego ciała L, to następujące warunki są równoważne:*
(i) L jest rozszerzeniem algebraicznym ciała K,
(ii) Jeżeli ciało algebraicznie domknięte M spełnia $K \subseteq M \subseteq L$, to $M = L$.

Dowód. $(i) \Rightarrow (ii)$. Niech ciało algebraicznie domknięte M spełnia $K \subseteq M \subseteq L$. Ponieważ z założenia L jest rozszerzeniem algebraicznym

ciała K, więc tym bardziej L jest rozszerzeniem algebraicznym ciała M. Z twierdzenia 13.23 wynika więc, że $M = L$.

$(ii) \Rightarrow (i)$. Niech M będzie zbiorem elementów ciała L algebraicznych względem K. Z Algebry I wiemy, że M jest ciałem. Jeżeli $f \in M[x]$ jest wielomianem stopnia dodatniego, to $f \in L[x]$ i z twierdzenia 13.23 wynika, że istnieje $a \in L$ takie, że $f(a) = 0$. Zatem element a jest algebraiczny względem ciała M, a więc i względem ciała K. Z określenia zbioru M wynika więc, że $a \in M$. Wobec tego z twierdzenia 13.23 otrzymujemy, że ciało M jest algebraicznie domknięte. Mamy więc $M = L$ na mocy (ii). □

Ciało nalgebraicznie domknięte L spełniające warunki podane w twierdzeniu 13.25 nazywamy *domknięciem algebraicznym* ciała K. Jest to więc minimalne algebraicznie domknięte ciało zawierające K. Domknięcie algebraiczne ciała K będziemy oznaczali przez $\overline{K}$. Udowodnimy w dalszym ciągu, że dla dowolnego ciała K istnieje jego algebraiczne domknięcie i to tylko jedno z dokładnością do K-izomorfizmu. W dowodach tych będziemy stosowali indukcję pozaskończoną.

Lemat 13.26. *Jeżeli $\{K_\alpha\}_{\alpha<\gamma}$ jest niepustą rodziną ciał indeksowaną za pomocą liczb porządkowych taką, że $K_\alpha \subseteq K_\beta$ dla $\alpha < \beta < \gamma$, to zbiór $K = \bigcup_{\alpha<\gamma} K_\alpha$ jest ciałem.*

Jeżeli $\{\varphi_\alpha\}_{\alpha<\gamma}$ jest rodziną zanurzeń $\varphi_\alpha \colon K_\alpha \to L$ ciał tej rodziny w ustalone ciało L taką, że dla $\alpha < \beta < \gamma$ zanurzenie φ_β jest rozszerzeniem zanurzenia φ_α, to istnieje dokładnie jedno takie zanurzenie $\varphi \colon K \to L$, które jest rozszerzeniem każdego z zanurzeń rodziny $\{\varphi_\alpha\}_{\alpha<\gamma}$.

Dowód. Jeżeli $a, b \in K$, to istnieją $\alpha, \beta < \gamma$ takie, że $a \in K_\alpha$ i $b \in K_\beta$. Bez zmniejszania ogólności możemy zakładać, że $\alpha \leqslant \beta$. Wtedy $K_\alpha \subseteq K_\beta$ i wobec tego $a, b \in K_\beta$. Ponieważ K_β jest ciałem, więc wyniki działań arytmetycznych wykonywanych na elementach a i b należą do K_β i tym bardziej - do K. Zauważmy jeszcze, że wyniki tych działań nie zależą od wyboru β, gdyż dla dowolnych $\sigma < \tau < \gamma$, K_σ jest podciałem ciała K_τ. Zatem K jest ciałem.

Odwzorowanie $\varphi\colon K \to L$ określamy, jak następuje. Jeżeli $a \in K$, to $a \in K_\alpha$ dla pewnego $\alpha < \gamma$. Przyjmujemy wtedy, że $\varphi(a) = \varphi_\alpha(a)$. Element $\varphi(a)$ jest poprawnie określony, tzn. nie zależy od wyboru wskaźnika α. Jeżeli bowiem $a \in K_\beta$ dla pewnego $\beta < \gamma$, to z założenia mamy $\varphi_\alpha(a) = \varphi_\beta(a)$.

Udowodnimy, że odwzorowanie φ jest zanurzeniem. Mamy oczywiście $\varphi(0) = 0$ i $\varphi(1) = 1$. Jeżeli zaś $a, b \in K$, to podobnie, jak w pierwszej części dowodu, wykazujemy, że $a, b \in K_\beta$ dla pewnego $\beta < \gamma$. Zatem $a + b, ab \in K_\beta$ i stąd $\varphi(a + b) = \varphi_\beta(a + b) = \varphi_\beta(a) + \varphi_\beta(b) = \varphi(a) + \varphi(b)$ oraz $\varphi(ab) = \varphi_\beta(ab) = \varphi_\beta(a)\varphi_\beta(b) = \varphi(a)\varphi(b)$.

Niech $\phi\colon K \to L$ będzie zanurzeniem, które jest rozszerzeniem każdego z zanurzeń rodziny $\{\varphi_\alpha\}_{\alpha<\gamma}$. Weźmy dowolne $a \in K$. Wtedy $a \in K_\alpha$ dla pewnego $\alpha < \gamma$, więc $\phi(a) = \varphi_\alpha(a) = \varphi(a)$. Zatem $\phi = \varphi$. □

Twierdzenie 13.27. *Dla każdego ciała K istnieje jego algebraiczne domknięcie.*

Dowód. Niech $\{f_\alpha\}_{\alpha<\gamma}$ będzie rodziną wszystkich wielomianów stopnia dodatniego należących do $K[x]$ ponumerowanych za pomocą liczb porządkowych i niech $f_0 = x$. Określimy ciąg ciał $\{K_\alpha\}_{\alpha<\gamma}$ spełniający warunki:
(1) jeżeli $\alpha < \beta < \gamma$, to K_α jest podciałem ciała K_β,
(2) jeżeli $\alpha < \gamma$, to wszystkie pierwiastki wielomianu f_α należą do K_α,
(3) jeżeli $\alpha < \gamma$, to K_α jest algebraicznym rozszerzeniem ciała K,
w następujący sposób:

1) $K_0 = K$,

2) Jeżeli już dla liczby porządkowej $\delta < \gamma$ został określony ciąg ciał $\{K_\alpha\}_{\alpha<\delta}$ spełniający warunki (1)-(3), to niech $K'_\delta = \bigcup\limits_{\alpha<\delta} K_\alpha$. Na mocy lematu 13.26 zbiór K'_δ jest ciałem i oczywiście $K \subseteq K'_\delta$. Ponadto każde z ciał K_α dla $\alpha < \delta$ jest algebraicznym rozszerzeniem ciała K, więc też K'_δ jest algebraicznym rozszerzeniem ciała K. Jako K_δ przyjmujemy ciało rozkładu wielomianu $f_\delta \in K'_\delta[x]$. Wówczas każdy pierwiastek wielomianu f_δ należy do K_δ i rozszerzenia $K \subseteq K'_\delta$ oraz $K'_\delta \subseteq K_\delta$ są algebraiczne. Zatem K_δ jest rozszerzeniem algebraicznym ciała K.

Na mocy lematu 13.26 zbiór $L = \bigcup_{\alpha<\gamma} K_\alpha$ jest ciałem. Wykażemy, że L jest algebraicznym domknięciem ciała K.

Ponieważ każde z ciał K_α dla $\alpha < \gamma$ jest rozszerzeniem algebraicznym ciała K i $L = \bigcup_{\alpha<\gamma} K_\alpha$, więc ciało L też jest rozszerzeniem algebraicznym ciała K.

Udowodnimy, że ciało L jest algebraicznie domknięte. Jeżeli M jest rozszerzeniem algebraicznym ciała L, to jest rozszerzeniem algebraicznym ciała K. Jeżeli więc $a \in M$, to istnieje wielomian dodatniego stopnia $f \in K[x]$ taki, że $f(a) = 0$. Z określenia rodziny $\{f_\alpha\}_{\alpha<\gamma}$ wynika, że $f = f_\alpha$ dla pewnego $\alpha < \gamma$. Ponieważ wszystkie pierwiastki wielomianu f_α należą do ciała K_α, więc $a \in K_\alpha$. Tym bardziej $a \in L$. Zatem $L = M$.

Z twierdzenia 13.23 wynika więc, że ciało L jest algebraicznie domknięte. Zatem z twierdzenia 13.25 otrzymujemy, że L jest algebraicznym domknięciem ciała K. □

Lemat 13.28. *Jeżeli $\varphi\colon K \to L$ jest zanurzeniem ciała K w algebraicznie domknięte ciało L, a K' jest algebraicznym rozszerzeniem ciała K, to istnieje zanurzenie $\phi\colon K' \to L$ będące rozszerzeniem zanurzenia φ.*

Dowód. Niech $\{a_\alpha\}_{\alpha<\gamma}$ będzie rodziną wszystkich elementów ciała K' ponumerowanych za pomocą liczb porządkowych i niech $a_0 = 0$. Określimy ciąg ciał $\{K_\alpha\}_{\alpha<\gamma}$ zawartych w K' oraz ciąg zanurzeń $\varphi_\alpha\colon K_\alpha \to L$ spełniające warunek:
(a) Jeżeli $\alpha < \beta < \gamma$, to K_α jest podciałem ciała K_β i φ_β jest rozszerzeniem φ_α.

Przyjmujemy $K_0 = K$, $\varphi_0 = \varphi$. Jeżeli zaś dla pewnej liczby porządkowej $\delta < \gamma$ zostały już określone ciągi ciał $\{K_\alpha\}_{\alpha<\delta}$ i ciągi zanurzeń $\{\varphi_\alpha\}_{\alpha<\delta}$ spełniające warunek (a), to określamy ciało K_δ i zanurzenie $\varphi_\delta\colon K_\delta \to L$ jak następuje.

Na mocy lematu 13.26 zbiór $K'_\delta = \bigcup_{\alpha<\delta} K_\alpha$ jest ciałem i istnieje zanurzenie $\varphi'_\delta\colon K'_\delta \to L$ będące rozszerzeniem każdego z zanurzeń φ_α dla $\alpha < \delta$. Określamy $K_\delta = K'_\delta(a_\delta)$.

Element $a_\delta \in K'$ jest z założenia algebraiczny względem ciała K, więc tym bardziej jest algebraiczny względem ciała K'_δ. Niech $f \in K'_\delta[x]$ będzie takim wielomianem nierozkładalnym, że $f(a_\delta) = 0$, zaś $g = \varphi'_\delta(f) \in \varphi'_\delta(K'_\delta)[x]$ - wielomianem odpowiadającym wielomianowi f przy izomorfizmie $\varphi'_\delta\colon K'_\delta \to \varphi'_\delta(K'_\delta)$. Ponieważ $\varphi'_\delta(K'_\delta) \subseteq L$ i ciało L jest algebraicznie domknięte, więc istnieje taki element $b \in L$, że $g(b) = 0$.

Z twierdzenia 13.17 istnieje izomorfizm $\varphi_\delta\colon K'_\delta(a_\delta) \to (\varphi'_\delta(K'_\delta))(b)$ będący rozszerzeniem izomorfizmu φ'_δ. Izomorfizm φ_δ określa więc zanurzenie $\varphi_\delta\colon K_\delta \to L$ będące rozszerzeniem zanurzenia $\varphi'_\delta\colon K'_\delta \to L$ a więc i każdego z zanurzeń $\varphi_\beta\colon K_\beta \to L$ dla $\beta < \delta$.

Do zakończenia dowodu wystarczy więc zastosować lemat 13.26. □

Wniosek 13.29. *Jeżeli K' jest rozszerzeniem algebraicznym ciała K, to istnieje K-zanurzenie $\phi\colon K' \to \overline{K}$.*

Dowód. Wystarczy w lemacie 13.28 przyjąć $L = \overline{K}$, a jako φ wziąć tożsamościowe zanurzenie ciała K w $\overline{K}$. □

Wniosek 13.30. *Każde dwa domknięcia algebraiczne ciała K są K-izomorficzne.*

Dowód. Niech K' i K'' będą domknięciami algebraicznyi ciała K. W szczególności ciało K' jest rozszerzeniem algebraicznym ciała K. Na mocy wniosku 13.29 istnieje K-zanurzenie $\varphi\colon K' \to K''$. Oczywiście ciało $\varphi(K')$ jest algebraicznie domknięte, więc z twierdzenia 13.25 wynika, że $\varphi(K') = K''$, czyli φ jest K-izomorfizmem. □

Z wniosków tych wynika, że badając algebraiczne rozszerzenia ciała K możemy się ograniczyć do rozpatrywania podciał ustalonego domknięcia algebraicznego $\overline{K}$ ciała K.

Lemat 13.31. *Każde K-zanurzenie $\varphi\colon \overline{K} \to \overline{K}$ jest K-automorfizmem.*

Dowód. Mamy wykazać, że $\varphi(\overline{K}) = \overline{K}$. Ponieważ ciało $\overline{K}$ jest algebraicznie domknięte, więc ciało $\varphi(\overline{K})$ jest również algebraicznie domknięte. Zatem na mocy twierdzenia 13.25 z inkluzji $K \subseteq \varphi(\overline{K}) \subseteq \overline{K}$ wynika, że $\varphi(\overline{K}) = \overline{K}$. □

Wniosek 13.32. *Jeżeli L jest rozszerzeniem algebraicznym ciała K, to każde K-zanurzenie $\varphi\colon L \to \overline{K}$ można rozszerzyć do K-automorfizmu $\phi\colon \overline{K} \to \overline{K}$.*

Dowód. Ponieważ $\overline{K}$ jest rozszerzeniem algebraicznym ciała K, więc tym bardziej jest rozszerzeniem algebraicznym ciała L. Zatem na mocy lematu 13.28 istnieje zanurzenie $\phi\colon \overline{K} \to \overline{K}$ będące rozszerzeniem K-zanurzenia φ. Na mocy lematu 13.31 ϕ jest K-automorfizmem. □

Rozdział 14

Teoria Galois

14.1 Grupa Galois

W całym tym rozdziale zakładamy, że wszystkie omawiane ciała są charakterystyki zero. Dobrze wiadomo, że zbiór wszystkich automorfizmów ciała L tworzy grupę ze względu na składanie przekształceń; będziemy ją oznaczali przez $Aut(L)$. Następujące stwierdzenie grupuje pewne dobrze znane własności automorfizmów ciał.

Stwierdzenie 14.1. *Niech σ będzie dowolnym automorfizmem ciała L. Wtedy dla dowolnych $a, a_1, \ldots, a_n, b \in L$ zachodzą wzory:*
(i) $\sigma(0) = 0$, $\sigma(1) = 1$,
(ii) $\sigma(a - b) = \sigma(a) - \sigma(b)$,
(iii) $\sigma\left(\frac{a}{b}\right) = \frac{\sigma(a)}{\sigma(b)}$ *dla* $b \neq 0$,
(iv) $\sigma(a_1 + a_2 + \ldots + a_n) = \sigma(a_1) + \sigma(a_2) + \ldots + \sigma(a_n)$,
(v) $\sigma(a_1 \cdot a_2 \cdot \ldots \cdot a_n) = \sigma(a_1) \cdot \sigma(a_2) \cdot \ldots \cdot \sigma(a_n)$.

