Algebra

Wykłady dla Studiów Doktoranckich

Kazimierz Szymiczek

29.11.2010

Spis treści

Przedmowa

Sometimes one has to say difficult things,
but one ought to say them as simply as one knows how.
G. H. Hardy

Program studiów doktoranckich w Uniwersytecie Śląskim przewiduje wykłady z czterech podstawowych dyscyplin matematycznych. Wykłady te są adresowane do wszystkich uczestników studiów doktoranckich i mają ustanowić pewien minimalny standard wykształcenia matematycznego wszystkich doktorów, niezależnie od ich specjalizacji naukowej. W związku z tym programy tych wykładów przewidują jedynie hasła o ogólnym znaczeniu i unikają problematyki ważnej jedynie dla specjalistów. Niniejszy skrypt jest zapisem takiego wykładu z algebry w roku akademickim 2008–2009.

Rozdział 1

Grupy

Ostatnie zmiany 16.09.2010 r.

1.1 Grupy, podgrupy, homomorfizmy

Rozpoczniemy od przypomnienia podstawowych pojęć i faktów z teorii grup, występujących w kursowym uniwersyteckim wykładzie algebry. Następujące książki będą przydatne w odświeżaniu tych wiadomości:

[BB] A. Białynicki-Birula, *Zarys algebry*. PWN Warszawa 1987.
[H] I. N. Herstein, *Topics in Algebra*. 2nd edition. Wiley, New York 1975.
[KM] M. I. Kargapołow, J. I. Mierzliakow, *Podstawy teorii grup*. PWN Warszawa 1989.
[L] S. Lang, *Algebra*. PWN Warszawa 1973.
[S] K. Szymiczek, *Zbiór zadań z teorii grup*. PWN Warszawa 1989.

1.1.1 Definicja i przykłady grup

Półgrupą nazywamy system złożony ze zbioru S i określonego w tym zbiorze łącznego działania binarnego.
Monoidem nazywamy półgrupę z jedynką (elementem neutralnym).
Grupą nazywamy monoid, w którym każdy element ma element odwrotny.
Inne definicje: zob. [S], zad. **051, 053**, niezależność aksjomatów: zad. **052**.

Przykład 1.1.1. (a) *Grupa symetryczna* $S(X)$ zbioru X. Jej elementami są *bijekcje* $\varphi : X \to X$, natomiast działaniem jest superpozycja bijekcji: dla $\varphi, \psi \in S(X)$ odwzorowanie $\varphi \circ \psi : X \to X$ działa następująco:

$$(\varphi \circ \psi)(x) = \varphi(\psi(x))$$

dla każdego $x \in X$. Gdy zbiór X jest skończony, grupę $S(X)$ nazywa się grupą permutacji zbioru X i oznacza $S(n)$ (lub S_n), gdzie n jest liczbą elementów zbioru X.
(b) *Grupa funkcji* $M(X, G)$ określonych na zbiorze X o wartościach w grupie G. Dla dwóch funkcji $f, g : X \to G$ ich iloczyn definiujemy jako funkcję $fg : X \to G$ taką, że

$$(fg)(x) = f(x) \cdot g(x)$$

dla każdego $x \in X$ (po prawej stronie mamy iloczyn dwóch elementów grupy G).
(c) *Pełna grupa liniowa* $\mathbf{GL}(n, F)$ składa się z wszystkich *odwracalnych* macierzy

kwadratowych stopnia n o elementach z ciała F. *Specjalna grupa liniowa* $\mathbf{SL}(n, F)$ składa się z wszystkich macierzy kwadratowych stopnia n o elementach z ciała F, których wyznacznik jest równy 1.
(d) *Grupa kwaternionów Quat*. W grupie $\mathbf{SL}(2, \mathbb{C})$ weźmy macierze

$$A = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \quad B = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Wtedy $A^4 = B^4 = I, A^2 = B^2, BAB^{-1} = A^{-1}$ i równości te pozwalają stwierdzić, że następujących 8 macierzy

$$I, A, A^2, A^3, B, AB, A^2B, A^3B$$

tworzy grupę. Nazywamy ją *grupą kwaternionów* i oznaczamy *Quat* lub Q.

(e) *Grupa diedralna* $D(n)$. W grupie permutacji $S(n)$ weźmy permutacje

$$x = (12 \dots n), \quad y = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}.$$

Sprawdzamy, że $x^n = y^2 = 1,\ yxy^{-1} = x^{-1}$. Równości te pozwalają stwierdzić, że $2n$ permutacji

$$1, x, \dots, x^{n-1}, y, xy, \dots, x^{n-1}y$$

tworzy grupę. Nazywamy ją grupą diedralną i oznaczamy $D(n)$ (lub D_n). Grupę tę nazywa się także grupą izometrii $n-$kąta foremnego, gdyż numerując wierzchołki $n-$kąta foremnego liczbami $1, 2, \dots, n$ stwierdzamy, że x i y, a także każdy element grupy $D(n)$, można zinterpretować jako izometrię tego $n-$kąta. Faktycznie są to wszystkie izometrie $n-$kąta foremnego.

Obszerną listę przykładów można znaleźć w [S], zad. **001**–**020**.

1.1.2 Podgrupy i warstwy

Podgrupą H grupy G nazywamy podzbiór grupy G zamknięty ze względu na działanie grupowe (jeśli $a, b \in H$, to także $ab \in H$), który sam jest grupą ze względu na działanie będące zacieśnieniem działania na G do H. Piszemy wtedy $H < G$.
$H < G$ wtedy i tylko wtedy, gdy spełniony jest warunek:

$$x, y \in H \Rightarrow xy^{-1} \in H.$$

Łatwo stwierdzić, że część wspólna dowolnej rodziny podgrup grupy G jest podgrupą grupy G. W szczególności, jeśli A jest podzbiorem grupy G, to część wspólna wszystkich podgrup grupy G zawierających zbiór A jest podgrupą grupy G. Nazywamy ją podgrupą generowaną przez zbiór A i oznaczamy $\langle A \rangle$. Na przykład, grupa kwaternionów *Quat* jest podgrupą grupy $\mathbf{SL}(2, \mathbb{C})$ generowaną przez macierze A, B z przykładu 1.1.1(d). Podobnie, grupa diedralna $D(n)$ jest podgrupą $S(n)$ generowaną przez permutacje x, y z przykładu 1.1.1(e), zatem w grupie $S(n)$ mamy $\langle x, y \rangle = D(n)$.
Dla podzbiorów A i B grupy G określamy ich *iloczyn kompleksowy*

$$A \cdot B := \{a \cdot b \in G : a \in A, b \in B\}.$$

Dla każdych trzech podzbiorów A, B, C grupy G mamy

$$(A \cdot B) \cdot C = A \cdot (B \cdot C).$$

Jeśli A i B są podgrupami grupy G, to iloczyn AB jest podgrupą grupy G wtedy i tylko wtedy gdy $AB = BA$.

Warstwą lewostronną grupy G względem podgrupy H wyznaczoną przez element $a \in G$ nazywamy zbiór

$$aH := \{a\} \cdot H = \{ah \in G : h \in H\}.$$

Podobnie definiuje się warstwę prawostronną $Ha := \{ha \in G : h \in H\}$.
Każda warstwa grupy G względem podgrupy H jest równoliczna z podgrupą H. Mianowicie odwzorowania $H \to aH, \quad h \mapsto ah$ oraz $H \to Ha, \quad h \mapsto ha$ są bijekcjami.
Jeśli dwie warstwy lewostronne aH i bH mają choć jeden element wspólny, to są identyczne: $aH = bH$. Podobnie dla warstw prawostronnych.
Ponieważ każdy element $a \in G$ należy do dokładnie jednej warstwy aH grupy G względem podgrupy H i różne warstwy są rozłączne, grupę G można przedstawić jako sumę mnogościową parami rozłącznych warstw

$$G = \bigcup_{i \in I} a_i H.$$

Łatwo sprawdzić, że odwzorowanie $aH \mapsto Ha^{-1}$ jest bijekcją pomiędzy zbiorem warstw lewostronnych i zbiorem warstw prawostronnych grupy G względem podgrupy H. Zatem zbiory te są równoliczne a ich wspólną moc nazywa się *indeksem* podgrupy H w grupie G. Zbiór parami rozłącznych warstw lewostronnych $a_i H$ oznacza się $G : H$. Moc $|G : H|$ zbioru warstw $G : H$, czyli moc zbioru I, jest więc indeksem podgrupy H w grupie G.
Rozkład grupy G na sumę mnogościową parami rozłącznych warstw wraz z faktem, że każde dwie warstwy grupy względem tej samej podgrupy są równoliczne, prowadzi natychmiast do twierdzenia Lagrange'a mówiącego, że dla grupy skończonej G i jej dowolnej podgrupy H mamy

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

Łatwo też zauważyć uogólnienie: dla grupy skończonej G, jeśli $K < H < G$, to

$$|G : H| \cdot |H : K| = |G : K|.$$

1.1.3 Podgrupy normalne

Podgrupa H grupy G nazywa się podgrupą *normalną*, jeśli

$$aH = Ha \quad \forall a \in G.$$

Piszemy wtedy $H \lhd G$. Zob. [S], zad. **213**, gdzie podanych jest 10 innych warunków definiujących podgrupę normalną.

Dwie podstawowe obserwacje:

1. Jeśli $H \lhd G$ i $K < G$, to $HK = KH$ i wobec tego HK jest podgrupą grupy G. A więc iloczyn kompleksowy dowolnej podgrupy normalnej i dowolnej podgrupy grupy G jest podgrupą grupy G.
2. Jeśli $H \lhd G$ oraz $a, b \in G$, to

$$aH \cdot bH = a(Hb)H = a(bH)H = abHH = abH.$$

A więc iloczyn kompleksowy dwóch warstw względem podgrupy normalnej H jest znów warstwą względem H. Zbiór $G : H$ wszystkich warstw aH grupy G względem podgrupy normalnej H oznacza się G/H. Zbiór G/H z kompleksowym mnożeniem warstw jest grupą (z jedynką H). Nazywa się ją *grupą ilorazową* grupy G względem podgrupy normalnej H.

Przykład 1.1.2. Jeśli grupa G jest *abelowa*, to każda podgrupa H grupy G jest podgrupą normalną.
W dowolnej grupie G jej *centrum*

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

jest podgrupą normalną w G.
W pełnej grupie liniowej $\mathbf{GL}(n, K)$ stopnia n nad ciałem K centrum składa się z wszystkich macierzy skalarnych aI, gdzie $a \in K^*$ oraz I jest macierzą jednostkową stopnia n (zob. [S], zad. **288**). Mamy także $\mathbf{SL}(n, K) \lhd \mathbf{GL}(n, K)$. Dla $A \in \mathbf{GL}(n, K)$ warstwa $A \cdot \mathbf{SL}(n, K)$ składa się z wszystkich macierzy grupy $\mathbf{GL}(n, K)$, których wyznacznik jest równy $\det A$.
Komutantem grupy G nazywa się podgrupę $[G, G]$ grupy G generowaną przez zbiór wszystkich komutatorów, czyli elementów postaci $[a, b] := a^{-1}b^{-1}ab$, gdzie a, b są dowolnymi elementami G. W grupie abelowej G mamy $[a, b] = 1$ dla każdych $a, b \in G$, zatem także $[G, G] = 1$. Natomiast w grupie nieabelowej G jej komutant $[G, G]$ jest zawsze nietrywialną podgrupą grupy G. Ponadto, $[G, G] \lhd G$ dla każdej grupy G. Łatwo stwierdzić, że grupa ilorazowa $G/[G, G]$ jest abelowa.

Grupę $G \neq \{1\}$ nazywa się *prostą*, jeśli podgrupa jednostkowa $E = \{1\}$ oraz cała grupa G są jedynymi podgrupami normalnymi w G.

Przykład 1.1.3. (a) Na podstawie twierdzenia Lagrange'a, jeśli rząd grupy G jest liczbą pierwszą, to grupa G nie posiada właściwych podgrup i tym bardziej nie posiada właściwych podgrup normalnych, jest zatem grupą prostą. A więc grupy reszt $\mathbb{Z}_p$, gdzie p jest liczbą pierwszą, są proste.
(b) W kursowym wykładzie algebry dowodzi się także, że grupy alternujące A_n (grupy permutacji parzystych) dla $n \geqslant 5$ są grupami prostymi.
(c) Jeszcze jedną serię nieskończoną skończonych grup prostych otrzymuje się jako grupy ilorazowe specjalnych grup liniowych. Grupa $\mathbf{SL}(n, K)$ ma centrum złożone z macierzy skalarnych o wyznaczniku 1, a więc

$$Z(\mathbf{SL}(n, K)) = \{aI : a \in K^*, \quad a^n = 1\}.$$

Grupa ilorazowa $\mathbf{SL}(n, K)/Z(\mathbf{SL}(n, K))$ nazywa się rzutową grupą specjalną stopnia n nad ciałem K i oznacza się ją $\mathbf{PSL}(n, K)$. Można udowodnić, że dla każdego ciała K, które ma co najmniej 4 elementy i dla każdej liczby naturalnej $n \geqslant 2$ grupa $\mathbf{PSL}(n, K)$ jest prosta (zob. [KM], str. 125).

1.1.4 Homomorfizmy

Homomorfizmem grupy G w grupę G' nazywamy każde odwzorowanie $h : G \to G'$ takie, że

$$h(ab) = h(a)h(b) \qquad \text{dla każdych} \quad a, b \in G.$$

Jeśli $f : G' \to G''$ jest także homomorfizmem grup, to złożenie $f \circ h : G \to G''$ jest także homomorfizmem grup. Często zamiast $f \circ h$ będziemy w takiej sytuacji pisać po prostu fh.

Obrazem $\operatorname{im} h$ homomorfizmu $h : G \to G'$ nazywamy obraz $h(G)$ grupy G w grupie G'. Jest to podgrupa grupy G'. *Jądrem* $\ker h$ homomorfizmu h nazywamy zbiór $h^{-1}(1')$, czyli zbiór tych elementów grupy G, których obrazem poprzez h jest jedynka $1' \in G'$ grupy G'. Łatwo sprawdza się, że $\ker h$ jest podgrupą grupy G.
Jeśli $h : G \to G'$ jest homomorfizmem, to dla każdego $a \in G$

$$\ker h \cdot a = h^{-1}(h(a)) = a \cdot \ker h. \tag{1.1}$$

Zatem $\ker h$ jest podgrupą normalną grupy G.
Dla dowodu (1.1) zauważmy, że

$$\begin{aligned} h^{-1}(h(a)) &= \{b \in G : h(b) = h(a)\} = \{b \in G : a^{-1}b \in \ker h\} \\ &= \{b \in G : b \in a \cdot \ker h\} = a \cdot \ker h. \end{aligned}$$

Ponieważ $h(a) = h(b)$ pociąga również $ba^{-1} \in \ker h$, czyli $b \in \ker h \cdot a$, więc także $\ker h \cdot a = h^{-1}(h(a))$.

Formułę (1.1) łatwo uogólnimy w następujący sposób: dla dowolnego niepustego podzbioru A grupy G

$$\ker h \cdot A = h^{-1}(h(A)) = A \cdot \ker h. \tag{1.2}$$

Rzeczywiście,

$$h^{-1}(h(A)) = \bigcup_{a \in A} h^{-1}(h(a)) = \bigcup_{a \in A} a \cdot \ker h = A \cdot \ker h$$

i podobnie otrzymamy drugą część równości (1.2). Z równości (1.2) otrzymujemy teraz

$$\ker h < H < G \quad \Rightarrow \quad h^{-1}(h(H)) = H \tag{1.3}$$

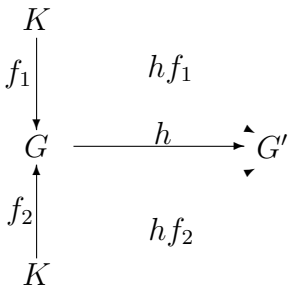
dla dowolnego homomorfizmu $h : G \to G'$.

Jeśli homomorfizm h jest odwzorowaniem różnowartościowym (injektywnym), to dla każdego $a \in G$ zbiór $h^{-1}(h(a))$ jest jednoelementowy. A więc na podstawie (1.1) homomorfizm h jest injektywny wtedy i tylko wtedy gdy $\ker h = \{1\}$.

Definicja **1.1.1.** Homomorfizm grup $h : G \to G'$ nazywa się *monomorfizmem kategoryjnym* grupy G w grupę G' jeśli dla dowolnej grupy K i homomorfizmów $f_1, f_2 : K \to G$ mamy następującą implikację:

$$hf_1 = hf_2 \quad \Rightarrow \quad f_1 = f_2.$$

Homomorfizmy występujące w tej definicji wygodnie jest zapisać w postaci następującego diagramu:

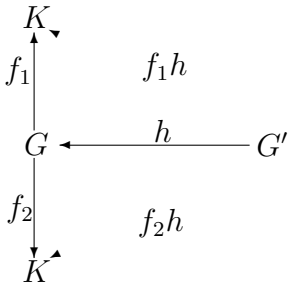


Rozważymy teraz własność homomorfizmów *dualną* w stosunku do kategoryjnej monomorficzności. Dualność ta polega na tym, że w definicji 1.1.1 zmieniamy kierunki działania wszystkich homomorfizmów.

DEFINICJA **1.1.2.** Homomorfizm grup $h : G' \to G$ nazywa się *epimorfizmem kategoryjnym* grupy G' w grupę G jeśli dla dowolnej grupy K i homomorfizmów $f_1, f_2 : G \to K$ mamy następującą implikację:

$$f_1 h = f_2 h \quad \Rightarrow \quad f_1 = f_2.$$

Homomorfizmy występujące w tej definicji tworzą następujący diagram:



STWIERDZENIE **1.1.3.** *Jeśli homomorfizm grup $h : G \to G'$ jest odwzorowaniem injektywnym, to h jest monomorfizmem kategoryjnym grupy G w grupę G'.*
Jeśli homomorfizm grup $h : G' \to G$ jest odwzorowaniem surjektywnym, to h jest epimorfizmem kategoryjnym grupy G' w grupę G.

Dowód. W oznaczeniach definicji 1.1.1 zakładamy, że $a \in K$ oraz $hf_1 = hf_2$. Wtedy

$$h(f_1(a)) = (hf_1)(a) = (hf_2)(a) = h(f_2(a)).$$

Jeśli h jest odwzorowaniem injektywnym, to stąd otrzymujemy $f_1(a) = f_2(a)$. Wobec tego $f_1 = f_2$.
Podobnie, w oznaczeniach definicji 1.1.2 zakładamy, że $a \in G$ oraz $f_1 h = f_2 h$. Jeśli h jest odwzorowaniem surjektywnym, to istnieje $b \in G'$ taki, że $a = h(b)$. Wobec tego

$$f_1(a) = f_1(h(b)) = (f_1 h)(b) = (f_2 h)(b) = f_2(h(b)) = f_2(a).$$

Stąd $f_1 = f_2$. □

Injektywny homomorfizm grup $h : G \to G'$ nazywa się zwykle *monomorfizmem*, zaś homomorfizm surjektywny nazywa się *epimorfizmem*. Tak więc każdy monomorfizm grup jest monomorfizmem kategoryjnym i każdy epimorfizm grup jest epimorfizmem kategoryjnym. Można pokazać, że twierdzenia odwrotne są także prawdziwe i w związku z tym nie ma konieczności rozróżniania morfizmów grupowych i kategoryjnych. W rozdziale 5 dyskutujemy ten problem w pełnej ogólności.

Homomorfizm, który jest równocześnie monomorfizmem i epimorfizmem nazywa się *izomorfizmem*.

Najważniejszym przykładem homomorfizmu grup jest homomorfizm kanoniczny $\kappa : G \to G/H$, gdzie H jest dowolną podgrupą normalną grupy G. Jest on określony następująco: $\kappa(a) = aH$ dla $a \in G$. Jest to epimorfizm oraz $\ker \kappa = H$. A więc każda podgrupa normalna H grupy G jest jądrem pewnego homomorfizmu grupy G w odpowiednio dobraną grupę G' (na przykład na grupę ilorazową G/H).
Sformułujemy teraz trzy podstawowe twierdzenia o homomorfizmach grup.

Twierdzenie **1.1.4.** (Twierdzenie o faktoryzacji.)
Jeśli $h : G \to G'$ jest homomorfizmem grup, $J := \ker h$ oraz $\kappa : G \to G/J$ jest homomorfizmem kanonicznym, to istnieje dokładnie jeden monomorfizm $h_* : G/J \to G'$ taki, że $h = h_* \circ \kappa$, a więc taki, że następujący diagram jest przemienny:

$$\begin{array}{ccc} G & \xrightarrow{\quad h \quad} & G' \\ & {\scriptstyle\kappa}\searrow \quad \nearrow{\scriptstyle h_*} & \\ & G/J & \end{array}$$

Homomorfizm h_* definiuje się kładąc $h_*(aJ) = h(a)$ dla $a \in G$.
Z tego twierdzenia wynika, że każdy homomorfizm $h : G \to G'$ ma rozkład postaci

$$G \xrightarrow{\kappa} G/J \xrightarrow{h_*} \operatorname{im} h \xrightarrow{j} G',$$

gdzie κ jest homomorfizmem kanonicznym, h_* jest izomorfizmem oraz j jest włożeniem. Innym bardzo użytecznym faktem jest następujący wniosek.

Wniosek **1.1.5.** *Jeśli $h : G \to G'$ jest epimorfizmem grup, to homomorfizm h_* jest izomorfizmem i wobec tego*

$$G/\ker h \cong G'.$$

Uwaga 1.1.6. Twierdzenie o faktoryzacji można sformułować w następującej nieco ogólniejszej formie.

Niech H będzie podgrupą normalną grupy G i niech $h : G \to G'$ będzie homomorfizmem grup. Jeśli $H \subseteq \ker h$, to istnieje dokładnie jeden homomorfizm $h_* : G/H \to G'$ taki, że $h = h_* \circ \kappa$, gdzie $\kappa : G \to G/H$ jest homomorfizmem kanonicznym. Ponadto, jeśli $H = \ker h$, to h_* jest monomorfizmem.

Założenie, że $H \subseteq \ker h$ pozwala określić h_* formułą $h_*(aH) = h(a)$. Rzeczywiście, jeśli $aH = bH$, to $a^{-1}b \in H \subseteq \ker h$, skąd wynika, że $h(a) = h(b)$. Ponadto, jeśli $H = \ker h$, to $h(a) = 1$ pociąga $aH = H$, zatem h_* jest monomorfizmem.

Dla grupy G symbolami $\mathsf{Sub}\,G$ i $\mathsf{NSub}\,G$ oznaczamy odpowiednio zbiór wszystkich podgrup grupy G i zbiór wszystkich podgrup normalnych grupy G. Jeśli H jest podgrupą grupy G, to $\mathsf{Sub}_H\,G$ i $\mathsf{NSub}_H\,G$ oznaczają odpowiednio zbiór wszystkich podgrup grupy G zawierających podgrupę H i zbiór wszystkich podgrup normalnych grupy G zawierających podgrupę H.

TWIERDZENIE **1.1.7.** (Twierdzenie o odpowiedniości.)
Niech $h : G \to G'$ będzie epimorfizmem grup. Wtedy przyporządkowanie

$$h^* : \mathsf{Sub}_J\,G \to \mathsf{Sub}\,G', \qquad h^*(H) = h(H)$$

każdej podgrupie H grupy G zawierającej jądro $J = \ker h$ jej obrazu $h(H)$ w grupie G' jest bijekcją taką, że $h^*(\mathsf{NSub}_J\,G) = \mathsf{NSub}\,G'$.
Ponadto, dla każdej podgrupy normalnej H grupy G zawierającej jądro $J = \ker h$ mamy izomorfizm

$$G/H \cong G'/h(H).$$

Dowód. Dla $L \in \mathsf{Sub}\,G'$ mamy $h(h^{-1}(L)) = L$, zatem h^* jest odwzorowaniem surjektywnym. Dla dowodu, że h^* jest odwzorowaniem injektywnym przypuśćmy, że $J < H_1, H_2 < G$ oraz $h(H_1) = h(H_2)$. Wtedy na podstawie (1.3) mamy

$$H_1 = h^{-1}(h(H_1)) = h^{-1}(h(H_2)) = H_2.$$

A więc h^* jest bijekcją.
Niech teraz $J < H \lhd G$ (to znaczy $H \in \mathsf{NSub}_J\,G$). Wtedy dla $x \in G'$ oraz $a \in G$ takiego, że $h(a) = x$ mamy

$$x \cdot h(H) \cdot x^{-1} = h(a) \cdot h(H) \cdot h(a^{-1}) = h(aHa^{-1}) = h(H).$$

Stąd wynika, że $h(H) \in \mathsf{NSub}\,G'$. Zatem zacieśnienie h^* do $\mathsf{NSub}_J\,G$ jest injekcją w zbiór $\mathsf{NSub}\,G'$. Pozostaje pokazać, że zacieśnienie to jest surjekcją. Niech więc $L \in \mathsf{NSub}\,G'$. Dla każdego $a \in G$ mamy

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

Zatem $a \cdot h^{-1}(L) \cdot a^{-1} \subseteq h^{-1}(L)$. Stąd wynika już, że $h^{-1}(L) \lhd G$ i wobec $h(h^{-1}(L)) = L$ odwzorowanie h^* jest surjekcją.

Dla dowodu ostatniej części twierdzenia określamy odwzorowanie

$$h' : G \to G'/h(H), \quad h'(a) = h(a)h(H).$$

Z łatwością stwierdzamy, że h' jest epimorfizmem grup. Ponadto, ponieważ $\ker h < H$, na podstawie (1.3) mamy

$$\ker h' = \{a \in G : h(a) \in h(H)\} = h^{-1}(h(H)) = H.$$

Zatem istnienie izomorfizmu $G/H \cong G'/h(H)$ wynika z wniosku 1.1.5. □

WNIOSEK **1.1.8.** *Jeśli $H \lhd G$, to homomorfizm kanoniczny $\kappa : G \to G/H$ indukuje bijekcję $\kappa^* : \mathsf{Sub}_H\,G \to \mathsf{Sub}\,G/H$ taką, że $\kappa^*(\mathsf{NSub}_H\,G) = \mathsf{NSub}\,G/H$.*

Wniosek **1.1.9.** *Jeśli* $K \lhd G$, $H \lhd G$ *i* $K < H$, *to* $K \lhd H$ *oraz*
(a) $H/K \lhd G/K$,
(b) $(G/K)/(H/K) \cong G/H$.

Dowód. Rozpatrzmy homomorfizm kanoniczny $\kappa : G \to G/K =: G'$. Wtedy na podstawie wniosku 1.1.8 mamy $\kappa(H) = H/K \lhd G/K$, oraz na podstawie twierdzenia 1.1.7 otrzymujemy $G/H \cong G'/\kappa(H) = (G/K)/(H/K)$.
Bardziej bezpośredni dowód otrzymamy rozpatrując odwzorowanie

$$G/K \to G/H, \quad gK \mapsto gH.$$

Jest to epimorfizm z jądrem H/K. Izomorfizm w części (b) wniosku otrzymujemy przez zastosowanie wniosku 1.1.5. □

Twierdzenie **1.1.10.** (Twierdzenie o izomorfizmie.)
Jeśli $H \lhd G$, $K < G$, *to*
(a) $H \cap K \lhd K$,
(b) $HK/H \cong K/H \cap K$.