Twierdzenie 14.2 (Dedekind)**.** *Jeżeli $\sigma_1, \sigma_2, \ldots, \sigma_n$ są różnymi automorfizmami ciała L, to dla dowolnych $a_1, a_2, \ldots, a_n \in L$ zachodzi implikacja:*

$$(\forall_{a \in L} \quad \sum_{i=1}^{n} a_i \sigma_i(a) = 0) \Rightarrow (a_1 = a_2 = \ldots = a_n = 0). \tag{14.1}$$

Dowód. Zastosujemy indukcyję ze względu na n. Gdy $n = 1$ to poprzednik implikacji (14.1) przyjmuje postać $\forall_{a\in L} a_1\sigma_1(a) = 0$. W szczególności dla $a = 1$ otrzymujemy $0 = a_1\sigma_1(1) = a_1$, stąd $a_1 = 0$.

Załóżmy prawdziwość twierdzenia dla pewnej liczby naturalnej n i niech $\sigma_1, ..., \sigma_{n+1}$ będą różnymi automorfizmami ciała L. Istnieje zatem taki element $b \in L$, że $\sigma_1(b) \neq \sigma_{n+1}(b)$. Załóżmy, że:

$$\forall_{a\in L} \quad a_1\sigma_1(a) + a_2\sigma_2(a) + \ldots + a_{n+1}\sigma_{n+1}(a) = 0. \tag{14.2}$$

W szczególności w równaniu (14.2) w miejsce a można podstawić element $a \cdot b$, gdzie $a \in L$, natomiast element b został określony powyżej. Otrzymamy wtedy:

$$\forall_{a\in L} \quad a_1\sigma_1(a)\sigma_1(b) + a_2\sigma_2(a)\sigma_2(b) + \ldots + a_{n+1}\sigma_{n+1}(a)\sigma_{n+1}(b) = 0. \tag{14.3}$$

Natomiast mnożąc obustronnie równanie (14.2) przez $\sigma_1(b)$ uzyskamy:

$$\forall_{a\in L} \quad a_1\sigma_1(a)\sigma_1(b)+a_2\sigma_2(a)\sigma_1(b)+\ldots+a_{n+1}\sigma_{n+1}(a)\sigma_1(b) = 0. \tag{14.4}$$

Odejmując stronami równania (14.3) i (14.4) otrzymujemy:

$$\forall_{a\in L} \quad a_2(\sigma_2(b) - \sigma_1(b))\sigma_2(a) + \ldots + a_{n+1}(\sigma_{n+1}(b) - \sigma_1(b))\sigma_{n+1}(a) = 0. \tag{14.5}$$

Lewa strona równania (14.5) jest kombinacją liniową n automorfizmów $\sigma_2, \ldots, \sigma_{n+1}$. Na mocy założenia indukcyjnego redukują się wszystkie współczynniki w tej kombinacji liniowej. W szczególności współczynnik przy σ_{n+1} jest równy zeru, tzn. $a_{n+1}(\sigma_{n+1}(b) - \sigma_1(b)) = 0$. Ponieważ $\sigma_1(b) \neq \sigma_{n+1}(b)$, więc $a_{n+1} = 0$. Wobec tego równanie (14.2) przyjmuje postać:

$$\forall_{a\in L} \quad a_1\sigma_1(a) + a_2\sigma_2(a) + \ldots + a_n\sigma_n(a) = 0. \tag{14.6}$$

Jest to kombinacja liniowa n automorfizmów. Na mocy założenia indukcyjnego otrzymujemy $a_1 = a_2 = \ldots = a_n = 0$. □

Definicja 14.3. Niech X będzie niepustym zbiorem pewnych automorfizmów ciała L. Wtedy $a \in L$ nazywamy elementem stałym ze względu na X, gdy $a = \sigma(a)$ dla każdego $\sigma \in X$. Zbiór wszystkich elementów ciała L stałych ze względu na X oznaczamy przez L^X, czyli $L^X = \{a \in L : \forall_{\sigma\in X} \quad \sigma(a) = a\}$.

Twierdzenie 14.4. *Niech X będzie niepustym zbiorem pewnych automorfizmów ciała L. Wtedy zbiór L^X jest podciałem ciała L.*

Dowód. Z własności automorfizmów ciał mamy, że $0, 1 \in L^X$. Niech $a, b \in L^X$. Dla dowolnego $\sigma \in X$ mamy $a = \sigma(a)$ i $b = \sigma(b)$. Zatem otrzymujemy $\sigma(a - b) = \sigma(a) - \sigma(b) = a - b$ oraz dla $b \neq 0$, $\sigma(\frac{a}{b}) = \frac{\sigma(a)}{\sigma(b)} = \frac{a}{b}$. Stąd $a - b \in L^X$, $\frac{a}{b} \in L^X$. Zatem L^X jest podciałem ciała L. □

Twierdzenie 14.5. *Niech $X = \{\sigma_1, \ldots, \sigma_n\}$ będzie skończonym zbiorem pewnych automorfizmów ciała L. Wówczas $(L : L^X) \geqslant n$.*

Dowód. Gdyby $(L : L^X) < n$, to oznaczając przez $\{a_1, \ldots, a_r\}$ bazę ciała L względem L^X mielibyśmy $r < n$. Wówczas układ równań

$$\sigma_1(a_1)x_1 + \sigma_2(a_1)x_2 + \ldots + \sigma_n(a_1)x_n = 0,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sigma_1(a_r)x_1 + \sigma_2(a_r)x_2 + \ldots + \sigma_n(a_r)x_n = 0$$

posiadałby niezerowe rozwiązanie $x_1, x_2, ..., x_n \in L$.

Z drugiej strony dowolny element $a \in L$ może być zapisany jako kombinacja liniowa elementów bazy: $a = \sum_{i=1}^{r} b_i a_i$, gdzie $b_i \in L^X$. Wówczas $\sigma_j(a) = \sum_{i=1}^{r} b_i \sigma_j(a_i)$. Zatem $\sum_{j=1}^{n} \sigma_j(a)x_j = \sum_{j=1}^{n} \sum_{i=1}^{r} b_i \sigma_j(a_i)x_j = \sum_{i=1}^{r} b_i (\sum_{j=1}^{n} \sigma_j(a_i)x_j) = 0$.

Uzyskana równość pokazuje, że automorfizmy $\sigma_1, \ldots, \sigma_n$ są liniowo zależne wbrew twierdzeniu Dedekinda 14.2. Otrzymana sprzeczność dowodzi, że $(L : L^X) \geqslant n$. □

Twierdzenie 14.6. *Niech $G = \{\sigma_1, \ldots, \sigma_n\}$ będzie grupą pewnych automorfizmów ciała L. Wówczas $(L : L^G) \leqslant n$.*

Dowód. Na mocy twierdzenia Dedekinda 14.2, $\sigma_1, \ldots, \sigma_n$ są liniowo niezależne, więc istnieje taki element $b \in L$, że $\sigma_1(b) + \ldots + \sigma_n(b) \neq 0$.

Niech $a_1, \ldots, a_{n+1} \in L$. Pokażemy, że elementy te są liniowo zależne nad ciałem L^G. Układ równań

$$x_1\sigma_1^{-1}(a_1) + x_2\sigma_1^{-1}(a_2) + \ldots + x_{n+1}\sigma_1^{-1}(a_{n+1}) = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$x_1\sigma_n^{-1}(a_1) + x_2\sigma_n^{-1}(a_2) + \ldots + x_{n+1}\sigma_n^{-1}(a_{n+1}) = 0$$

ma niezerowe rozwiązanie $x_1, \ldots, x_{n+1} \in L$, ponieważ liczba niewiadomych jest większa od liczby równań. Możemy przyjąć, że $x_1 \neq 0$. Ponadto, gdy pewien układ elementów ciała L spełnia liniowy jednorodny układ, to spełnia go też każdy proporcjonalny układ elementów. W szczególności elementy

$$x_1 \cdot \frac{b}{x_1} = b, \quad x_2 \cdot \frac{b}{x_1}, \ldots, x_{n+1} \cdot \frac{b}{x_1}$$

spełniają układ równań. Można przyjąć, że $x_1 = b$.
Stosujemy automorfizm σ_i do i- tego równania układu. Otrzymujemy wówczas

$$a_1\sigma_1(x_1) + a_2\sigma_1(x_2) + \ldots + a_{n+1}\sigma_1(x_{n+1}) = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_1\sigma_n(x_1) + a_2\sigma_n(x_2) + \ldots + a_{n+1}\sigma_n(x_{n+1}) = 0.$$

Dodając powyższe równania stronami otrzymujemy

$$(\sigma_1(x_1)+\sigma_2(x_1)+\ldots+\sigma_n(x_1))a_1+(\sigma_1(x_2)+\sigma_2(x_2)+\ldots+\sigma_n(x_2))a_2+\ldots$$

$$+(\sigma_1(x_{n+1}) + \sigma_2(x_{n+1}) + \ldots + \sigma_n(x_{n+1}))a_{n+1} = 0. \tag{14.7}$$

Udowodnimy, że w równaniu (14.7) współczynniki przy $a_1, \ldots, a_{n+1}$ należą do ciała L^G. Wystarczy pokazać, że są one stałe ze względu na automorfizmy grupy G. Gdy $\sigma_j \in G$, to $\{\sigma_j\sigma_1, \sigma_j\sigma_2, \ldots, \sigma_j\sigma_n\} = G$, ponieważ przesunięcie G o element σ_j jest różnowartościowym odwzorowaniem grupy G na siebie. Zatem dla $i = 1, 2, \ldots, n+1$ mamy

$$\sigma_j(\sigma_1(x_i)+\sigma_2(x_i)+\ldots+\sigma_n(x_i)) = \sigma_j\sigma_1(x_i)+\sigma_j\sigma_2(x_i)+\ldots+\sigma_j\sigma_n(x_i) =$$

$$\sigma_1(x_i) + \sigma_2(x_i) + \ldots + \sigma_n(x_i).$$

Stąd współczynnik przy a_i w kombinacji liniowej (14.7) nie ulega zmianie przy działaniu dowolnego automorfizmu $\sigma_j \in G$, należy więc do ciała L^G. Ponadto współczynnik przy a_1 jest różny od zera, ponieważ

$$\sigma_1(x_1) + \sigma_2(x_1) + \ldots + \sigma_n(x_1) = \sigma_1(b) + \sigma_2(b) + \ldots + \sigma_n(b) \neq 0.$$

Stąd (14.7) określa liniową zależność elementów $a_1, \ldots, a_{n+1}$ nad ciałem L^G. Dowiedliśmy więc, że każdy układ $n+1$ elementów ciała L jest liniowo zależny nad ciałem L^G, czyli $(L : L^G) \leqslant n$. □

Wniosek 14.7. *Niech G będzie grupą automorfizmów ciała L taką, że $(L : L^G) < \infty$ lub $|G| < \infty$. Wówczas $|G| = (L : L^G)$.*

Dowód. Jeżeli $|G| < \infty$, to z twierdzeń 14.5 i 14.6 mamy tezę. Załóżmy, że $s = (L : L^G) < \infty$. Przypuśćmy, że $|G| > s$. Niech X będzie $(s+1)$-elementowym podzbiorem G. Wtedy z twierdzenia 14.5 $(L : L^X) \geqslant s+1$. Ale $L^G \subseteq L^X \subseteq L$, więc $s = (L : L^G) = (L : L^X)(L^X : L^G) \geqslant s+1$. Otrzymana sprzeczność dowodzi, że $|G| \leqslant s$ i z pierwszej części dowodu $|G| = (L : L^G)$. □

Twierdzenie 14.8. *Jeżeli L jest rozszerzeniem ciała K, to zbiór wszystkich automorfizmów ciała L stałych na ciele K wraz z działaniem składania odwzorowań tworzy grupę.*

Dowód. Niech $\sigma, \tau \in G(L/K)$. Ponieważ złożenie dwóch izomorfizmów i przekształcenie odwrotne do izomorfizmu jest izomorfizmem, więc $\sigma\tau, \sigma^{-1}$ są izomorfizmami ciała L. Pozostaje sprawdzić, czy odwzorowania te przekształcają tożsamościowo K na siebie. Weźmy dowolny element $a \in K$. Wtedy $\sigma(\tau(a)) = \sigma(a) = a$. Więc z dowolności wyboru elementu a, $\sigma\tau \in G(L/K)$. Jeśli wiemy, że dla każdego $a \in K$, $a = \sigma(a)$, to przykładając do obu stron odwzorowanie odwrotne otrzymujemy $\sigma^{-1}(a) = \sigma^{-1}(\sigma(a)) = a$. Stąd $\sigma^{-1} \in G(L/K)$. Zatem $G(L/K)$ jest grupą. □

Definicja 14.9. Grupę opisaną w twierdzeniu 14.8 nazywamy **grupą Galois** rozszerzenia $K \subseteq L$ i oznaczamy $G(L/K)$.

Stwierdzenie 14.10. *Jeżeli L jest rozszerzeniem ciała K oraz $a \in L$ jest pierwiastkiem wielomianu $f \in K[x]$, to dla każdego $\sigma \in G(L/K)$, $\sigma(a)$ też jest pierwiastkiem wielomianu f.*

Dowód. Mamy, że $f = a_0 + a_1x + \ldots + a_nx^n$ dla pewnego $n \in \mathbb{N}_0$ i dla pewnych $a_0, a_1, \ldots, a_n \in K$ oraz $0 = f(a) = a_0 + a_1a + \ldots + a_na^n$. Zatem $0 = \sigma(0) = \sigma(a_0) + \sigma(a_1)\sigma(a) + \ldots + \sigma(a_n)[\sigma(a)]^n$. Ale $\sigma \in G(L/K)$, więc $\sigma(a_i) = a_i$ dla $i = 0, 1, \ldots, n$ i wobec tego $a_0 + a_1\sigma(a) + \ldots + a_n[\sigma(a)]^n = 0$, czyli $\sigma(a)$ jest pierwiastkiem wielomianu f. □

14.2 Rozszerzenia Galois

Definicja 14.11. Rozszerzenie skończone ciał $K \subseteq L$ nazywamy rozszerzeniem Galois, jeżeli istnieje taka grupa G automorfizmów ciała L, że $K = L^G$.

Twierdzenie 14.12. *Niech $K \subseteq L$ będzie skończonym rozszerzeniem ciał. Wówczas następujące warunki są równoważne:*
(i) $K \subseteq L$ jest rozszerzeniem Galois,
(ii) każdy wielomian nierozkładalny z $K[x]$ i posiadający pierwiastek w L rozkłada się w $L[x]$ na iloczyn wielomianów liniowych,
(iii) L jest ciałem rozkładu pewnego wielomianu z $K[x]$,
(iv) $(L : K) = |G(L/K)|$,
(v) $K = L^{G(L/K)}$.

Dowód. $(i) \Rightarrow (ii)$. Z założenia $K = L^G$ dla pewnej podgrupy G grupy $Aut(L)$. Niech $f \in K[x]$ będzie wielomianem nierozkładalnym i $b \in L$ będzie takie, że $f(b) = 0$. Niech M będzie ciałem rozkładu wielomianu f nad ciałem L. Niech $b = b_1, b_2, \ldots, b_n \in M$ będą wszystkimi pierwiastkami wielomianu f. Przypuśćmy, że nie wszystkie te pierwiastki należą do L. Można przyjąć, że $b_1, b_2, \ldots, b_j \in L$ i $b_{j+1}, \ldots, b_n \notin L$ dla pewnego $j < n$. Weźmy dowolne $\sigma \in G$. Ponieważ współczynniki wielomianu f należą do K i $K = L^G$, więc ze stwierdzenia 14.10 $\{\sigma(b_1), \ldots, \sigma(b_j)\} = \{b_1, \ldots, b_j\}$, czyli σ wyznacza pewną permutację elementów $b_1, \ldots, b_j$. Wynika stąd, że $\sigma(b_1 + \ldots + b_j) = b_1 + \ldots + b_j$,

a nawet więcej, jeśli $c_k = \sum_{1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant j} b_{i_1} b_{i_2} \ldots b_{i_k}$, to $\sigma(c_k) = c_k$ dla wszystkich $k = 1, \ldots, j$. Ponieważ σ jest dowolnym elementem z G i $L^G = K$, więc $c_k \in K$ dla $k = 1, \ldots, j$. Rozpatrzmy wielomian $h = (x - b_1)(x - b_2) \ldots (x - b_j) \in L[x]$. Ze wzorów Viety wynika, że $h = x^j - c_1 x^{j-1} + c_2 x^{j-2} + \ldots + (-1)^j c_j$. Zatem $h \in K[x]$. Ale $h(b) = 0$ i $st(h) < st(f)$, więc mamy sprzeczność z tym, że f jest wielomianem minimalnym elementu b.

$(ii) \Rightarrow (iii)$. Ponieważ $(L : K) < \infty$ i $ch(K) = 0$, więc z twierdzenia Abela istnieje taki element $c \in L$, że $L = K(c)$. Niech $f \in K[x]$ będzie wielomianem minimalnym elementu c. Ponieważ $c \in L$, więc na mocy (ii) wszystkie pierwiastki wielomianu f należą do L. Zatem L jest ciałem rozkładu wielomianu $f \in K[x]$.

$(iii) \Rightarrow (iv)$. Załóżmy, że L jest ciałem rozkładu wielomianu $f \in K[x]$, którego wszystkimi pierwiastkami są $a_1, \ldots, a_n$. Wówczas $L = K(a_1, \ldots, a_n)$. Ponieważ $ch(K) = 0$, więc z twierdzenia Abela istnieje $c \in L$ takie, że $L = K(c)$. Niech $h \in K[x]$ będzie wielomianem minimalnym elementu c. Oznaczmy przez M ciało rozkładu wielomianu h nad ciałem L i niech $c = c_1, \ldots, c_m \in M$ będą wszystkimi pierwiastkami wielomianu h. Wtedy, w szczególności $(L : K) = m$. Z wniosku 13.18 dla każdego $i = 1, \ldots, m$ istnieje izomorfizm ciał $\varphi\colon K(c) \to K(c_i)$ stały na K i taki, że $\varphi(c) = c_i$. Ponieważ $f(\varphi_i(a_j)) = \varphi_i(f(a_j)) = \varphi_i(0) = 0$, więc $\varphi_i(a_1), \varphi_i(a_2), \ldots, \varphi_i(a_n)$ jest pewną permutacją elementów $a_1, a_2, \ldots, a_n$. Stąd $\varphi_i(L) = \varphi_i(K(a_1, \ldots, a_n)) = K(\varphi_i(a_1), \ldots, \varphi_i(a_n)) = K(a_1, \ldots, a_n) = L$. Zatem każde z przekształceń φ_i jest automorfizmem ciała L stałym na K, tzn. $\varphi_i \in G(L/K)$ Wynika stąd, że $|G(L/K)| \geqslant m = (L : K)$. Ponieważ, na mocy twierdzenia 14.5 mamy, że $|G(L/K)| \leqslant (L : K)$, więc $(L : K) = |G(L/K)|$.

$(iv) \Rightarrow (v)$. Niech $M = L^{G(L/K)}$ i załóżmy, że $M \neq K$. Wtedy $G(L/K) \subseteq G(L/M)$ oraz $K \subset M \subseteq L$. Stąd $|G(L/K)| \leqslant |G(L/M)| \leqslant (L : M) < (L : K) = |G(L/K)|$, co prowadzi do sprzeczności.

$(v) \Rightarrow (i)$. Ta implikacja jest oczywista. □

Wniosek 14.13. *Jeżeli $K \subseteq M \subseteq L$ są rozszerzeniami ciał, $ch(K) = 0$ i $K \subseteq L$ jest rozszerzeniem Galois, to $M \subseteq L$ jest rozszerzeniem Galois.*

Dowód. Z twierdzenia 14.12 wynika, że L jest ciałem rozkładu pewnego wielomianu $f \in K[x]$. Ponieważ $K \subseteq M$, więc $f \in M[x]$ i L jest ciałem rozkładu tego wielomianu nad ciałem M. Zatem na mocy twierdzenia 14.12 $M \subseteq L$ jest rozszerzeniem Galois. □

Przykład 14.14. Jeżeli $K \subseteq M \subseteq L$ i $K \subseteq L$ jest rozszerzeniem Galois, to $K \subseteq M$ może nie być rozszerzeniem Galois. Rzeczywiście, rozważmy rozszerzenia ciał $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$. Zauważmy, że $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2}, i)$ jest rozszerzeniem Galois, gdyż $\mathbb{Q}(\sqrt[2]{2}, i)$ jest ciałem rozkładu wielomianu $x^4 - 2 \in \mathbb{Q}[x]$. Z kryterium Eisensteina wynika, że wielomian $x^4 - 2$ jest nierozkładalny w $\mathbb{Q}[x]$. Ponadto nie wszystkie pierwiastki tego wielomianu należą do $\mathbb{Q}(\sqrt[4]{2})$ (np. $i\sqrt[4]{2} \notin \mathbb{Q}(\sqrt[4]{2})$). Zatem na mocy twierdzenia 14.12, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ nie jest rozszerzeniem Galois.

Wniosek 14.15. *Jeżeli K, L, M są podciałami ciała N oraz L jest skończonym rozszerzeniem Galois ciała K, to $M(L)$ jest skończonym rozszerzeniem ciała $M(K)$ i grupa $G(M(L)/M(K))$ zanurza się w grupę $G(L/K)$.*

Dowód. Na mocy twierdzenia 14.12 L jest ciałem rozkładu pewnego wielomianu $f \in K[x]$. Niech $a_1, \ldots, a_r \in M$ będą wszystkimi pierwiastkami wielomianu f. Wtedy $L = K(a_1, \ldots, a_r)$, więc $M(L) = M(K)(a_1, \ldots, a_r)$, czyli $M(L)$ jest ciałem rozkładu wielomianu $f \in M(K)[x]$. Zatem na mocy twierdzenia 14.12 $M(L)$ jest rozszerzeniem Galois ciała $M(K)$.

Aby udowodnić drugą część wniosku definiujemy odwzorowanie $\alpha\colon G(M(L)/M(K)) \to G(L/K)$, jak następuje: $\alpha(\varphi) = \varphi|L$ dla $\varphi \in G(M(L)/M(K))$. Każdy automorfizm $\varphi \in G(M(L)/M(K))$ jest oczywiście K-automorfizmem. Ponadto dla $a \in L$ istnieje wielomian nierozkładalny $h \in K[x]$ taki, że $h(a) = 0$. Ze stwierdzenia 14.10 $\varphi(a)$ jest pierwiastkiem h. Ale z twierdzenia 14.12 każdy pierwiastek wielomianu h należy do L. Zatem $h(a) \in L$ i wobec tego $\varphi(L) \subseteq L$. Zamieniając φ na φ^{-1} uzyskamy stąd, że $\varphi^{-1}(L) \subseteq L$, czyli $L \subseteq \varphi(L)$ i ostatecznie $\varphi(L) = L$. Zatem odwzorowanie α jest poprawnie określone. Jest ono oczywiście homomorfizmem grup. Niech $\varphi \in G(M(L)/M(K))$ oraz $\varphi \in$

$Ker\ \alpha$. Wtedy $\varphi|L = id_L$. Ale $M \subseteq M(K)$ i $\varphi|M(K) = id_{M(K)}$, więc $\varphi|M = id_M$. Stąd $\varphi|M(L) = id_{M(L)}$. Wobec tego $Ker\ \alpha = \{id_{M(L)}\}$, czyli α jest zanurzeniem. □

14.3 Twierdzenia Galois

Niech $K \subseteq L$ będzie rozszerzeniem ciał, $\mathcal{F}$ będzie zbiorem ciał M spełniających warunek $K \subseteq M \subseteq L$ oraz $\mathcal{G}$ będzie zbiorem podgrup grupy Galois $G(L/K)$. Określamy dwa przyporządkowania:
$\alpha : \mathcal{F} \to \mathcal{G}$, $\alpha(M) = G(L/M)$ i $\beta : \mathcal{G} \to \mathcal{F}$, $\beta(H) = L^H$.

Twierdzenie 14.16 (Galois)**.** *Jeżeli $K \subseteq L$ jest skończonym rozszerzeniem Galois, to przyporządkowania α i β wyżej określone są wzajemnie jednoznaczne i względem do siebie odwrotne.*

Dowód. Pokażemy najpierw, że $\beta \circ \alpha = id_{\mathcal{F}}$. Niech $M \in \mathcal{F}$. Wtedy $(\beta \circ \alpha)(M) = L^{\alpha(M)} = L^{G(L/M)}$. Ponieważ $K \subseteq L$ jest rozszerzeniem Galois i $K \subseteq M \subseteq L$, więc na mocy wniosku 14.13 także $M \subseteq L$ jest rozszerzeniem Galois i dlatego $L^{G(L/M)} = M$. Stąd $(\beta \circ \alpha)(M) = L^{G(L/M)} = M$. Zatem $\beta \circ \alpha = id_{\mathcal{F}}$.

Teraz pokażemy, że $\alpha \circ \beta = id_{\mathcal{G}}$. Niech $H \in \mathcal{G}$. Wtedy $(\alpha \circ \beta)(H) = G(L/\beta(H)) = G(L/L^H) \supseteq H$. Z drugiej strony, ponieważ $K \subseteq L^H \subseteq L$, więc $L^H \subseteq L$ jest rozszerzeniem Galois na mocy wniosku 14.13. Zatem $|G(L/L^H)| = (L : L^H)$, więc z wniosku 14.7 $(L : L^H)) = |H|$ i wobec tego $|G(L/L^H)| = |H|$. Ale $H \subseteq G(L/L^H)$, więc $G(L/L^H) = H$, czyli $(\alpha \circ \beta)(H) = H$. Zatem $\alpha \circ \beta = id_{\mathcal{G}}$. □

Twierdzenie 14.17 (Galois)**.** *Jeżeli $K \subseteq L$ jest skończonym rozszerzeniem Galois oraz $K \subseteq M \subseteq L$, to $K \subseteq M$ jest rozszerzeniem Galois wtedy i tylko wtedy, gdy $G(L/M)$ jest podgrupą normalną grupy $G(L/K)$. Jeśli $G(L/M)$ jest podgrupą normalną grupy $G(L/K)$, to grupa $G(M/K)$ jest izomorficzna z grupą ilorazową $G(L/K)/G(L/M)$.*

Dowód. Z twierdzenia 14.12 mamy, że L jest ciałem rozkładu pewnego wielomianu $f \in K[x]$. Ale $ch(K) = 0$, więc z twierdzenia Abela $M = K(a)$ dla pewnego $a \in M$. Niech b będzie pierwiastkiem wielomianu minimalnego g elementu a nad ciałem K i niech M_1 będzie

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

ciałem rozkładu wielomianu g nad ciałem K. Zauważmy, że L jest ciałem rozkładu wielomianu f nad ciałem M_1. Z wniosku 13.21 istnieje automorfizm τ ciała M_1 stały na K i taki, że $\tau(a) = b$. Zatem z twierdzenia 13.19 istnieje automorfizm σ ciała L będący rozszerzeniem τ. Stąd $\sigma \in G(L/K)$ i $\sigma(a) = b$.

Załóżmy najpierw, że $K \subseteq M$ jest rozszerzeniem Galois. Należy pokazać, że dla dowolnych $\sigma \in G(L/K)$ i $\tau \in G(L/M)$ jest $\sigma^{-1}\tau\sigma \in G(L/M)$. Ponadto $K \subseteq M$ jest rozszerzeniem Galois, więc na mocy twierdzenia 14.12 wszystkie pierwiastki wielomianu minimalnego elementu a należą do M. Ponieważ $\sigma(a)$ jest jednym z tych pierwiastków, więc $\sigma(a) \in M$. Ponadto $\tau \in G(L/M)$, więc $\tau(\sigma(a)) = \sigma(a)$ i stąd $(\sigma^{-1}\tau\sigma)(a) = a$. Ale każdy element ciała $M = K(a)$ jest kombinacją liniową potęg elementu a o współczynnikach z ciała K, więc z otrzymanej równości wynika, że $(\sigma^{-1}\tau\sigma)(m) = m$ dla każdego $m \in M$. Zatem $\sigma^{-1}\tau\sigma$ jest automorfizmem ciała L stałym na ciele M, czyli $\sigma^{-1}\tau\sigma \in G(L/M)$. Stąd $G(L/M) \lhd G(L/K)$.

Załóżmy teraz, że $G(L/M) \lhd G(L/K)$. Wobec tego dla dowolnych $\sigma \in G(L/K)$ i $\tau \in G(L/M)$ mamy $\sigma^{-1}\tau\sigma \in G(L/M)$. Zatem $(\sigma^{-1}\tau\sigma)(a) = a$, skąd $\tau(\sigma(a)) = \sigma(a)$, więc $\sigma(a)$ jest elementem stałym względem grupy $G(L/M)$, a zatem $\sigma(a) \in M$, gdyż $M \subseteq L$ jest rozszerzeniem Galois na mocy wniosku 14.13. Ale każdy pierwiastek wielomianu minimalnego elementu a nad ciałem K ma postać $\sigma(a)$ dla odpowiedniego $\sigma \in G(L/K)$, więc M jest ciałem rozkładu tego wielomianu, a stąd wynika, że $K \subseteq M$ jest rozszerzeniem Galois na mocy twierdzenia 14.12.