Dowód. Przede wszystkim $HK < G$, gdyż z założeń wynika, że $HK = KH$, a to wystarcza by iloczyn dwóch podgrup grupy G był jej podgrupą. H jest podgrupą normalną w G, zatem jest także podgrupą normalną w HK. Dla dowodu twierdzenia rozważamy homomorfizm

$$K \to HK/H, \quad k \mapsto kH.$$

Jest to epimorfizm i ma jądro $K \cap H$ skąd wobec wniosku 1.1.5 otrzymujemy (b). □

1.1.5 Automorfizmy wewnętrzne

Automorfizmem grupy G nazywamy każdy izomorfizm $\alpha : G \to G$. Zbiór $\mathsf{Aut}\, G$ wszystkich automorfizmów grupy G jest podgrupą grupy symetrycznej $S(G)$ zbioru G. Dla każdego elementu $a \in G$ definiujemy odwzorowanie

$$i_a : G \to G, \quad i_a(x) = axa^{-1}.$$

Łatwo sprawdza się, że $i_a \in \mathsf{Aut}\, G$. Automorfizm i_a nazywa się *automorfizmem wewnętrznym* grupy G. Dla $a, b \in G$ mamy $i_a \circ i_b = i_{ab}$ oraz $i_a^{-1} = i_{a^{-1}}$. Stąd wynika, że automorfizmy wewnętrzne tworzą podgrupę w grupie automorfizmów grupy G. Nazywamy ją grupą automorfizmów wewnętrznych grupy G i oznaczamy $\operatorname{Inn} G$.
Odwzorowanie $G \to \operatorname{Inn} G, \quad a \mapsto i_a$ jest epimorfizmem grup. Jądrem tego epimorfizmu jest podgrupa normalna

$$\{a \in G : i_a = \mathrm{id}_G\} = \{a \in G : ax = xa \ \ \forall x \in G\} = Z(G).$$

Na podstawie wniosku 1.1.5 mamy zatem izomorfizm

$$\operatorname{Inn} G \cong G/Z(G),$$

gdzie $Z(G)$ jest centrum grupy G.

1.1.6 Twierdzenie Jordana-Höldera

Jeśli $H \lhd G$ i grupa G/H nie jest prosta, to na podstawie wniosku 1.1.8 istnieje podgrupa K grupy G różna od H i G taka, że

$$H \lhd K \lhd G.$$

Podobnie, jeśli grupa K/H nie jest prosta (lub gdy G/K nie jest prosta), to istnieje podgrupa K_1 grupy K różna od H i K taka, że $H \lhd K_1 \lhd K$ (istnieje podgrupa K_2 grupy G różna od K i G taka, że $K \lhd K_2 \lhd G$). Kontynuując to postępowanie dla grupy skończonej G skonstruujemy *ciąg podnormalny*

$$H_0 = E \lhd H_1 \lhd \cdots \lhd H_{k-1} \lhd G = H_k \tag{1.4}$$

którego *faktory* H_{i+1}/H_i są grupami prostymi dla $i = 0, 1, \ldots, k-1$. Taki ciąg podnormalny grupy G nazywa się ciągiem *kompozycyjnym* grupy G a liczba k nazywa się *długością* ciągu kompozycyjnego (1.4).
Każda grupa skończona posiada więc przynajmniej jeden ciąg kompozycyjny, ale jak sugeruje konstrukcja przedstawiona powyżej, grupa mająca wiele podgrup normalnych będzie na ogół miała wiele ciągów kompozycyjnych. Podstawowe pytania jakie się nasuwają są następujące:
(a) Czy grupa skończona może mieć ciągi kompozycyjne o różnych długościach?
(b) Czy faktory proste ciągu kompozycyjnego są wyznaczone jednoznacznie (z dokładnością do izomorfizmu) przez grupę G, czy też zależą od ciągu kompozycyjnego?

Na obydwa te pytania istnieje bardzo satysfakcjonująca odpowiedź znana jako twierdzenie Jordana-Höldera (zob. [L], str.123):
Długości wszystkich ciągów kompozycyjnych grupy skończonej są równe.
Zbiory faktorów prostych $F_1, \ldots, F_k$ oraz $G_1, \ldots, G_k$ dowolnych dwóch ciągów kompozycyjnych grupy skończonej G różnią się (z dokładnością do izomorfizmu) co najwyżej porządkiem. Oznacza to, że istnieje permutacja $\pi \in S(k)$ taka, że grupy F_i oraz $G_{\pi(i)}$ są izomorficzne dla $i = 1, \ldots, k$.

Z twierdzenia Jordana-Höldera wynika, że jeśli dwie grupy skończone mają różne długości ciągów kompozycyjnych lub jeśli ich ciągi kompozycyjne mają różne zbiory faktorów prostych, to grupy te nie mogą być izomorficzne. Jest to jeden z motywów zainteresowania problemem klasyfikacji skończonych grup prostych. Problem ten polega na charakteryzacji z dokładnością do izomorfizmu wszystkich skończonych grup prostych. Praca nad klasyfikacją skończonych grup prostych trwa już ponad 110 lat (od 1892 roku). Okres największej koncentracji pracy przypadł na lata 1960–1980. Wreszcie w roku 1981 ogłoszono że problem został kompletnie rozwiązany. Oceniano, że kompletny dowód twierdzenia klasyfikacyjnego tworzy zestaw co najmniej 500 prac zajmujących co najmniej 10000 stronic w profesjonalnych czasopismach matematycznych i napisanych przez około 100 matematyków. Pierwszą próbą objaśnienia twierdzenia klasyfikacyjnego była monografia Daniela Gorensteina *Finite simple groups. An introduction to their classification.* Plenum Press 1982. Pod koniec lat 90-tych znaleziono jednak pewne luki w argumentacji (w 800-stronicowej pracy Masona) i podjęto próbę uratowania twierdzenia klasyfikacyjnego. W 2004 roku ukazały się dwie książki Aschbachera i Smitha pod wspólnym tytułem *The classification*

of quasithin groups (razem ponad 1200 stronic), które według przekonania autorów definitywnie usuwają znalezione luki i w ten sposób stanowią ostatnie ogniwo w klasyfikacji skończonych grup prostych (zob. informację bibliograficzną w Notices of the AMS Vol. **51** No. 8 (2004), p. 977). Jednakże kompletny dowód twierdzenia klasyfikacyjnego nie jest jeszcze napisany i ciągle istnieją wątpliwości, czy nie pojawią się luki trudne do uzupełnienia. Trwa realizacja programu Gorensteina, Lyonsa i Solomona przedstawienia głównych części dowodu twierdzenia klasyfikacyjnego. W latach 1994–2005 opublikowano 6 monografii w wydawnictwie American Mathematical Society, ale program ten jest jeszcze daleki od finalizacji. Autorzy tego projektu przewidują, że uda im się napisać kompletny dowód twierdzenia klasyfikacyjnego w serii monografii, które w sumie będą miały około 3000 do 4000 stronic tekstu. Zapowiedź autorów w pierwszym tomie serii brzmi dość skromnie:

It is our purpose in these monographs to prove the following theorem:
Classification Theorem. *Every finite simple group is cyclic of prime order, an alternating group, a finite simple group of Lie type, or one of the twenty-six sporadic finite simple groups.*

Historię całego przedsięwzięcia przedstawia interesująco praca Ronalda Solomona *A brief history of the classification of the finite simple groups*, Bulletin of the Amer. Math. Soc. Vol. **38** (2001), pp. 315–352. Sytuację po ukazaniu się książek Aschbachera i Smitha opisuje Micheal Aschbacher w artykule *The status of the classification of finite simple groups*, Notices of the Amer. Math. Soc. Vol. **51**, No. 7 (2004), pp. 736–740.

Powracając do ciągu kompozycyjnego (1.4), jeśli faktory tego ciągu są abelowe (a więc izomorficzne z grupami $\mathbb{Z}_p$ dla liczb pierwszych p), to grupa G nazywa się *grupą rozwiązalną*. Wszystkie grupy małych rzędów są rozwiązalne. Najmniejszą grupą skończoną, która nie jest rozwiązalna jest grupa alternująca A_5 rzędu 60. Jest to mianowicie najmniejsza nieabelowa grupa prosta. Żadna nieabelowa grupa prosta G nie jest rozwiązalna, gdyż $E \lhd G$ jest jej ciągiem kompozycyjnym i jedyny faktor prosty $G/E \cong G$ jest grupą nieabelową.
Najsławniejszym twierdzeniem o grupach rozwiązalnych jest zapewne twierdzenie Feita i Thompsona z 1963 roku mówiące, że każda grupa skończona rzędu nieparzystego jest rozwiązalna. Wynika stąd w szczególności, że każda nieabelowa skończona grupa prosta ma rząd parzysty.

1.2 Działanie grupy na zbiorze

Mówimy, że grupa G działa na zbiorze X jeśli jest dane odwzorowanie

$$G \times X \to X, \ \ (g, x) \mapsto gx,$$

takie, że spełnione są dwa warunki:

(a) $f(gx) = (fg)x$ dla $f, g \in G, \ \ x \in X$,
(b) $1x = x$ dla $x \in X$.

Uwaga 1.2.1. Każdy element $g \in G$ wyznacza odwzorowanie g' zbioru X w siebie

$$g' : X \to X, \qquad g'(x) = gx.$$

Odwzorowanie to jest *bijekcją*. Injektywność g' wynika stąd, że

$$gx = gy \quad \Rightarrow \quad g^{-1}(gx) = g^{-1}(gy) \quad \Rightarrow \quad (g^{-1}g)x = (g^{-1}g)y \quad \Rightarrow \quad x = y.$$

Natomiast surjektywność g' wynika z faktu, że $x = g(g^{-1}x)$ dla każdego $x \in X$. Krótko mówiąc, $(g^{-1})'$ jest odwzorowaniem odwrotnym do g'.

Uwaga 1.2.2. Odwzorowanie $G \to S(X), \quad g \mapsto g'$ jest homomorfizmem grup. Mamy mianowicie

$$(fg)'(x) = (fg)x = f(gx) = f'(g'(x)) = (f' \circ g')(x)$$

dla każdych $x \in X,\ f, g \in G$. Zatem $(fg)' = f' \circ g'$.
Na odwrót, każdy homomorfizm $G \to S(X), \quad g \mapsto g'$ wyznacza działanie grupy G na zbiorze X poprzez odwzorowanie

$$G \times X \to X, \quad (g, x) \mapsto gx = g'(x).$$

Rzeczywiście, dla $f, g \in G$ mamy $f' \circ g' = (fg)'$ zatem dla dowolnego $x \in X$ otrzymujemy

$$\begin{aligned} f(gx) &= f(g'(x)) = f'(g'(x)) = (f' \circ g')(x) = (fg)'(x) = (fg)x, \\ 1x &= 1'(x) = x, \end{aligned}$$

gdzie $1'$ jest jedynką grupy $S(X)$.
Przyporządkowanie każdemu homomorfizmowi grupy G w grupę symetryczną $S(X)$ zbioru X odpowiadającego mu w ten sposób działania grupy G na zbiorze X ustala wzajemnie jednoznaczną odpowiedniość między homomorfizmami grupy G w grupę $S(X)$ i działaniami grupy G na zbiorze X. W związku z tym działaniem grupy G na zbiorze X można nazwać dowolny homomorfizm $G \to S(X)$.

Przykład 1.2.1. Najbardziej naturalnym przykładem działania grupy na zbiorze jest działanie grupy symetrycznej $G = S(X)$ zbioru X na zbiorze X:

$$S(X) \times X \to X, \quad (\sigma, x) \mapsto \sigma(x).$$

Odpowiadający temu działaniu homomorfizm $G \to S(X)$ jest homomorfizmem identycznościowym.

Definicja **1.2.3.** Niech grupa G działa na zbiorze X. Elementy $x, y \in X$ nazywają się *sprzężone*, jeśli istnieje $g \in G$ taki, że $y = gx$. Piszemy wtedy $x \sim y$. O elemencie g takim, że $y = gx$ mówimy, że transformuje x na y.

Relacja sprzężenia $\sim$ jest relacją równoważnościową w zbiorze X.

Definicja **1.2.4.** Klasę abstrakcji relacji sprzężenia $\sim$ nazywa się *orbitą* zbioru X, lub G-orbitą zbioru X.

G-orbita zbioru X zawierająca element $x \in X$ ma postać:

$$\{y \in X : y \sim x\} = \{gx \in X : g \in G\} =: Gx.$$

Zbiór X można więc przedstawić jako sumę mnogościową rozłącznych orbit:

$$X = \bigcup Gx_i$$

gdzie x_i przebiega zbiór reprezentantów orbit zbioru X. Stąd, dla zbioru skończonego X, otrzymujemy

$$|X| = \sum |Gx_i|.$$

Bardzo ważnym dla zastosowań jest fakt, że liczbę elementów $|Gx|$ orbity Gx można przedstawić jako indeks pewnej podgrupy grupy G. Przystępujemy do opisu tego przedstawienia.

DEFINICJA **1.2.5.** Niech grupa G działa na zbiorze X. *Stabilizatorem* elementu $x \in X$ nazywamy zbiór

$$\mathsf{Stab}\, x = \{f \in G : fx = x\}.$$

Łatwo zauważyć, że $\mathsf{Stab}\, x$ jest podgrupą grupy G. Jeśli $s \in \mathsf{Stab}\, x$, to dla dowolnego elementu $g \in G$ mamy $(gs)x = g(sx) = gx$. A więc każdy element warstwy $g \cdot \mathsf{Stab}\, x$ transformuje element x na ten sam element gx. Pokażemy, że poza warstwą $g \cdot \mathsf{Stab}\, x$ nie ma w grupie G elementów, które transformują x na gx.

TWIERDZENIE **1.2.6.** *Niech grupa G działa na zbiorze X i niech $x \in X$, $g \in G$.*
(a) *Jeśli $y = gx$, to zbiór elementów $h \in G$ transformujących x na y (tzn. takich, że $y = hx$) jest warstwą $g \cdot \mathsf{Stab}\, x$ w grupie G.*
(b) *Przyporządkowanie elementowi $y = gx \in Gx$ zbioru wszystkich elementów $h \in G$ transformujących x na y jest bijekcją orbity Gx na zbiór warstw $G : \mathsf{Stab}\, x$.*

Dowód. (a) wynika z następujących równoważności:

$$gx = hx \;\Leftrightarrow\; x = g^{-1}hx \;\Leftrightarrow\; g^{-1}h \in \mathsf{Stab}\, x \;\Leftrightarrow\; h \in g \cdot \mathsf{Stab}\, x.$$

(b) Na podstawie (a) mamy odwzorowanie

$$Gx \to G : \mathsf{Stab}\, x, \quad gx \mapsto \{h \in G : gx = hx\} = g \cdot \mathsf{Stab}\, x. \tag{1.5}$$

Jest to oczywiście surjekcja (bo g przebiega całą grupę G). Injektywność wynika z następujących równoważności:

$$f \cdot \mathsf{Stab}\, x = g \cdot \mathsf{Stab}\, x \;\Leftrightarrow\; f^{-1}g \in \mathsf{Stab}\, x \;\Leftrightarrow\; fx = gx.$$

Zatem odwzorowanie (1.5) jest bijekcją. □

WNIOSEK **1.2.7.** *Jeśli grupa G działa na zbiorze X, to dla każdego $x \in X$,*

$$|Gx| = |G : \mathsf{Stab}\, x|.$$

W szczególności, jeśli grupa G jest skończona, to liczba elementów w orbicie Gx jest dzielnikiem rzędu grupy G.

WNIOSEK **1.2.8.** *Jeśli grupa skończona G działa na zbiorze skończonym X oraz $\{x_1, \ldots, x_k\}$ jest zbiorem reprezentantów wszystkich orbit zbioru X, to*

$$|X| = \sum_{i=1}^{k} |G : \mathsf{Stab}\, x_i|.$$

Tę równość nazywa się *równaniem klas* dla działania grupy G na zbiorze X.

1.2.1 Działanie grupy przez automorfizmy wewnętrzne

Rozpatrujemy działanie grupy G na zbiorze $X = G$ określone następująco:

$$G \times G \to G, \quad (g, x) \mapsto gxg^{-1} =: x^g.$$

Gdybyśmy zachowali oznaczenie gx dla obrazu pary (g, x) w zbiorze $X = G$, to mielibyśmy $gx = gxg^{-1}$, co byłoby mylące. Dlatego w tym specjalnym przypadku stosujemy symbolikę "wykładniczą" i piszemy x^g zamiast gx. Zauważmy, że związana z tym działaniem grupy G na G bijekcja $g' \in S(G)$ działa następująco:

$$g'(x) = gxg^{-1} = i_g(x) \quad \forall\, x \in G.$$

A więc g' jest automorfizmem wewnętrznym i_g. W związku z tym, opisane wyżej działanie grupy G na G nazywa się działaniem przez automorfizmy wewnętrzne. Orbitę

$$x^G = \{x^g \in G : g \in G\} = \{gxg^{-1} : g \in G\}$$

nazywa się *klasą elementów sprzężonych* grupy G. Natomiast stabilizator

$$\mathsf{Stab}\, x = \{f \in G : fxf^{-1} = x\} = \{f \in G : fx = xf\}$$

nazywa się *centralizatorem* elementu x i oznacza $Z(x)$.
Dla grupy skończonej G równanie klas przyjmuje następującą postać:

$$|G| = \sum_{i=1}^{k} |G : \mathsf{Stab}\, x_i| = \sum_{i=1}^{k} |G : Z(x_i)|.$$

Tutaj $x_1, \ldots, x_k$ są elementami reprezentującymi wszystkie różne klasy elementów sprzężonych grupy G oraz $|G : Z(x_i)| = |x_i^G|$ jest liczbą elementów w klasie elementów sprzężonych z elementem x_i. Na szczególną uwagę zasługują klasy jednoelementowe:

$$|x^G| = 1 \quad \Leftrightarrow \quad gx = xg \;\; \forall g \in G \quad \Leftrightarrow \quad x \in Z(G).$$

A więc klasa jest jednoelementowa wtedy i tylko wtedy gdy jej element należy do centrum $Z(G)$ grupy G. Stąd rozbicie grupy G na rozłączne klasy elementów sprzężonych zapisujemy zwykle w postaci

$$G = Z(G) \;\cup\; x_1^G \;\cup \cdots \cup\; x_r^G,$$

gdzie elementy x_i reprezentują różne klasy elementów sprzężonych oraz $|x_i^G| > 1$ dla $i = 1, \ldots, r$, a równanie klas

$$|G| \;=\; |Z(G)| + \sum_{i=1}^{r} |x_i^G| \;=\; |Z(G)| + \sum_{i=1}^{r} |G : Z(x_i)|,$$

gdzie $x_i \in G$ reprezentują różne klasy elementów sprzężonych oraz $|G : Z(x_i)| > 1$ dla $i = 1, \ldots, r$.

1.2.2 Zastosowania w teorii grup skończonych

Wskażemy teraz trzy zastosowania równania klas w teorii grup skończonych.

TWIERDZENIE **1.2.9.** *Jeśli rząd grupy G jest potęgą liczby pierwszej p, to grupa G ma nietrywialne centrum. Zatem*

$$|Z(G)| \geqslant p.$$

Dowód. W równaniu klas mamy

$$p^n = |G| \ = \ |Z(G)| + \sum_{i=1}^{r} |G : Z(x_i)|,$$

gdzie n jest pewną liczbą naturalną oraz $|G : Z(x_i)| > 1$ dla $i = 1, \ldots, r$. Ponadto, każdy indeks $|G : Z(x_i)|$ jest dzielnikiem rzędu grupy G a więc jest także potęgą liczby p. Zatem $|Z(G)|$ musi dzielić się przez p. □

TWIERDZENIE **1.2.10.** (Twierdzenie Cauchy'ego.)
Jeśli liczba pierwsza p dzieli rząd grupy skończonej G, to w grupie G istnieje element rzędu p.

Dowód. Dla grupy abelowej G twierdzenie to udowodnimy w rozdziale 4 innymi metodami. Tutaj zakładamy, że twierdzenie jest prawdziwe dla grup abelowych. Niech więc G będzie grupą nieabelową. Przeprowadzimy dowód indukcyjny ze względu na rząd grupy G. Zakładamy więc, że grupy rzędu mniejszego niż rząd grupy G i podzielnego przez p zawierają elementy rzędu p. Pokażemy, że grupa G ma podgrupę właściwą o rzędzie podzielnym przez p.
Rozpatrujemy dwa przypadki.
(a) Jeśli w równaniu klas wszystkie indeksy $|G : Z(x_i)|$ dzielą się przez p, to także p dzieli rząd centrum $Z(G)$, które jest właściwą podgrupą grupy G.
(b) Jeśli dla pewnego $x \in G \setminus Z(G)$ liczba p nie dzieli indeksu $|G : Z(x)|$, to na podstawie twierdzenia Lagrange'a liczba p dzieli rząd podgrupy $Z(x)$, która jest właściwą podgrupą grupy G.
W każdym więc przypadku G ma podgrupę właściwą o rzędzie podzielnym przez p. Na podstawie założenia indukcyjnego ta podgrupa ma element rzędu p, a więc także G ma element rzędu p. □

TWIERDZENIE **1.2.11.** (Twierdzenie Sylowa.)
Jeśli p jest liczbą pierwszą i potęga p^k liczby p dzieli rząd grupy skończonej G, to grupa G ma podgrupę rzędu p^k.

Dowód. Przeprowadzimy dowód indukcyjny ze względu na rząd grupy G. Wobec twierdzenia Cauchy'ego możemy założyć, że $k \geqslant 2$.
Przypadek (a): Istnieje podgrupa właściwa $H < G$, której indeks $|G : H|$ nie dzieli się przez p.
Wtedy na podstawie twierdzenia Lagrange'a $|G| = |G : H| \cdot |H|$, zatem p^k dzieli rząd podgrupy H. Na podstawie założenia indukcyjnego H, a zatem także G, ma podgrupę rzędu p^k.
Przypadek (b): Dla każdej podgrupy właściwej $H < G$ indeks $|G : H|$ dzieli się

przez p.
Z równania klas (niezależnie od tego czy grupa jest abelowa czy też nie) wynika, że centrum $Z(G)$ grupy G ma rząd podzielny przez p. Na podstawie twierdzenia Cauchy'ego istnieje element $a \in Z(G)$ rzędu p, a więc $H := \langle a \rangle$ jest podgrupą $Z(G)$. Mamy więc

$$H < Z(G) \lhd G,$$

skąd wynika, że $H \lhd G$. Rozpatrzmy homomorfizm kanoniczny

$$\kappa : G \to G/H.$$

Ponieważ p^k dzieli $|G|$ oraz $p = |H|$, więc p^{k-1} dzieli $|G/H|$. Na podstawie założenia indukcyjnego G/H ma podgrupę P rzędu p^{k-1}. Niech $S := \kappa^{-1}(P)$ będzie przeciwobrazem podgrupy P w grupie G. Wtedy $\kappa(S) = P$ i zacieśnienie κ do S jest epimorfizmem na grupę P z jądrem H. Zatem $S/H \cong P$, skąd wynika, że

$$|S| = |H| \cdot |P| = p \cdot p^{k-1} = p^k.$$

Grupa G ma więc podgrupę S rzędu p^k. □

DEFINICJA **1.2.12.** Niech G będzie grupą skończoną i niech p będzie liczbą pierwszą dzielącą rząd grupy G. Jeśli p^n jest *największą* potęgą liczby p dzielącą rząd grupy G, to każdą podgrupę S rzędu p^n grupy G nazywamy *$p-$podgrupą Sylowa* grupy G.

Z twierdzenia Sylowa wynika, że każda grupa skończona ma $p-$podgrupy Sylowa dla każdej liczby pierwszej p dzielącej rząd grupy G. Przy tym $p-$podgrupy Sylowa są maksymalnymi $p-$podgrupami grupy G. A oto inne twierdzenia o podgrupach Sylowa, których dowody można znaleźć w książce S. Langa (rozdział I, §6). Zakładamy poniżej, że G jest grupą skończoną i liczba pierwsza p dzieli rząd grupy G.

Każda podgrupa H grupy G, której rząd jest potęgą liczby p zawiera się w pewnej $p-$podgrupie Sylowa grupy G.

Każde dwie $p-$podgrupy Sylowa grupy G są sprzężone w G.
Oznacza to, że dla każdych dwóch $p-$podgrup Sylowa S_1 i S_2 grupy G istnieje automorfizm wewnętrzny i_a grupy G taki, że

$$i_a(S_1) = S_2.$$

Stąd wynika, że jeśli grupa G ma tylko jedną $p-$podgrupę Sylowa S, to $S \lhd G$.

Liczba $s(p, G)$ wszystkich $p-$podgrup Sylowa grupy G jest postaci $1+pm$, gdzie $m \geqslant 0$ jest liczbą całkowitą. Ponadto, $s(p, G)$ dzieli rząd grupy G.
A więc jeśli grupa G ma więcej niż jedną $p-$podgrupę Sylowa, to ma ich co najmniej $p + 1$.

1.3 Iloczyn prosty i półprosty grup

1.3.1 Iloczyny wewnętrzne

Niech H i K będą podgrupami grupy G. Iloczyn kompleksowy HK nie jest na ogół podgrupą grupy G. Mamy jednak następujące kryterium na to by $HK < G$:

$$HK < G \quad \Leftrightarrow \quad HK = KH.$$

Szczególnie interesujący jest przypadek, gdy $HK = G$. Oznacza to, że każdy element g grupy G można przedstawić w postaci $g = hk$ gdzie $h \in H, k \in K$. Nasuwa się naturalne pytanie, kiedy takie przedstawienie każdego elementu $g \in G$ jest jednoznaczne.

LEMAT **1.3.1.** *Niech H i K będą podgrupami grupy G. Następujące warunki są równoważne.*
(a) $G = HK$ *i* $H \cap K = 1$.
(b) *Każdy element $g \in G$ ma dokładnie jedno przedstawienie w postaci $g = hk$ gdzie $h \in H, k \in K$.*

Dowód. Załóżmy (a) i przypuśćmy, że $hk = h_1k_1$ dla pewnych $h, h_1 \in H$ oraz $k, k_1 \in K$. Wtedy $h_1^{-1}h = k_1k^{-1} \in H \cap K = 1$. Stąd otrzymujemy $h = h_1$ i $k = k_1$, co dowodzi (b).
Załóżmy (b) i przypuśćmy, że $g \in H \cap K$. Wtedy $g = g \cdot 1 = 1 \cdot g$, skąd wobec (b) wynika, że $g = 1$. □

DEFINICJA **1.3.2.** Grupę G nazywamy *iloczynem ogólnym* podgrup H i K jeśli spełniony jest jeden (zatem obydwa) z warunków (a) i (b) lematu 1.3.1.
Grupę G nazywamy *iloczynem półprostym* podgrup H i K jeśli G jest iloczynem ogólnym tych podgrup oraz $H \lhd G$ lub $K \lhd G$.
Grupę G nazywamy *iloczynem prostym* podgrup H i K jeśli G jest iloczynem ogólnym tych podgrup oraz $H \lhd G$ i $K \lhd G$.

Istnieje wiele grup, które rozkładają się na iloczyn półprosty, ale nie mają rozkładu na iloczyn prosty nietrywialnych podgrup normalnych. A więc, na przykład,

$$\begin{aligned} D(n) &= \mathsf{Obr}(n) \cdot \mathsf{Odb}(n), \\ S(n) &= A_n \cdot \{1, (12)\}, \\ O(n) &= SO(n) \cdot \{1, \tau\}, \\ \mathsf{Isom}\, E^n &= \mathsf{Tran}E^n \cdot \mathsf{Obr}E^n, \\ \mathsf{Af}(n, K) &= \mathsf{TAf}(n, K) \cdot \mathsf{CAf}(n, K). \end{aligned}$$

Tutaj użyliśmy następujących oznaczeń: $\mathsf{Obr}(n)$ oznacza $n-$elementową podgrupę obrotów i $\mathsf{Odb}(n)$ jakąkolwiek $2-$elementową podgrupę zawierającą odbicie $n-$kąta foremnego, τ oznacza jakąkolwiek nietrywialną symetrię względem hiperpłaszczyzny w przestrzeni euklidesowej, Tran i Obr oznaczają odpowiednio podgrupę translacji i podgrupę obrotów w grupie izometrii przestrzeni euklidesowej afinicznej, TAf i CAf oznaczają podgrupę translacji i podgrupę środkowo-afiniczną w grupie przekształceń afinicznych $n-$wymiarowej przestrzeni liniowej nad ciałem K. W każdym rozkładzie pierwszy czynnik jest podgrupą normalną, natomiast drugi nie jest podgrupą normalną w rozpatrywanej grupie.