Aby udowodnić ostatnią część twierdzenia zauważmy, że przyporządkowując automorfizmowi $\sigma \in G(L/K)$ jego obcięcie do M, określamy automorfizm ciała M. Stwierdziliśmy wyżej, że $\sigma(a) \in M$, więc $\sigma(M) \subseteq M$. Ale elementy $\sigma(a)$ i a mają ten sam stopień nad ciałem K i $\sigma(M) = K(\sigma(a))$ oraz $M = K(a)$, więc $\sigma(M) = M$. Przyporządkowanie to wyznacza homomorfizm grup $f\colon G(L/K) \to G(M/K)$. Jądrem tego homomorfizmu jest zbiór automorfizmów ciała L stałych na M, a więc $G(L/M)$. Wystarczy zatem wykazać, że $f(G(L/K)) = G(M/K)$. Z algebry I mamy $|f(G(L/K))| = \frac{|G(L/K)|}{|G(L/M)|}$. Ponieważ $K \subseteq L$, $K \subseteq M$ i $M \subseteq L$ są rozszerzeniami Galois, więc na mocy twier-

dzenia 14.12 $\frac{|G(L/K)|}{|G(L/M)|} = \frac{(L:K)}{(L:M)}$. Ale z algebry I wiemy, że $(L : K) = (L : M)(M : K)$, więc $\frac{(L:K)}{(L:M)} = (M : K)$. Ponadto z twierdzenia 14.12 $(M : K) = |G(M/K)|$. Zatem $|f(G(L/K))| = |G(M/K)|$. Ale $f(G(L/K)) \subseteq G(M/K)$, więc $f(G(L/K)) = G(M/K)$. □

Wniosek 14.18. *Niech L będzie skończonym rozszerzeniem Galois ciała K. Wówczas istnieje tylko skończona liczba ciał M takich, że $K \subseteq M \subseteq L$.*

Dowód. Ponieważ $|G(L/K)| = (L : K)$, więc $G(L/K)$ jest skończona i stąd ma skończoną liczbę podgrup. Na mocy twierdzenia Galois 14.16 istnieje wzajemnie jednoznaczna odpowiedniość między podgrupami grupy $G(L/K)$ a ciałami pośrednimi między K i L. Wobec tego musi być skończona ilość ciał pośrednich między K i L. □

14.4 Grupa Galois wielomianu

Definicja 14.19. Niech $f \in K[x]$ taki, że $st(f) > 0$ oraz L będzie ciałem rozkładu tego wielomianu. Wówczas grupę $G(L/K)$ nazywamy **grupą Galois wielomianu** f.

Twierdzenie 14.20. *Grupa Galois wielomianu $f \in K[x]$ jest przechodnią grupą permutacji zbioru pierwiastków tego wielomianu wtedy i tylko wtedy, gdy f jest potęgą wielomianu nierozkładalnego w $K[x]$.*

Dowód. $\Leftarrow$. Niech $f = g^r$ dla wielomianu nierozkładalnego $g \in K[x]$. Jeżeli $f(a) = f(b) = 0$, to $g(a) = g(b) = 0$. Wówczas z wniosku 13.18 istnieje taki K-izomorfizm $\varphi : K(a) \to K(b)$, że $\varphi(a) = b$. Dany K-izomorfizm można rozszerzyć do automorfizmu φ' ciała rozkładu L wielomianu $f \in K[x]$ na mocy twierdzenia 13.19. Wobec tego $\varphi' \in G(L/K)$ spełnia $\varphi'(a) = b$. Stąd grupa Galois wielomianu f jest przechodnią grupą permutacji zbioru jego pierwiastków.

$\Rightarrow$. Załóżmy, że wielomian $f \in K[x]$ nie jest potęgą wielomianu nierozkładalnego w $K[x]$. Wtedy istnieją takie wielomiany nierozkładalne $g, h \in K[x]$, że $gh \mid f$ oraz $(g, h) = 1$. Wielomiany g i h nie mają zatem

wspólnych pierwiastków oraz obraz pierwiastka wielomianu g przy dowolnym K- automorfizmie ciała rozkładu wielomianu $f \in K[x]$ jest też pierwiastkiem tego wielomianu. Wobec tego żaden K-automorfizm nie przekształca pierwiastka wielomianu g na pierwiastek wielomianu h. Grupa Galois wielomianu f nie jest przechodnią grupą przekształceń zbioru jego pierwiastków. □

Definicja 14.21. *Niech L będzie rozszerzeniem Galois ciała K oraz grupa $G(L/K)$ będzie grupą cykliczną (odpowiednio abelową lub rozwiązalną). Wtedy L nazywamy rozszerzeniem cyklicznym (abelowym lub rozwiązalnym) ciała K.*

Twierdzenie 14.22. *Jeżeli $K \subseteq L$ jest skończonym rozszerzeniem cyklicznym (abelowym) oraz M jest ciałem pośrednim między K i L, to każde z rozszerzeń $K \subseteq M$ i $M \subseteq L$ jest cykliczne (abelowe).*

Dowód. Każda podgrupa grupy abelowej (również cyklicznej) jest jej dzielnikiem normalnym, zatem $G(L/M) \triangleleft G(L/K)$. Z twierdzenia 14.17 otrzymujemy, że M jest rozszerzeniem Galois ciała K oraz z wniosku 14.13 wynika, że L jest rozszerzeniem Galois ciała M. Ponieważ $G(L/M)$ jest podgrupą, a $G(M/K)$ obrazem homomorficznym grupy cyklicznej (abelowej) $G(L/K)$ oraz podgrupa i obraz homomorficzny dowolnej grupy cyklicznej (abelowej) jest grupą cykliczną (abelową), więc grupy $G(L/M)$ i $G(M/K)$ są cykliczne (abelowe). □

Twierdzenie 14.23. *Niech $K \subseteq L$ będzie skończonym rozszerzeniem rozwiązalnym. Jeżeli $K \subseteq M \subseteq L$, to L jest rozszerzeniem rozwiązalnym ciała M. Jeżeli dodatkowo M jest rozszerzeniem Galois ciała K, to M jest rozszerzeniem rozwiązalnym ciała K.*

W drugą stronę, jeżeli L jest skończonym rozszerzeniem Galois ciała K, $K \subseteq M \subseteq L$ oraz rozszerzenia $K \subseteq M$ i $M \subseteq L$ są rozwiązalne, to L jest rozszerzeniem rozwiązalnym ciała K.

Dowód. Ponieważ $K \subseteq L$ jest rozszerzeniem Galois, zatem na mocy wniosku 14.13 $M \subseteq L$ też jest rozszerzeniem Galois. Grupa $G(L/M)$ jest podgrupą grupy rozwiązalnej $G(L/K)$, zatem na mocy stwierdzenia 3.10 jest ona rozwiązalna.

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Jeżeli M jest rozszerzeniem Galois ciała K, to grupa $G(M/K)$ jest obrazem homomorficznym grupy rozwiązalnej, więc na mocy stwierdzenia 3.10 jest rozwiązalna.

Na odwrót, zauważmy, że $G(L/M) \triangleleft G(L/K)$ na mocy twierdzenia 14.17. Grupy $G(L/M)$ oraz $G(M/K) \cong G(L/K)/G(L/M)$ są rozwiązalne, zatem grupa $G(L/K)$ jest rozwiązalna na mocy twierdzenia 3.11. □

Lemat 14.24. *Dla dowolnego ciała K grupa Galois wielomianu $x^n - 1 \in K[x]$ jest abelowa.*

Dowód. Ze stwierdzenia 13.14 wynika, że ciało rozkładu wielomianu $x^n - 1$ jest równe $K(\varepsilon) = L$ oraz wszystkimi pierwiastkami wielomianu $x^n - 1$ są $1, \varepsilon, \ldots, \varepsilon^{n-1}$. Niech $\varphi, \psi \in G(L/K)$. Każdy automorfizm należący do $G(L/K)$ przekształca pierwiastki wielomianu $x^n - 1$ na pierwiastki tego wielomianu, zatem istnieją takie liczby naturalne $r, k \leqslant n$, że $\varphi(\varepsilon) = \varepsilon^r$ i $\psi(\epsilon) = \epsilon^k$. Stąd

$$(\varphi\psi)(\varepsilon) = \varphi(\varepsilon^k) = \varepsilon^{kr} \quad \text{i} \quad (\psi\varphi)(\varepsilon) = \psi(\varepsilon^k) = \varepsilon^{rk} = \varepsilon^{kr},$$

a więc $(\varphi\psi)(\varepsilon) = (\psi\varphi)(\varepsilon)$. Zatem $(\varphi\psi)(m) = (\psi\varphi)(m)$ dla każdego $m \in L$, czyli $\varphi\psi = \psi\varphi$ i grupa $G(L/K)$ jest abelowa. □

Lemat 14.25. *Niech K będzie ciałem takim, że w grupie K^* istnieje element ε rzędu n. Wówczas grupa Galois wielomianu $x^n - a \in K[x]$ jest cykliczna. Ponadto istnieje liczba naturalna s dzieląca n i element b z ciała rozkładu L wielomianu $x^n - a \in K[x]$ takie, że $b^n = a$, $L = K(b)$, $b^s \in K$, L jest ciałem rozkładu wielomianu $x^s - b^s \in K[x]$, $(L : K) = s$ i wielomian $x^s - b^s$ jest nierozkładalny w $K[x]$.*

Dowód. Teza jest oczywista dla $a = 0$. Niech dalej $a \neq 0$. Jeżeli b jest pierwiastkiem wielomianu $x^n - a$, to pozostałymi jego pierwiastkami są $b\varepsilon, \ldots, b\varepsilon^{n-1}$. Zatem ciało rozkładu L wielomianu $x^n - a \in K[x]$ jest równe $K(b, b\varepsilon, \ldots, b\varepsilon^{n-1})$. Stąd $L = K(b)$, ponieważ $\varepsilon \in K$.

Niech s będzie najmniejszą liczbą naturalną taką, że $b^s \in K$. Oczywiście $s \leqslant n$, gdyż $b^n = a \in K$. Gdyby s nie było dzielnikiem n, to

$n = qs + r$ dla pewnych $q, r \in \mathbb{N}$, $r < s$. Ale wtedy $b^r = \frac{b^n}{(b^s)^q} \in K$, co przeczy minimalności s. Zatem $s \mid n$ i wobec tego w grupie K^* element $\omega = \varepsilon^{\frac{n}{s}}$ ma rząd s. Wynika stąd, że wszystkimi pierwiastkami wielomianu $g = x^s - b^s \in K[x]$ w ciele L są $b, b\omega, \ldots, b\omega^{s-1}$. Zatem ciałem rozkładu wielomianu $g \in K[x]$ jest $K(b, b\omega, \ldots, b\omega^{s-1}) = K(b) = L$, bo $\omega \in K$. Niech $h \in K[x]$ będzie unormowanym wielomianem minimalnym elementu b i niech $t = st(h)$. Wtedy $h \mid g$, bo $g \in K[x]$ i $g(b) = 0$. Zatem $t \leqslant s$ oraz istnieją liczby całkowite $0 = l_0 < l_1 < \ldots < l_{t-1} \leqslant s$ takie, że $h = (x - b\omega^{l_0})(x - b\omega^{l_1}) \ldots (x - b\omega^{l_{t-1}})$. Ponadto $h \in K[x]$, więc $h(0) \in K$. Ale $h(0) = (-1)^t \omega^{l_0 + l_1 + \ldots + l_{t-1}} b^t$ oraz $\omega \in K$, więc $b^t \in K$. Stąd z minimalności s, $t = s$ oraz $h = g$. Zatem wielomian $g = x^s - b^s$ jest nierozkładalny w $K[x]$ i wobec tego $(L : K) = s$. Z twierdzenia 14.12 mamy, że $|G(L/K)| = s$.

Niech $\sigma \in G(L/K)$. Wtedy $\sigma(b)$ jest pierwiastkiem wielomianu g, więc $\sigma(b) = b\omega^l$ dla pewnego $l = 0, 1, \ldots, s-1$. Poza tym $L = K(b)$, więc σ jest jednoznacznie wyznaczone przez $\sigma(b)$. Ale $|G(L/K)| = s$, więc $G(L/K) = \{\sigma_0, \sigma_1, \ldots, \sigma_{s-1}\}$, gdzie $\sigma_l(b) = b\omega^l$ dla $l = 0, 1, \ldots, s-1$. Stąd uzyskujemy, że $\sigma_l = \sigma_1^l$ dla $l = 0, 1, \ldots, s-1$. Zatem σ_1 jest generatorem grupy $G(L/K)$. □

Wniosek 14.26. *Ciało rozkładu wielomianu $x^n - a \in K[x]$ jest rozszerzeniem rozwiązalnym ciała K.*

Dowód. Jeżeli $a = 0$, to teza wniosku jest oczywista. Niech więc $a \neq 0$. Ze stwierdzenia 13.15 wynika, że w grupie L^* istnieje element ε rzędu n. Ponadto, jeżeli $b \in L$ jest pierwiastkiem wielomianu $x^n - a$, to $L = K(b, b\varepsilon, \ldots, b\varepsilon^{n-1}) = K(b, \varepsilon) = (K(\varepsilon))(b)$ oraz L jest ciałem rozkładu wielomianu $x^n - a \in K(\varepsilon)[x]$ i $K(\varepsilon)$ jest ciałem rozkładu wielomianu $x^n - 1 \in K[x]$. Z lematu 14.24 mamy, że rozszerzenie $K \subseteq K(\varepsilon)$ jest abelowe, a z lematu 14.25 rozszerzenie $K(\varepsilon) \subseteq L$ jest abelowe. Zatem z twierdzenia 14.23 rozszerzenie $K \subseteq L$ jest rozwiązalne. □

Rozdział 15

Zastosowania teorii Galois

15.1 Zastosowania algebraiczne

15.1.1 Rozszerzenia pierwiastnikowe

Określimy teraz kilka klas elementów algebraicznych, które odegrały ważną rolę w historii badań nad elementami algebraicznymi. Rozpoczniemy od zdefiniowania zbioru elementów pierwiastnikowych. Pojęcie to odpowiada intuicji liczb, które dają się zapisać przy użyciu czterech działań arytmetycznych i działania pierwiastkowania. Wszystkie nasze rozważania dotyczą jedynie ciał charaterystyki zero. Ponadto dla ustalonego ciała K ustalamy jego algebraiczne domknięcie $\overline{K}$ i wszystkie rozszerzenia algebraiczne ciała K traktujemy jako podciała ciała $\overline{K}$.

Definicja 15.1. Mówimy, że element $a \in \overline{K}$ jest **pierwiastnikowy** względem ciała K (albo, że wyraża się przez pierwiastniki względ-em ciała K), jeżeli istnieje skończony ciąg podciał ciała $\overline{K}$: $K = K_0 \subseteq K_1 \subseteq ... \subseteq K_r$ taki, że $a \in K_r$ oraz dla $i = 1, 2, \ldots, r$, K_i jest ciałem rozkładu wielomianu postaci $x^{n_i} - a_i \in K_{i-1}[x]$.

Zbiór elementów $a \in \overline{K}$ pierwiastnikowych względem ciała K oznaczamy przez $r(K)$ i nazywamy **domknięciem pierwiastnikowym** ciała K.