Zauważmy, że w każdym z trzech rodzajów iloczynów podgrup H i K mamy $HK = KH$, gdyż iloczyn kompleksowy HK jest grupą. Ta przemienność podgrup H i K ma jednak specyficzny charakter w każdym z trzech przypadków.

Jeśli G jest iloczynem ogólnym podgrup H i K, to można tylko powiedzieć, że dla każdych $h \in H$ i $k \in K$ istnieją $h_1, h_2 \in H$ i $k_1, k_2 \in K$ takie, że

$$hk = k_1 h_1 \quad \text{oraz} \quad kh = h_2 k_2.$$

Jeśli G jest iloczynem półprostym podgrup H i K oraz $H \lhd G$, to dla każdych $h \in H$ i $k \in K$ mamy

$$hk = k \cdot k^{-1} hk \quad \text{oraz} \quad kh = khk^{-1} \cdot k,$$

gdzie $k^{-1}hk, khk^{-1} \in H$, gdyż $H \lhd G$.
Wreszcie gdy G jest iloczynem prostym podgrup H i K, to dla każdych $h \in H$ i $k \in K$ mamy

$$hk = kh.$$

Rzeczywiście,

$$\begin{aligned} hkh^{-1}k^{-1} &= h \cdot kh^{-1}k^{-1} \in H \\ &= hkh^{-1} \cdot k^{-1} \in K. \end{aligned}$$

A więc komutator $hkh^{-1}k^{-1} \in H \cap K = 1$, skąd wynika, że $hk = kh$, dla każdych $h \in H,\ k \in K$.

Jeśli G jest iloczynem ogólnym podgrup H i K, to nie można wskazać żadnej praktycznej formuły dla iloczynu

$$hk \cdot h_1 k_1, \quad \text{gdzie} \quad h, h_1 \in H,\ k, k_1 \in K.$$

Natomiast jeśli $G = HK$ jest iloczynem półprostym i $H \lhd G$, to mamy

$$hk \cdot h_1 k_1 = h \cdot kh_1 k^{-1} \cdot kk_1 \tag{1.6}$$

gdzie $kh_1 k^{-1} \in H$ gdyż $H \lhd G$ i wobec tego

$$h \cdot kh_1 k^{-1} \in H, \quad kk_1 \in K.$$

Podobnie, jeśli $G = HK$ jest iloczynem półprostym i $K \lhd G$, to mamy

$$hk \cdot h_1 k_1 = hh_1 \cdot h_1^{-1} kh_1 \cdot k_1 \tag{1.7}$$

gdzie $h_1^{-1} kh_1 \in K$ gdyż $K \lhd G$ i wobec tego

$$hh_1 \in H, \quad h_1^{-1} kh_1 \cdot k_1 \in K.$$

W przypadku gdy $G = HK$ jest iloczynem prostym podgrup normalnych H i K, to wobec przemienności elementów podgrup H i K mamy następującą bardzo prostą formułę mnożenia elementów

$$hk \cdot h_1 k_1 = hh_1 \cdot kk_1. \tag{1.8}$$

1.3.2 Iloczyny zewnętrzne

Istnieją także konstrukcje grup, które pozwalają zbudować nową grupę G z dwóch danych grup H i K nie będących podgrupami jakiejś jednej grupy. Najprostszą z tych konstrukcji jest iloczyn kartezjański grup.

Iloczyn prosty

Niech H i K będą dowolnymi grupami. Przez analogię do formuły (1.8), w iloczynie kartezjańskim $H \times K$ zbiorów H i K określamy działanie następująco:

$$(h,k)\cdot(h_1,k_1) := (hh_1, kk_1).$$

Tutaj hh_1 i kk_1 są iloczynami elementów w grupach H i K, odpowiednio. Z łatwością pokazuje się, że zbiór $H \times K$ z tak określonym działaniem jest grupą z jedynką $(1_H, 1_K)$. Reguła konstrukcji elementu odwrotnego do $(h,k) \in H \times K$ jest bardzo prosta:

$$(h,k)^{-1} = (h^{-1}, k^{-1}).$$

Tę grupę nazywamy *iloczynem kartezjańskim* grup H i K.
Rozpatrzymy związek pomiędzy iloczynem kartezjańskim grup i iloczynem prostym podgrup grupy. Niech H i K będą podgrupami grupy G i załóżmy, że G jest iloczynem ogólnym podgrup H i K. Zatem $G = HK$ oraz $H \cap K = 1$. Wtedy można też oczywiście rozpatrywać iloczyn kartezjański $H \times K$ grup H i K. Porównanie grup $G = HK$ i $H \times K$ zawiera się w następującym twierdzeniu.

Twierdzenie **1.3.3.** *Niech H i K będą podgrupami grupy G. Następujące warunki są równoważne.*
(a) *Odwzorowanie $\varphi : H \times K \to G$, $(h,k) \mapsto hk$ jest izomorfizmem grup.*
(b) *$G = HK$, $H \cap K = 1$ oraz $hk = kh$ dla wszystkich $h \in H, k \in K$.*
(c) *G jest iloczynem prostym podgrup H i K.*

Dowód. (a) $\Rightarrow$ (b) Surjektywność odwzorowania φ oznacza, że $G = HK$. Ponadto, dla $h \in H, k \in K$ mamy

$$kh = (h^{-1}k^{-1})^{-1} = \varphi(h^{-1}, k^{-1})^{-1} = \varphi(h,k) = hk.$$

Wreszcie, jeśli $1 \neq g \in H \cap K$, to $\varphi(1,g) = g = \varphi(g,1)$, wbrew różnowartościowości φ. Zatem $H \cap K = 1$.
(b) $\Rightarrow$ (c) Należy dowieść, że $H \lhd G$ i $K \lhd G$. Dla $g = hk$ mamy

$$gHg^{-1} = hkHk^{-1}h^{-1} = hHkk^{-1}h^{-1} = hHh^{-1} = H.$$

A więc $H \lhd G$. Podobnie

$$gKg^{-1} = hkKk^{-1}h^{-1} = hKh^{-1} = Khh^{-1} = K,$$

skąd $K \lhd G$. W obydwu przypadkach skorzystaliśmy z przemienności elementów podgrup H i K.
(c) $\Rightarrow$ (a) Jeśli G jest iloczynem prostym podgrup H i K, to

$$\varphi : H \times K \to G, \quad (h,k) \mapsto hk$$

jest dobrze określoną bijekcją. Pozostaje pokazać, że zachowuje działanie grupowe:

$$\varphi((h_1,k_1)(h_2,k_2)) = \varphi(h_1h_2, k_1k_2) = h_1h_2k_1k_2 = h_1k_1 \cdot h_2k_2 = \varphi(h_1,k_1)\varphi(h_2,k_2),$$

gdzie wykorzystaliśmy fakt przemienności elementów podgrup normalnych H i K. □

Z twierdzenia tego wynika, że można identyfikować iloczyn prosty podgrup H i K grupy G z iloczynem kartezjańskim $H \times K$.
Również iloczyn kartezjański dwóch dowolnych grup H i K można zawsze przedstawić jako iloczyn prosty podgrup normalnych $H' := H \times 1$ oraz $K' := 1 \times K$. W związku z tym, przy odpowiednich utożsamieniach elementów, można używać zamiennie pojęć iloczynu prostego i iloczynu kartezjańskiego grup.

Konstrukcja iloczynu kartezjańskiego grup przenosi się natychmiast na *skończone* iloczyny kartezjańskie $G_1 \times \cdots \times G_n$, gdzie G_i są dowolnymi grupami. Ogólniej, dla dowolnej rodziny grup $\{G_i : i \in I\}$ rozpatrujemy iloczyn kartezjański

$$P = \prod\{G_i : i \in I\}$$

zbiorów G_i i określamy na nim działanie następująco:

$$(g_i)_{i\in I} \cdot (f_i)_{i\in I} = (g_i f_i)_{i\in I}.$$

Z łatwością sprawdzamy, że system $(P, \cdot\,, (1_i)_{i\in I})$ jest grupą. Nazywamy ją *iloczynem* lub *produktem kartezjańskim* rodziny grup $\{G_i : i \in I\}$.
W szczególnym przypadku gdy $G_i = G$ dla każdego $i \in I$, grupę P nazywamy *potęgą kartezjańską* grupy G i oznaczamy G^I.
Gdy zbiór I jest skończony, $|I| = n$, to zamiast G^I piszemy oczywiście G^n.
W produkcie $P = \prod\{G_i : i \in I\}$ wyróżnijmy podzbiór S złożony z wszystkich elementów $(g_i)_{i\in I}$ takich, że $g_i = 1$ dla prawie wszystkich $i \in I$ (dla wszystkich z wyjątkiem skończonej liczby elementów zbioru I). Jest rzeczą oczywistą, że podzbiór S produktu P jest zamknięty ze względu na mnożenie oraz odwracanie elementów, jest zatem podgrupą produktu P.

Tak skonstruowaną grupę S nazywa się *zewnętrzną sumą prostą* rodziny grup $\{G_i : i \in I\}$, lub *koproduktem* tej rodziny grup i oznacza się ją

$$S = \coprod\{G_i : i \in I\}.$$

W przypadku gdy $G_i = G$ dla każdego $i \in I$, sumę prostą S oznaczamy $G^{(I)}$. Oczywiście, gdy zbiór I jest skończony (i tylko wtedy) mamy $G^I = G^{(I)}$.

Iloczyn półprosty

Zauważmy, że jeśli $G = HK$ jest iloczynem półprostym podgrup H i K grupy G, gdzie $H \lhd G$, to na iloczynie kartezjańskim $H \times K$ zbiorów H i K można określić działanie mnożenia następująco:

$$(h, k) \cdot (h_1, k_1) = (h \cdot kh_1k^{-1},\ kk_1).$$

Taką definicję mnożenia par podpowiada formuła (1.6). Łatwe sprawdzenie pokazuje, że z tak określonym działaniem zbiór $H \times K$ staje się grupą izomorficzną z iloczynem półprostym $G = HK$. Co więcej, założenie, że $G = HK$ jest iloczynem półprostym jest wykorzystane tylko dla zapewnienia, że $i_k(h_1) \in H$, co gwarantuje, iż iloczyn dwóch par z $H \times K$ jest znowu elementem tego zbioru. Wykorzystamy te obserwacje dla wprowadzenia ogólnego pojęcia iloczynu półprostego grup.

Niech więc H i K będą *dowolnymi* grupami i niech dany będzie homomorfizm

$$\alpha : K \to \mathsf{Aut}\, H,$$

który każdemu elementowi $k \in K$ przyporządkowuje automorfizm $\alpha(k)$ grupy H (w rozpatrywanym wyżej przypadku iloczynu półprostego mieliśmy $\alpha(k) = i_k$). Ponieważ $\mathsf{Aut}\, H$ jest podgrupą grupy symetrycznej $S(H)$, homomorfizm α wyznacza *działanie grupy K na grupie H*. Na iloczynie kartezjańskim $H \times K$ zbiorów H i K definiujemy *mnożenie* następująco:

$$(h, k) \cdot (h_1, k_1) = (h \cdot \alpha(k)(h_1),\ kk_1).$$

Ta definicja jest naturalnym rozszerzeniem rozpatrywanego wyżej przypadku iloczynu półprostego, w którym w miejsce automorfizmu $\alpha(k)$ mieliśmy automorfizm wewnętrzny i_k. Sprawdzamy teraz bez większego trudu, że zbiór $H \times K$ z tak określonym mnożeniem jest grupą.
Grupa ta zależy oczywiście od wybranego przez nas działania α grupy K na grupie H. Nazywa się ją zewnętrznym *iloczynem półprostym grup H i K* wyznaczonym przez działanie α grupy K na grupie H. Oznaczamy ją następująco:

$$H \rtimes_\alpha K.$$

Zauważmy, że jeśli homomorfizm $\alpha : K \to \mathsf{Aut}\, H$ jest trywialny, to znaczy $\alpha(k)$ jest automorfizmem identycznościowym grupy H dla każdego $k \in K$, to iloczyn półprosty $H \rtimes K$ pokrywa się z iloczynem prostym $H \times K$.
Grupa $H \rtimes K$ ma podgrupy $H' = H \times \Big\{1\Big\}$, $K' = \Big\{1\Big\} \times K$ oraz

$$H \rtimes K = H'K', \quad H' \cap K' = \Big\{(1, 1)\Big\},$$

a więc $H \rtimes K$ jest iloczynem ogólnym podgrup H', K'. Faktycznie jest to iloczyn półprosty, gdyż $H' \lhd H \rtimes K$. Rzeczywiście, odwzorowanie

$$\varphi : H \rtimes K \to K', \quad \varphi(h, k) = (1, k)$$

jest epimorfizmem grup oraz $\ker \varphi = H'$. Zatem $H' \lhd H \rtimes K$.

Przykład 1.3.1. Niech p, q będą liczbami pierwszymi i niech $H = \mathbb{Z}_p, K = \mathbb{Z}_q$ będą grupami cyklicznymi rzędów p i q. Grupa automorfizmów grupy $\mathbb{Z}_p$ składa się z przekształceń liniowych $\tau : \mathbb{Z}_p \to \mathbb{Z}_p$, $\tau_a(x) = ax$, gdzie $a \in \mathbb{Z}_p^*$ jest dowolnym niezerowym elementem grupy $\mathbb{Z}_p$. Dla dwóch automorfizmów τ_a, τ_b mamy

$$(\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x)) = abx = \tau_{ab}(x) \quad \text{dla każdego} \quad x \in \mathbb{Z}_p.$$

Stąd wynika, że grupa $\mathsf{Aut}\, \mathbb{Z}_p$ jest izomorficzna z grupą multyplikatywną $\mathbb{Z}_p^*$ reszt pierwszych względem p. Ta ostatnia grupa jest grupą cykliczną. Jeśli zatem weźmiemy homomorfizm

$$\alpha : \mathbb{Z}_q \to \mathsf{Aut}\, \mathbb{Z}_p$$

to $\alpha(\mathbb{Z}_q)$ jest podgrupą grupy cyklicznej $\mathsf{Aut}\, \mathbb{Z}_p$. Ponieważ $\mathbb{Z}_q$ jest grupą prostą, jej homomorficzny obraz jest bądź grupą jednostkową bądź też jest izomorficzny z

$\mathbb{Z}_q$. Jeśli homomorfizm α jest nietrywialny, to $\alpha(\mathbb{Z}_q)$ jest podgrupą rzędu q grupy $(p-1)-$elementowej $\mathsf{Aut}\,\mathbb{Z}_p$. Zatem

$$q \mid p-1$$

na podstawie twierdzenia Lagrange'a. Na odwrót, jeśli $q \mid p-1$, to $\mathsf{Aut}\,\mathbb{Z}_p$ jako grupa cykliczna rzędu $p-1$ ma (dokładnie jedną) podgrupę H rzędu q i każdy izomorfizm $\mathbb{Z}_q \cong H$ można traktować jako homomorfizm $\alpha : \mathbb{Z}_q \to \mathsf{Aut}\,\mathbb{Z}_p$. Jeśli więc $q \mid p-1$, to możemy rozpatrywać iloczyn półprosty

$$\mathbb{Z}_p \rtimes \mathbb{Z}_q.$$

Ta grupa jest nieabelową grupą rzędu pq. Rzeczywiście, niech $\alpha : \mathbb{Z}_q \to \mathsf{Aut}\,\mathbb{Z}_p$ będzie nietrywialnym homomorfizmem. Wtedy $\alpha(0)(1) \neq \alpha(1)(1)$, gdyż $1 \in \mathbb{Z}_p$ jest generatorem grupy cyklicznej $\mathbb{Z}_p$ i dwa automorfizmy równe na generatorze, są równe na każdym elemencie grupy cyklicznej. Tymczasem homomorfizm nietrywialny $\alpha : \mathbb{Z}_q \to \mathsf{Aut}\,\mathbb{Z}_p$ jest różnowartościowy, zatem $\alpha(0) \neq \alpha(1)$. Stąd wynika, że w grupie $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ mamy

$$(1,0)(1,1) = (1+\alpha(0)(1), 0+1) \neq (1+\alpha(1)(1), 1+0) = (1,1)(1,0).$$

Udowodniliśmy więc, że *jeśli p i q są liczbami pierwszymi oraz $q \mid p-1$, to istnieją nietrywialne homomorfizmy $\alpha : \mathbb{Z}_q \to \mathsf{Aut}\,\mathbb{Z}_p$ i dla każdego z nich iloczyn półprosty $\mathbb{Z}_p \rtimes \mathbb{Z}_q$ jest nieabelową grupą rzędu pq*. Z drugiej strony, można udowodnić, że jeśli dla liczb pierwszych p, q mamy $q < p$ oraz $q \nmid p-1$, to każda grupa rzędu pq jest cykliczna (zob. [S], zadania **384, 385**).

Rozważymy jeszcze przypadek gdy $G = HK$ jest iloczynem półprostym podgrup H i K grupy G, gdzie $K \lhd G$. Wtedy formuła (1.7) sugeruje określenie na iloczynie kartezjańskim $H \times K$ zbiorów H i K działania mnożenia następująco:

$$(h,k)\cdot(h_1,k_1) = (hh_1, h_1^{-1}kh_1 \cdot k_1).$$

Łatwe sprawdzenie pokazuje, że z tak określonym działaniem zbiór $H \times K$ staje się grupą izomorficzną z iloczynem półprostym $G = HK$. Założenie, że $G = HK$ i $K \lhd G$ jest wykorzystane tylko dla zapewnienia, że $i_{h_1^{-1}}(k) \in K$, co gwarantuje, iż iloczyn dwóch par z $H \times K$ jest znowu elementem tego zbioru. Podobnie jak w przypadku gdy $H \lhd G$ wprowadzimy drugą wersję definicji ogólnego pojęcia iloczynu półprostego grup.

Niech więc H i K będą *dowolnymi* grupami i niech dany będzie homomorfizm

$$\beta : H \to \mathsf{Aut}\,K,$$

który każdemu elementowi $h \in H$ przyporządkowuje automorfizm $\beta(h)$ grupy K (w rozpatrywanym wyżej przypadku iloczynu półprostego mieliśmy $\beta(h) = i_{h^{-1}}$). Ponieważ $\mathsf{Aut}\,K$ jest podgrupą grupy symetrycznej $S(K)$, homomorfizm β wyznacza *działanie grupy H na grupie K*. Na iloczynie kartezjańskim $H \times K$ zbiorów H i K definiujemy *mnożenie* następująco:

$$(h,k)\cdot(h_1,k_1) = (hh_1, \beta(h_1)(k)\cdot k_1).$$

Ta definicja jest naturalnym rozszerzeniem rozpatrywanego wyżej przypadku iloczynu półprostego, w którym w miejsce automorfizmu $\beta(h_1)$ mieliśmy automorfizm wewnętrzny $i_{h_1^{-1}}$. Sprawdzamy teraz bez większego trudu, że zbiór $H \times K$ z tak określonym mnożeniem jest grupą.
Grupa ta zależy oczywiście od wybranego przez nas działania β grupy H na grupie K. Nazywa się ją zewnętrznym *iloczynem półprostym grup* H i K wyznaczonym przez działanie β grupy H na grupie K. Oznaczamy ją następująco:

$$H \ {}_{\beta}\ltimes K.$$

Zauważmy, że jeśli homomorfizm $\beta : H \to \mathsf{Aut}\, K$ jest trywialny, to znaczy $\beta(h)$ jest automorfizmem identycznościowym grupy K dla każdego $h \in H$, to iloczyn półprosty $H \ltimes K$ pokrywa się z iloczynem prostym $H \times K$.
Grupa $H \ltimes K$ ma podgrupy $H' = H \times \{1\}$, $K' = \{1\} \times K$ oraz

$$H \ltimes K = H'K', \quad H' \cap K' = \{(1,1)\},$$

a więc $H \ltimes K$ jest iloczynem ogólnym podgrup H', K'. Faktycznie jest to iloczyn półprosty, gdyż $K' \lhd H \ltimes K$. Rzeczywiście, odwzorowanie

$$\varphi : H \ltimes K \to H', \quad \varphi(h,k) = (h,1)$$

jest epimorfizmem grup oraz $\ker \varphi = K'$. Zatem $K' \lhd H \ltimes K$.

Przykład 1.3.2. W pełnej grupie liniowej $\mathbf{GL}(n,F)$ nad dowolnym ciałem F rozpatrzmy podgrupę G złożoną z wszystkich macierzy

$$\begin{bmatrix} 1 & a_2 & \cdots & a_n \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

których pierwsza kolumna jest wektorem jednostkowym $(1,0,\ldots,0)^T$. Rozpatrzmy dwie następujące podgrupy H i K grupy G:

$$H = \left\{ \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{bmatrix} \in \mathbf{GL}(n,F) \right\}, \quad K = \left\{ \begin{bmatrix} 1 & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} \in \mathbf{GL}(n,F) \right\}.$$

Oczywiście $H \cap K = 1$ i wobec

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{bmatrix} \cdot \begin{bmatrix} 1 & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} 1 & a_2 & \cdots & a_n \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

widzimy, że grupa G jest iloczynem ogólnym podgrup H i K. Faktycznie jest to iloczyn półprosty, gdyż udowodnimy teraz, że $K \lhd G$. Wprowadźmy następujące uproszczone oznaczenia dla macierzy w grupach G, H i K:

$$\begin{bmatrix} 1 & a_2 & \cdots & a_n \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{bmatrix} =: g(A; a_2, \ldots, a_n), \qquad \begin{bmatrix} 1 & a_2 & \cdots & a_n \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} =: k(a_2, \ldots, a_n),$$

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & a_{n2} & \cdots & a_{nn} \end{bmatrix} =: h(A), \quad \text{gdzie} \quad A = \begin{bmatrix} a_{22} & \cdots & a_{2n} \\ \vdots & \ldots & \vdots \\ a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

Wtedy mamy

$$h(A) \cdot k(a_2, \ldots, a_n) = g(A; a_2, \ldots, a_n),$$

$$h(A) \cdot h(B) = h(AB), \qquad k(a_2, \ldots, a_n) \cdot k(b_2, \ldots, b_n) = k(a_2 + b_2, \ldots, a_n + b_n)$$

oraz

$$h(A)^{-1} = h(A^{-1}), \quad k(a_2, \ldots, a_n)^{-1} = k(-a_2, \ldots, -a_n).$$

Dla sprawdzenia, że $K \lhd G$ obieramy dowolne macierze $g \in G$, $k \in K$ i pokażemy, że $g^{-1}kg \in K$. Możemy przyjąć, że

$$k = k(b_2, \ldots, b_n) \quad \text{oraz} \quad g = h(A) \cdot k(a_2, \ldots, a_n),$$

gdyż G jest iloczynem ogólnym H i K. Wobec tego

$$\begin{aligned} g^{-1}kg &= k(-a_2, \ldots, -a_n) \cdot h(A^{-1}) \cdot k(b_2, \ldots, b_n) \cdot h(A) \cdot k(a_2, \ldots, a_n) \\ &= k(-a_2, \ldots, -a_n) \cdot g(A^{-1}; b_2, \ldots, b_n) \cdot g(A; a_2, \ldots, a_n) \\ &= k(-a_2, \ldots, -a_n) \cdot k(c_2, \ldots, c_n) \in K \end{aligned}$$

dla pewnych $c_2, \ldots, c_n \in F$. Mamy więc $G = HK$, $H \cap K = 1$, $K \lhd G$, czyli G jest iloczynem półprostym

$$G = H \ltimes K$$

swoich podgrup H i K.

Ten rezultat można też zinterpretować geometrycznie w sposób następujący. Niech V będzie $n-$wymiarową przestrzenią wektorową nad ciałem F z bazą $\{v_1, \ldots, v_n\}$. Niech Aut_1 oznacza podgrupę grupy wszystkich automorfizmów przestrzeni V pozostawiających wektor bazowy v_1 na miejscu. Wtedy grupa Aut_1 jest izomorficzna z grupą G. Zauważmy też, że mamy izomorfizmy grup

$$H \cong \mathbf{GL}(n-1, F), \qquad K \cong (F^{n-1}, +),$$

gdzie $(F^{n-1}, +)$ oznacza addytywną grupę przestrzeni wektorowej F^{n-1}. Zatem rozkład $G = H \ltimes K$ można zinterpretować jako przedstawienie grupy automorfizmów Aut_1 w postaci następującego iloczynu półprostego

$$\mathsf{Aut}_1 \cong \mathbf{GL}(n-1, F) \ltimes (F^{n-1}, +).$$

1.3.3 Holomorf grupy

Niech A będzie podgrupą normalną grupy G. Wtedy

$$gAg^{-1} = A$$

dla każdego $g \in G$. Wynika stąd, że automorfizm wewnętrzny i_g grupy G, zacieśniony do podgrupy A, jest automorfizmem (ale już niekoniecznie wewnętrznym) grupy A. Nasuwa się pytanie, czy dla każdej grupy A istnieje grupa G zawierająca A jako podgrupę normalną i taka, że *każdy* automorfizm grupy A jest zacieśnieniem do A pewnego automorfizmu *wewnętrznego* grupy G.

Przykład 1.3.3. Rozważymy najpierw przypadek, gdy grupa A jest *czynnikiem prostym* grupy G. Oznacza to, że obok podgrupy normalnej A mamy drugą podgrupę normalną B w grupie G oraz

$$G = A \cdot B = \{a \cdot b : \ a \in A, \ b \in B\}, \quad A \cap B = 1.$$

Wtedy, jak już wiemy, każdy element $a \in A$ jest przemienny z każdym elementem $b \in B$, to znaczy $ab = ba$, dla każdych $a \in A, \ b \in B$. Wobec tego jeśli $g = ab \in G$ jest dowolnym elementem grupy G, to dla każdego $x \in A$ mamy

$$i_g(x) = i_{ab}(x) = abxb^{-1}a^{-1} = axa^{-1},$$

gdyż $x \in A$ jest przemienny z elementem $b \in B$. Wynika stąd jednak, że i_g działa na podgrupie A dokładnie tak samo jak automorfizm wewnętrzny grupy A wyznaczony przez $a \in A$. Jeśli grupa A ma automorfizm zewnętrzny, to nie jest on zacieśnieniem do A automorfizmu wewnętrznego grupy G. Stwierdzamy więc, że gdy A jest czynnikiem prostym grupy G, to grupa G nie rozwiązuje naszego problemu.

Rozważymy teraz iloczyn półprosty $A \rtimes_h B$ dowolnych grup A i B wyznaczony przez działanie $h : B \to \mathsf{Aut}\, A$ grupy B na grupie A. Jak wiemy, A jest podgrupą normalną w $A \rtimes_h B$. Odwzorowania

$$a \mapsto (a, 1) \quad \text{oraz} \quad b \mapsto (1, b)$$

są monomorfizmami grup A i B w grupę $A \rtimes_h B$ i w związku z tym utożsamimy element a grupy A z jego obrazem $(a, 1)$, oraz element b grupy B z jego obrazem $(1, b)$ w grupie $A \rtimes_h B$. W ten sposób każdy element (a, b) iloczynu półprostego $A \rtimes_h B$ można przedstawić w postaci

$$(a, b) = (a, 1) \cdot (1, b) = a \cdot b.$$

Reguła mnożenia w grupie $A \rtimes_h B$ zapisze się teraz następująco:

$$ab \cdot a_1b_1 = (a, b) \cdot (a_1, b_1) = (a \cdot h(b)(a_1), bb_1) = a \cdot h(b)(a_1) \cdot bb_1.$$

Skracając lewostronnie a oraz prawostronnie b_1 oraz mnożąc prawostronnie przez b^{-1} otrzymujemy zatem następującą równość

$$ba_1b^{-1} = h(b)(a_1)$$

dla wszystkich $a_1 \in A,\ b \in B$. Stąd wynika, że automorfizm $h(b)$ grupy A jest zacieśnieniem automorfizmu wewnętrznego i_b grupy $A \rtimes_h B$ do podgrupy normalnej A. Pozostaje teraz wybrać odpowiednio grupę B i homomorfizm $h : B \to \mathsf{Aut}\, A$ tak, by $h(b)$ przebiegał *wszystkie* automorfizmy grupy A. Istnieje prosty i uniwersalny sposób spełnienia tych postulatów: wystarczy wziąć $B = \mathsf{Aut}\, A$ zaś w charakterze homomorfizmu h wziąć homomorfizm tożsamościowy $\mathrm{id} : \mathsf{Aut}\, A \to \mathsf{Aut}\, A$. Otrzymany w ten sposób iloczyn półprosty $A \rtimes_{\mathrm{id}} \mathsf{Aut}\, A$ nazywamy *holomorfem* grupy A i oznaczamy

$$\mathsf{Hol}(A) := A \rtimes_{\mathrm{id}} \mathsf{Aut}\, A.$$

Udowodniliśmy więc następujące twierdzenie, które rozwiązuje postawiony wcześniej problem.