Rozszerzenie L ciała K nazywamy **rozszerzeniem pierwiastnikowym** ciała K, jeżeli każdy element ciała L jest pierwiastnikowy względem ciała K, tzn. jeżeli $L \subseteq r(K)$.

Lemat 15.2. *Jeżeli L jest ciałem rozkładu wielomianu $x^n - a \in K[x]$, gdzie $n = r \cdot s$, $r, s \in \mathbb{N}$, $r, s > 1$; $a_1, a_2, \ldots, a_r \in \overline{K}$ są wszystkimi pierwiastkami wielomianu $x^r - a \in K[x]$; $L_0 = K(a_1, \ldots, a_r)$ jest ciałem rozkładu wielomianu $x^r - a \in K[x]$ oraz L_i jest ciałem rozkładu wielomianu $x^s - a_i \in L_{i-1}[x]$ dla $i = 1, 2, \ldots, r$, to $K \subseteq L_0 \subseteq L_1 \subseteq \ldots \subseteq L_r = L$.*

Dowód. Wystarczy wykazać, że $L_r = L$. Z przyjętych oznaczeń wynika, że $a_i^r = a$ dla $i = 1, 2, \ldots, r$. Jeżeli b jest jednym z pierwiastków wielomianu $x^n - a$, to $a = b^n = (b^s)^r$. Zatem b^s jest pierwiastkiem wielomianu $x^r - a$, czyli $b^s = a_i$ dla pewnego $i = 1, \ldots, r$. Wobec tego b jest też pierwiastkiem wielomianu $x^s - a_i$ i stąd $b \in L_i$. Tym bardziej $b \in L_r$. Ponieważ element b był dowolnym pierwiastkiem wielomianu $x^n - a$, więc ciało L rozkładu tego wielomianu jest zawarte w L_r.

Na odwrót, ciało rozkładu L_0 wielomianu $x^r - a \in K[x]$ jest zawarte w ciele rozkładu wielomianu $x^{rs} - a \in K[x]$. Każdy pierwiastek pierwszego z tych wielomianów jest bowiem s-tą potęgą odpowiedniego pierwiastka drugiego wielomianu. Podobnie, każdy pierwiastek wielomianu $x^s - a_i$ jest pierwiastkiem wielomianu $x^{rs} - a_i^r = x^n - a$. Zatem $L_i \subseteq L$ dla $i = 1, 2, \ldots, r$. W szczególności $L_r \subseteq L$. □

Z lematu 15.2 i ze stwierdzenia 13.15 wynika, że w określeniu elementu pierwiastnikowego względem ciała K można przyjąć, że każda z liczb n_i jest liczbą pierwszą oraz, że $(K_i : K_{i-1}) \leqslant n_i$ dla $i = 1, 2, \ldots, r$.

Mianowicie lemat 15.2 pozwala zastąpić ciało rozkładu wielomianu $x^n - a$ ciałami rozkładu wielomianów $x^r - b$ i $x^s - c$, gdzie r i s są właściwymi dzielnikami liczby n. Stosując ten lemat wielokrotnie dochodzimy do przypadku, gdy stopnie rozważanych wielomianów są liczbami pierwszymi. Natomiast stwierdzenie 13.15 pozwala zastąpić ciało rozkładu wielomianu $x^n - a$ ciałami rozkładu wielomianów $x^n - 1$ i $x^n - a$ i przy tym stopnie odpowiednich rozszerzeń nie przekraczają n.

Wprowadzimy jeszcze pewną klasyfikację elementów pierwiastnikowych.

Definicja 15.3. *Mówimy, że element $a \in \overline{K}$ wyraża się przez pierwiastniki stopni co najwyżej n względem ciała K, jeżeli istnieje skończony ciąg podciał ciała $\overline{K}$: $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$ taki, że $a \in K_r$ oraz dla $i = 1, 2, \ldots, r$, K_i jest ciałem rozkładu wielomianu postaci $x^{n_i} - a_i \in K_{i-1}[x]$ i $(K_i : K_{i-1}) \leqslant n$.*

Zbiór elementów ciała $\overline{K}$ wyrażających się przez pierwiastniki stopni co najwyżej n względem ciała K oznaczamy przez $r_n(K)$. W szczególności, gdy $n = 2$, to zbiór $r_2(K)$ elementów wyrażających się względem ciała K przez pierwiastniki kwadratowe składa się z elementów $a \in \overline{K}$, dla których istnieje taki ciąg ciał $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r$, że $a \in K_r$ oraz $(K_i : K_{i-1}) = 2$ dla $i = 1, 2, \ldots, r$.

Jeżeli bowiem $ch(L) \neq 2$, to każde rozszerzenie kwadratowe ciała L jest ciałem rozkładu wielomianu postaci $x^2 - b \in L[x]$.

Bezpośrednio z określenia elementów wyrażających się przez pierwiastniki stopni nie większych od n wynika, że jeżeli $a \in \overline{K}$, to $(K(a) : K)$ jest dzielnikiem liczby

$$(K_r : K) = (K_r : K_{r-1})(K_{r-1} : K_{r-2}) \ldots (K_1 : K_0).$$

Każdy z czynników $(K_i : K_{i-1})$ jest nie większy od n. Zatem każdy dzielnik pierwszy liczby $(K(a) : K)$ nie przekracza n. W szczególności, jeżeli $a \in r_2(K)$, to liczba $(K(a) : K)$ jest potęgą dwójki o całkowitym nieujemnym wykładniku. Wynika stąd

Twierdzenie 15.4. *Jeżeli L jest rozszerzeniem skończonym ciała K i $L \subseteq r_n(K)$, to każdy dzielnik pierwszy liczby $(L : K)$ jest nie większy od n.*

Wniosek 15.5. *Jeżeli L jest rozszerzeniem skończonym ciała K i $L \subseteq r_2(K)$, to liczba $(L : K)$ jest potęgą dwójki o całkowitym nieujemnym wykładniku.*

Podamy teraz kilka podstawowych własności zbiorów $r(K)$ i $r_n(K)$.

Twierdzenie 15.6. *Dla dowolnego ciała K:*
(i) zbór $r(K)$ jest ciałem,
(ii) każdy element pierwiastnikowy względem $r(K)$ należy do $r(K)$,
(iii) jeżeli $\varphi\colon \overline{K} \to \overline{K}$ jest K-izomorfizmem, to $\varphi(r(K)) = r(K)$.

Dowód. (i). Niech $a, b \in r(K)$ i $b \neq 0$. Wykażemy, że $a+b, a-b, ab, \frac{a}{b} \in r(K)$. Z określenia zbioru $r(K)$ wynika, że istnieją takie skończone ciągi ciał

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r, \qquad K = L_0 \subseteq L_1 \subseteq \ldots \subseteq L_s,$$

że $a \in K_r$, $b \in L_s$ oraz każde z ciał K_i, L_j $(i = 1, 2, \ldots, r; j = 1, 2, \ldots, s)$ powstaje z ciała poprzedniego przez dołaczenie wszystkich pierwiastków wielomianu postaci $x^n - a$. Rozpatrzmy ciąg ciał

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r = L_0(K_r) \subseteq L_1(K_r) \subseteq \ldots \subseteq L_s(K_r).$$

Każde z ciał tego ciągu powstaje oczywiście z ciała poprzedniego przez dołączenie wszystkich pierwiastków pewnego wielomianu podanej wyżej postaci. Zatem $L_s(K_r) \subseteq r(K)$. Ponieważ $a, b \in L_s(K_r)$ i $L_s(K_r)$ jest ciałem, więc $a + b, a - b, ab, \frac{a}{b} \in r(K)$. Wynika stąd, że $r(K)$ jest ciałem.

(ii). Niech $x^n - a \in r(K)[x]$. Wykażemy, że w $r(K)[x]$ wielomian $x^n - a$ jest iloczynem wielomianów liniowych. Ponieważ $a \in r(K)$, więc istnieje taki ciąg ciał

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r,$$

że $a \in K_r$ i każde z ciał K_i $(i = 1, 2, \ldots, r)$ powstaje z ciała poprzedniego przez dołaczenie wszystkich pierwiastków wielomianu postaci $x^{n_i} - a_i$. Wtedy $x^n - a \in K_r[x]$. Niech K_{r+1} będzie ciałem rozkładu wielomianu $x^n - a \in K_r[x]$. Z określenia zbioru $r(K)$ wynika, że wtedy $K_{r+1} \subseteq r(K)$. Wielomian $x^n - a$ jest iloczynem wielomianów liniowych należących do $K_{r+1}[x]$, a więc tym bardziej jest on iloczynem wielomianów liniowych należących do $r(K)[x]$.

Z powyższego wynika, że każdy element pierwiastnikowy względem ciała $r(K)$ należy do $r(K)$.

(*iii*). Jeżeli $a \in r(K)$, to istnieje taki ciąg ciał

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r,$$

że $a \in K_r$ oraz dla $i = 1, 2, \ldots, r$ ciało K_i jest ciałem rozkładu wielomianu postaci $x^{n_i} - a_i \in K_{i-1}[x]$. Wtedy

$$K = \varphi(K) = \varphi(K_0) \subseteq \varphi(K_1) \subseteq \ldots \subseteq \varphi(K_r),$$

$\varphi(a) \in \varphi(K_r)$ oraz dla $i = 1, 2, \ldots, r$ ciało $\varphi(K_i)$ jest ciałem rozkładu wielomianu postaci $x^{n_i} - \varphi(a_i) \in \varphi(K_{i-1})[x]$. Zatem $\varphi(a) \in r(K)$.

Wynika stąd, że $\varphi(r(K)) \subseteq r(K)$. Rozpatrując automorfizm φ^{-1} odwrotny do φ otrzymujemy inkluzję $\varphi^{-1}(r(K)) \subseteq r(K)$, czyli $r(K) \subseteq \varphi(r(K))$. Zatem $\varphi(r(K)) = r(K)$. □

Analogicznie można udowodnić następujące

Twierdzenie 15.7. *Dla dowolnego ciała K:*
(i) zbór $r_n(K)$ jest ciałem;
(ii) każdy element wyrażający się przez pierwiastniki stopni nie większych od n względem $r_n(K)$ należy do $r_n(K)$;
(iii) jeżeli $\varphi\colon \overline{K} \to \overline{K}$ jest K-izomorfizmem, to $\varphi(r_n(K)) = r_n(K)$.

15.1.2 Własności ciała $r(K)$

Niech $f \in K[x]$ i $st(f) > 0$. Mówimy, że równanie $f(x) = 0$ jest **rozwiązalne w pierwiastnikach** względem ciała K, jeżeli każdy pierwiastek wielomianu f wyraża się przez pierwiastniki względem ciała K, lub, co na jedno wychodzi, jeżeli ciało rozkładu L wielomianu $f \in K[x]$ jest zawarte w $r(K)$.

Badanie rozwiązalności równań w pierwiastnikach sprowadza się więc do opisania skończonych rozszerzeń Galois ciała K zawartych w $r(K)$.

Lemat 15.8 (Lagrange)**.** *Niech L będzie cyklicznym rozszerzeniem ciała K stopnia n i niech w grupie K^* istnieje element ε rzędu n. Wówczas istnieje element $a \in L$ taki, że $L = K(a)$ oraz $a^n \in K$. Ponadto L jest ciałem rozkładu wielomianu $x^n - a^n \in K[x]$.*

Dowód. Niech σ będzie generatorem grupy $G(L/K)$. Mamy wtedy $o(\sigma) = |G(L/K)| = (L : K)$ oraz $G(L/K) = \{id_K, \sigma, \ldots, \sigma^{n-1}\}$. Z twierdzenia Dedekinda, wynika, że istnieje element $b \in L$ taki, że

$$a = b + \varepsilon\sigma(b) + \varepsilon^2\sigma^2(b) + ... + \varepsilon^{n-1}\sigma^{n-1}(b) \neq 0.$$

Ponieważ $\varepsilon \in K$, więc

$$\sigma(a) = \sigma(b) + \varepsilon\sigma^2(b) + ... + \varepsilon^{n-1}\sigma^n(b) =$$

$$= \varepsilon^{-1}(\varepsilon\sigma(b) + \varepsilon^2\sigma^2(b) + ... + \varepsilon^{n-1}\sigma^{n-1}(b) + b) = \varepsilon^{-1}a.$$

Załóżmy, że dla pewnego $1 \leqslant k < n$, $\sigma^k(a) = \varepsilon^{-k}a$. Wówczas $\sigma^{k+1}(a) = \sigma(\sigma^k(b)) = \sigma(\varepsilon^{-k}a)) = \sigma(\varepsilon^{-k})\sigma(a) = \varepsilon^{-k}\varepsilon^{-1}a = \varepsilon^{-(k+1)}a$. Zatem dla dowolnego $k = 1, 2, \ldots, n-1$ mamy, że $\sigma^k(a) = \varepsilon^{-k}a$. Ale $\varepsilon^{-k} \neq 1$ dla $k = 1, 2, \ldots, n-1$, gdyż $o(\varepsilon) = n$. Ponieważ $a \neq 0$, więc wynika stąd, że $\sigma^k(a) \neq a$ dla $k = 1, 2, \ldots, n-1$. Zatem dla każdego automorfizmu należącego do grupy $G(L/K)$ różnego od automorfizmu tożsamościowego element a nie jest stały. Stąd $G(L/K(a)) = \{id_K\}$. Na mocy wniosku 14.13 L jest rozszerzeniem Galois ciała $K(a)$, więc z twierdzenia 14.12 $(L : K(a)) = |G(L/K(a))| = 1$, czyli $L = K(a)$.

Mamy też $\sigma(a^n) = [\sigma(a)]^n = [\varepsilon^{-1}a]^n = a^n$, gdyż $\varepsilon^n = 1$. Stąd $\sigma^k(a^n) = a^n$ dla dowolnego $k = 0, 1, \ldots, n-1$. Zatem $a^n \in L^{G(L/K)} = K$. Skąd a jest pierwiastkiem wielomianu $x^n - a^n \in K[x]$. Ciałem rozkładu tego wielomianu jest więc $K(a, a\varepsilon, \ldots, a\varepsilon^{n-1}) = K(a, \varepsilon) = K(a) = L$, bo $\varepsilon \in K$. □

Wniosek 15.9. *Jeżeli L jest cyklicznym rozszerzeniem stopnia n ciała K, to $L \subseteq r_n(K)$.*

Dowód. Ze stwierdzenia 13.14 w grupie $\overline{K}^*$ istnieje element ε rzędu n. Na mocy wniosku 14.15 ciało $L(\varepsilon)$ jest cyklicznym rozszerzeniem Galois ciała $K(\varepsilon)$ i stopień r tego rozszerzenia jest dzielnikiem liczby n, $n = r \cdot s$. Zatem element $\varepsilon^s \in K(\varepsilon)$ ma rząd r w grupie $K(\varepsilon)^*$. Z lematu 15.8 wynika, że $L(\varepsilon)$ jest ciałem rozkładu wielomianu postaci $x^r - b \in K(\varepsilon)[x]$. Ciało $K(\varepsilon)$ jest oczywiście ciałem rozkładu wielomianu $x^n - 1 \in K[x]$. Wobec tego na mocy stwierdzenia 13.15 mamy $L(\varepsilon) \subseteq r_n(K)$ i tym bardziej $L \subseteq r_n(K)$. □

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

Twierdzenie 15.10. *Jeżeli L jest rozszerzeniem skończonym i rozwiązalnym ciała K, to $L \subseteq r_n(K)$, gdzie n jest największym dzielnikiem pierwszym liczby $(L : K)$.*

Dowód. Zastosujemy indukcję ze względu na liczbę czynników pierwszych liczby $(L : K)$. Jeżeli stopień $(L : K)$ jest liczbą pierwszą, to teza wynika z wniosku 15.9.