TWIERDZENIE **1.3.4.** *Dla każdej grupy A istnieje grupa $\mathsf{Hol}(A)$ zawierająca A jako podgrupę normalną i mająca następującą własność. Każdy automorfizm grupy A jest zacieśnieniem do A pewnego automorfizmu wewnętrznego grupy $\mathsf{Hol}(A)$.*

Jako przykład rozważmy grupę cykliczną $A = \mathbb{Z}_n$. Jej grupa automorfizmów jest izomorficzna z multyplikatywną grupą $\mathbb{Z}_n^*$ reszt pierwszych względem n. Zatem

$$\mathsf{Hol}(\mathbb{Z}_n) \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^* \cong \mathsf{Af}(1, \mathbb{Z}_n),$$

gdzie $\mathsf{Af}(1, \mathbb{Z}_n)$ jest grupą afiniczną stopnia n nad pierścieniem $\mathbb{Z}_n$ reszt modulo n. Ponieważ $\mathsf{Aut}\, D_n \cong \mathsf{Af}(1, \mathbb{Z}_n)$ (zob. [S], zad. **331**), więc mamy także

$$\mathsf{Aut}\, D_n \cong \mathsf{Hol}(\mathbb{Z}_n).$$

Można także udowodnić, że dla iloczynu półprostego $G = \mathbb{Z}_n \rtimes \mathbb{Z}_m$ dwóch grup cyklicznych, jeśli $Z(G) = 1$, to $\mathsf{Aut}\, G \cong \mathsf{Hol}(\mathbb{Z}_n)$ (zob. G. L. Walls, Automorphism groups, *Amer. Math. Monthly* **93**(1986), 459–462).

1.4 Grupy wolne i kody genetyczne grup

Jedną z metod prezentacji grup jest zadanie grupy za pomocą generatorów i relacji lub inaczej mówiąc, podanie kodu genetycznego grupy. Precyzyjne objaśnienie tej metody wymaga wprowadzenia pojęcia *grupy wolnej z wolnym zbiorem generatorów*. Rozpoczniemy od prostszej konstrukcji monoidu wolnego.

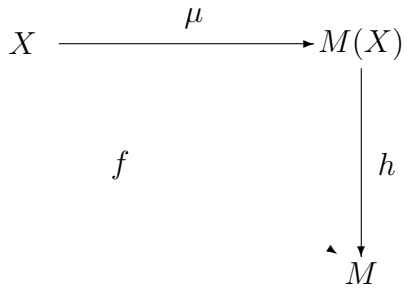
1.4.1 Monoidy wolne

Niech X będzie zbiorem niepustym. Zbiór ten będziemy nazywać *alfabetem*. Skończony ciąg elementów alfabetu X będziemy nazywać *słowem* a liczbę elementów tego ciągu nazywamy *długością* słowa. A więc, na przykład, jeśli $x, y \in X$ to $x, yy, xy, xxyyxy$ są słowami o długościach $1, 2, 2, 7$. Pusty ciąg jest także dopuszczalny i będziemy go oznaczać symbolem $\mathbf{1}$. Na zbiorze wszystkich słów w alfabecie X definiujemy operację *mnożenia* słów, która polega na dopisywaniu do pierwszego słowa drugiego słowa. Niech $*$ będzie znakiem tej operacji binarnej. Wtedy mamy, na przykład,

$$x * yy = xyy, \quad xy * xxyyxy = xyxxyyxy.$$

Jest rzeczą oczywistą, że operacja $*$ w zbiorze słów jest łączna oraz dla każdego słowa w w alfabecie X mamy $\mathbf{1} * w = w = w * \mathbf{1}$. A więc zbiór wszystkich słów w alfabecie X z operacją $*$ jest monoidem. Monoid ten oznaczamy symbolem $M(X)$ i nazywamy *monoidem wolnym* z alfabetem X.
Zauważmy, że formalnie rzecz biorąc zbiór X nie jest podzbiorem $M(X)$. W dalszym ciągu dla każdego $x \in X$ będziemy utożsamiać słowo jednoelementowe x (czyli ciąg jednoelementowy) z elementem x, i wobec tego będziemy mogli uważać, że $X \subset M(X)$. Włożenie $\mu : X \hookrightarrow M(X)$ ma następującą własność uniwersalną.

Twierdzenie **1.4.1.** *Niech X będzie zbiorem niepustym. Dla dowolnego monoidu M i dowolnego odwzorowania $f : X \to M$ istnieje dokładnie jeden homomorfizm monoidów $h : M(X) \to M$ taki, że $h \circ \mu = f$ a więc taki, że następujący diagram jest przemienny:*



Dowód. Definiujemy $h : M(X) \to M$ kładąc $h(\mathbf{1}) = 1_M$, gdzie 1_M jest jedynką monoidu M, oraz $h(x_1x_2 \dots x_n) = f(x_1) \cdot f(x_2) \cdots f(x_n)$ dla dowolnego niepustego słowa $x_1x_2 \dots x_n$ w alfabecie X. Tutaj, po prawej stronie równości definiującej odwzorowanie h, kropki oznaczają działanie w monoidzie M. Jest rzeczą oczywistą, że wtedy $h(w_1 * w_2) = h(w_1) \cdot h(w_2)$ dla dowolnych słów $w_1, w_2 \in M(X)$. A więc h jest homomorfizmem monoidów i ponadto, wobec utożsamienia $x \in X$ ze słowem jednoelementowym $x \in M(X)$ mamy $\mu(x) = x$, czyli $h \circ \mu(x) = h(x) = f(x)$ dla każdego $x \in X$. Dowiedliśmy więc istnienia homomorfizmu h.
Z drugiej strony, jeśli $h : M(X) \to M$ jest jakimkolwiek homomorfizmem monoidów spełniającym warunek $h \circ \mu = f$, to dla każdego $x \in X$ mamy $h(x) = h \circ \mu(x) = f(x)$ i dla każdego słowa $x_1x_2 \dots x_n \in M(X)$ mamy

$$h(x_1x_2 \dots x_n) = h(x_1 * x_2 * \cdots * x_n) = h(x_1) \cdot h(x_2) \cdots h(x_n) = f(x_1) \cdot f(x_2) \cdots f(x_n).$$

A więc homomorfizm h jest jednoznacznie wyznaczony przez warunek $h \circ \mu = f$. □

Własność uniwersalną z twierdzenia 1.4.1 można także odczytać w następujący sposób. Każde odwzorowanie f zbioru X w dowolny monoid M można przedłużyć do *homomorfizmu* h monoidu wolnego $M(X)$ w monoid M. Rzeczywiście, dla każdego $x \in X$ mamy $h(x) = h(\mu(x)) = f(x)$.

1.4.2 Grupy wolne

Monoid wolny $M(X)$ nie jest grupą, żadne bowiem niepuste słowo nie jest odwracalne. Tym niemniej istnieje sposób rozszerzenia monoidu wolnego $M(X)$ do grupy, którą nazywa się grupą wolną o alfabecie X. Opiszemy teraz tę konstrukcję.

Przede wszystkim rozszerzymy nasz wyjściowy alfabet X dołączając do niego dla każdego elementu $x \in X$ nowy element, który oznaczać będziemy x^{-1}. Zbiór wszystkich dołączonych elementów oznaczamy X^{-1} i tworzymy nowy alfabet X' zdefiniowany jako

$$X' = X \cup X^{-1}.$$

Zatem zbiór X' wraz z każdym elementem $x \in X$ zawiera także związany z nim element $x^{-1} \in X^{-1}$. Rozpatrujemy teraz monoid wolny $M(X')$ o alfabecie X'. Oczywiście $M(X')$ nie jest grupą, gdyż dopisanie do słowa niepustego innego słowa daje słowo niepuste i wobec tego niepuste słowa w $M(X')$ nie są odwracalne. Pokażemy, że można w monoidzie $M(X')$ określić relację równoważnościową zgodną z działaniem w $M(X')$ i taką, że klasy abstrakcji tej relacji z działaniem indukowanym z $M(X')$ tworzą grupę. Punktem wyjścia tej konstrukcji jest następująca definicja.

Definicja **1.4.2.** 1. Słowo $w \in M(X')$ nazywamy *redukowalnym* jeśli w ciągu w występują dwa kolejne elementy xx^{-1} lub $x^{-1}x$ dla pewnego $x \in X$.
2. Słowo, które nie jest redukowalne nazywa się słowem *zredukowanym*.
3. Słowo w' powstaje przez redukcję słowa w jeśli w' jest ostatnim słowem w ciągu skończonym słów

$$w_1 = w, w_2, w_3, \ldots,$$

w którym słowo w_{i+1} powstaje ze słowa w_i przez usunięcie ze słowa w_i przynajmniej jednej pary kolejnych elementów postaci xx^{-1} lub $x^{-1}x$, gdzie $x \in X$.
4. Słowo w' nazywa się *zredukowaną postacią* słowa w jeśli w' jest słowem zredukowanym i powstaje przez redukcję słowa w.

Konieczność użycia opisanego w punkcie 3 definicji ciągu słów ilustruje następujący przykład. Niech $w = xyy^{-1}x^{-1}z$. W słowie w tylko jedna para kolejnych elementów podlega redukcji, po której otrzymujemy słowo $w_1 = xx^{-1}z$. Po redukcji w słowie w_1 otrzymujemy $w_2 = z$. A więc z jest postacią zredukowaną słowa w.

Wprawdzie jest jasne, że każde słowo ma postać zredukowaną, jednakże nie jest rzeczą całkiem oczywistą, że każde słowo ma tylko jedną postać zredukowaną. Wątpliwości powstają przede wszystkim dlatego, że proces redukcji słowa można na ogół przeprowadzić na wiele sposobów i w związku z tym można byłoby oczekiwać różnych rezultatów redukcji słowa. Na przykład, słowo $x^{-1}xyy^{-1}x^{-1}y$ można redukować na dwa różne sposoby następująco

$$x^{-1}xyy^{-1}x^{-1}y \mapsto yy^{-1}x^{-1}y \mapsto x^{-1}y$$

$$x^{-1}xyy^{-1}x^{-1}y \mapsto x^{-1}xx^{-1}y \mapsto x^{-1}y$$

otrzymując zresztą to samo słowo zredukowane. Okazuje się, że postać zredukowana słowa nie zależy od wyboru kolejności operacji w procesie redukcji słowa.

Lemat **1.4.3.** *Każde słowo ma tylko jedną postać zredukowaną.*

Dowód. Pominiemy techniczny dowód tego faktu. Zainteresowanego Czytelnika odsyłamy do książki Kargapołowa i Mierzliakowa [KM], str. 129–130. □

Definicja **1.4.4.** Słowa w i v nazywają się *równoważnymi*, jeśli ich zredukowane postaci są identyczne. Piszemy wtedy $w \sim v$.

Relacja $\sim$ jest oczywiście relacją równoważnościową na zbiorze $M(X')$. Z łatwością stwierdzamy także, że relacja $\sim$ jest zgodna z działaniem mnożenia słów w monoidzie $M(X')$:

$$w \sim w' \quad \wedge \quad v \sim v' \quad \Rightarrow \quad w * v \sim w' * v'.$$

Wystarczy zauważyć, że słowa w i w' mają tę samą postać zredukowaną w_0 oraz podobnie v i v' mają tę samą postać zredukowaną v_0. Zatem poprzez odpowiednie redukcje ze słowa $w * v$ można otrzymać słowo $w_0 * v_0$ i podobnie, ze słowa $w' * v'$ można także otrzymać słowo $w_0 * v_0$. Teraz jest jasne, że $w * v$ i $w' * v'$ mają tę samą postać zredukowaną.

Niech $F(X)$ oznacza zbiór klas abstrakcji relacji równoważnościowej $\sim$ na monoidzie $M(X')$. Klasę zawierającą słowo w będziemy oznaczać $[w]$. W zbiorze $F(X)$ możemy teraz określić działanie mnożenia klas kładąc

$$[w] \cdot [v] := [w * v].$$

Oczywiście $F(X)$ staje się w ten sposób monoidem, w którym jedynką jest klasa $[\mathbf{1}]$ słowa pustego $\mathbf{1}$. Faktycznie monoid ten jest grupą, gdyż dla dowolnego słowa $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$, gdzie $x_i \in X$ oraz $\epsilon_i = \pm 1$ mamy

$$x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} x_n^{-\epsilon_n} \dots x_2^{-\epsilon_2} x_1^{-\epsilon_1} \sim \mathbf{1}.$$

Zatem w monoidzie $F(X)$ każdy element $[w] = [x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}]$ jest odwracalny i elementem odwrotnym do niego jest $[w]^{-1} := [x_n^{-\epsilon_n} \dots x_2^{-\epsilon_2} x_1^{-\epsilon_1}]$. Wobec tego $F(X)$ jest grupą. Zauważmy, że grupa ta jest generowana przez zbiór klas postaci $[x]$, gdzie $x \in X$. Grupę $F(X)$ nazywamy *grupą wolną z wolnym zbiorem generatorów* X.

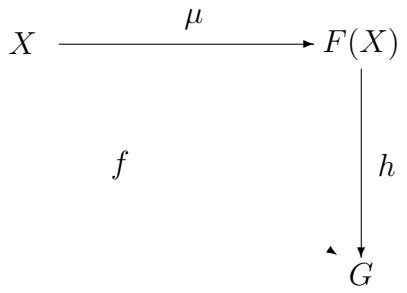
Przykład 1.4.1. Niech $X = \{x\}$ będzie zbiorem jednoelementowym. Grupa wolna $F(X)$ z jednoelementowym wolnym zbiorem generatorów $X = \{x\}$ jest generowana przez klasę $[x]$, jest zatem grupą cykliczną z generatorem $[x]$. Jest to *nieskończona* grupa cykliczna, gdyż w przeciwnym przypadku mielibyśmy $[x]^n = 1$ dla pewnej liczby naturalnej n wbrew temu, że słowo $xx \cdots x$ jest zredukowane i nie jest równoważne ze słowem pustym.

1.4.3 Własność uniwersalna grupy wolnej

Udowodnimy teraz własność uniwersalną grupy wolnej analogiczną do własności uniwersalnej monoidu wolnego z twierdzenia 1.4.1. Przede wszystkim więc formalizujemy związek grupy wolnej $F(X)$ z jej wolnym zbiorem generatorów X określając odwzorowanie

$$\mu : X \to F(X), \quad \mu(x) = [x].$$

TWIERDZENIE **1.4.5.** *Niech X będzie zbiorem niepustym. Dla dowolnej grupy G i dowolnego odwzorowania $f : X \to G$ istnieje dokładnie jeden homomorfizm grup $h : F(X) \to G$ taki, że $h \circ \mu = f$, a więc taki, że następujący diagram jest przemienny:*



Dowód. Najpierw rozszerzamy odwzorowanie f do odwzorowania $f' : X' \to G$, gdzie $X' = X \cup X^{-1}$ kładąc $f'(x) = f(x)$ oraz $f'(x^{-1}) = f(x)^{-1}$ dla każdego $x \in X$. Na podstawie twierdzenia 1.4.1 istnieje dokładnie jeden homomorfizm monoidów $h' : M(X') \to G$ taki, że $h' \circ \mu' = f'$, gdzie $\mu' : X' \hookrightarrow M(X')$ jest włożeniem. Stwierdzamy, że homomorfizm h' działa identycznie na słowach równoważnych. Rzeczywiście, wystarczy zauważyć, że

$$h'(x^{-1}x) = h'(x^{-1}) \cdot h'(x) = f'(x^{-1}) \cdot f'(x) = f'(x)^{-1} \cdot f'(x) = 1.$$

Można zatem h' określić na klasach słów równoważnych, czyli na elementach grupy $F(X)$. To nowe odwzorowanie oznaczamy $h : F(X) \to G$. Zatem dla dowolnego słowa w w alfabecie X' kładziemy $h([w]) = h'(w)$. Jest to oczywiście homomorfizm grup, gdyż dla dowolnych słów $w, v \in M(X')$ mamy

$$h([w] \cdot [v]) = h([w * v]) = h'(w * v) = h'(w) \cdot h'(v) = h([w]) \cdot h([v]).$$

Ponadto, dla dowolnego $x \in X$ mamy

$$(h \circ \mu)(x) = h([x]) = h'(x) = (h' \circ \mu')(x) = f'(x) = f(x).$$

Pozostaje udowodnić jedyność homomorfizmu h. Ponieważ $(h \circ \mu)(x) = f(x)$, więc $h([x]) = f(x)$ dla każdego $x \in X$. Homomorfizm h jest więc jednoznacznie określony na zbiorze generatorów $\{[x] : x \in X\}$ grupy $F(X)$, zatem jest jednoznacznie określony na grupie $F(X)$. □

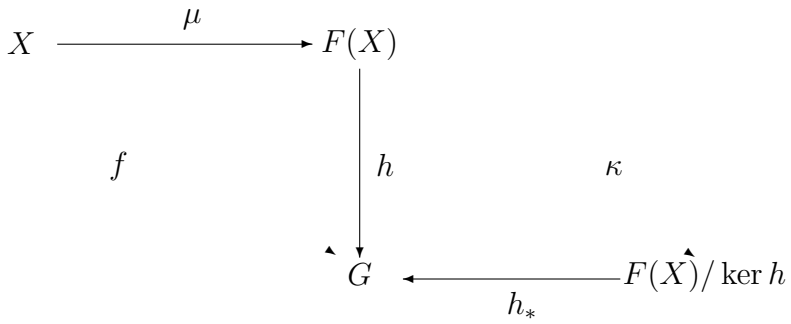
Podobnie jak w przypadku własności uniwersalnej monoidu wolnego także twierdzenie 1.4.5 można zinterpretować jako twierdzenie o przedłużaniu odwzorowań $f : X \to G$ zbioru X w grupę G do *homomorfizmu* $h : F(X) \to G$ grupy wolnej z wolnym zbiorem generatorów X w grupę G.

Wniosek **1.4.6.** *Każda grupa jest izomorficzna z grupą ilorazową pewnej grupy wolnej.*

Dowód. Niech G będzie dowolną grupą i niech X będzie dowolnym zbiorem generatorów grupy G. Wtedy na podstawie twierdzenia 1.4.5 włożenie $f : X \hookrightarrow G$ wyznacza homomorfizm grup $h : F(X) \to G$ taki, że $h([x]) = f(x) = x$ dla $x \in X$. Ogólniej, jeśli $[w] \in F(X)$ jest klasą słowa $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$, gdzie $x_i \in X$, $\epsilon_i = \pm 1$, to

$$h([w]) = h([x_1^{\epsilon_1}])h([x_2^{\epsilon_2}]) \dots h([x_n^{\epsilon_n}]) = x_1^{\epsilon_1} \cdot x_2^{\epsilon_2} \cdot \dots \cdot x_n^{\epsilon_n} = w_G,$$

gdzie przez w_G oznaczyliśmy element grupy G będący iloczynem potęg $x_i^{\epsilon_i}$ generatorów $x_i \in X$.



Zatem każdy element x zbioru generatorów X grupy G leży w obrazie homomorfizmu h i wobec tego h jest epimorfizmem grup. Na podstawie wniosku 1.1.5 z twierdzenia o faktoryzacji wynika stąd, że homomorfizm indukowany

$$h_* : F(X)/\ker h \to G, \quad h_*([w]\ker h) = h([w]) = w_G \quad \text{dla} \quad [w] \in F(X) \tag{1.9}$$

jest izomorfizmem grup i stąd $G \cong F(X)/\ker h$. □

Uwaga 1.4.7. Warto zauważyć, że przedstawienie grupy G jako grupy ilorazowej grupy wolnej jest w wysokim stopniu niejednoznaczne. Każdy zbiór generatorów X grupy G daje bowiem przedstawienie $G \cong F(X)/\ker h$.

1.4.4 Kod genetyczny grupy

Objaśnimy teraz pojęcie kodu genetycznego grupy. Niech G będzie dowolną grupą, X zbiorem generatorów grupy G, $F(X)$ grupą wolną z wolnym zbiorem generatorów X i niech

$$h_* : F(X)/\ker h \to G$$

będzie izomorfizmem grup określonym przez (1.9). W dalszym ciągu będziemy pisać N zamiast $\ker h$ i zamiast h_* będziemy rozpatrywać izomorfizm $\iota = h_*^{-1}$ odwrotny do h_*. Zatem

$$\iota : G \to F(X)/N, \quad \iota(g) = [g]N.$$

Tutaj decydujemy się na uproszczenie oznaczeń traktując w równości $\iota(g) = [g]N$ element g po lewej stronie jako element grupy G, a więc $g = x_1^{\epsilon_1} \cdots x_m^{\epsilon_m} \in G$ gdzie $x_i \in X$, $\epsilon_i = \pm 1$, natomiast po prawej stronie $g = x_1^{\epsilon_1} \cdots x_m^{\epsilon_m}$ jest odpowiadającym elementowi $g \in G$ słowem zapisanym w alfabecie $X \cup X^{-1}$. Jeśli dla pewnych $x_1, \ldots, x_n \in X$ mamy w grupie G równość

$$x_1^{k_1} \cdots x_n^{k_n} = 1, \tag{1.10}$$

to biorąc obrazy obydwu stron poprzez ι otrzymamy $[x_1]^{k_1} \cdots [x_n]^{k_n} N = N$, czyli

$$[x_1]^{k_1} \cdots [x_n]^{k_n} \in N. \tag{1.11}$$

A więc każdej relacji postaci (1.10) pomiędzy generatorami grupy G ze zbioru X odpowiada element postaci (1.11) w podgrupie normalnej N grupy $F(X)$. Oczywiście także na odwrót, jeśli elementy $x_1, \ldots, x_n \in X$ spełniają (1.11), to w grupie G mamy relację postaci (1.10).

W związku z tą sytuacją, elementy podgrupy normalnej N nazywamy *relacjami* grupy G w alfabecie X, zaś o grupie $G \cong F(X)/N$ mówimy, że jest zadana za pomocą zbioru generatorów X i zbioru relacji N.

Przykład 1.4.2. Rozważmy dwie grupy G i G' przedstawione za pomocą tego samego zbioru generatorów X i zbiorów relacji $K \subseteq N$:

$$G \cong F(X)/K, \quad G' \cong F(X)/N, \quad \text{gdzie} \quad K < N.$$

Zakładamy więc, że K i N są podgrupami normalnymi grupy wolnej $F(X)$. Na podstawie wniosku 1.1.9 z twierdzenia o odpowiedniości mamy $K \lhd N$ oraz

$$F(X)/N \cong (F(X)/K)/(N/K).$$

Grupa $G' \cong F(X)/N$ jest zatem izomorficzna z pewną grupą ilorazową grupy $G \cong F(X)/K$. A więc powiększenie zbioru relacji z K do N zamienia grupę G ze zbiorem relacji K na grupę G' ze zbiorem relacji N izomorficzną z grupą ilorazową grupy G (czyli grupę "mniejszą" niż G).

Przykład 1.4.3. Niech $G = \{1, a, a^2, a^3\}$ będzie grupą cykliczną rzędu 4. Grupa ta jest generowana przez zbiór jednoelementowy $X = \{a\}$. Grupa wolna $F(X)$ jest zatem nieskończoną grupą cykliczną z generatorem $[a]$. Ponadto mamy homomorfizm

$$h : F(X) \to G, \quad h([a]^n) = a^n$$

oraz izomorfizm $h_* : F(X)/N \to G$, przy czym podgrupa normalna $N = \ker h$ grupy $F(X)$ składa się z elementów odtwarzających wszystkie relacje spełniane przez element a grupy G. Z pewnością

$$[a]^4 \in N.$$

Pokażemy, że N *jest minimalną podgrupą normalną grupy* $F(X)$ *o własności* $[a]^4 \in N$. Przypuśćmy, że istnieje podgrupa normalna K grupy G taka, że

$$K \subseteq N \quad \text{oraz} \quad [a]^4 \in K.$$

Wtedy istnieje epimorfizm $f : F(X)/K \to F(X)/N$ taki, że $f(wK) = wN$ dla każdego elementu $w \in F(X)$. Dla warstwy $A := [a]K$ mamy $A^4 = [a]^4K = K$, zatem grupa $F(X)/K$ ma co najwyżej 4 elementy. Ponieważ jednak f jest surjekcją na grupę 4−elementową, grupa $F(X)/K$ też jest 4−elementowa i wobec tego f jest izomorfizmem grup. Gdyby istniał element $w \in F(X)$ taki, że $w \in N$ i $w \notin K$, to mielibyśmy

$$f(wK) = wN = N,$$

to znaczy, wK byłby nietrywialnym elementem w jądrze f, wbrew temu, że f jest izomorfizmem. Zatem $K = N$, co oznacza, że N jest minimalną podgrupą normalną $F(X)$ zawierającą element $[a]^4$.

Definicja **1.4.8.** Niech $G \cong F(X)/N$ będzie przedstawieniem grupy G za pomocą zbioru generatorów X i zbioru relacji N. Niech $\mathcal{R}$ będzie podzbiorem podgrupy normalnej N w grupie $F(X)$. Jeśli N jest minimalną podgrupą normalną grupy $F(X)$ zawierającą zbiór $\mathcal{R}$, to parę $X, \mathcal{R}$ nazywamy *kodem genetycznym* grupy G i piszemy

$$G = \mathrm{gr}(X \,||\, \mathcal{R}).$$

Przykład 1.4.4. Dla grupy cyklicznej rzędu 4 mamy kod genetyczny $\mathrm{gr}(a \mid\mid [a]^4)$. Rzeczywiście, na podstawie przykładu 1.4.3, grupa cykliczna rzędu 4 ma przedstawienie w postaci $F(X)/N$, gdzie N jest minimalną podgrupą normalną grupy $F(X)$ zawierającą jednoelementowy zbiór $\mathcal{R} = \left\{[a]^4\right\}$.

Dla grupy cyklicznej nieskończonej $G = \langle a \rangle$ mamy zbiór generatorów $X = \left\{a\right\}$. Grupa wolna $F(X) = F(\left\{a\right\})$ jest wtedy grupą cykliczną nieskończoną. Podgrupa N w izomorfizmie $G \cong F(X)/N$ jest podgrupą jednostkową, gdyż jedyną relacją jaką spełnia element a jest $a^0 = 1$. Można zatem napisać $G = \mathrm{gr}(a \mid\mid 1)$ lub $G = \mathrm{gr}(a \mid\mid \emptyset)$, jeśli nie chcemy zaliczać jedynki grupy do zbioru generatorów.

Przykład 1.4.5. Rozpatrzmy grupę kwaternionów $Quat$ z przykładu 1.1.1(d). Jest ona generowana przez dwa elementy A, B spełniające relacje $A^4 = B^4 = 1, A^2 = B^2, BAB^{-1} = A^{-1}$ i składa się z 8 następujących elementów:

$$1, A, A^2, A^3, B, AB, A^2B, A^3B.$$

Znajdziemy kod genetyczny grupy $Quat$. Dla zbioru $X = \left\{A, B\right\}$ generatorów grupy $Quat$ istnieje epimorfizm $h : F(X) \to Quat$ taki, że $h([A]) = A, h([B]) = B$ oraz indukowany izomorfizm $h_* : F(X)/\ker h \to Quat$. Wobec relacji spełnianych przez generatory A, B w grupie $Quat$ mamy

$$[A]^4, [B]^4, [A]^2[B]^{-2}, [B][A][B]^{-1}[A] \in \ker h =: N.$$

Udowodnimy, że N jest minimalną podgrupa normalną grupy $F(X)$ zawierającą te cztery elementy. Niech $K \subseteq N$ oznacza podgrupę normalną grupy $F(X)$ zawierającą te cztery elementy. Pokażemy, że $K = N$.
Stąd, że $K \subseteq N$ wynika, że odwzorowanie $f : F(X)/K \to F(X)/N, \quad f(wK) = wN$ jest epimorfizmem grup. Zatem złożenie $\varphi = h_* \circ f : F(X)/K \to Quat$ jest epimorfizmem grup. Najpierw sprawdzimy, że φ jest izomorfizmem. Wobec $|Quat| = 8$ wystarczy pokazać, że $|F(X)/K| \leqslant 8$. Grupa $F(X)/K$ jest generowana przez warstwy

$$a := [A]K, \quad b := [B]K.$$

Ponieważ $[A]^4, [B]^4, [A]^2[B]^{-2}, [B][A][B]^{-1}[A] \in K$, elementy a, b spełniają relacje

$$a^4 = b^4 = 1, \quad a^2 = b^2, \quad bab^{-1} = a^{-1}$$

i wobec tego tak samo jak w przypadku grupy kwaternionów sprawdzamy, że grupa $F(X)/K$ generowana przez a, b ma co najwyżej 8 elementów

$$1, a, a^2, a^3, b, ab, a^2b, a^3b.$$

Jak już zauważyliśmy, wynika stąd, że $\varphi = h_* \circ f$ jest izomorfizmem. Wobec tego także $f : F(X)/K \to F(X)/N, \ f(wK) = wN$ jest izomorfizmem grup. Stąd wynika już, że $K = N$. Rzeczywiście, gdyby istniał element $w \in N$ nie należący do K, to $wK \neq K$ oraz $f(wK) = wN = N$, to znaczy wK jest nietrywialnym elementem w jądrze izomorfizmu f, sprzeczność.

Pokazaliśmy więc, że minimalna podgrupa normalna grupy $F(X)$ zawierająca elementy $[A]^4$, $[B]^4$, $[A]^2[B]^{-2}, [B][A][B]^{-1}[A]$ jest równa N, gdzie $F(X)/N \cong Quat$. Znaleźliśmy więc kod genetyczny grupy kwaternionów:

$$Quat = \mathrm{gr}(\{A, B\} \mid\mid [A]^4, [B]^4, [A]^2[B]^{-2}, [B][A][B]^{-1}[A]\,).$$

W kodzie genetycznym $G = \mathrm{gr}(X \,||\, \mathcal{R})$ grupy G występuje zbiór generatorów X grupy G oraz zbiór $\mathcal{R}$ pewnych elementów grupy wolnej $F(X)$ otrzymany z relacji spełnianych przez generatory. Czasami wygodniej jest w kodzie genetycznym podać relacje spełniane przez generatory zamiast odpowiadających im elementów grupy wolnej. W tej konwencji kod genetyczny grupy kwaternionów wygląda bardziej naturalnie:

$$Quat = \mathrm{gr}(\{A, B\} \mid\mid A^4 = B^4 = 1, A^2 = B^2, BAB^{-1} = A^{-1}\,).$$

Uwaga 1.4.9. Spośród wielu twierdzeń o grupach wolnych wymienimy tylko dwa. Po pierwsze, grupa wolna jest z dokładnością do izomorfizmu wyznaczona przez moc zbioru wolnych generatorów, to znaczy, dwie grupy wolne $F(X)$ i $F(Y)$ są izomorficzne wtedy i tylko wtedy, gdy zbiory X i Y są równoliczne. W związku z tym moc zbioru X nazywa się *rangą* (lub *stopniem*) grupy wolnej $F(X)$.
Po drugie, można udowodnić, że każda nietrywialna podgrupa grupy wolnej jest grupą wolną. Jest to twierdzenie Nielsena-Schreiera (zob. [KM], str. 139).

1.5 Zadania

1. (a) Udowodnić, że jeśli grupa ilorazowa $G/Z(G)$ jest cykliczna, to grupa G jest abelowa
($Z(G)$ oznacza centrum grupy G).
(b) Udowodnić, że nie istnieje grupa G, której centrum jest podgrupą o indeksie 2 lub 3.

2. Dowieść, że istnieją tylko dwie nieizomorficzne grupy nieabelowe rzędu 8.

3. Dowieść, że każda grupa rzędu 15 jest cykliczna.

4. Niech A będzie grupą cykliczną rzędu n. Udowodnić, że dla każdego dzielnika d liczby n istnieje dokładnie jedna podgrupa grupy A rzędu d.

5. Dowieść, że każda skończona grupa abelowa, która nie jest grupą cykliczną, zawiera podgrupę H, która jest sumą prostą dwóch grup cyklicznych rzędu p, gdzie p jest pewną liczbą pierwszą.

6. Niech p będzie liczbą naturalną i niech $G \neq E$ będzie grupą, w której każdy $\neq 1$ element ma rząd będący potęgą liczby p. Udowodnić, że p jest liczbą pierwszą. Ponadto, jeśli grupa G jest skończona, to jej rząd jest potęgą liczby p.

7. Niech G będzie grupą skończoną i niech p będzie najmniejszą liczbą pierwszą dzielącą rząd grupy G. Dowieść, że każda podgrupa H grupy G, której indeks $|G : H|$

jest równy p, jest podgrupą normalną grupy G.

8. Niech $n \geqslant 2$ i niech

$$0 \longrightarrow A_1 \longrightarrow A_2 \longrightarrow \cdots \longrightarrow A_n \longrightarrow 0$$

będzie ciągiem dokładnym grup skończonych.
(a) Jeśli n jest liczbą parzystą, udowodnić, że $|A_1|\cdot|A_3|\cdots|A_{n-1}| = |A_2|\cdot|A_4|\cdots|A_n|$.
(b) Jeśli n jest liczbą nieparzystą, udowodnić, że $|A_1|\cdot|A_3|\cdots|A_n| = |A_2|\cdot|A_4|\cdots|A_{n-1}|$.

9. Pokazać, że grupa czwórkowa Kleina $G = V_4$ jest jedyną grupą G rzędu $\geqslant 4$, której grupa automorfizmów $\mathsf{Aut}\, G$ składa się z wszystkich bijekcji zbioru G pozostawiających jedynkę grupy G na miejscu.

10. Dla ciał kwadratowych $K = \mathbb{Q}(\sqrt{-2}\,)$ oraz $F = \mathbb{Q}(\sqrt{-7}\,)$ udowodnić, że
(a) Addytywne grupy ciał K i F są izomorficzne.
(b) Multyplikatywne grupy ciał K i F są izomorficzne.
(c) Ciała K i F nie są izomorficzne.

11. Udowodnić, że część wspólna wszystkich $p-$podgrup Sylowa grupy skończonej G jest podgrupą normalną grupy G.

12. Niech G będzie grupą rzędu 168. Udowodnić, że grupy G nie można zanurzyć w grupę symetryczną S_6. Pokazać, że jeśli grupa G jest prosta, to ma 8 podgrup rzędu 7 i można ją zanurzyć w grupę S_8.

13. Udowodnić, że każda grupa wolna jest beztorsyjna i jest nieabelowa jeśli jej ranga jest $\geqslant 2$.

14. Udowodnić, że grupa z kodem genetycznym

$$\mathrm{gr}(\,\{x_1, \ldots, x_n\} \,||\, x_i x_j x_i^{-1} x_j^{-1}, \quad 1 \leqslant i < j \leqslant n)$$

jest wolną grupą abelową rangi n (tzn. jest sumą prostą n grup cyklicznych nieskończonych).

15. Znaleźć kod genetyczny grupy czwórkowej Kleina $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$.

Rozdział 2

Pierścienie

Ostatnie zmiany 15.11.2008 r.

2.1 Podstawowe pojęcia

DEFINICJA **2.1.1.** Zbiór P z dwoma działaniami $+$ i $\cdot$ zwanymi odpowiednio *dodawaniem* i *mnożeniem* oraz z dwoma wyróżnionymi elementami 0 i 1 zwanymi *zerem* i *jedynką* nazywa się *pierścieniem*, jeśli spełnione są następujące warunki:

1. $(P, +, 0)$ jest grupą abelową.
2. $(P, \cdot, 1)$ jest monoidem (półgrupą z jedynką).
3. Mnożenie jest rozdzielne względem dodawania, to znaczy

$$a(b+c) = ab + ac \quad \text{oraz} \quad (b+c)a = ba + ca$$

dla każdych $a, b, c \in P$.

Zwracamy uwagę, że każdy pierścień ma jedynkę. Może się jednak zdarzyć, że $0 = 1$ i wtedy $a = a \cdot 1 = a \cdot 0 = 0$ dla każdego $a \in P$, a więc $P = \{0\}$ jest *pierścieniem zerowym*. Ponadto, mnożenie w pierścieniu P musi być łączne ale może być *nieprzemienne*. Jeśli mnożenie w pierścieniu P jest przemienne, to znaczy jeśli $ab = ba$ dla każdych $a, b \in P$, to pierścień P nazywa się pierścieniem *przemiennym*. *Podpierścieniem* pierścienia P nazywamy podgrupę P_1 addytywnej grupy pierścienia P zawierającą jedynkę pierścienia P i zamkniętą ze względu na mnożenie. Łatwo sprawdzić, że P_1 jest wtedy także pierścieniem ze względu na działania dodawania i mnożenia będące zacieśnieniami odpowiednich działań w P.
Element a pierścienia P nazywa się *lewostronnie* odwracalny, jeśli istnieje $b \in P$ taki, że $ba = 1$. Element b nazywa się wtedy lewostronnie odwrotnym do elementu a. Podobnie, $a \in P$ jest *prawostronnie* odwracalny, jeśli istnieje $c \in P$ taki, że $ac = 1$. Element c jest wtedy prawostronnie odwrotny do a. To rozróżnienie pomiędzy elementami lewostronnie i prawostronnie odwracalnymi jest niezbędne w teorii pierścieni nieprzemiennych. Przykład 2.1.6 wskazuje pierścień nieprzemienny (endomorfizmów addytywnej grupy pierścienia wielomianów), w którym istnieją elementy jednostronnie, ale nie obustronnie odwracalne.

Element $a \in P$ nazywa się *odwracalny*, jeśli jest równocześnie lewostronnie i prawostronnie odwracalny. Zauważmy, że jeśli $ba = 1$ oraz $ac = 1$, to

$$b = b \cdot ac = ba \cdot c = c.$$

A więc element odwracalny a ma tylko jeden element lewostronnie odwrotny, jak również tylko jeden element prawostronnie odwrotny i elementy te są równe (jedynemu) elementowi odwrotnemu do a. W związku z tą jednoznacznością elementu odwrotnego do a wprowadzamy dla niego oznaczenie a^{-1}.
Stwierdzamy z łatwością, że zbiór $U(P)$ wszystkich elementów odwracalnych pierścienia P tworzy grupę ze względu na mnożenie elementów. Nazywa się ją *grupą elementów odwracalnych* pierścienia P.
Pierścień P nazywa się *pierścieniem z dzieleniem*, jeśli każdy różny od zera element pierścienia P jest odwracalny. Przemienny pierścień z dzieleniem jest więc ciałem.
Element a pierścienia P nazywa się *lewostronnym dzielnikiem zera*, jeśli istnieje $b \in P,\ b \neq 0$, taki, że $ab = 0$. Podobnie, $a \in P$ jest *prawostronnym dzielnikiem zera*, jeśli istnieje $c \in P,\ c \neq 0$, taki, że $ca = 0$. Element $a \in P$ nazywa się *dzielnikiem zera* w P jeśli jest równocześnie lewostronnym i prawostronnym dzielnikiem zera.
Centrum $Z(P)$ pierścienia P nazywamy zbiór wszystkich elementów pierścienia P przemiennych z każdym elementem pierścienia P :

$$Z(P) := \Big\{a \in P : ab = ba \ \ \forall b \in P\Big\}.$$

Łatwo sprawdzić, że $Z(P)$ jest (przemiennym) podpierścieniem pierścienia P.

Przykład 2.1.1. Najbardziej naturalnym przykładem pierścienia jest pierścień $\mathbb{Z}$ liczb całkowitych. Nie ma on podpierścieni właściwych (różnych od $\mathbb{Z}$). Ponieważ $\mathbb{Z}$ jest pierścieniem przemiennym, więc $Z(\mathbb{Z}) = \mathbb{Z}$. Ponadto, $U(\mathbb{Z}) = \{\pm 1\}$. Pierścień $\mathbb{Z}$ nie ma dzielników zera.
Bardzo naturalnych przykładów dostarczają także *pierścienie reszt* $\mathbb{Z}_n$. Tutaj także nie ma właściwych podpierścieni (gdyż addytywna grupa $\mathbb{Z}_n$ jest grupą cykliczną generowaną przez jedynkę 1 pierścienia $\mathbb{Z}_n$), natomiast

$$U(\mathbb{Z}_n) = \Big\{a \bmod n : \mathrm{NWD}(a, n) = 1\Big\}.$$

Jeśli n jest liczbą złożoną, $n = ab$, gdzie a i b są liczbami naturalnymi większymi niż 1, to $a \cdot b = 0$ w $\mathbb{Z}_n$. A więc jeśli n jest liczbą złożoną, to pierścień reszt $\mathbb{Z}_n$ ma dzielniki zera.

Przykład 2.1.2. Niech P będzie dowolnym pierścieniem przemiennym i niech $P[X]$ będzie pierścieniem wielomianów jednej zmiennej X (lub zespołu zmiennych $X = [X_1, \ldots, X_n]$). $P[X]$ jest pierścieniem przemiennym. Jeśli P nie ma dzielników zera, to $P[X]$ także nie ma dzielników zera oraz $U(P[X]) = U(P)$.

Przykład 2.1.3. Niech P będzie dowolnym pierścieniem i niech $M(X, P)$ będzie zbiorem wszystkich funkcji określonych na niepustym zbiorze X o wartościach w pierścieniu P. W zbiorze $M(X, P)$ określamy działania dodawania i mnożenia funkcji w zwykły sposób. A więc dla $f, g \in M(X, P)$ funkcje $f + g : X \to P$ oraz $f \cdot g : X \to P$ określone są następująco:

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

dla każdego $x \in X$. Funkcje $\mathbf{0} : X \to P,\ \mathbf{0}(x) = 0$ oraz $\mathbf{1} : X \to P,\ \mathbf{1}(x) = 1$ są elementami neutralnymi dodawania i mnożenia w $M(X, P)$. Sprawdzamy bez

trudu, że system $(M(X,P),\ +\ ,\ \cdot\ ,\mathbf{0},\mathbf{1})$ jest pierścieniem. Jeśli P jest pierścieniem przemiennym, to $M(X,P)$ jest także pierścieniem przemiennym. W szczególności, jeśli $X = P$, to $M(P,P)$ jest pierścieniem funkcji $P \to P$. Wśród nich wyróżniamy podpierścień $\mathrm{Pol}(P,P)$ funkcji wielomianowych $\widehat{f} : P \to P$ takich, że $f \in P[X]$. Tutaj $\widehat{f}(a) = f(a)$ jest wartością wielomianu f w punkcie $a \in P$.

Przykład 2.1.4. Dla pierścienia P symbolem $M_n(P)$ oznacza się zbiór wszystkich macierzy kwadratowych stopnia n o elementach z pierścienia P. *Sumą* i *iloczynem* macierzy $A = [a_{ij}]$ i $B = [b_{ij}]$ nazywamy macierze

$$A + B = [a_{ij} + b_{ij}], \quad AB = [c_{ij}], \quad \text{gdzie} \quad c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Rutynowe rachunki pozwalają stwierdzić, że $M_n(P)$ jest pierścieniem. Nazywamy go *pierścieniem macierzy stopnia n nad pierścieniem P*. Jeśli $n \geqslant 2$, to $M_n(P)$ jest pierścieniem nieprzemiennym.

Przykład 2.1.5. Niech A będzie grupą abelową i niech $\mathsf{End}\, A$ będzie monoidem wszystkich endomorfizmów grupy A (ze składaniem endomorfizmów jako działaniem). Obok składania endomorfizmów rozpatrujemy także dodawanie endomorfizmów określone tak samo jak w pierścieniu funkcji $M(A,A)$. Dzięki abelowości grupy A dodawanie endomorfizmów jest także działaniem przemiennym. $\mathsf{End}\, A$ jest podgrupą addytywnej grupy pierścienia $M(A,A)$. Bezpośrednim rachunkiem stwierdzamy, że składanie endomorfizmów jest rozdzielne względem dodawania:

$$f(g+h)(a) = f((g+h)(a)) = f(g(a)+h(a)) = f(g(a)) + f(h(a)) = (fg+fh)(a)$$

dla dowolnych $f, g, h \in \mathsf{End}\, A$ i $a \in A$, i podobnie dla prawostronnej rozdzielności mnożenia względem dodawania endomorfizmów. A więc $\mathsf{End}\, A$ jest pierścieniem. Jest to *pierścień endomorfizmów grupy abelowej A*.

Przykład 2.1.6. Niech P będzie dowolnym pierścieniem przemiennym i niech $A = P[X]$ będzie addytywną grupą pierścienia wielomianów jednej zmiennej X o współczynnikach z P. Będziemy rozpatrywać pierścień endomorfizmów $\mathsf{End}\, P[X]$ grupy abelowej $P[X]$.

Niech $\mathcal{D}$ oraz $\mathcal{I}$ będą odwzorowaniami $P[X] \to P[X]$ określonymi następująco:

$$\mathcal{D}(f) = \frac{d}{dX} f, \qquad \mathcal{I}(f) = \int_1^X f(t)dt.$$

Tutaj $\mathcal{D}(f)$ jest formalną pochodną wielomianu f natomiast $\mathcal{I}(f)$ jest formalną całką oznaczoną wielomianu f. Operacje $\mathcal{D}$ i $\mathcal{I}$ są oczywiście endomorfizmami grupy abelowej $A = P[X]$. Zauważamy, że dla dowolnego wielomianu $f \in P[X]$ mamy

$$\mathcal{D}\mathcal{I}(f) = \mathcal{D}\Big(\int_1^X f(t)dt\Big) = f(X) = f,$$

oraz z drugiej strony

$$\mathcal{I}\mathcal{D}(f) = \int_1^X \mathcal{D}(f)(t)dt = f(X) - f(1).$$

Zatem $\mathcal{D} \cdot \mathcal{I} = 1_A$, natomiast $\mathcal{I} \cdot \mathcal{D} \neq 1_A$, gdyż jeśli tylko wielomian f nie zeruje się w punkcie $X = 1$, to $\mathcal{I}\mathcal{D}(f) \neq f$. Zatem endomorfizm różniczkowania $\mathcal{D}$ jest prawostronnie odwracalny i prawostronnie odwrotnym endomorfizmem jest endomorfizm całkowania $\mathcal{I}$. Natomiast $\mathcal{I}$ nie jest endomorfizmem lewostronnie odwrotnym do $\mathcal{D}$. Ponieważ element odwracalny ma tylko jeden element lewostronnie odwrotny, wynika stąd, że operacja różniczkowania (a także operacja całkowania) nie jest odwracalnym endomorfizmem addytywnej grupy abelowej $P[X]$.

2.2 Homomorfizmy i ideały

Jeśli P i R są pierścieniami, to każdą funkcję $h : P \to R$ spełniającą warunki

$$h(a + b) = h(a) + h(b), \quad h(ab) = h(a)h(b), \quad h(1) = 1$$

dla każdych $a, b \in P$, nazywamy *homomorfizmem* pierścienia P w pierścień R. Homomorfizm h nazywamy *epimorfizmem* lub *monomorfizmem*, jeśli jest on odwzorowaniem surjektywnym lub injektywnym, odpowiednio. Łatwo sprawdzić, że jeśli $h : P \to R$ jest epimorfizmem pierścieni, to

$$h(Z(P)) \subseteq Z(R), \quad h(U(P)) \subseteq U(R).$$

Niech $h : P \to R$ będzie homomorfizmem pierścieni. Wtedy h jest także homomorfizmem addytywnej grupy pierścienia P w addytywną grupę pierścienia R. Jądro $\ker h$ tego homomorfizmu (grup addytywnych) nazywamy *jądrem* homomorfizmu h pierścienia P w pierścień R. A więc

$$\ker h = \Big\{a \in P : h(a) = 0\Big\}$$

jest podgrupą addytywnej grupy pierścienia P i ponadto,

$$a \in \ker h \quad \Rightarrow \quad ab,\ ba \in \ker h$$

dla każdego $b \in P$. Mamy bowiem $h(ab) = h(a)h(b) = 0 \cdot h(b) = 0$ i podobnie $h(ba) = 0$. Jądro homomorfizmu pierścieni $h : P \to R$ jest więc podgrupą addytywnej grupy pierścienia P zamkniętą ze względu na mnożenie przez elementy pierścienia P. Jest to własność charakteryzująca *ideały* pierścienia P.

Definicja **2.2.1.** Ideałem lewostronnym (prawostronnym) pierścienia P nazywamy podgrupę $\mathcal{I}$ addytywnej grupy pierścienia P zamkniętą ze względu na mnożenie z lewej (prawej) strony przez elementy pierścienia P.
Ideał lewostronny $\mathcal{I}$ pierścienia P, który jest równocześnie ideałem prawostronnym nazywa się *ideałem* (lub *ideałem dwustronnym*) pierścienia P.

Najważniejszymi przykładami ideałów pierścienia P są jądra homomorfizmów pierścienia P w dowolne pierścienie. Przykładami ideałów jednostronnych są ideały *główne* aP oraz Pa przy odpowiednim doborze elementu a i pierścienia nieprzemiennego P. Przy pomocy twierdzenia o dzieleniu z resztą można udowodnić, że w pierścieniu $\mathbb{Z}$ liczb całkowitych każdy ideał jest ideałem głównym. Podobnie, w

pierścieniu wielomianów $K[X]$ jednej zmiennej X nad ciałem K każdy ideał jest ideałem głównym.
Ogólniej, każdy podzbiór S pierścienia P generuje pewien ideał. Łatwo sprawdzamy, że zbiory

$$SP := \Big\{ s_1x_1 + \cdots + s_nx_n \in P : s_i \in S,\ x_i \in P,\ n \in \mathbb{N} \Big\}$$

$$PS := \Big\{ x_1s_1 + \cdots + x_ns_n \in P : s_i \in S,\ x_i \in P,\ n \in \mathbb{N} \Big\}$$

są odpowiednio prawo- i lewostronnymi ideałami pierścienia P. Ponadto, SP jest najmniejszym ideałem prawostronnym pierścienia P zawierającym zbiór S i PS jest najmniejszym ideałem lewostronnym pierścienia P zawierającym zbiór S. Nazywamy je ideałami jednostronnymi *generowanymi* przez zbiór S. Zauważmy, że gdy $1 \in S$, to $SP = PS = P$. Ogólniej, jeśli $\mathcal{I}$ jest ideałem jednostronnym (lub obustronnym) i $1 \in \mathcal{I}$, to $\mathcal{I} = P$.

Niech teraz $\mathcal{I}$ będzie ideałem pierścienia P. Zatem $\mathcal{I}$ można traktować jako podgrupę addytywnej grupy pierścienia P i utworzyć grupę ilorazową $P/\mathcal{I}$. Jak wiemy, zbiór warstw jest zamknięty ze względu na dodawanie kompleksowe warstw:

$$(a + \mathcal{I}) + (b + \mathcal{I}) = (a + b) + \mathcal{I}.$$

Okazuje się, że zbiór warstw $P/\mathcal{I}$ nie jest na ogół zamknięty ze względu na mnożenie kompleksowe warstw. Rzeczywiście, mamy jedynie

$$\begin{aligned}(a + \mathcal{I})(b + \mathcal{I}) &= \Big\{ (a + j_1)(b + j_2) : j_1, j_2 \in \mathcal{I} \Big\} \\ &= \Big\{ ab + aj_2 + j_1b + j_1j_2 : j_1, j_2 \in \mathcal{I} \Big\} \\ &\subseteq\ ab + \mathcal{I}\end{aligned}$$

gdyż $aj_2 + j_1b + j_1j_2 \in \mathcal{I}$ dla wszystkich $j_1, j_2 \in \mathcal{I}$ (wykorzystujemy tutaj także fakt, że $\mathcal{I}$ jest ideałem obustronnym). Tutaj nie można oczekiwać równości nawet w najprostszych sytuacjach. Na przykład w pierścieniu $\mathbb{Z}$ liczb całkowitych dla ideału głównego $10\mathbb{Z}$ i iloczynu kompleksowego warstw zawierających 2 i 4 mamy

$$(2 + 10\mathbb{Z})(4 + 10\mathbb{Z}) = 8 + 20\mathbb{Z} \subsetneq 8 + 10\mathbb{Z}.$$

Zauważmy, że dla iloczynu kompleksowego mamy oczywistą własność

$$a + \mathcal{I} = a' + \mathcal{I}, \quad b + \mathcal{I} = b' + \mathcal{I} \quad \Rightarrow \quad (a + \mathcal{I})(b + \mathcal{I}) = (a' + \mathcal{I})(b' + \mathcal{I})$$

a więc iloczyn kompleksowy $(a + \mathcal{I})(b + \mathcal{I})$ nie zależy od sposobu reprezentacji warstw. Ponieważ różne warstwy są rozłączne, iloczyn kompleksowy $(a + \mathcal{I})(b + \mathcal{I})$ jest podzbiorem dokładnie jednej warstwy $ab + \mathcal{I}$ i w związku z tym tę warstwę nazywamy iloczynem warstw $(a + \mathcal{I}) \cdot (b + \mathcal{I})$. Definiujemy więc działanie mnożenia warstw

$$(a + \mathcal{I}) \cdot (b + \mathcal{I}) = ab + \mathcal{I}.$$

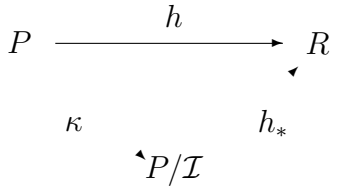
W dalszym ciągu nigdzie nie będziemy używać iloczynu kompleksowego warstw pierścienia względem jego ideału. W związku z tym iloczyn warstw w sensie powyższej definicji będziemy pisać bez kropki, to znaczy odtąd piszemy $(a+\mathcal{I})(b+\mathcal{I}) = ab+\mathcal{I}$.

Na zbiorze warstw $P/\mathcal{I}$ mamy zatem określone dwa działania: dodawania i mnożenia warstw. Wykorzystując łączność mnożenia i rozdzielność mnożenia względem dodawania w P dowodzimy łączności mnożenia i rozdzielności mnożenia względem dodawania w $P/\mathcal{I}$. Ponadto, $(1+\mathcal{I})(a+\mathcal{I}) = a+\mathcal{I} = (a+\mathcal{I})(1+\mathcal{I})$. Zatem $P/\mathcal{I}$ jest pierścieniem z jedynką $1+\mathcal{I}$. Pierścień ten nazywamy *pierścieniem ilorazowym* pierścienia P względem ideału $\mathcal{I}$ (lub modulo $\mathcal{I}$). Zauważmy jeszcze, że dla $\mathcal{I} = P$ jako pierścień ilorazowy P/P otrzymujemy pierścień zerowy. Jest to główny powód, dla którego w definicji pierścienia nie wymagaliśmy by $0 \neq 1$. Odwzorowanie

$$\kappa : P \to P/\mathcal{I}, \quad \kappa(a) = a+\mathcal{I}$$

jest homomorfizmem pierścieni oraz $\ker\kappa = \mathcal{I}$. Homomorfizm κ nazywamy *homomorfizmem kanonicznym* pierścienia P na pierścień ilorazowy $P/\mathcal{I}$. Zauważamy też od razu, że każdy ideał $\mathcal{I}$ pierścienia P jest jądrem pewnego homomorfizmu pierścienia P. A więc ideały będą odgrywały w twierdzeniach o homomorfizmach pierścieni podobną rolę jak podgrupy normalne w twierdzeniach o homomorfizmach grup. W teorii pierścieni prawdziwe są odpowiedniki wszystkich trzech podstawowych twierdzeń o homomorfizmach grup: o faktoryzacji, odpowiedniości i izomorfizmie. Sformułujemy tutaj pierwsze dwa z nich.