Niech więc liczba $(L : K)$ będzie złożona. Ponieważ grupa rozwiązalna, której rząd nie jest liczbą pierwszą, nie jest prosta, więc istnieje taki dzielnik normalny H grupy $G = G(L/K)$, że $1 < |H| < |G|$. Niech $M = L^H$. Wtedy $K \subseteq M \subseteq L$ i każde z rozszerzeń $K \subseteq M$ i $M \subseteq L$ jest rozwiązalne. Mamy też $G(L/M) = H$ i $G(M/K) = G/H$.

Z założenia indukcyjnego wynika, że $M \subseteq r_k(K)$ i $L \subseteq r_m(M)$, gdzie k i m są największymi dzielnikami pierwszymi liczb $|G(M/K)| = |G/H|$ i $|G(L/M)| = |H|$ odpowiednio. Zatem $k, m \leqslant n$ i stąd $M \subseteq r_n(K)$ i $L \subseteq r_n(M) \subseteq r_n(r_n(K)) = r_n(K)$. □

Z twierdzeń 3.14 i 15.10 wynika od razu następujący

Wniosek 15.11. *Jeżeli L jest rozszerzeniem Galois ciała K i liczba $(L : K)$ jest potęgą dwójki, to $L \subseteq r_2(K)$.*

Twierdzenie 15.12. *Jeżeli L jest skończonym rozszerzeniem Galois ciała K zawartym w $r(K)$, to grupa $G(L/K)$ jest rozwiązalna.*

Dowód. Z określenia ciała $r(K)$ wynika, że istnieje taki ciąg ciał

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r,$$

że $L \subseteq K_r$ oraz dla $i = 1, 2, \ldots, r$ ciało K_i jest ciałem rozkładu wielomianu postaci $x^{n_i} - a_i \in K_{i-1}[x]$.

Zastosujemy indukcję względem r. Jeżeli $r = 0$, to $K = L$ i teza twierdzenia jest oczywista. Niech więc $r \geqslant 1$.

Ponieważ L i K_1 są rozszerzeniami Galois ciała K, więc z wniosku 14.15 ciało $K_1(L)$ jest rozszerzeniem Galois ciała $K_1(K) = K_1$. Ciało $K_1(L)$ jest zawarte w $r(K_1)$, ponieważ $L \subseteq r(K) \subseteq r(K_1)$. Na mocy założenia indukcyjnego zastosowanego do ciała $K_1(L)$ i ciągu ciał

$$K_1 \subseteq K_2 \subseteq \ldots \subseteq K_r$$

dostajemy, że grupa $G(K_1(L)/K)$ jest rozwiązalna. Grupa $G(K_1/K)$ jest rozwiązalna na mocy wniosku 14.26 .

Ponieważ $K \subseteq K_1 \subseteq K_1(L)$, $K_1(K)$ jest rozszerzeniem Galois ciała K i każde z rozszerzeń $K \subseteq K_1$ i $K_1 \subseteq K_1(L)$ jest, jak wykazaliśmy, rozwiązalne, więc na mocy twierdzenia 14.23 ciało $K_1(L)$ jest rozszerzeniem rozwiązalnym ciała K.

Mamy też $K \subseteq L \subseteq K_1(L)$ i L jest rozszerzeniem Galois ciała K. Ponieważ $K_1(L)$ jest rozszerzeniem rozwiązalnym ciała K, więc na mocy twierdzenia 14.23, L jest rozszerzeniem rozwiązalnym ciała K. Grupa $G(L/K)$ jest więc rozwiązalna. □

Wniosek 15.13. *Jeżeli L jest skończonym rozszerzeniem Galois ciała K i n jest największym dzielnikiem pierwszym liczby $(L : K)$, to następujące warunki są równoważne:*
(i) $L \subseteq r_n(K)$,
(ii) $L \subseteq r(K)$,
(iii) grupa $G(L/K)$ jest rozwiązalna.

Dowód. Implikacja $(i) \Rightarrow (ii)$ jest oczywista, implikacja $(ii) \Rightarrow (iii)$ wynika z twierdzenia 15.12, a implikacja $(iii) \Rightarrow (i)$ z twierdzenia 15.10. □

Wniosek 15.14. *Dla dowolnego wielomian $f \in K[x]$ dodatniego stopnia równanie $f(x) = 0$ jest rozwiązalne w pierwiastnikach wtedy i tylko wtedy, gdy grupa Galois wielomianu $f \in K[x]$ jest rozwiązalna.*

Dowód. Z twierdzenia 14.12 ciało rozkładu wielomianu $f \in K[x]$ jest rozszerzeniem Galois ciała K. Wobec tego na mocy wniosku 15.13 grupa $G(L/K)$ jest rozwiązalna wtedy i tylko wtedy, gdy $L \subseteq r(K)$, tzn. gdy wszystkie pierwiastki wielomianu f wyrażają się przez pierwiastniki względem ciała K. □

15.1.3 Przykłady równań nierozwiązalnych w pierwiastnikach

Lemat 15.15. *Jeżeli wszystkie pierwiastki wielomianu $f = x^n + a_3x^{n-3} + a_4x^{n-4} + ... + a_n \in \mathbb{R}[x]$ są rzeczywiste, to $f = x^n$.*

Dowód. Niech $b_1, b_2, ..., b_n$ będą wszystkimi pierwiastkami wielomianu f. Na podstawie wzorów Vieta mamy $\sum_{i=1}^{n} b_i = 0$ oraz $\sum_{1 \leqslant i < j \leqslant n} b_i b_j = 0$, więc

$$0 = (\sum_{i=1}^{n} b_i)^2 = \sum_{i=1}^{n} b_i^2 + 2 \sum_{1 \leqslant i < j \leqslant n} b_i b_j = \sum_{i=1}^{n} b_i^2.$$

Ponieważ liczby $b_1, b_2, ..., b_n$ są rzeczywiste, więc z równości $\sum\limits_{i=1}^{n} b_i^2 = 0$ wynika, że $b_1 = b_2 = ... = b_n = 0$. Zatem $f = x^n$. □

Twierdzenie 15.16. *Jeżeli K jest podciałem ciała liczb rzeczywistych, wielomian $f \in K[x]$ jest nierozkładalny nad ciałem K, $st(f) = p$ jest liczba pierwszą oraz f ma dokładnie $p-2$ pierwiastki rzeczywiste, to grupą Galois wielomianu f jest $\mathbb{S}_p$.*

Dowód. Niech $b_1, b_2 = \overline{b_1}$ będą zespolonymi, nierzeczywistymi pierwiastkami wielomianu f, natomiast $b_3, b_4, ..., b_p \in \mathbb{R}$ będą pozostałymi jego pierwiastkami. Wówczas $L = K(b_1, ..., b_p)$ jest ciałem rozkładu wielomianu $f \in K[x]$ oraz $L = K(\overline{b_1}, \overline{b_2}, \ldots, \overline{b_p})$. Ale $K \subseteq \mathbb{R}$, więc $\overline{a} \in L$ dla każdego $a \in L$. Wynika stąd, że odwzorowanie $\sigma\colon L \to L$ dane wzorem $\sigma(a) = \overline{a}$ dla $a \in L$ jest automorfizmem ciała L stałym na K, czyli $\sigma \in G(L/K)$. Ponadto $\sigma(b_1) = b_2$, $\sigma(b_2) = b_1$ oraz $\sigma(b_k) = k_k$ dla $k = 3, 4, \ldots, p$. Zatem σ wyznacza transpozycję (b_1, b_2) zbioru $\{b_1, b_2, b_3, \ldots, b_p\}$.

Dla dowolnego $\tau \in G(L/K)$ i dla $k = 1, 2, \ldots, p$, $\tau(b_k)$ jest pierwiastkiem wielomianu f, więc $\tau(b_k) \in \{b_1, b_2, \ldots, b_p\}$. Bez zmniejszania ogólności możemy więc zakładać, że $G(L/K)$ jest podgrupą grupy $\mathbb{S}_p$.

Ponadto mamy $(K(b_1) : K) = st(f) = p$ oraz $K \subseteq K(b_1) \subseteq L$. Wobec tego $p \mid (L : K) = |G(L/K)|$. Zatem z wniosku 4.2 $G(L/K) = \mathbb{S}_p$. □

Wniosek 15.17. *Jeżeli k jest liczbą naturalną posiadającą dzielnik pierwszy q taki, że $q^2 \nmid k$, to grupą Galois wielomianu $f = x^5 - 2kx - k \in \mathbb{Q}[x]$ jest $\mathbb{S}_5$.*

Dowód. Wielomian f jest nierozkładalny w $\mathbb{Q}[x]$ na mocy kryterium Eisensteina. Na mocy twierdzenia 15.16 wystarczy więc udowodnić,

że ma on dokładnie trzy pierwiastki rzeczywiste. Z lematu 15.15 wynika, że ma on co najmniej dwa pierwiastki nierzeczywiste. Ponadto $f(-k) = -k(k^4 - 2k + 1) < 0$, $f(-1) = k - 1 > 0$, $f(0) = -k < 0$, $f(k) = k(k^4 - 2k - 1) > 0$, więc wielomian f ma pierwiastek w każdym z przedziałów $(-k, -1)$, $(-1, 0)$, $(0, k)$. Ma więc on co najmniej trzy pierwiastki rzeczywiste. Ponieważ wielomian f ma pięć pierwiastków, więc ma on dokładnie trzy pierwiastki rzeczywiste. □

Twierdzenie 15.18. *Niech K będzie ciałem i niech $f \in K[x]$ będzie wielomianem nierozkładalnym, $st(f) = p$ będzie liczbą pierwszą i niech grupa Galois wielomianu f będzie rozwiązalna. Wówczas ciało rozkładu L wielomianu $f \in K[x]$ jest generowane przez dowolne dwa jego pierwiastki.*

Dowód. Niech $b_1, b_2, \ldots, b_p$ będą wszystkimi pierwiastkami wielomianu f. Grupę $G(L/K)$ można więc traktować jako podgrupę grupy $\mathbb{S}_p$. Jest to podgrupa przechodnia, ponieważ wielomian f jest nierozkładalny. Na mocy twierdzenia 4.8 grupa $G(L/K(b_1, b_2))$ składa się tylko z automorfizmu tożsamościowego, ponieważ każdy inny automorfizm należący do grupy $G(L/K)$ wyznacza taką permutację zbioru $\{b_1, b_2, \ldots, b_p\}$, która ma co najwyżej jeden punkt stały. Zatem $L = K(b_1, b_2)$. □

Wniosek 15.19. *Jeżeli K jest podciałem ciała L, wielomian $f \in K[x]$ jest nierozkładalny stopnia p, gdzie p jest liczba pierwszą oraz grupa Galois wielomianu f jest rozwiązalna, to liczba pierwiastków wielomianu f w ciele L jest równa 0, 1 lub p.*

Dowód. Jeżeli do L należą co najmniej dwa pierwiastki wielomianu f, to na mocy twierdzenia 15.18 do L należą wszystkie pierwiastki tego wielomianu. □

Twierdzenie 15.20. *Niech $p \geqslant 5$ będzie liczbą pierwszą oraz l, s będą takimi liczbami naturalnymi, że istnieje liczba pierwsza q: $q \mid l$, $q \mid s$ i $q^2 \nmid l$. Wtedy dla wielomianu $f = x^p - (l + s)x - l \in \mathbb{Q}[x]$, równanie $f(x) = 0$ nie jest rozwiązalne w pierwiastnikach.*

Dowód. Z założenia mamy, że $q \mid l+s$. Ponieważ dodatkowo $q^2 \nmid l$, więc na mocy kryterium Eisensteina wielomian $f = x^p - (l+s)x - l \in \mathbb{Q}[x]$ jest nierozkładalny. Z lematu 15.15 wynika, że nie wszystkie pierwiastki wielomianu f są rzeczywiste. Zauważmy również, że liczby $l, s > 1$. Stąd $f(-1) = (-1)^p + (l+s) - l = s - 1 > 0$ oraz $f(0) = -l < 0$. Zatem z własności funkcji ciągłych istnieje $x_1 \in (-1, 0)$ taki, że $f(x_1) = 0$. Ponadto $\lim\limits_{x\to\infty} x^p - (l+s)x - l = \lim\limits_{x\to\infty} x^p(1 - \frac{l+s}{x^{p-1}} - \frac{l}{x^p}) = \infty$, więc istnieje liczba rzeczywista $a > 0$ taka, że $f(a) > 0$. Stąd istnieje $x_2 \in (0, a)$ takie, że $f(x_2) = 0$. Zatem wielomian f ma co najmniej dwa pierwiastki rzeczywiste. Teza wynika więc z wniosku 15.19, jeżeli jako L przyjmie się ciało liczb rzeczywistych. □

15.2 Konstrukcje geometryczne

15.2.1 Liczby wyrażające się przez pierwiastniki kwadratowe

Zastosujemy podane wcześniej pojęcia i twierdzenia teorii ciał do badania wykonalności konstrukcji geometrycznych za pomocą cyrkla i linijki. Udowodnimy, że mając dany pewien układ punktów na płaszczyźnie dowolny punkt daje się skonstruować za pomocą cyrkla i linijki wtedy i tylko wtedy, gdy jego współrzędne wyrażają się przez pierwiastniki kwadratowe względem odpowiedniego ciała. W związku z tym podamy na początku kilka własności ciała $r_2(K)$. W szczególności zbadamy, które pierwiastki z jedynki należą do $r_2(\mathbb{Q})$, tzn. wyrażają się przez pierwiastniki kwadratowe względem ciała liczb wymiernych. Wszystkie ciała rozpatrywane w tym paragrafie są podciałami ciała $\mathbb{C}$ liczb zespolonych. Ponieważ ciało $\mathbb{C}$ jest algebraicznie domknięte, więc można zakładać, że dla takich K, $\overline{K}$ jest podciałem ciała $\mathbb{C}$. Łatwo też zauważyć, że wówczas $\mathbb{Q} \subseteq K$.

Lemat 15.21. *Jeżeli K jest podciałem ciała liczb rzeczywistych i liczba zespolona $a \in r_2(K)$, to $\overline{a} \in r_2(K)$.*

Dowód. Ponieważ $K \subseteq \mathbb{R}$, więc sprzęganie liczb zespolonych jest automorfizmem ciała $\mathbb{C}$ stałym na K. Zatem dla $b \in \overline{K}$ mamy, że $\overline{b} \in \overline{K}$.