Twierdzenie **2.2.2.** (Twierdzenie o faktoryzacji.)
Jeśli $h : P \to R$ jest homomorfizmem pierścieni, $\mathcal{I} = \ker h$ oraz $\kappa : P \to P/\mathcal{I}$ jest homomorfizmem kanonicznym, to istnieje dokładnie jeden injektywny homomorfizm $h_* : P/\mathcal{I} \to R$ taki, że $h = h_* \circ \kappa$, to znaczy taki, że następujący diagram jest przemienny:



Dowód. Wykorzystujemy twierdzenie 1.1.4 o faktoryzacji homomorfizmów grup dla homomorfizmu h traktowanego jako homomorfizm addytywnych grup pierścieni P i R i stwierdzamy, że h_* jest homomorfizmem pierścieni. □

Przykład 2.2.1. Dla pierścienia przemiennego P rozpatrujemy odwzorowanie

$$P[X] \to \mathrm{Pol}(P,P), \quad f \mapsto \widehat{f}$$

pierścienia $P[X]$ wielomianów jednej zmiennej w pierścień $\mathrm{Pol}(P,P)$ funkcji wielomianowych $P \to P$. Jest to homomorfizm pierścieni. Niech $\mathcal{J}$ będzie jądrem tego homomorfizmu,

$$\mathcal{J} = \Big\{ f \in P[X] : f(a) = 0 \quad \forall\, a \in P \Big\}.$$

Wiadomo, że $\mathcal{J} = 0$ gdy P jest nieskończonym pierścieniem bez dzielników zera. Wtedy homomorfizm ten jest izomorfizmem. Ale $\mathcal{J} \neq 0$, na przykład, gdy P jest ciałem skończonym. Jeśli p jest liczbą pierwszą i $P = \mathbb{F}_p$ jest ciałem $p-$elementowym,

to $a^p = a$ dla każdego $a \in \mathbb{F}_p$ i wobec tego $X^p - X \in \mathcal{J}$. Łatwo stwierdzić, że $\mathcal{J} = (X^p - X)\,\mathbb{F}_p[X]$ jest ideałem głównym generowanym przez wielomian $X^p - X$. Mamy zatem

$$\mathbb{F}_p[X]/(X^p - X)\,\mathbb{F}_p[X] \cong \mathrm{Pol}(\mathbb{F}_p, \mathbb{F}_p).$$

Fakt, że ideał $\mathcal{J}$ nie zawsze jest ideałem zerowym zmusza do rozróżniania pierścienia wielomianów od pierścienia funkcji wielomianowych.

Twierdzenie **2.2.3.** (Twierdzenie o odpowiedniości.)
Jeśli $h : P \to R$ jest epimorfizmem pierścieni, to przyporządkowanie $\mathcal{I} \mapsto h(\mathcal{I})$ jest bijekcją rodziny ideałów $\mathcal{I}$ pierścienia P zawierających $\ker h$ *na rodzinę wszystkich ideałów pierścienia R. Odwzorowaniem odwrotnym jest $\mathcal{J} \mapsto h^{-1}(\mathcal{J})$.*
Ponadto, dla każdego ideału $\mathcal{I}$ pierścienia P zawierającego jądro $\ker h$ *homomorfizmu h mamy izomorfizm*

$$P/\mathcal{I} \cong R/h(\mathcal{I}).$$

Dowód. Dla homomorfizmu h traktowanego jako homomorfizm addytywnych grup pierścieni P i R wykorzystujemy teorio-grupowe twierdzenie 1.1.7 o odpowiedniości. Pozostaje prześledzić dowód twierdzenia 1.1.7 i uzupełnić go sprawdzeniem odpowiednich własności multyplikatywnych. Pozostawiamy to jako ćwiczenie dla Czytelnika. □

2.3 Ideały w pierścieniach przemiennych

Wprawdzie część dyskutowanych tu pojęć i faktów ma swoje odpowiedniki w dowolnych pierścieniach, jednak dla uproszczenia zakładać będziemy stale, że rozpatrywane pierścienie są przemienne. W związku z tym, od tego miejsca począwszy, słowo *pierścień* oznacza zawsze *pierścień przemienny*. Dla podkreślenia tego stałego założenia pierścienie będziemy oznaczać literami A, B w odróżnieniu od dotychczasowej praktyki oznaczania pierścieni literami P, R.
Wśród pierścieni przemiennych krańcową z naszego punktu widzenia klasę tworzą *ciała*. Z łatwością bowiem stwierdzamy, że każde ciało K ma tylko dwa ideały: ideał zerowy $0K = \{0\}$ oraz ideał jednostkowy $1K = K$. Łatwo także stwierdzić, że jeśli pierścień A ma tylko dwa ideały, mianowicie $0A$ i A, to A jest ciałem.

Jeśli $S = \{s_1, \ldots, s_n\}$ jest skończonym podzbiorem pierścienia A, to ideał SA generowany przez zbiór S oznaczać będziemy $(s_1, \ldots, s_n)$. Zatem

$$SA = AS = (s_1, \ldots, s_n) = \Big\{s_1x_1 + \cdots + s_nx_n \in A : x_1, \ldots, x_n \in A\Big\}.$$

Wprowadzimy teraz trzy podstawowe operacje na ideałach pierścienia.
Sumą ideałów $\mathfrak{a}$ oraz $\mathfrak{b}$ pierścienia A nazywamy zbiór $\mathfrak{a} + \mathfrak{b}$ wszystkich elementów postaci $a + b$, gdzie $a \in \mathfrak{a}$ oraz $b \in \mathfrak{b}$. Jest to więc zwykła suma podgrup $\mathfrak{a}$ i $\mathfrak{b}$ addytywnej grupy A. Ponieważ suma ta jest zamknięta ze względu na mnożenie przez elementy pierścienia A, jest ona ideałem w A.
Jeśli S i T są podzbiorami pierścienia A oraz $\mathfrak{a} = AS$, $\mathfrak{b} = AT$ są ideałami generowanymi przez zbiory S i T, to suma ideałów $\mathfrak{a} + \mathfrak{b}$ jest ideałem generowanym przez sumę mnogościową zbiorów $S \cup T$. W szczególności, dla dowolnych

$a_1, \ldots, a_n, b_1, \ldots, b_m \in A$,

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_m) = (a_1, \ldots, a_n, b_1, \ldots, b_m).$$

Iloczynem ideałów $\mathfrak{a}$ oraz $\mathfrak{b}$ pierścienia A nazywamy zbiór $\mathfrak{a}\cdot\mathfrak{b}$ wszystkich skończonych sum postaci

$$c_1d_1 + \cdots + c_nd_n, \quad c_i \in \mathfrak{a}, \quad d_i \in \mathfrak{b}, \quad n \in \mathbb{N}.$$

Iloczyn $\mathfrak{a} \cdot \mathfrak{b}$ jest ideałem pierścienia A.
Zauważmy, że jeśli $\mathfrak{a} = (a_1, \ldots, a_n)$, $\mathfrak{b} = (b_1, \ldots, b_m)$ to

$$\mathfrak{a} \cdot \mathfrak{b} = (a_1b_1, a_2b_1, \ldots, a_ib_j, \ldots, a_nb_m).$$

Zarówno dodawanie jak i mnożenie ideałów są operacjami przemiennymi i łącznymi. Ponadto, mnożenie ideałów jest rozdzielne względem dodawania ideałów, to znaczy, dla każdych trzech ideałów $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ pierścienia A mamy

$$(\mathfrak{a} + \mathfrak{b}) \cdot \mathfrak{c} = \mathfrak{a} \cdot \mathfrak{c} + \mathfrak{b} \cdot \mathfrak{c}.$$

Przekrojem ideałów $\mathfrak{a}$ oraz $\mathfrak{b}$ nazywamy część wspólną $\mathfrak{a} \cap \mathfrak{b}$ ideałów $\mathfrak{a}$ i $\mathfrak{b}$. Jest to ideał pierścienia A. Przekrój ideałów nie jest na ogół rozdzielny względem dodawania ideałów. Można tylko pokazać, że dla ideałów $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ pierścienia A, jeśli $\mathfrak{a} \subseteq \mathfrak{c}$ lub $\mathfrak{b} \subseteq \mathfrak{c}$, to

$$(\mathfrak{a} + \mathfrak{b}) \cap \mathfrak{c} = \mathfrak{a} \cap \mathfrak{c} + \mathfrak{b} \cap \mathfrak{c}.$$

Jest to tak zwane *prawo modularności*. Warto zwrócić uwagę, że zawsze $\mathfrak{a}\cdot\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$. Natomiast jak pokazują najprostsze przykłady (powiedzmy $A = \mathbb{Z}$, $\mathfrak{a} = 2\mathbb{Z}$, $\mathfrak{b} = 4\mathbb{Z}$), nie ma tu na ogół równości. Łatwo jednak wskazać ogólny warunek wystarczający na to, by iloczyn dwóch ideałów był równy ich przekrojowi. Korzystając z rozdzielności mnożenia ideałów względem dodawania otrzymujemy dla dowolnych ideałów $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ pierścienia A

$$(\mathfrak{a} + \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a} \cdot (\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b} \cdot (\mathfrak{a} \cap \mathfrak{b}).$$

Zatem $(\mathfrak{a} + \mathfrak{b}) \cdot (\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{a} \cdot \mathfrak{b}$. Jeśli więc $\mathfrak{a} + \mathfrak{b} = (1)$ jest ideałem jednostkowym $(1) = A$, to otrzymujemy $\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a} \cdot \mathfrak{b}$. Wobec tego,

$$\mathfrak{a} + \mathfrak{b} = (1) \quad \Rightarrow \quad \mathfrak{a} \cdot \mathfrak{b} = \mathfrak{a} \cap \mathfrak{b}.$$

Ideały $\mathfrak{a}$ i $\mathfrak{b}$ spełniające warunek $\mathfrak{a} + \mathfrak{b} = (1)$ nazywamy ideałami *względnie pierwszymi*. Jeśli więc ideały są względnie pierwsze, to ich iloczyn i przekrój są równe. Twierdzenie odwrotne nie jest prawdziwe: w pierścieniu $\mathbb{Z}[X]$ wielomianów jednej zmiennej o współczynnikach całkowitych dla ideałów głównych $\mathfrak{a} = (2)$, $\mathfrak{b} = (X)$ mamy $\mathfrak{a} \cdot \mathfrak{b} = (2X) = \mathfrak{a} \cap \mathfrak{b}$, natomiast $\mathfrak{a} + \mathfrak{b} = (2, X) \neq (1)$.

2.3.1 Ideały pierwsze i maksymalne

Ideał $\mathfrak{p}$ pierścienia A nazywa się ideałem *pierwszym* jeśli dla dowolnych $a, b \in A$,

$$ab \in \mathfrak{p} \quad \Rightarrow \quad a \in \mathfrak{p} \quad \text{lub} \quad b \in \mathfrak{p}.$$

Wygodnie jest też posługiwać się równoważnym warunkiem

$$a \notin \mathfrak{p} \quad \text{i} \quad b \notin \mathfrak{p} \quad \Rightarrow \quad ab \notin \mathfrak{p} \tag{2.1}$$

dla $a, b \in A$. A więc ideał $\mathfrak{p}$ pierścienia A jest pierwszy wtedy i tylko wtedy gdy zbiór $A \setminus \mathfrak{p}$ jest zamknięty ze względu na mnożenie. Zauważmy także, że ideał $\mathfrak{p}$ pierścienia A jest pierwszy wtedy i tylko wtedy gdy pierścień ilorazowy $A/\mathfrak{p}$ nie ma niezerowych dzielników zera. Mamy bowiem

$$(a + \mathfrak{p})(b + \mathfrak{p}) = \mathfrak{p} \quad \Leftrightarrow \quad ab \in \mathfrak{p}$$

oraz

$$a + \mathfrak{p} = \mathfrak{p} \quad \text{lub} \quad b + \mathfrak{p} = \mathfrak{p} \quad \Leftrightarrow \quad a \in \mathfrak{p} \quad \text{lub} \quad b \in \mathfrak{p}.$$

Prototypem ideałów pierwszych są ideały $p\mathbb{Z}$ pierścienia liczb całkowitych $\mathbb{Z}$ generowane przez liczby pierwsze p. Tutaj $\mathbb{Z}/p\mathbb{Z}$ jest ciałem, nie ma więc niezerowych dzielników zera.
Ideał $p\mathbb{Z}$ ma więc nieco silniejszą własność niż potrzeba do stwierdzenia, że jest ideałem pierwszym. Rozpatrzmy nieco dokładniej tę subtelną różnicę. Załóżmy więc, że $\mathfrak{p}$ jest ideałem pierścienia A i pierścień ilorazowy $A/\mathfrak{p}$ jest ciałem. Wtedy dla każdego elementu $a \in A \setminus \mathfrak{p}$ istnieje element $z \in A$ taki, że

$$(a + \mathfrak{p})(z + \mathfrak{p}) = 1 + \mathfrak{p},$$

a więc taki, że $az - 1 \in \mathfrak{p}$. Jeśli więc $\mathcal{I}$ jest jakimkolwiek ideałem pierścienia A zawierającym $\mathfrak{p}$ i różnym od $\mathfrak{p}$, to dla każdego $a \in \mathcal{I} \setminus \mathfrak{p}$ istnieje element $z \in A$ taki, że

$$\mathcal{I} = az + \mathcal{I} = 1 + \mathcal{I}.$$

Tutaj pierwsza równość wynika stąd, że $a \in \mathcal{I}$ pociąga $az \in \mathcal{I}$, natomiast druga stąd, że $az - 1 \in \mathfrak{p} \subset \mathcal{I}$. A więc $1 \in \mathcal{I}$, skąd dla każdego $x \in A$ mamy $x = 1 \cdot x \in \mathcal{I}$. Otrzymujemy więc $\mathcal{I} = A$. Oznacza to, że jedynym ideałem $\mathcal{I}$ pierścienia A zawierającym $\mathfrak{p}$ i różnym od $\mathfrak{p}$ jest cały pierścień A. Ideały o tej własności nazywamy ideałami maksymalnymi.

Definicja **2.3.1.** Ideał $\mathfrak{m}$ pierścienia A nazywamy ideałem *maksymalnym* pierścienia A, jeśli $\mathfrak{m} \neq A$ i dla każdego ideału $\mathcal{I}$ pierścienia A,

$$\mathfrak{m} \subseteq \mathcal{I} \quad \Rightarrow \quad \mathfrak{m} = \mathcal{I} \quad \text{lub} \quad \mathcal{I} = A.$$

Twierdzenie **2.3.2.** *Ideał $\mathfrak{m}$ pierścienia A jest ideałem maksymalnym wtedy i tylko wtedy, gdy pierścień ilorazowy $A/\mathfrak{m}$ jest ciałem.*

Dowód. Jedną część twierdzenia udowodniliśmy już powyżej. Załóżmy więc, że $\mathfrak{m}$ jest ideałem maksymalnym pierścienia A i niech $a+\mathfrak{m}$ będzie dowolnym niezerowym elementem pierścienia $A/\mathfrak{m}$. Wtedy $a \notin \mathfrak{m}$, zatem suma ideałów $\mathfrak{m}+aA$ jest ideałem różnym od $\mathfrak{m}$. Wobec maksymalności $\mathfrak{m}$ mamy $\mathfrak{m}+aA = A$. W szczególności istnieją elementy $m \in \mathfrak{m}$ oraz $z \in A$ takie, że $m + az = 1$. Wtedy

$$(a + \mathfrak{m})(z + \mathfrak{m}) = az + \mathfrak{m} = 1 + \mathfrak{m},$$

skąd wynika, że $a + \mathfrak{m}$ jest elementem odwracalnym pierścienia $A/\mathfrak{m}$. A więc $A/\mathfrak{m}$ jest ciałem. □

Uwaga 2.3.3. Powyższy dowód twierdzenia 2.3.2 jest całkowicie elementarny i bezpośredni. Zauważmy jednak, że twierdzenie to jest natychmiastowym wnioskiem z twierdzenia 2.2.3 o odpowiedniości zastosowanym do homomorfizmu kanonicznego $\kappa : A \to A/\mathfrak{m}$. Wystarczy jedynie przypomnieć, że $A/\mathfrak{m}$ jest ciałem wtedy i tylko wtedy, gdy ma tylko dwa ideały, zerowy i jednostkowy. Zatem na podstawie twierdzenia 2.2.3 ma to miejsce dokładnie wtedy, gdy rodzina wszystkich ideałów pierścienia A zawierających $\mathfrak{m}$ składa się tylko z dwóch ideałów: $\mathfrak{m}$ i A, to znaczy wtedy gdy ideał $\mathfrak{m}$ jest maksymalny w A.

Wniosek **2.3.4.** *Każdy ideał maksymalny jest ideałem pierwszym.*

Twierdzenie **2.3.5.** *Każdy ideał $\mathcal{I} \neq A$ pierścienia A zawiera się w pewnym ideale maksymalnym pierścienia A.*

Dowód. Rozpatrujemy rodzinę wszystkich ideałów właściwych (to znaczy $\neq A$) pierścienia A zawierających ideał $\mathcal{I}$. Jest to zbiór częściowo uporządkowany przez inkluzję. To uporządkowanie jest induktywne, to znaczy, dla każdego łańcucha $\{\mathfrak{a}_i : i \in I\}$ ideałów zawierających ideał $\mathcal{I}$ suma mnogościowa $\mathcal{J} := \bigcup\{\mathfrak{a}_i : i \in I\}$ jest ideałem właściwym pierścienia A (bo $1 \notin \mathcal{J}$) zawierającym $\mathcal{I}$ i oczywiście $\mathfrak{a}_i \subseteq \mathcal{J}$. Na podstawie lematu Kuratowskiego–Zorna rodzina ideałów właściwych pierścienia A zawierających $\mathcal{I}$ ma element maksymalny $\mathfrak{m}$. Jest to ideał maksymalny pierścienia A zawierający ideał $\mathcal{I}$. □

Wniosek **2.3.6.** *W każdym pierścieniu istnieje co najmniej jeden ideał maksymalny.*

Dowód. Wystarczy wziąć ideał zerowy $\mathcal{I} = 0$ w twierdzeniu 2.3.5. □

2.3.2 Rozszerzenie i zwężenie ideału

Jeśli $h : A \to B$ jest homomorfizmem pierścieni oraz $\mathcal{I}$ jest ideałem w pierścieniu A, to jego obraz $h(\mathcal{I})$ nie jest, na ogół, ideałem w B. Na przykład, monomorfizm $\mathbb{Z} \hookrightarrow \mathbb{Q}$ przeprowadza każdy niezerowy ideał pierścienia $\mathbb{Z}$ na addytywną podgrupę $\mathbb{Q}$, która nie jest ideałem w $\mathbb{Q}$.
Można natomiast rozpatrywać w B ideał $Bh(\mathcal{I})$ *generowany* przez $h(\mathcal{I})$ w B. Ideał ten składa się z wszystkich skończonych sum

$$\sum x_i h(a_i), \quad x_i \in B, \;\; a_i \in \mathcal{I}.$$

Ideał $Bh(\mathcal{I})$ nazywa się *rozszerzeniem* ideału $\mathcal{I}$ pierścienia A w pierścieniu B (za pomocą homomorfizmu $h : A \to B$). Jeśli nie ma wątpliwości jaki homomorfizm h rozpatrujemy, to rozszerzenie $Bh(\mathcal{I})$ ideału $\mathcal{I}$ oznaczamy $\mathcal{I}^{\mathrm{e}}$ (od angielskiego *extension*).

Operacja rozszerzania ideałów nie zachowuje, na ogół, charakterystycznych własności ideałów. Na przykład, rozszerzenie ideału pierwszego nie jest, na ogół, ideałem pierwszym.

Przykład 2.3.1. Dla włożenia $h : \mathbb{Z} \hookrightarrow \mathbb{Q}$ i dowolnego niezerowego ideału $\mathcal{I}$ pierścienia $\mathbb{Z}$ mamy $\mathcal{I}^{\mathrm{e}} = \mathbb{Q}$. Rozszerzenie niezerowego ideału pierwszego nie jest więc ideałem pierwszym.

Przykład 2.3.2. Rozpatrzmy teraz włożenie $h : \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$, gdzie $i = \sqrt{-1} \in \mathbb{C}$, oraz ideał główny $(2) = 2\mathbb{Z}$ liczb parzystych w $\mathbb{Z}$. Jego obraz generuje ideał główny $2\mathbb{Z}[i]$, to znaczy $(2)^{\mathrm{e}} = 2\mathbb{Z}[i]$. Ponieważ $(1+i)^2 = 2i$ oraz i jest elementem odwracalnym w $\mathbb{Z}[i]$, mamy

$$(2)^{\mathrm{e}} = 2\mathbb{Z}[i] = (1+i)^2\mathbb{Z}[i] = ((1+i)\mathbb{Z}[i])^2,$$

to znaczy, rozszerzeniem ideału pierwszego $(2) = 2\mathbb{Z}$ jest kwadrat $(1+i)^2$ ideału generowanego przez liczbę $1+i$ w pierścieniu $\mathbb{Z}[i]$. Nie jest to ideał pierwszy, bo na przykład liczba $(1+i)^2$ należy do ideału generowanego przez siebie, ale jej czynniki $1+i$ nie należą do tego ideału.
Podobnie (wobec równości $5 = (2+i)(2-i)$) rozszerzeniem ideału pierwszego $(5) = 5\mathbb{Z}$ okazuje się iloczyn dwóch ideałów pierwszych pierścienia $\mathbb{Z}[i]$:

$$(5)^{\mathrm{e}} = (2+i)\mathbb{Z}[i] \cdot (2-i)\mathbb{Z}[i].$$

Można też sprawdzić, że $(3)^{\mathrm{e}} = 3\mathbb{Z}[i]$ jest ideałem pierwszym pierścienia $\mathbb{Z}[i]$.
Na podstawie klasycznego twierdzenia Fermata, jeśli p jest liczbą pierwszą i $p \equiv 1 \pmod 4$, to p można przedstawić w postaci sumy dwóch kwadratów liczb naturalnych: $p = a^2 + b^2$. Wtedy liczba p jest rozkładalna w pierścieniu $\mathbb{Z}[i]$ gdyż $p = (a+bi)(a-bi)$ i żaden z czynników tego rozkładu nie jest elementem odwracalnym w $\mathbb{Z}[i]$. Dla ideału głównego $(p) = p\mathbb{Z}$ mamy zatem

$$(p)^{\mathrm{e}} = (a+bi)\mathbb{Z}[i] \cdot (a-bi)\mathbb{Z}[i],$$

przy czym $(a \pm bi)\mathbb{Z}[i]$ są ideałami pierwszymi w $\mathbb{Z}[i]$. Jeśli natomiast p jest liczbą pierwszą i $p \equiv 3 \pmod 4$, to można udowodnić, że $(p)^{\mathrm{e}} = p\mathbb{Z}[i]$ jest ideałem pierwszym pierścienia $\mathbb{Z}[i]$.

Powracając teraz do homomorfizmu $h : A \to B$ zauważmy, że zupełnie inaczej niż obrazy zachowują się *przeciwobrazy* ideałów pierścienia B w A. Jeśli $\mathcal{J}$ jest ideałem w B to jego przeciwobraz $h^{-1}(\mathcal{J})$ jest ideałem w A. Po pierwsze bowiem, przeciwobraz addytywnej grupy ideału $\mathcal{J}$ jest addytywną podgrupą w A, po drugie, jeśli $a \in h^{-1}(\mathcal{J})$ oraz $x \in A$, to $h(a) \in \mathcal{J}$, zatem $h(ax) = h(a)h(x) \in \mathcal{J}$, skąd $ax \in h^{-1}(\mathcal{J})$.

Ideał $h^{-1}(\mathcal{J})$ nazywa się *zwężeniem* ideału $\mathcal{J}$ pierścienia B w pierścieniu A (za pomocą homomorfizmu h) i oznacza się $\mathcal{J}^{\mathrm{c}}$ (od angielskiego *contraction*). Zauważmy, że jeśli A jest podpierścieniem B i $h : A \to B$ jest identycznościowym włożeniem A w B, to zwężenie ideału $\mathcal{J}$ pierścienia B w pierścieniu A jest równe $A \cap \mathcal{J}$.

Poniższe twierdzenie pokazuje, że operacja zwężania ideału zachowuje ideały pierwsze, a przy założeniu, że homomorfizm h jest epimorfizmem, także ideały maksymalne.

Twierdzenie **2.3.7.** *Niech $h : A \to B$ będzie homomorfizmem pierścieni.*
(a) *Jeśli $\mathfrak{p}'$ jest ideałem pierwszym w pierścieniu B, to $\mathfrak{p} = h^{-1}(\mathfrak{p}')$ jest ideałem pierwszym w pierścieniu A.*
(b) *Jeśli h jest epimorfizmem i $\mathfrak{m}'$ jest ideałem maksymalnym w pierścieniu B, to $\mathfrak{m} = h^{-1}(\mathfrak{m}')$ jest ideałem maksymalnym w pierścieniu A.*

Dowód. (a) Niech $\mathfrak{p} := h^{-1}(\mathfrak{p}')$ i niech $a, b \in A$, $ab \in \mathfrak{p}$, $a \notin \mathfrak{p}$. Wtedy $h(a) \notin \mathfrak{p}'$. Ale $h(a)h(b) = h(ab) \in \mathfrak{p}'$, zatem $h(b) \in \mathfrak{p}'$ oraz $b \in h^{-1}(\mathfrak{p}') = \mathfrak{p}$.
(b) wynika z twierdzenia 2.2.3 o odpowiedniości dla homomorfizmów pierścieni. □

2.3.3 Twierdzenie chińskie o resztach

Ideały $\mathfrak{a}$ oraz $\mathfrak{b}$ pierścienia A nazywamy *względnie pierwszymi* jeśli $\mathfrak{a} + \mathfrak{b} = A$. Motywację dla tej nazwy odnajdujemy w pierścieniu liczb całkowitych $\mathbb{Z}$. Ideały główne $\mathfrak{a} = a\mathbb{Z}$ i $\mathfrak{b} = b\mathbb{Z}$ są względnie pierwsze gdy $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$, a więc wtedy i tylko wtedy, gdy istnieją liczby całkowite x, y takie, że $ax + by = 1$. Wynika stąd, że ideały główne $a\mathbb{Z}$ i $b\mathbb{Z}$ są względnie pierwsze wtedy i tylko wtedy gdy ich generatory a i b są względnie pierwsze.
Następujące twierdzenie znane jest jako *twierdzenie chińskie o resztach*. Dla ideału $\mathfrak{a}$ pierścienia A i elementów $a, b \in A$ piszemy $a \equiv b \bmod \mathfrak{a}$ jeśli $a - b \in \mathfrak{a}$.

TWIERDZENIE **2.3.8.** *Niech $n \geqslant 2$. Jeśli $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ są ideałami pierścienia A oraz $\mathfrak{a}_i + \mathfrak{a}_j = A$ dla $i \neq j$, to dla każdych $x_1, \ldots, x_n \in A$ istnieje element $x \in A$ taki, że*

$$x \equiv x_i \bmod \mathfrak{a}_i, \quad i = 1, \ldots, n.$$

Dowód. Ponieważ $\mathfrak{a}_1 + \mathfrak{a}_j = A$ dla $j = 2, \ldots, n$, istnieją więc elementy $a_j \in \mathfrak{a}_1$ oraz $b_j \in \mathfrak{a}_j$ takie, że $a_j + b_j = 1$ dla $j = 2, \ldots, n$. Wtedy

$$1 = \prod_{j=2}^{n} (a_j + b_j) = a \ + \ b_2 \cdots b_n,$$

gdzie a jest sumą iloczynów, w których co najmniej jeden czynnik należy do ideału $\mathfrak{a}_1$. Zatem $a \in \mathfrak{a}_1$. Połóżmy $y_1 := b_2 \cdots b_n$. Wtedy wobec $a + y_1 = 1$ mamy

$$y_1 \equiv 1 \bmod \mathfrak{a}_1, \quad y_1 \equiv 0 \bmod \mathfrak{a}_j \ \text{ dla } \ j = 2, \ldots, n.$$

Podobnie dla każdego $i \leqslant n$ istnieje $y_i \in A$ taki, że

$$y_i \equiv 1 \bmod \mathfrak{a}_i, \quad y_i \equiv 0 \bmod \mathfrak{a}_j \ \text{ dla } \ j \neq i.$$

Stąd otrzymujemy

$$x := x_1 y_1 + \cdots + x_n y_n \equiv x_i y_i \equiv x_i \bmod \mathfrak{a}_i$$

dla $i = 1, \ldots, n$. □

WNIOSEK **2.3.9.** *Jeśli $\mathfrak{a}_i + \mathfrak{a}_j = A$ dla $i \neq j$, to*

$$A \Big/ \bigcap_{i=1}^{n} \mathfrak{a}_i \ \cong \ \prod_{i=1}^{n} A/\mathfrak{a}_i.$$

Dowód. Na podstawie chińskiego twierdzenia o resztach homomorfizm

$$h : A \to \prod_{i=1}^{n} A/\mathfrak{a}_i, \ \ h(a) = (a + \mathfrak{a}_1, \ldots, a + \mathfrak{a}_n)$$

jest epimorfizmem. Ponadto,

$$\ker h = \bigcap_{i=1}^{n} \mathfrak{a}_i.$$

Zatem rezultat wynika z twierdzenia 2.2.2 o faktoryzacji homomorfizmów pierścieni. □

Jako zastosowanie twierdzenia chińskiego o resztach wskażemy wzór dla wartości funkcji Eulera występującej w teorii liczb.
Funkcją Eulera nazywamy funkcję $\varphi : \mathbb{N} \to \mathbb{N}$ określoną następująco:

$$\varphi(n) := |U(\mathbb{Z}/n\mathbb{Z})|.$$

A więc $\varphi(n)$ jest liczbą elementów odwracalnych pierścienia reszt $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Jeśli $n = p$ jest liczbą pierwszą, to $\mathbb{Z}_p$ jest ciałem i wszystkie różne od zera elementy $\mathbb{Z}_p$ są odwracalne. Wobec tego

$$\varphi(p) = p - 1$$

dla każdej liczby pierwszej p. Ogólniej,

$$\varphi(p^m) = (p-1)p^{m-1}$$

dla każdej liczby pierwszej p i każdej liczby naturalnej m. Dla $a \in \mathbb{Z}$ mamy bowiem

$$\begin{aligned} a + p^m\mathbb{Z} \in U(\mathbb{Z}/p^m\mathbb{Z}) &\Leftrightarrow \exists\, y \in \mathbb{Z} \quad (a + p^m\mathbb{Z})(y + p^m\mathbb{Z}) = 1 + p^m\mathbb{Z} \\ &\Leftrightarrow \exists\, x, y \in \mathbb{Z} \quad ay + p^m x = 1 \\ &\Leftrightarrow p \nmid a. \end{aligned}$$

Zatem spośród elementów $a + p^m\mathbb{Z}$, $a = 1, 2, \ldots, p^m - 1$ te i tylko te są odwracalne, dla których $p \nmid a$. Ponieważ wśród liczb $1, 2, \ldots, p^m - 1$ jest $p^{m-1} - 1$ wielokrotności liczby p, więc

$$\varphi(p^m) = p^m - 1 - (p^{m-1} - 1) = p^m - p^{m-1} = (p-1)p^{m-1}.$$

Jeśli teraz n jest dowolną liczbą naturalną i $n = \prod p^\alpha$ jest rozkładem kanonicznym liczby n na iloczyn potęg liczb pierwszych, to ideały $p^\alpha\mathbb{Z}$ są parami względnie pierwsze i wobec tego $\bigcap p^\alpha\mathbb{Z} = n\mathbb{Z}$. Z wniosku 2.3.9 mamy izomorfizm pierścieni

$$\mathbb{Z}/n\mathbb{Z} \cong \prod \mathbb{Z}/p^\alpha\mathbb{Z}.$$

Ponieważ izomorficzne pierścienie mają izomorficzne grupy elementów odwracalnych, wynika stąd, że

$$\varphi(n) = \prod_{p|n} \varphi(p^\alpha) = \prod_{p|n} (p-1)p^{\alpha-1} = \prod_{p|n} p^\alpha \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

2.3.4 Elementy nilpotentne i dzielniki zera

Element x pierścienia A nazywa się elementem *nilpotentnym*, jeśli $x^n = 0$ dla pewnej liczby naturalnej n. Jeśli $x, y, z \in A$ oraz $x^n = 0$, $y^m = 0$ dla liczb naturalnych n, m, to łatwo sprawdzić, że wtedy także $(x \pm y)^{n+m} = 0$ oraz $(xz)^n = 0$. Wynika stąd, że zbiór $\mathsf{Nil}\, A$ wszystkich elementów nilpotentnych pierścienia A jest ideałem pierścienia A. Ten ideał nazywa się *nilradykałem* pierścienia A.

Jeśli $x \in \mathsf{Nil}\, A$ oraz $\mathfrak{p}$ jest dowolnym ideałem pierwszym pierścienia A, to $x \in \mathfrak{p}$. Rzeczywiście, jeśli $x^n = 0$ i $n > 1$, to $x^n = x \cdot x^{n-1} \in \mathfrak{p}$ pociąga, że $x \in \mathfrak{p}$ lub $x^{n-1} \in \mathfrak{p}$. A więc prosty argument indukcyjny pokazuje, że $x \in \mathfrak{p}$. Udowodniliśmy

zatem, że $\mathsf{Nil}\, A \subseteq \mathfrak{p}$ dla każdego ideału pierwszego $\mathfrak{p}$.

Zbiór wszystkich ideałów pierwszych pierścienia A nazywa się *spektrum pierwszym* pierścienia A i oznacza się $\mathsf{Spec}\, A$. Mamy więc

$$\mathsf{Nil}\, A \subseteq \bigcap\{\mathfrak{p} : \mathfrak{p} \in \mathsf{Spec}\, A\}.$$

TWIERDZENIE **2.3.10.** *Dla każdego pierścienia przemiennego A,*

$$\mathsf{Nil}\, A = \bigcap\{\mathfrak{p} : \mathfrak{p} \in \mathsf{Spec}\, A\}.$$

Dowód. Połóżmy $Y := \bigcap\{\mathfrak{p} : \mathfrak{p} \in \mathsf{Spec}\, A\}$. Zauważyliśmy już, że $\mathsf{Nil}\, A \subseteq Y$. Aby pokazać, że $\mathsf{Nil}\, A \supseteq Y$ wystarczy sprawdzić, że

$$x \notin \mathsf{Nil}\, A \quad \Rightarrow \quad x \notin Y. \tag{2.2}$$

W dowodzie tego faktu użyjemy lematu Kuratowskiego-Zorna.
A więc załóżmy, że $x \notin \mathsf{Nil}\, A$. Wtedy $x^n \neq 0$ dla każdej liczby naturalnej n. Rozpatrzmy rodzinę $\mathcal{F}$ wszystkich ideałów $\mathfrak{a}$ pierścienia A takich, że $x^n \notin \mathfrak{a}$ dla każdej liczby naturalnej n.
Rodzina $\mathcal{F}$ jest niepusta, gdyż ideał zerowy (0) należy do $\mathcal{F}$.
Jeśli $\mathcal{C} = \{\mathfrak{a}_j : j \in J\}$ jest łańcuchem w rodzinie $\mathcal{F}$, to łatwo sprawdzić, że łańcuch $\mathcal{C}$ jest ograniczony przez ideał $\mathfrak{a} = \bigcup\{\mathfrak{a}_j : j \in J\}$ oraz $\mathfrak{a} \in \mathcal{F}$.
Na podstawie lematu Kuratowskiego-Zorna rodzina $\mathcal{F}$ ma element maksymalny $\mathfrak{p}$.
Pokażemy, że $\mathfrak{p}$ jest ideałem pierwszym pierścienia A. Wykorzystamy definicję (2.1).
A więc niech $a, b \in A$ oraz $a \notin \mathfrak{p}$ i $b \notin \mathfrak{p}$. Wtedy suma ideałów $\mathfrak{p} + aA$ spełnia

$$\mathfrak{p} \subset \mathfrak{p} + aA \quad \text{i} \quad \mathfrak{p} \neq \mathfrak{p} + aA.$$

Podobnie ideał $\mathfrak{p} + bA$ spełnia

$$\mathfrak{p} \subset \mathfrak{p} + bA \quad \text{i} \quad \mathfrak{p} \neq \mathfrak{p} + bA.$$

Wobec maksymalności $\mathfrak{p}$ w $\mathcal{F}$, ideały $\mathfrak{p} + aA$ i $\mathfrak{p} + bA$ nie należą do $\mathcal{F}$. Istnieją więc liczby naturalne n i m takie, że

$$x^n \in \mathfrak{p} + aA \quad \text{i} \quad x^m \in \mathfrak{p} + bA.$$

Wynika stąd, że iloczyn $x^n \cdot x^m = x^{n+m}$ należy do iloczynu ideałów

$$(\mathfrak{p} + aA) \cdot (\mathfrak{p} + bA) = \mathfrak{p}^2 + aA \cdot \mathfrak{p} + bA \cdot \mathfrak{p} + abA.$$

Jednakże $\mathfrak{p}^2 + aA \cdot \mathfrak{p} + bA \cdot \mathfrak{p} \subseteq \mathfrak{p}$, zatem $x^{n+m} \in \mathfrak{p} + abA$.
Wobec tego ideał $\mathfrak{p} + abA$ nie należy do rodziny $\mathcal{F}$, zatem także $ab \notin \mathfrak{p}$ (gdyż w przeciwnym razie $\mathfrak{p} + abA = \mathfrak{p} \in \mathcal{F}$). Udowodniliśmy więc, że $\mathfrak{p}$ jest ideałem pierwszym.

Ideał pierwszy $\mathfrak{p}$ ma zatem następującą własność: $x^n \notin \mathfrak{p}$ dla każdej liczby naturalnej n. W szczególności, $x \notin \mathfrak{p}$, co pokazuje, że $x \notin Y$. Dowodzi to (2.2). □

Okazuje się, że także zbiór $\mathsf{Dz}(A)$ wszystkich dzielników zera pierścienia A można opisać przy pomocy ideałów pierwszych pierścienia A.

TWIERDZENIE **2.3.11.** *Niech A będzie dowolnym pierścieniem przemiennym.*
(a) *Dla każdego $x \in \mathsf{Dz}(A)$ istnieje ideał pierwszy $\mathfrak{p}$ pierścienia A taki, że*

$$x \in \mathfrak{p} \quad \text{oraz} \quad \mathfrak{p} \subseteq \mathsf{Dz}(A).$$

(b) *Istnieje rodzina $\{\mathfrak{p}_j : j \in J\}$ ideałów pierwszych pierścienia A taka, że*

$$\mathsf{Dz}(A) = \bigcup\{\mathfrak{p}_j : j \in J\}.$$

Dowód. (b) wynika łatwo z (a), zatem udowodnimy tylko część (a). Niech x będzie dzielnikiem zera w A. Rozpatrzmy rodzinę $\mathcal{F}$ wszystkich ideałów $\mathfrak{a}$ pierścienia A o następującej własności:

$$x \in \mathfrak{a} \quad \text{i} \quad \mathfrak{a} \subseteq \mathsf{Dz}(A).$$

Rodzina $\mathcal{F}$ jest niepusta gdyż ideał główny xA należy do $\mathcal{F}$. Łatwo stwierdzić, że suma mnogościowa wszystkich ideałów dowolnego łańcucha zawartego w $\mathcal{F}$ jest ideałem należącym do $\mathcal{F}$. Zatem każdy łańcuch w $\mathcal{F}$ jest ograniczony z góry przez pewien element rodziny $\mathcal{F}$. Na podstawie lematu Kuratowskiego-Zorna istnieje element maksymalny $\mathfrak{p}$ rodziny $\mathcal{F}$. Dla dowodu (a) wystarcza pokazać, że $\mathfrak{p}$ jest ideałem pierwszym w A.
Niech więc $a, b \in A$ i załóżmy, że $ab \in \mathfrak{p}$ oraz $a \notin \mathfrak{p}, b \notin \mathfrak{p}$. Ideały $\mathfrak{p} + aA$ i $\mathfrak{p} + bA$ zawierają $\mathfrak{p}$ ale nie są równe $\mathfrak{p}$, zatem nie należą one do rodziny $\mathcal{F}$. Istnieją więc $y, z \in A$ z których żaden nie jest dzielnikiem zera w A takie, że $y \in \mathfrak{p} + aA$ i $z \in \mathfrak{p} + bA$. Zauważmy, że $yz \notin \mathsf{Dz}(A)$ (ponieważ y i z nie są dzielnikami zera) oraz $\mathfrak{p} \subseteq \mathsf{Dz}(A)$ (ponieważ $\mathfrak{p} \in \mathcal{F}$). Wynika stąd, że $yz \notin \mathfrak{p}$. Z drugiej strony mamy

$$yz \in (\mathfrak{p} + aA) \cdot (\mathfrak{p} + bA) = \mathfrak{p}^2 + aA \cdot \mathfrak{p} + bA \cdot \mathfrak{p} + abA \subseteq \mathfrak{p} + abA = \mathfrak{p},$$

sprzeczność. A więc $\mathfrak{p}$ jest ideałem pierwszym. □

2.4 Pierścienie ułamków i lokalizacja

Podobnie jak w §2.3 rozpatrujemy tutaj tylko pierścienie przemienne. Słowo *pierścień* oznacza więc *pierścień przemienny.*

DEFINICJA **2.4.1.** *Zbiorem multyplikatywnym S* w pierścieniu A nazywamy podzbiór S pierścienia A spełniający dwa następujące warunki:
(a) $1 \in S$ i $0 \notin S$.
(b) $x, y \in S \Rightarrow xy \in S$.

Następujące przykłady przedstawiają kilka typowych zbiorów multyplikatywnych w dowolnym pierścieniu A.

Przykład 2.4.1. $S = U(A)$, grupa elementów odwracalnych pierścienia, jest zbiorem multyplikatywnym w A.

Przykład 2.4.2. Jeśli A jest pierścieniem bez dzielników zera, to $S = A \setminus \{0\}$ jest zbiorem multyplikatywnym w A. Ogólniej, jeśli $\mathfrak{p}$ jest ideałem pierwszym dowolnego pierścienia A, to $S = A \setminus \mathfrak{p}$ jest zbiorem multyplikatywnym w A. Wynika to bezpośrednio z definicji ideału pierwszego (zobacz (2.1)).

Przykład 2.4.3. Niech A będzie dowolnym pierścieniem i niech $\mathsf{Dz}(A)$ oznacza zbiór dzielników zera pierścienia A. Wtedy $S = A \setminus \mathsf{Dz}(A)$ jest zbiorem multyplikatywnym w pierścieniu A.

Przykład 2.4.4. Niech $\mathfrak{a}$ będzie ideałem w pierścieniu A, $\mathfrak{a} \neq A$. Wtedy

$$1 + \mathfrak{a} = \left\{1 + a \in A : a \in \mathfrak{a}\right\}$$

jest zbiorem multyplikatywnym w A.

Zbiory multyplikatywne pojawiają się także gdy badamy podpierścienie niektórych ciał, na przykład ciała $\mathbb{Q}$ liczb wymiernych. Dla podpierścienia B ciała $\mathbb{Q}$ oznaczmy przez S zbiór tych liczb całkowitych, które są mianownikami liczb wymiernych należących do B. Oczywiście $1 \in S$ (gdyż $1 = 1/1 \in B$), jeśli zaś $x, y \in S$ oraz $a/x, b/y \in B$, gdzie a, b są liczbami całkowitymi, to zarówno suma jak i iloczyn liczb a/x oraz b/y ma mianownik xy, zatem $xy \in S$. A więc zbiór S jest zbiorem multyplikatywnym w pierścieniu $\mathbb{Z}$ liczb całkowitych.
Łatwo zauważyć, że także na odwrót, jeśli S jest jakimkolwiek zbiorem multyplikatywnym w $\mathbb{Z}$, to zbiór B wszystkich liczb wymiernych (czyli "ułamków") o mianownikach ze zbioru S tworzy podpierścień ciała liczb wymiernych.
Pokażemy, że ten oczywisty fakt jest szczególnym przypadkiem znacznie ogólniejszej konstrukcji. Okazuje się bowiem, że dla dowolnego pierścienia (przemiennego) A i dla dowolnego zbioru multyplikatywnego S można skonstruować pierścień B "ułamków" a/s, gdzie $a \in A$ i $s \in S$, to znaczy pierścień ułamków o mianownikach ze zbioru multyplikatywnego S i licznikach z danego pierścienia A.
W tej ogólnej sytuacji nie możemy jednak oczekiwać, że pierścień B będzie można zidentyfikować jako podpierścień pewnego ciała, gdyż pierścień A zawiera się oczywiście w B, natomiast może się nie zawierać w żadnym ciele K (gdy, na przykład, A ma dzielniki zera). Tak więc pierścień "ułamków" B należy skonstruować posługując się tylko danym pierścieniem A i jego zbiorem multyplikatywnym S.

2.4.1 Konstrukcja

Niech A będzie dowolnym pierścieniem (przemiennym) i niech S będzie zbiorem multyplikatywnym w A. Na zbiorze $A \times S$ definiujemy relację $\sim$ określoną następująco:

$$(a_1, s_1) \sim (a_2, s_2) \quad \Leftrightarrow \quad \exists s \in S \quad s(s_2 a_1 - s_1 a_2) = 0.$$

Pozostawiamy Czytelnikowi do sprawdzenia, że relacja $\sim$ jest relacją równoważnościową na zbiorze $A \times S$.
Klasę abstrakcji $[(a, s)]_\sim$ oznacza się a/s lub $\frac{a}{s}$ i nazywa się *ułamkiem* o liczniku a i mianowniku s. Na podstawie definicji relacji $\sim$ mamy następującą charakteryzację równości ułamków:

$$\frac{a_1}{s_1} = \frac{a_2}{s_2} \quad \Leftrightarrow \quad \exists s \in S \quad s(s_2 a_1 - s_1 a_2) = 0.$$

Gdy pierścień A jest pierścieniem całkowitym, to równość ułamków ma jeszcze prostszy opis:

$$\frac{a_1}{s_1} = \frac{a_2}{s_2} \quad \Leftrightarrow \quad s_2 a_1 - s_1 a_2 = 0.$$

Zbiór wszystkich klas abstrakcji relacji $\sim$ czyli zbiór wszystkich ułamków o licznikach z A i mianownikach z S oznaczamy $S^{-1}A$. A więc

$$S^{-1}A = \left\{ \frac{a}{s} : a \in A,\ s \in S \right\}.$$

Definiujemy teraz dodawanie i mnożenie ułamków kładąc

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{s_2a_1 + s_1a_2}{s_1s_2}, \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}.$$

Można pokazać, że te definicje nie zależą od wyboru par reprezentujących poszczególne ułamki. Pozostawiamy to jako ćwiczenie dla Czytelnika.

TWIERDZENIE **2.4.2.**
Niech S będzie zbiorem multyplikatywnym w pierścieniu A. Wtedy:
(a) *System* $\left(S^{-1}A,\ +\ ,\ \cdot\ ,\ \frac{0}{1},\ \frac{1}{1}\right)$ *jest pierścieniem.*
(b) *Odwzorowanie*

$$\varphi_S : A \to S^{-1}A, \quad \varphi_S(a) = \frac{a}{1}$$

jest homomorfizmem pierścieni.
(c) *Dla każdego $s \in S$ element $\varphi_S(s)$ jest odwracalny w pierścieniu $S^{-1}A$.*

Dowód. (a) i (b) sprawdza się bezpośrednim rachunkiem. Co do (c), elementem odwrotnym do $s/1 = \varphi_S(s)$ jest $1/s$. □

Zauważmy, że zgodnie z określeniem równości ułamków, mamy $0/1 \neq 1/1$, gdyż w przeciwnym razie mielibyśmy dla pewnego $s \in S$ równość $s(0 \cdot 1 - 1 \cdot 1) = 0$, skąd $0 = s \in S$, sprzeczność. Założenie w definicji zbioru multyplikatywnego, że $0 \notin S$ gwarantuje więc, że pierścień $S^{-1}A$ jest pierścieniem niezerowym. Można także zauważyć, że dla $a \in A$ mamy $a \in \ker \varphi_S$ wtedy i tylko wtedy gdy istnieje element $s \in S$ taki, że $as = 0$. Stąd wynika, że jeśli A jest pierścieniem całkowitym, to dla każdego zbioru multyplikatywnego S w A homomorfizm φ_S jest injektywny.

DEFINICJA **2.4.3.** $S^{-1}A$ nazywa się *pierścieniem ułamków* pierścienia A względem zbioru multyplikatywnego S.

Przykład 2.4.5. Jeśli zbiorem multyplikatywnym S pierścienia A jest grupa elementów odwracalnych pierścienia, $S = U(A)$, to mamy następujący opis równości ułamków w $S^{-1}A$:

$$\frac{a_1}{s_1} = \frac{a_2}{s_2} \ \Leftrightarrow\ s_2a_1 = s_1a_2 \ \Leftrightarrow\ s_1^{-1}a_1 = s_2^{-1}a_2.$$

Zatem $a/1 = 0/1$ wtedy i tylko wtedy gdy $a = 0$. Homomorfizm $\varphi_S : A \to S^{-1}A$, $\varphi_S(a) = a/1$ ma więc jądro zerowe, jest zatem monomorfizmem. Ponadto,

$$\frac{a}{s} = \frac{s^{-1}a}{1} = \varphi_S(s^{-1}a)$$

dla każdych $a \in A,\ s \in S$. Zatem homomorfizm φ_S jest także epimorfizmem i wobec tego φ_S jest izomorfizmem pierścieni. A więc konstrukcja pierścienia ułamków pierścienia A względem zbioru multyplikatywnego S złożonego z wszystkich elementów odwracalnych pierścienia A daje pierścień izomorficzny z A.

Przykład 2.4.6. W pierścieniu A bez dzielników zera (czyli w pierścieniu całkowitym) weźmy zbiór multyplikatywny $S = A \setminus \{0\}$. Wtedy

$$S^{-1}A = \left\{ \frac{a}{b} : a, b \in A,\ b \neq 0 \right\}$$

i każdy niezerowy element pierścienia $S^{-1}A$ jest odwracalny. Jeśli bowiem $a/b \neq 0/1$, to $a \neq 0$, zatem $b/a \in S^{-1}A$ oraz $a/b \cdot b/a = 1/1$. A więc $S^{-1}A$ jest ciałem. Ciało $S^{-1}A$ nazywa się *ciałem ułamków* pierścienia całkowitego A. Homomorfizm $\varphi_S : A \to S^{-1}A$ jest w tym przypadku monomorfizmem (gdyż $a/1 = 0/1$ wtedy i tylko wtedy gdy $a = 0$) i ułamki o mianowniku 1 można utożsamić z ich licznikami. W ten sposób pierścień A staje się podpierścieniem swojego ciała ułamków $S^{-1}A$.
Przykład ten pokazuje, że każdy pierścień całkowity jest podpierścieniem pewnego ciała. Klasycznymi przykładami ciał ułamków pierścieni całkowitych są ciało $\mathbb{Q}$ liczb wymiernych (ciało ułamków pierścienia $\mathbb{Z}$ liczb całkowitych) i ciało funkcji wymiernych $K(X)$ o współczynnikach z ciała K (ciało ułamków pierścienia wielomianów $K[X]$).

Przykład 2.4.7. Jak wiemy, jeśli $\mathfrak{p}$ jest ideałem pierwszym pierścienia A, to $S = A \setminus \mathfrak{p}$ jest zbiorem multyplikatywnym w A. Pierścień ułamków względem tego zbioru multyplikatywnego nazywa się *lokalizacją pierścienia* A ze względu na ideał pierwszy $\mathfrak{p}$ i oznacza $A_{\mathfrak{p}}$. A więc

$$S^{-1}A = A_{\mathfrak{p}} = \left\{ \frac{a}{s} : a \in A,\ s \in A \setminus \mathfrak{p} \right\}$$

Zbiór

$$S^{-1}\mathfrak{p} := \left\{ \frac{a}{s} : a \in \mathfrak{p},\ s \in A \setminus \mathfrak{p} \right\}$$

jest ideałem w pierścieniu $A_{\mathfrak{p}}$. Każdy ułamek, który nie należy do $S^{-1}\mathfrak{p}$ ma postać a/s, gdzie $a, s \in A \setminus \mathfrak{p}$. A więc każdy taki ułamek jest elementem odwracalnym w pierścieniu $A_{\mathfrak{p}}$. Poza ideałem $S^{-1}\mathfrak{p}$ są więc tylko elementy odwracalne. Wynika stąd, że $S^{-1}\mathfrak{p}$ jest *ideałem maksymalnym* w pierścieniu $A_{\mathfrak{p}}$, a także, że $S^{-1}\mathfrak{p}$ zawiera wszystkie ideały właściwe pierścienia $A_{\mathfrak{p}}$. W szczególności, $S^{-1}\mathfrak{p}$ jest jedynym ideałem maksymalnym pierścienia $A_{\mathfrak{p}}$.
Pierścień mający tylko jeden ideał maksymalny nazywa się pierścieniem *lokalnym*.
Pierścień $A_{\mathfrak{p}}$, będący lokalizacją pierścienia A względem ideału pierwszego $\mathfrak{p}$, jest więc pierścieniem lokalnym.

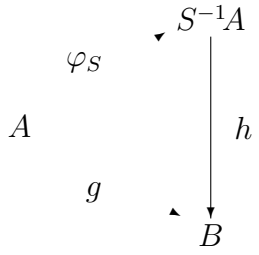
Przykład 2.4.8. Wśród typowych pierścieni ułamków są jeszcze następujące trzy przykłady.
(a) Jeśli $\mathfrak{a}$ jest dowolnym ideałem w pierścieniu A, to $1 + \mathfrak{a}$ jest zbiorem multyplikatywnym w A. Można więc rozpatrywać pierścień $(1 + \mathfrak{a})^{-1}A$.
(b) Jeśli $s \in A$ oraz s nie jest elementem nilpotentnym w A, to zbiór $S = \left\{ s^n : n \in \mathbb{N} \cup \{0\} \right\}$ wszystkich nieujemnych potęg elementu s jest zbiorem multyplikatywnym w A. Pierścień ułamków $S^{-1}A$ jest więc zbiorem ułamków postaci a/s^n, gdzie $a \in A$ oraz $n \in \mathbb{N} \cup \{0\}$.
Na przykład, jeśli p jest liczbą pierwszą i $S = \left\{ p^n : n \in \mathbb{N} \cup \{0\} \right\}$, to $S^{-1}\mathbb{Z}$ jest

pierścieniem złożonym z wszystkich liczb wymiernych, których mianowniki są potęgami liczby pierwszej p. Natomiast lokalizacja $\mathbb{Z}_{\mathfrak{p}}$ pierścienia liczb całkowitych $\mathbb{Z}$ względem ideału pierwszego $\mathfrak{p} = p\mathbb{Z}$ jest podpierścieniem ciała $\mathbb{Q}$ liczb wymiernych złożonym z liczb wymiernych m/n, gdzie $m, n \in \mathbb{Z}$ oraz liczba n nie jest podzielna przez p.
(c) Dla zbioru $\mathsf{Dz}(A)$ dzielników zera pierścienia A zbiór $S = A \setminus \mathsf{Dz}(A)$ jest zbiorem multyplikatywnym w pierścieniu A i pierścień ułamków $S^{-1}A$ pierścienia A względem S nazywa się *pełnym pierścieniem ułamków* pierścienia A. Jeśli A jest pierścieniem całkowitym, to jego pełny pierścień ułamków jest jego ciałem ułamków.