Wobec tego odwzorowanie $\varphi\colon r_2(K) \to \overline{K}$ dane wzorem $\varphi(b) = \overline{b}$ jest K-zanurzeniem. Zatem na mocy twierdzenia 15.7 mamy $\varphi(r_2(K)) = r_2(K)$. W szczególności $\overline{a} = \varphi(a) \in r_2(K)$. □

Wniosek 15.22. *Jeżeli K jest podciałem ciała liczb rzeczywistych, $a, b \in \mathbb{R}$, to $a + bi \in r_2(K)$ wtedy i tylko wtedy, gdy $a, b \in r_2(K)$.*

Dowód. Załóżmy, że $a, b \in r_2(K)$. Ponieważ $i \in r_2(K)$ oraz $r_2(K)$ jest ciałem zawierającym także a i b, więc $a + bi \in r_2(K)$.

Na odwrót, niech $a + bi \in r_2(K)$. Wtedy z lematu 15.21 $\overline{a + bi} = a - bi \in r_2(K)$. Ale $r_2(K)$ jest ciałem, więc stąd $a = \frac{1}{2}[(a + bi) + (a - bi)] \in r_2(K)$ i w konsekwencji $bi = (a + bi) - a \in r_2(K)$. Ponadto $i \in r_2(K)$, więc $b = (-i) \cdot (bi) \in r_2(K)$. □

Niech ε_n będzie zespolonym pierwiastkiem pierwotnym z jedynki stopnia n. Można na przykład przyjąć, że

$$\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

Z przykładu 12.16 wynika natychmiast prawdziwość następującego lematu.

Lemat 15.23. *Jeżeli p jest liczbą pierwszą, to $(\mathbb{Q}(\varepsilon_p) : \mathbb{Q}) = p - 1$ oraz $(\mathbb{Q}(\varepsilon_{p^2}) : \mathbb{Q}) = p(p - 1)$.*

Lemat 15.24. *(i) Jeżeli $\varepsilon_n \in r_2(\mathbb{Q})$, to $\varepsilon_{2n} \in r_2(\mathbb{Q})$,*
(ii) Jeżeli $\varepsilon_r, \varepsilon_s \in r_2(\mathbb{Q})$ i liczby r, s są względnie pierwsze, to $\varepsilon_{rs} \in r_2(\mathbb{Q})$,
(iii) Jeżeli $r, s \in \mathbb{N}$ oraz $\varepsilon_{rs} \in r_2(\mathbb{Q})$, to $\varepsilon_r \in r_2(\mathbb{Q})$.

Dowód. (i). Ze wzoru de Moivre'a wynika, że liczba ε_{2n} jest pierwiastkiem wielomianu $x^2 - \varepsilon_n \in r_2(\mathbb{Q})[x]$. Zatem z twierdzenia 15.7 mamy, że $\varepsilon_{2n} \in r_2(\mathbb{Q})$.

(ii). Istnieją liczby całkowite u, v takie, że $ru + sv = 1$. Wobec tego $\varepsilon_{rs} = \varepsilon_{rs}^1 = \varepsilon_{rs}^{ru}\varepsilon_{rs}^{sv} = \varepsilon_s^u\varepsilon_r^v \in r_2(\mathbb{Q})$, gdyż $r_2(\mathbb{Q})$ jest ciałem.

(iii). Ponieważ $r_2(\mathbb{Q})$ jest ciałem oraz ze wzoru de Moivre'a $\varepsilon_r = \varepsilon_{rs}^s$, więc $\varepsilon_r \in r_2(\mathbb{Q})$. □

Lemat 15.25. *Jeżeli p jest liczbą pierwszą nieparzystą, to $\varepsilon_p \in r_2(\mathbb{Q})$ wtedy i tylko wtedy, gdy istnieje taka liczba naturalna n, że $p = 2^n + 1$.*

Dowód. Załóżmy, że $\varepsilon_p \in r_2(\mathbb{Q})$. Ponieważ $\varepsilon_p \notin \mathbb{Q}$, więc na mocy wniosku 15.5 mamy $(\mathbb{Q}(\varepsilon_p) : \mathbb{Q}) = 2^n$ przy pewnym naturalnym n. Z lematu 15.23 wynika więc, że $2^n = p - 1$, czyli $p = 2^n + 1$.

Na odwrót, załóżmy, że $p = 2^n + 1$ dla pewnego $n \in \mathbb{N}$. Jak wiemy, ciało $\mathbb{Q}(\varepsilon_p)$ jest rozszerzeniem Galois ciała $\mathbb{Q}$. Z lematu 15.23 otrzymujemy $(\mathbb{Q}(\varepsilon_p) : \mathbb{Q}) = p - 1 = 2^n$. Wobec tego z wniosku 15.11 wynika, że $\mathbb{Q}(\varepsilon_p) \subseteq r_2(\mathbb{Q})$, skąd $\varepsilon_p \in r_2(\mathbb{Q})$. □

Zauważmy jeszcze, że jeżeli liczba p postaci $2^n + 1$ jest pierwsza, to $n = 2^k$ dla pewnego $k \in \mathbb{N}_0$. Istotnie, gdyby liczba n nie była potęgą dwójki, to miałaby czynnik nieparzysty $2r+1 > 1$, tzn. $n = (2r+1) \cdot s$. Wtedy

$$p = 2^n + 1 = (2^s)^{2r+1} + 1 = (2^s + 1)[(2^s)^{2r} - (2^s)^{2r-1} + \ldots - 2^s + 1)].$$

Zatem liczba p byłaby złożona.

Liczby pierwsze postaci $F_k = 2^{2^k} + 1$ $(k = 0, 1, \ldots)$ nazywamy liczbami pierwszymi Fermata. Znanych jest pięć liczb pierwszych Fermata: $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$. Nie wiadomo, czy istnieje co najmniej jedna liczba pierwsza Fermata różna od wyżej wymienionych. Udowodniono, że dla kilkudziesięciu wartości $k > 4$ liczby F_k są złożone. Już Euler zauważył, że $641 \mid F_5$.

Twierdzenie 15.26. *Jeżeli n jest liczbą naturalną, to $\varepsilon_n \in r_2(\mathbb{Q})$ wtedy i tylko wtedy, gdy n ma postać $n = 2^a p_1 p_2 \ldots p_r$, gdzie $a, r \in \mathbb{N}_0$ i $p_1, p_2, \ldots, p_r$ są różnymi liczbami pierwszymi Fermata.*

Dowód. $\Leftarrow$. Z lematu 15.25 wynika, że $\varepsilon_{p_i} \in r_2(\mathbb{Q})$ dla $i = 1, 2, \ldots, r$. Z lematu 15.24 otrzymujemy więc, że $\varepsilon_n \in r_2(\mathbb{Q})$.

$\Rightarrow$. Niech $n = 2^a q_1^{k_1} q_2^{k_2} \ldots q_s^{k_s}$ będzie rozkładem liczby n na iloczyn potęg różnych liczb pierwszych, gdzie $a, s \in \mathbb{N}_0$ oraz $k_i \in \mathbb{N}$ dla $i = 1, 2, \ldots, s$. Udowodnimy, że $k_1 = k_2 = \ldots = k_s = 1$ oraz $q_1, q_2, \ldots, q_s$ są liczbami pierwszymi Fermata. Z lematu 15.24 mamy,

że $\varepsilon_{q_i} \in r_2(\mathbb{Q})$dla $i = 1, 2, \ldots, s$, a więc q_i jest liczbą pierwszą Fermata na mocy lematu 15.25. Gdyby dla pewnej liczby $i = 1, 2, \ldots, s$ zachodziło $k_i \geqslant 2$, to $q_1^2 \mid n$. Wobec tego $\varepsilon_{q_i^2} \in r_2(\mathbb{Q})$. Z wniosku 15.5 wynika więc, że liczba $(\mathbb{Q}(\varepsilon_{q_i^2}) : \mathbb{Q})$ jest potęgą dwójki. Z drugiej strony z lematu 15.23 otrzymujemy, że liczba ta jest równa $q_i(q_i - 1)$. Nie jest ona potęgą dwójki, ponieważ jest podzielna przez liczbę pierwszą nieparzystą q_i. Uzyskana sprzeczność dowodzi, że $k_1 = k_2 = \ldots = k_s = 1$. □

15.2.2 Punkty konstruowalne

Wiele zadań konstrukcyjnych można sformułować w następującej postaci. Na płaszczyźnie dane są pewne punkty i figury. Posługując się cyrklem i linijką należy skonstruować pewien nowy punkt lub figurę.

Opiszemy najpierw zbiór wszystkich punktów, które mogą być otrzymane w ten sposób – są to tzw. punkty konstruowalne za pomocą cyrkla i linijki. Następnie udowodnimy twierdzenie charaktyryzujące punkty konstruowalne. Jak się okazuje, punkt jest konstruowalny wtedy i tylko wtedy, gdy jego współrzędne wyrażają się przez pierwiastniki kwadratowe względem odpowiedniego ciała.

Niech na płaszczyźnie dane będą punkty $P_1, P_2, \ldots, P_n$ i figury $F_1, F_2, \ldots, F_r$, gdzie $n \geqslant 2$ i $r \geqslant 0$. Niech $A_0 = \{P_1, P_2, \ldots, P_n\}$ będzie zbiorem danych punktów. Wykonujemy następujące czynności:
(*) Przez każde dwa dane punkty prowadzimy prostą i z każdego z danych punktów zakreślamy okręgi, których promienie mają długości równe odległościom pewnych danych punktów.

Niech A_1 będzie zbiorem punktów przecięcia narysowanych figur: prostych, okręgów i figur $F_1, F_2, \ldots, F_r$. Ponownie wykonujemy czynność (*) traktując A_1 jako zbiór punktów danych. W wyniku otrzymujemy zbiór punktów przecięcia wszystkich narysowanych figur, który oznaczamy przez A_2. Znów wykonujemy czynność (*) traktując A_2 jako zbiór punktów danych itd. Nietrudno zauważyć, że $A_0 \subseteq A_1 \subseteq A_2 \subseteq \ldots$.

Punkty przecięcia narysowanych w ten sposób figur nazywamy **punktami konstruowalnymi za pomocą cyrkla i linijki przy danych punktach** $P_1, P_2, \ldots, P_n$ **i figurach** $F_1, F_2, \ldots, F_r$ lub krótko

- **punktami konstruowalnymi**. Zatem zbiorem wszystkich punktów konstruowalnych jest $\bigcup_{n=0}^{\infty} A_n$. W dalszym ciągu będziemy zakładali, że układ współrzędnych na płaszczyźnie jest tak obrany, iż $P_1 = (0,0)$, $P_2 = (1,0)$. Nie zmniejsza to ogólności rozważań.

Twierdzenie 15.27 (Wantzel)**.** *Niech dane będą punkty* $P_1, \ldots, P_n$*, gdzie* $P_i = (a_i, b_i)$ *dla* $i = 1, 2, \ldots, n$ *oraz* $P_1 = (0,0)$ *i* $P_1 = (1,0)$*. Punkt* $P = (a,b)$ *jest konstruowalny wtedy i tylko wtedy, gdy* $a, b \in r_2(K)$*, gdzie* $K = \mathbb{Q}(a_1, b_1, \ldots, a_n, b_n)$*.*

Dowód. Załóżmy, że punkt (a,b) jest konstruowalny. Zatem $(a,b) \in A_m$ dla pewnego $m \in \mathbb{N}_0$. Przez indukcję ze względu na m udowodnimy, że $a, b \in r_2(K)$. Dla $m = 0$ mamy $(a,b) = (a_i, b_i)$ dla pewnego $i \leqslant n$. Zatem $a, b \in K$ i tym bardziej $a, b \in r_2(K)$. Załóżmy, że dla pewnego $m \in \mathbb{N}$ każdy punkt zbioru A_{m-1} ma współrzędne należące do ciała $r_2(K)$ i niech $P = (a,b) \in A_m$.

Z określenia zbioru A_m wynika, że P jest punktem przecięcia dwóch figur (prostych, okręgów) wyznaczonych przez punkty należące do zbioru A_{m-1}. Są trzy możliwości:
(1) P jest punktem przecięcia prostych L_1 i L_2 wyznaczonych przez punkty należące do A_{m-1}. Z geometrii analitycznej wynika zatem, że równanie prostej L_i ma postać $A_i x_1 + B_i x_2 + C_i = 0$ dla pewnych $A_i, B_i, C_i \in r_2(K)$, $i = 1, 2$. Zatem liczby a i b są rozwiązaniem układu równań liniowych $A_1 x_1 + B_1 x_2 + C_1 = 0$, $A_2 x_1 + B_2 x_2 + C_2 = 0$. Rozwiązanie to można wyznaczyć za pomocą wzorów Cramera. Zatem liczby a, b otrzymujemy wykonując na liczbach $A_1, A_2, B_1, B_2, C_1, C_2 \in r_2(K)$ działania arytmetyczne. Wobec tego $a, b \in r_2(K)$.
(2) P jest punktem przecięcia prostej L_1 i okręgu O_1, które są wyznaczone przez punkty należące do A_{m-1}. Niech prosta L_1 będzie wyznaczona przez punkty $(c_{11}, c_{12}), (d_{11}, d_{12}) \in A_{m-1}$. Z założenia indukcyjnego $c_{11}, c_{12}, d_{11}, d_{12} \in r_2(K)$. Zatem z geometrii analitycznej równanie ogólne prostej L_1 ma postać $Ax_1 + Bx_2 + C = 0$ dla pewnych $A, B, C \in r_2(K)$. Niech środkiem okręgu O_1 będzie punkt $(c_1, c_2) \in A_{m-1}$, a długością promienia - odległość punktów (d_1, d_2) i (e_1, e_2) należących do A_{m-1}. Z założenia indukcyjnego wynika, że $c_1, c_2, d_1, d_2, e_1, e_2 \in r_2(K)$.

Równanie okręgu O_1 ma więc postać

$$(x_1 - c_1)^2 + (x_2 - c_2)^2 = (d_1 - e_1)^2 + (d_2 - e_2)^2.$$

Aby znaleźć współrzędne a, b punktu przecięcia prostej L_1 z okręgiem O_1, wystarczy więc rozwiązać układ równań złożony z równana liniowego i równania kwadratowego. Współczynniki tych równań należą do ciała $r_2(K)$. Wyznaczając jedną z niewiadomych z równania liniowego i podstawiając do równania kwadratowego otrzymujemy do rozwiązania jedno równanie kwadratowe z jedną niewiadomą o współczynnikach w ciele $r_2(K)$. Z twierdzenia 15.5 wynika, że pierwiastki tego równania należą do $r_2(K)$. Zatem $a, b \in r_2(K)$.
(3) P jest punktem przecięcia okręgów O_1 i O_2 wyznaczonych przez punkty należące do A_{m-1}. Dla $i = 1, 2$ niech środkiem okręgu O_i będzie punkt $(e_{i1}, e_{i2}) \in A_{m-1}$, a długością promienia - odległość punktów (d_{i1}, d_{i2}) i (e_{i1}, e_{i2}) należących do A_{m-1}. Z założenia indukcyjnego wynika, że $c_{ij}, d_{ij}, e_{ij} \in r_2(K)$. Równania okręgów O_1 i O_2 mają postać

$$(x_1 - c_{11})^2 + (x_2 - c_{12})^2 = (d_{11} - e_{11})^2 + (d_{12} - e_{12})^2,$$

$$(x_1 - c_{21})^2 + (x_2 - c_{22})^2 = (d_{21} - e_{21})^2 + (d_{22} - e_{22})^2.$$

Odejmując stronami pierwsze równanie od drugiego otrzymujemy układ równań równoważny złożony z równania liniowego i równania kwadratowego. Współczynniki tego układu należą do $r_2(K)$. Rozpatrując przypadek (2) wykazaliśmy, że rozwiązania takiego układu należą do $r_2(K)$. Zatem $a, b \in r_2(K)$.

Załóżmy z kolei, że współrzędne punktu $P = (a, b)$ należą do ciała $r_2(K)$. Udowodnimy, że punkt P jest konstruowalny.

Ponieważ $i \in r_2(K)$ i $r_2(K)$ jest ciałem, więc na mocy wniosku 15.22 $a + bi \in r_2(K)$. Istnieje zatem taki ciąg ciał

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_r,$$

że $a + bi \in K_r$ oraz $(K_j : K_{j-1}) = 2$ dla $j = 1, 2, \ldots, r$. Przez indukcję ze względu na j wykażemy, że jeżeli liczba zespolona $c + di$ należy do ciała K_j, to odpowiadający jej punkt (c, d) jest konstruowalny.

Rozpatrzmy najpierw przypadek $j = 0$. Niech $c, d \in K_0 = K = \mathbb{Q}(a_1, b_1, \ldots, a_n, b_n)$. Mamy udowodnić, że punkt (c, d) jest konstruowalny. Wystarczy oczywiście udowodnić, że konstruowalne są punkty $(c, 0)$ i $(d, 0)$.

Ponieważ punkty $(a_1, 0), (b_1, 0), \ldots, (a_n, 0), (b_n, 0)$ są konstruowalne, a każda liczba należąca do ciała K powstaje przez wykonanie działań arytmetycznych na liczbach $a_1, b_1, \ldots, a_n, b_n$, więc zadanie sprowadza się do tego, by wykazać, że jeżeli dane są punkty $(p, 0)$ i $(q, 0)$, to można skonstruować punkty $(p + q, 0)$, $(-q, 0)$, $(pq, 0)$, $(\frac{p}{q}, 0)$ (ten ostatni w przypadku, gdy $q \neq 0$). Pierwsze dwie konstrukcje są oczywiste, dwie ostatnie wynikają z twierdzenia Talesa.

Załóżmy z kolei, że dla pewnej liczby naturalnej $j \leqslant r$, jeżeli liczba zespolona należy do ciała K_{j-1}, to punkt jej odpowiadający jest konstruowalny. Wykażemy, że jeżeli liczba zespolona należy do ciała K_j, to punkt jej odpowiadający jest konstruowalny. Ponieważ $(K_j : K_{j-1}) = 2$, więc istnieje taka liczba zespolona $z \in K_{j-1}$, że $K_j = K_{j-1}(\sqrt{z})$. Dowolna liczba należąca do ciała K_j ma więc postać $u + w\sqrt{z}$, gdzie $u, w \in K_{j-1}$. Z założenia indukcyjnego wynika, że punkty odpowiadające liczbom zespolonym u, w, z są konstruowalne. Mamy udowodnić, że konstruowalny jest punkt odpowiadający liczbie zespolonej $u + w\sqrt{z}$.

Zadanie sprowadza się więc do tego, by mając dane dwa punkty na płaszczyźnie skonstruować punkt, któremu odpowiada liczba zespolona równa

a) sumie liczb zespolonych odpowiadających punktom danym,

b) iloczynowi liczb zespolonych odpowiadających punktom danym,

c) pierwiastkowi kwadratowemu z liczby zespolonej odpowiadającej jednemu z punktów danych.

Konstrukcja a) sprowadza się do konstrukcji sumy dwóch danych wektorów.

Konstrukcja b). Zapisując w postaci trygonometrycznej liczby zespolone x i x' odpowiadające punktom danym

$$x = r(\cos\alpha + i\sin\alpha), \qquad x' = r'(\cos\alpha' + i\sin\alpha')$$

stwierdzamy, że

$$xx' = rr'(\cos(\alpha + \alpha') + i\sin(\alpha + \alpha')).$$

Szukany punkt odpowiadający liczbie zespolonej xx' leży więc na okręgu o środku w punkcie $(0,0)$ i promieniu długości rr' oraz na półprostej o początku w punkcie $(0,0)$, która tworzy kąt $\alpha + \alpha'$ z osią odciętych.

Zadanie sprowadza się więc do tego, by mając dane odcinki o długościach r i r' skonstruować odcinek o długości rr' oraz mając dane kąty α i α' skonstruować kąt $\alpha + \alpha'$. Pierwsza konstrukcja wynika z twierdzenia Talesa, druga jest oczywista.

Konstrukcja c). Zapisując w postaci trygonometrycznej liczbę zespoloną x odpowiadającą punktowi danemu, $x = r(\cos\alpha + i\sin\alpha)$ stwierdzamy, że

$$\sqrt{x} = \pm\sqrt{r}(\cos\frac{\alpha}{2} + i\sin\frac{\alpha}{2}).$$

Szukany punkt odpowiadający liczbie zespolonej $\sqrt{x}$ leży więc na okręgu o środku w punkcie $(0,0)$ i promieniu długości $\sqrt{r}$ oraz na prostej przechodzącej przez punkt $(0,0)$, która tworzy kąt $\frac{\alpha}{2}$ z osią odciętych. Zadanie sprowadza się więc do tego, by mając dany odcinek o długości r skonstruować odcinek o długości $\sqrt{r}$ oraz mając dany kąt α skonstruować kąt $\frac{\alpha}{2}$. Obie konstrukcje są dobrze znane. □

Wniosek 15.28. *Jeżeli dane są punkty $P_i = (a_i, b_i)$, gdzie $i = 1, 2, \ldots, n$ oraz $P_1 = (0,0)$, $P_2 = (1,0)$ i punkt (a,b) jest konstruowalny oraz $K = \mathbb{Q}(a_1, b_1, \ldots, a_n, b_n)$, to każda z liczb $(K(a,b) : K)$ i $(K(a + bi) : K)$ jest potęgą dwójki o całkowitym nieujemnym wykładniku.*

Dowód. Na mocy twierdzenia 15.27 i wniosku 15.22 liczby a, b i $a + bi$ należą do ciała $r_2(K)$. Teza wniosku wynika więc z wniosku 15.5. □

Wniosek 15.29. *Jeżeli liczba rzeczywista a jest przestępna względem ciała $K = \mathbb{Q}(a_1, b_1, \ldots, a_n, b_n)$, gdzie $a_1, b_1, \ldots, a_n, b_n \in \mathbb{R}$, to punkt $(a,0)$ nie jest konstruowalny przy danych punktach $P_i = (a_i, b_i)$, gdzie $i = 1, 2, \ldots, n$ oraz $P_1 = (0,0)$ i $P_2 = (1,0)$.*

Dowód. W tym przypadku stopień $(K(a) : K)$ jest nieskończony. Nie jest on więc potęgą dwójki o całkowitym nieujemnym wykładniku. Teza wynika więc z poprzedniego wniosku. □

15.2.3 Przykłady zadań konstrukcyjnych

Zastosujemy teraz twierdzenia udowodnione w poprzednich punktach do rozwiązania konkretnych zadań konstrukcyjnych.

a) Podwojenie sześcianu. Dany jest sześcian o krawędzi długości 1, zbudować sześcian o dwa razy większej objętości.

Udowodnimy, że za pomocą cyrkla i linijki nie można skonstruować odcinka o długości a równej długości krawędzi tego sześcianu, tzn. $a = \sqrt[3]{2}$. Istotnie, liczba $(\mathbb{Q}(a) : \mathbb{Q}) = 3$ nie jest potęgą dwójki, a więc na mocy wniosku 15.28 odcinek o długości a nie jest konstruowalny.

b) Kwadratura koła. Dane jest koło o promieniu długości 1, zbudować kwadrat o polu równym polu tego koła.

Udowodnimy, że za pomocą cyrkla i linijki nie można skonstruować odcinka o długości a równej długości boku tego kwadratu, tzn. $a = \sqrt{\pi}$. Gdyby $a \in r_2(\mathbb{Q})$, to $\pi = a^2 \in r_2(\mathbb{Q})$ i byłby konstruowalny punkt $P = (\pi, 0)$. Jednak F.Lindemann w r. 1882 udowodnił, że liczba π jest przestępna, a więc na mocy wniosku 15.29 punkt P nie jest konstruowalny. Uzyskana sprzeczność dowodzi, że odcinek o długości $\sqrt{\pi}$ nie jest konstruowalny.

c) Trysekcja kąta. Dany jest kąt φ, zbudować kąt $\frac{\varphi}{3}$. Dla pewnych kątów φ ta konstrukcja jest wykonalna za pomocą cyrkla i linijki, a dla pewnych - nie jest. Mówi o tym następujące

Twierdzenie 15.30. *Kąt φ można podzielić na trzy równe części za pomocą cyrkla i linijki wtedy i tylko wtedy, gdy wielomian $f = x^3 - 3x - 2\cos\varphi$ jest rozkładalny w $\mathbb{Q}(\cos\varphi)[x]$.*

Dowód. Zakładamy, jak zwykle, że dane są punkty $(0,0)$ i $(1,0)$. Łatwo zauważyć, że kąt α daje się skonstruować za pomocą cyrkla i linijki wtedy i tylko wtedy, gdy punkt $(\cos\alpha, 0)$ jest konstruowalny. Zadanie nasze można więc sformułować tak:

Dane są punkty $(0,0)$, $(1,0)$, $(\cos\varphi, 0)$, skonstruować punkt $(\cos\frac{\varphi}{3}, 0)$.

Z tożsamości $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$ wynika, że

$$8\cos^3\frac{\varphi}{3} - 6\cos\frac{\varphi}{3} - 2\cos\varphi = 0,$$

Zdigitalizowano i udostępniono w ramach projektu pn.
Rozbudowa otwartych zasobów naukowych Repozytorium Uniwersytetu w Białymstoku – kontynuacja,
dofinansowanego z programu „Społeczna odpowiedzialność nauki" Ministra Edukacji i Nauki
na podstawie umowy BIBL/SP/0040/2023/01

czyli liczba $a = 2\cos\frac{\varphi}{3}$ jest pierwiastkiem wielomianu $f = x^3 - 3x - 2\cos\varphi$.

Jeżeli wielomian f jest nierozkładalny w $\mathbb{Q}(\cos\varphi)[x]$, to liczba $(\mathbb{Q}(\cos\varphi)(a) : \mathbb{Q}(\cos\varphi)) = 3$ nie jest potęgą dwójki, a więc na mocy wniosku 15.28 punkt $(a, 0)$ nie jest konstruowalny i tym bardziej nie jest konstruowalny punkt $(\frac{a}{2}, 0) = (\cos\frac{\varphi}{3}, 0)$.

Jeżeli wielomian f jest rozkładalny w $\mathbb{Q}(\cos\varphi)[x]$, to każdy jego pierwiastek jest pierwiastkiem pewnego wielomianu stopnia co najwyżej drugiego o współczynnikach w ciele $\mathbb{Q}(\cos\varphi)$. W szczególności $a = 2\cos\frac{\varphi}{3} \in r_2(\mathbb{Q}(\cos\varphi))$. Zatem punkt $(a, 0)$ jest konstruowalny, a więc i punkt $(\frac{a}{2}, 0)$ jest konstruowalny. □

Pokażemy teraz, że kąta $\varphi = \frac{\pi}{3}$ nie można podzielić na trzy równe części za pomocą cyrkla i linijki. Wielomian f z twierdzenia 15.30 ma w tym przypadku postać $f = x^3 - 3x - 1$. Nie jest on rozkładalny w $\mathbb{Q}(\cos\varphi)[x] = \mathbb{Q}[x]$, ponieważ każda liczba wymierna będąca pierwiastkiem tego wielomianu jest liczbą całkowitą i jest dzielnikiem wyrazu wolnego. Mamy jednak $f(1), f(-1) \neq 0$.

Zatem z twierdzenia 15.30 wynika, że nie można podzielić kąta $\varphi = \frac{\pi}{3}$ na trzy równe części za pomocą cyrkla i linijki. Tym bardziej nie jest konstruowalny kąt $\frac{\varphi}{3} = \frac{\pi}{9} = 20°$.

d) Konstrukcja wielokątów foremnych. Zbadamy, dla jakich liczb naturalnych n można skonstruować za pomocą cyrkla i linijki n-kąt foremny.

Twierdzenie 15.31 (Gauss)**.** *Za pomocą cyrkla i linijki można skonstruować n-kąt foremny wtedy i tylko wtedy, gdy $n > 2$ oraz $n = 2^a p_1 \dots p_r$, gdzie $a, r \in \mathbb{N}_0$ oraz $p_1, \dots, p_r$ są różnymi liczbami pierwszymi Fermata.*

Dowód. Zakładamy, jak zwykle, że dane są punkty $(0, 0)$ i $(1, 0)$. Jeżeli można skonstruować pewien n-kąt foremny, to można też skonstruować kąt $\frac{2\pi}{n}$. Można więc skonstruować n-kąt foremny wpisany w koło $x_1^2 + x_2^2 = 1$, którego jednym z wierzchołków jest punkt $(1, 0)$, a sąsiednim wierzchołkiem, punkt $P = (\cos\frac{2\pi}{n}, \sin\frac{2\pi}{n})$. Zatem za pomocą cyrkla i linijki można skonstruować pewien n-kąt foremny wtedy i tylko

wtedy, gdy można skonstruować punkt P. Na mocy wniosku 15.22 oraz twierdzenia 15.27 punkt P jest konstruowalny wtedy i tylko wtedy, gdy $\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n} \in r_2(\mathbb{Q})$. Z twierdzenia 15.26 wynika więc teza twierdzenia. □

Literatura

[1] R. R. Andruszkiewicz, *Wykłady z algebry ogólnej I*, Wydawnictwo Uniwersytetu w Białymstoku, Białystok 2005.
[2] Cz. Bagiński, *Wstęp do teorii grup*, SCRIPT, Warszawa 2002.
[3] A. Białynicki-Birula, *Algebra*, PWN, Warszawa 1971.
[4] J. Browkin, *Teoria ciał*, PWN, Warszawa 1977.
[5] M. Bryński i J. Jurkiewicz, *Zbiór zadań z algebry*, PWN, Warszawa 1978.
[6] A. I. Kostrykin, *Wstęp do algebry*, PWN, Warszawa 1984.
[7] A. I. Kostrykin, *Zbiór zadań z algebry*, PWN, Warszawa 1995.
[8] J. Rutkowski, *Algebra abstrakcyjna w zadaniach*, PWN, Warszawa 2000.