2.4.2 Własność uniwersalna

Dla dowolnego pierścienia ułamków $S^{-1}A$ zauważyliśmy już, że dla każdego elementu s zbioru multyplikatywnego S element $\varphi_S(s) = s/1$ jest elementem odwracalnym pierścienia ułamków $S^{-1}A$ (elementem odwrotnym do $s/1$ jest $1/s$). A więc obrazy elementów zbioru multyplikatywnego S stają się elementami odwracalnymi w pierścieniu ułamków $S^{-1}A$. Ta własność prowadzi do następującej charakteryzacji pierścienia ułamków.

Twierdzenie **2.4.4.** *Niech S będzie zbiorem multyplikatywnym w pierścieniu A. Dla każdego homomorfizmu pierścieni $g : A \to B$ takiego, że $g(s)$ jest odwracalny w B dla każdego $s \in S$, istnieje dokładnie jeden homomorfizm pierścieni $h : S^{-1}A \to B$, dla którego następujący diagram jest przemienny:*



Dowód. Pokażemy najpierw, że dla dowolnego homomorfizmu $g : A \to B$ takiego, że $g(s)$ jest odwracalny w B dla każdego $s \in S$, istnieje co najwyżej jeden homomorfizm $h : S^{-1}A \to B$ taki, że $h \circ \varphi_S = g$. Jeśli h spełnia ten warunek, to dla każdego $a \in A$ mamy

$$h\Big(\frac{a}{1}\Big) = h(\varphi_S(a)) = (h \circ \varphi_S)(a) = g(a).$$

W szczególności więc dla każdego $s \in S$ element $h(s/1) = g(s)$ jest odwracalny w B i wobec tego

$$g(s)^{-1} = h\Big(\frac{s}{1}\Big)^{-1} = h\Big(\frac{1}{s}\Big).$$

Zatem dla dowolnych $a \in A,\ s \in S$ mamy

$$h\Big(\frac{a}{s}\Big) = h\Big(\frac{a}{1} \cdot \frac{1}{s}\Big) = h\Big(\frac{a}{1}\Big) \cdot h\Big(\frac{1}{s}\Big) = g(a) \cdot g(s)^{-1}.$$

Jeśli więc homomorfizm h istnieje, jest jednoznacznie określony na elementach pierścienia $S^{-1}A$.

Udowodnimy teraz istnienie homomorfizmu h. Wiemy już, że dla dowolnego homomorfizmu $g : A \to B$ takiego, że $g(s)$ jest odwracalny w B dla każdego $s \in S$, odwzorowanie h musi być określone następująco:

$$h\left(\frac{a}{s}\right) = g(a) \cdot g(s)^{-1}.$$

Sprawdzimy, że $h(a/s)$ nie zależy od przedstawienia a/s w postaci ułamka. Mamy bowiem

$$a/s = a_1/s_1 \;\Rightarrow\; \exists s_2 \in S \;\; s_2 s_1 a = s_2 s a_1 \;\Rightarrow\; g(s_2)g(s_1)g(a) = g(s_2)g(s)g(a_1),$$

skąd wobec odwracalności elementów $g(s), g(s_1), g(s_2)$ mamy

$$g(a)g(s)^{-1} = g(a_1)g(s_1)^{-1}.$$

Sprawdzenie, że h jest homomorfizmem pierścieni takim, że $h \circ \varphi_S = g$, pozostawiamy Czytelnikowi. □

2.4.3 Ideały pierścienia ułamków

Główne zastosowania pierścieni ułamków w teorii pierścieni bazują na następującym twierdzeniu ustalającym związek pomiędzy ideałami pierścienia A i jego pierścienia ułamków $S^{-1}A$.

Twierdzenie **2.4.5.** *Niech S będzie zbiorem multyplikatywnym w pierścieniu A. Niech $\varphi = \varphi_S$ będzie homomorfizmem $\varphi : A \to S^{-1}A, \quad \varphi(a) = \frac{a}{1}$.*

(a) *Każdy ideał $\mathfrak{A}$ pierścienia $S^{-1}A$ jest rozszerzeniem pewnego ideału $\mathfrak{a}$ pierścienia A za pomocą homomorfizmu φ, to znaczy, $\mathfrak{A} = \varphi(\mathfrak{a})S^{-1}A$.*
(b) *Każdy ideał pierwszy $\mathfrak{P}$ pierścienia $S^{-1}A$ jest rozszerzeniem pewnego ideału pierwszego $\mathfrak{p}$ pierścienia A rozłącznego ze zbiorem S, to znaczy*

$$\mathfrak{P} = \varphi(\mathfrak{p})S^{-1}A, \qquad \mathfrak{p} \cap S = \emptyset.$$

(c) *Dla każdego ideału pierwszego $\mathfrak{p}$ pierścienia A rozłącznego ze zbiorem S rozszerzenie $\varphi(\mathfrak{p})S^{-1}A$ jest ideałem pierwszym pierścienia $S^{-1}A$.*

Dowód. (a) Niech $\mathfrak{A}$ będzie dowolnym ideałem pierścienia $S^{-1}A$ i niech $\mathfrak{a} = \varphi^{-1}(\mathfrak{A})$ będzie zwężeniem ideału $\mathfrak{A}$ w pierścieniu A za pomocą homomorfizmu φ. Jak wiemy, $\mathfrak{a}$ jest ideałem w A. Ponadto $\varphi(\mathfrak{a}) \subseteq \mathfrak{A}$, więc także $\varphi(\mathfrak{a})S^{-1}A \subseteq \mathfrak{A}$. Z drugiej strony, jeśli $x = \frac{a}{s} \in \mathfrak{A}$, gdzie $a \in A$, $s \in S$, to $x = (a/1)/(s/1) = \varphi(a)/\varphi(s)$, zatem $\varphi(a) = \varphi(s)x \in \mathfrak{A}$. Wobec tego $a \in \mathfrak{a}$ oraz

$$x = \tfrac{a}{s} = \varphi(a) \cdot \tfrac{1}{s} \in \varphi(\mathfrak{a})S^{-1}A.$$

A więc $\mathfrak{A} \subseteq \varphi(\mathfrak{a})S^{-1}A$.
(b) Niech $\mathfrak{P}$ będzie ideałem pierwszym w $S^{-1}A$. Na podstawie (a), $\mathfrak{P}$ jest rozszerzeniem pewnego ideału $\mathfrak{p}$ pierścienia A i na podstawie twierdzenia 2.3.7 (a), $\mathfrak{p}$ jest ideałem pierwszym w A. Ponadto, $\mathfrak{P}$ jest ideałem właściwym, nie zawiera zatem elementów odwracalnych pierścienia $S^{-1}A$, w szczególności więc jest rozłączny ze

zbiorem $\varphi(S)$. Stąd wynika, że $\mathfrak{p}$ jest rozłączny ze zbiorem S.
(c) Niech $\mathfrak{p}$ będzie ideałem pierwszym w A rozłącznym z S i niech $\mathfrak{P} = \varphi(\mathfrak{p})S^{-1}A$ będzie jego rozszerzeniem w $S^{-1}A$. Pokażemy, że $\mathfrak{P}$ jest ideałem pierwszym. Weźmy więc dwa ułamki $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$, gdzie $s, t \in S$ i przypuśćmy, że $\frac{a}{s}\frac{b}{t} \in \mathfrak{P}$. Istnieją więc elementy $p_i \in \mathfrak{p}$, $c_i \in A$, $r_i \in S$ takie, że

$$\frac{a}{s}\frac{b}{t} = \sum_i \frac{p_i}{1}\frac{c_i}{r_i}.$$

Sumę po prawej stronie tej równości można zapisać w postaci $\frac{p}{r}$, gdzie $r = \prod_i r_i \in S$ oraz p jest pewnym elementem ideału $\mathfrak{p}$. Zatem istnieje element $u \in S$ taki, że

$$u(rab - pst) = 0.$$

Tak więc $u(rab - pst) \in \mathfrak{p}$, a ponieważ $\mathfrak{p} \cap S = \emptyset$, wnioskujemy, że $rab - pst \in \mathfrak{p}$. Stąd wobec $p \in \mathfrak{p}$ mamy $rab \in \mathfrak{p}$ i wobec $r \notin \mathfrak{p}$ otrzymujemy $ab \in \mathfrak{p}$. Ponieważ $\mathfrak{p}$ jest ideałem pierwszym, otrzymujemy $a \in \mathfrak{p}$ lub $b \in \mathfrak{p}$ a to oznacza, że

$$\frac{a}{s} = \varphi(a)\frac{1}{s} \in \mathfrak{P} \quad \text{lub} \quad \frac{b}{t} = \varphi(b)\frac{1}{t} \in \mathfrak{P}.$$

Zatem $\mathfrak{P}$ jest ideałem pierwszym jeśli tylko $\mathfrak{P} \neq S^{-1}A$. Gdyby $1 \in \mathfrak{P}$, to mielibyśmy równość

$$\frac{1}{1} = \frac{p}{r}$$

dla pewnych $p \in \mathfrak{p}$, $r \in S$. Stąd wynika, że istnieje element $u \in S$ taki, że $u(r - p) = 0$ i podobnie jak wyżej wnioskujemy stąd, że $r \in \mathfrak{p}$, co jest niemożliwe wobec rozłączności S i $\mathfrak{p}$.
A więc $\mathfrak{P} = \varphi(\mathfrak{p})S^{-1}A$ jest ideałem pierwszym w $S^{-1}A$. □

2.5 Zadania

1. Niech A będzie pierścieniem przemiennym, który ma tylko skończoną liczbę n dzielników zera. Udowodnić, że A jest pierścieniem skończonym i ma co najwyżej $(n+1)^2$ elementów.

Wskazówka. Niech $0 \neq a \in A$ będzie dzielnikiem zera i niech J będzie anihilatorem elementu a. Udowodnić, że $|J| \leqslant n+1$ oraz $|A/J| \leqslant n+1$.

2. Niech R będzie pierścieniem (niekoniecznie przemiennym), w którym każda podgrupa addytywnej grupy pierścienia jest ideałem pierścienia R. Udowodnić, że pierścień R jest izomorficzny bądź z pierścieniem liczb całkowitych $\mathbb{Z}$ bądź z pewnym pierścieniem reszt $\mathbb{Z}/n\mathbb{Z}$, gdzie $n \in \mathbb{N}$.

3. Niech $f \in \mathbb{Z}[X]$. Skończony ciąg różnych liczb całkowitych $x_0, x_1, \ldots, x_{k-1}$ nazywamy $f-$cyklem o długości k, jeśli $f(x_0) = x_1, \quad f(x_1) = x_2, \quad \ldots, \quad f(x_{k-1}) = x_0$.
(a) Wskazać wielomiany f i g takie, że f ma cykl długości 1 i g ma cykl długości 2.
(b) Udowodnić, że wielomian $f \in \mathbb{Z}[X]$ nie może mieć cyklu o długości $\geqslant 3$.

4. Niech $f \in \mathbb{Q}[X]$. Udowodnić, że jeśli $f(\mathbb{Q}) = \mathbb{Q}$, to f jest wielomianem liniowym: $f = aX + b$, $a, b \in \mathbb{Q}$, $a \neq 0$.

5. Udowodnić, że dla każdej liczby naturalnej n wielomian $X^n + X + 3$ jest nierozkładalny w pierścieniu $\mathbb{Q}[X]$.

6. Niech $f, g \in \mathbb{Z}[X]$ i niech f będzie wielomianem unormowanym (najwyższy współczynnik równy 1). Udowodnić, że jeśli $f(n)$ dzieli $g(n)$ dla nieskończenie wielu liczb naturalnych n, to f dzieli g w $\mathbb{Z}[X]$.

7. Udowodnić, że nie istnieje homomorfizm pierścienia $\mathbb{Z}[\sqrt{2}\,]$ na pierścień $\mathbb{Z}[\sqrt{3}\,]$. Czy istnieje homomorfizm pierścienia wielomianów $\mathbb{Q}[X]$ na pierścień $\mathbb{Z}[X]$?

8. Znaleźć wszystkie ideały maksymalne pierścienia funkcji rzeczywistych ciągłych na odcinku $[0, 1]$.

9. Niech A będzie pierścieniem przemiennym i niech $\mathfrak{a}, \mathfrak{b}$ będą ideałami w A.

(a) Udowodnić, że jeśli $\mathfrak{a} \cdot \mathfrak{b} = A$, to $\mathfrak{a} = \mathfrak{b} = A$.
(b) Dla $A = \mathbb{Z}[\sqrt{-5}\,]$ i $\mathfrak{a} = (2, 1+\sqrt{-5})$ znaleźć ideał $\mathfrak{b}$ w A taki, że $\mathfrak{a}\cdot\mathfrak{b}$ jest ideałem głównym.
(c) Dla $A = \mathbb{Z}[fi]$, gdzie $f > 1$ jest liczbą naturalną oraz $i^2 = -1$, i dla $\mathfrak{a} = f\mathbb{Z}[i]$, sprawdzić, że $\mathfrak{a}$ jest ideałem w A i nie istnieje niezerowy ideał $\mathfrak{b}$ w A taki, że $\mathfrak{a} \cdot \mathfrak{b}$ jest ideałem głównym.

10. Niech S będzie podzbiorem multyplikatywnym pierścienia przemiennego A.
(a) Udowodnić, że w zbiorze ideałów pierścienia A rozłącznych ze zbiorem S istnieje element maksymalny $\mathfrak{p}$.
(b) Udowodnić, że $\mathfrak{p}$ jest ideałem pierwszym.

11. Niech A będzie pierścieniem przemiennym i niech Σ będzie zbiorem wszystkich podzbiorów multyplikatywnych $S \subset A$.
(a) Zauważyć, że Σ jest zbiorem częściowo uporządkowanym przez relację inkluzji. Udowodnić, że w Σ istnieje element maksymalny.
(b) Udowodnić, że zbiór $S \in \Sigma$ jest elementem maksymalnym w Σ wtedy i tylko wtedy, gdy $A\backslash S$ jest minimalnym ideałem pierwszym pierścienia A.

12. Niech K będzie ciałem i niech $A = K[X]/(X^m)$. Udowodnić, że A jest pierścieniem lokalnym i jego jedyny ideał maksymalny jest ideałem głównym.

13. Udowodnić, że pierścień przemienny A jest pierścieniem lokalnym wtedy i tylko wtedy gdy dla dowolnych $a, b \in A$ z tego, że $a + b = 1$ wynika, że a jest elementem odwracalnym lub b jest elementem odwracalnym.

Rozdział 3

Moduły

Ostatnie zmiany 1.12.2008 r.

3.1 Definicje i przykłady

W tym rozdziale R będzie dowolnym (a więc niekoniecznie przemiennym) pierścieniem. Będziemy rozpatrywać uogólnienie pojęcia przestrzeni wektorowej nad ciałem K, w którym rolę ciała K przejmie pierścień R.

Niech M będzie addytywną grupą abelową. Grupę abelową M nazywamy $R-$*modułem*, jeśli na grupie M określone jest *działanie zewnętrzne* z pierścieniem skalarów R :

$$R \times M \to M, \quad (a, m) \mapsto am$$

i działanie to ma następujące własności:

$$\begin{aligned} a(m_1 + m_2) &= am_1 + am_2 && (3.1)\\ (a_1 + a_2)m &= a_1m + a_2m && (3.2)\\ (a_1a_2)m &= a_1(a_2m) && (3.3)\\ 1m &= m && (3.4) \end{aligned}$$

dla wszystkich $a, a_1, a_2 \in R,\ m_1, m_2, m \in M$.
Działanie zewnętrzne $R \times M \to M,\ (a, m) \mapsto am$ nazywamy także *mnożeniem* elementów grupy abelowej M przez elementy pierścienia R.
Tak więc grupa abelowa M jest $R-$modułem wtedy i tylko wtedy, gdy na M jest określone mnożenie elementów grupy M przez elementy pierścienia R spełniające warunki (3.1)–(3.4).

Zauważmy, że jeśli M jest $R-$modułem, to działanie zewnętrzne na M ma także następujące własności: dla dowolnych $a, b \in R$ oraz $m \in M$,

$$0m = 0, \quad (-1)m = -m, \quad (a - b)m = am - bm.$$

Mamy bowiem $(a - b)m + bm = (a - b + b)m = am$, skąd wynika, że $(a - b)m$ jest różnicą elementów am i bm w grupie M. Kładąc $a = b = 1$ otrzymujemy $0m = (1 - 1)m = 1m - 1m = m - m = 0$, natomiast kładąc $a = 0, b = 1$ otrzymujemy $(-1)m = (0 - 1)m = 0m - 1m = 0 - m = -m$.

Istnieje także inne podejście do definicji $R-$modułu, nie odwołujące się do najprostszej definicji przestrzeni wektorowej. Przypomnijmy, że dla dowolnej grupy abelowej

M zbiór $\mathsf{End}\, M$ wszystkich endomorfizmów grupy M jest pierścieniem (zob. przykład 2.1.5).

DEFINICJA **3.1.1.** Niech M będzie addytywną grupą abelową i niech R będzie pierścieniem. Parę (M, φ), gdzie $\varphi : R \to \mathsf{End}\, M$ jest homomorfizmem pierścienia R w pierścień endomorfizmów $\mathsf{End}\, M$ grupy abelowej M, nazywamy $R-$modułem.

Jeśli (M, φ) jest $R-$modułem w sensie tej definicji, to dla każdego $a \in R$ obraz $\varphi(a)$ elementu a jest endomorfizmem grupy abelowej M. Dla $m \in M$ element $\varphi(a)(m)$ oznacza się po prostu am, natomiast $R-$moduł (M, φ) oznacza się krótko M.

Jeśli więc (M, φ) jest $R-$modułem, to na grupie abelowej M określone jest *działanie zewnętrzne* z pierścieniem skalarów R :

$$R \times M \to M, \quad (a, m) \mapsto \varphi(a)(m) = am.$$

To działanie zewnętrzne na M ma własności (3.1) – (3.4). Pierwsza z tych równości wynika z faktu, że $\varphi(a)$ jest endomorfizmem grupy M, natomiast trzy pozostałe wynikają z tego, że φ jest homomorfizmem pierścieni.
Interpretacja homomorfizmu $\varphi : R \to \mathsf{End}\, M$ jako mnożenia elementów grupy M przez elementy pierścienia R prowadzi więc do definicji $R-$modułu jako bezpośredniego uogólnienia pojęcia przestrzeni wektorowej.
Z drugiej strony, jeśli na grupie abelowej M jest określone działanie zewnętrzne z pierścieniem skalarów R i działanie to ma własności (3.1)–(3.4), to łatwo sprawdzić, że odwzorowanie $\varphi : R \to \mathsf{End}\, M$ takie, że $\varphi(a)(m) = am$ dla każdego $m \in M$, jest homomorfizmem pierścieni. A więc (M, φ) jest $R-$modułem w sensie definicji 3.1.1. Tak więc obydwa podejścia do definicji pojęcia $R-$modułu są równoważne.

Następujące przykłady wskazują jak pojemne jest pojęcie modułu.

Przykład 3.1.1. Każda grupa abelowa M jest $\mathbb{Z}-$modułem jeśli za działanie zewnętrzne na M przyjąć mnożenie elementów grupy M przez liczby całkowite.

Przykład 3.1.2. Pierścień R jest $R-$modułem jeśli za działanie zewnętrzne na R przyjąć mnożenie w pierścieniu R. Ogólniej, każdy ideał lewostronny $\mathcal{J}$ pierścienia R jest $R-$modułem, jeśli za działanie zewnętrzne na $\mathcal{J}$ przyjąć mnożenie elementów ideału $\mathcal{J}$ przez elementy pierścienia R. W szczególności, każdy ideał pierścienia R jest $R-$modułem. Na odwrót, jeśli addytywna podgrupa $\mathcal{J}$ pierścienia R jest $R-$modułem (z mnożeniem jako działaniem zewnętrznym), to $\mathcal{J}$ jest ideałem lewostronnym pierścienia R.

Przykład 3.1.3. Niech K będzie ciałem. Każda przestrzeń wektorowa V nad K jest $K-$modułem. Każdy $K-$moduł V jest przestrzenią wektorową nad ciałem K.

Przykład 3.1.4. Niech $R = K[X]$ będzie pierścieniem wielomianów jednej zmiennej nad ciałem K. Niech $M = V$ będzie przestrzenią wektorową nad ciałem K i niech τ będzie endomorfizmem przestrzeni V. Rozpatrzmy homomorfizm podstawiania endomorfizmu τ przestrzeni V w miejsce zmiennej wielomianu $f \in K[X]$:

$$\varphi_\tau : K[X] \to \mathsf{End}_K\, V, \quad \varphi_\tau(f) = f(\tau).$$

Zgodnie z definicją 3.1.1, przestrzeń wektorowa V jest $K[X]-$modułem. Tak skonstruowany $K[X]-$moduł oznaczamy V_τ. W module V_τ działanie zewnętrzne jest określone następująco:

$$K[X] \times V \to V, \quad (f, v) \mapsto f(\tau)(v).$$

A więc $fv := f(\tau)(v)$. Ten przykład stanowi podstawę zastosowań teorii modułów w algebrze liniowej.

Przykład 3.1.5. Niech A będzie pierścieniem przemiennym i niech S będzie zbiorem multyplikatywnym w pierścieniu A. Niech M będzie $A-$modułem. Na zbiorze $M \times S$ definiujemy relację $\sim$ określoną następująco:

$$(m_1, s_1) \sim (m_2, s_2) \quad \Leftrightarrow \quad \exists s \in S \quad s(s_2 m_1 - s_1 m_2) = 0.$$

Relacja $\sim$ jest relacją równoważnościową na zbiorze $M \times S$.
Klasę abstrakcji $[(m, s)]_\sim$ oznacza się m/s lub $\frac{m}{s}$ i nazywa się *ułamkiem* o liczniku m i mianowniku s. Podobnie jak w rozdziale 2 sprawdza się, że zbiór $S^{-1}M$ wszystkich ułamków jest grupą abelową ze względu na dodawanie ułamków określone następująco:

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2}.$$

Na grupie $S^{-1}M$ określamy teraz działanie zewnętrzne z pierścieniem skalarów $S^{-1}A$:

$$S^{-1}A \times S^{-1}M \to S^{-1}M, \quad \left(\frac{a}{s_1}, \frac{m}{s_2}\right) \mapsto \frac{am}{s_1 s_2}$$

i z łatwością stwierdzamy, że ma ono własności (3.1)–(3.4). A więc $S^{-1}M$ jest $S^{-1}A-$modułem. Nazywamy go *modułem ułamków* modułu M ze względu na zbiór multyplikatywny S pierścienia A.

Przykład 3.1.6. Niech M będzie $R-$modułem i niech $f : P \to R$ będzie homomorfizmem pierścieni. Wtedy określamy działanie zewnętrzne na M z pierścieniem skalarów P kładąc

$$bm := f(b)m$$

dla każdego $b \in P$. Z łatwością stwierdza się, że z tak zdefiniowanym działaniem zewnętrznym M staje się $P-$modułem. Mówimy, że ten $P-$moduł powstaje z $R-$modułu M przez *zwężenie* lub *ograniczenie* pierścienia skalarów (z R do P).
W szczególności więc w poprzednim przykładzie możemy zauważyć, że dla $A-$modułu M, skonstruowany tam $S^{-1}A-$moduł ułamków $S^{-1}M$ jest także $A-$modułem (zwężenie pierścienia skalarów jest tutaj wyznaczone przez homomorfizm naturalny $\varphi_S : A \to S^{-1}A,\ \varphi_S(a) = a/1$).

Definicja **3.1.2.** Niech M będzie $R-$modułem. Podmodułem N modułu M nazywamy podgrupę N addytywnej grupy M zamkniętą ze względu na mnożenie przez elementy pierścienia R, to znaczy, podgrupę N grupy M spełniającą warunek

$$RN \subseteq N.$$

Jeśli N jest podmodułem modułu M, to piszemy $N < M$.

Przykład 3.1.7. Każda podgrupa N grupy abelowej M jest podmodułem $\mathbb{Z}-$modułu M. Każdy ideał lewostronny $\mathcal{J}$ pierścienia R jest podmodułem $R-$modułu R. Każda podprzestrzeń wektorowa przestrzeni wektorowej V nad ciałem K jest podmodułem $K-$modułu V.
Jeśli $\mathcal{J}$ jest ideałem lewostronnym pierścienia R oraz M jest $R-$modułem, to

$$\mathcal{J}M := \Big\{a_1m_1 + \cdots + a_nm_n \in M \ : \ a_i \in \mathcal{J},\ m_i \in M,\ n \in \mathbb{N}\Big\}$$

jest podmodułem modułu M.
Dla endomorfizmu τ przestrzeni wektorowej V, każda podprzestrzeń $\tau-$niezmiennicza U przestrzeni V (to znaczy, podprzestrzeń spełniająca $\tau(U) \subseteq U$) jest podmodułem $K[X]-$modułu V_τ. Rzeczywiście, jeśli $\tau(U) \subseteq U$ to także $\tau^m(U) \subseteq U$ dla każdej liczby naturalnej m, a stąd otrzymujemy łatwo $f(\tau)(U) \subseteq U$ dla każdego wielomianu $f \in K[X]$. Także na odwrót, jeśli U jest podmodułem $K[X]-$modułu V_τ, to dla każdego wielomianu $f \in K[X]$ mamy $f(\tau)(U) \subseteq U$. Zatem w szczególności także $\tau(U) \subseteq U$.
A więc U jest podmodułem $K[X]-$modułu V_τ wtedy i tylko wtedy, gdy U jest podprzestrzenią niezmienniczą endomorfizmu τ.

Definicja **3.1.3.** Niech M będzie $R-$modułem.
(a) Mówimy, że podmoduł N jest *generowany* przez zbiór $S \subseteq M$, jeśli każdy element podmodułu N można przedstawić w postaci kombinacji liniowej skończonego podzbioru zbioru S ze współczynnikami z pierścienia R.

(b) Mówimy, że podmoduł N jest *skończenie generowany*, jeśli jest generowany przez podzbiór skończony modułu M.

(c) Podmoduł N modułu M nazywamy podmodułem *cyklicznym*, jeśli N jest generowany przez zbiór jednoelementowy, to znaczy, jeśli istnieje element $m \in M$ taki, że

$$N = \Big\{am \in M : \quad a \in R\Big\}.$$

Przykład 3.1.8. Każda podgrupa cykliczna N grupy abelowej M jest podmodułem cyklicznym $\mathbb{Z}-$modułu M.
Każdy ideał główny $\mathcal{J}$ pierścienia R jest podmodułem cyklicznym $R-$modułu R.
Każda jedno-wymiarowa podprzestrzeń wektorowa przestrzeni wektorowej V nad ciałem K jest podmodułem cyklicznym $K-$modułu V.
Każda skończenie wymiarowa przestrzeń wektorowa V nad ciałem K jest skończenie generowanym $K-$modułem.
Jeśli V jest skończenie wymiarową przestrzenią wektorową nad ciałem K, to rozpatrywany w przykładzie 3.1.4 $K[X]-$moduł V_τ jest skończenie generowany.

3.1.1 Operacje na modułach

Niech M będzie $R-$modułem i niech N_1 i N_2 będą podmodułami modułu M. Wtedy przekrój $N_1 \cap N_2$ jest podmodułem $R-$modułu M. Również suma $N_1 + N_2$ podgrup grupy abelowej M jest podmodułem $R-$modułu M. Nazywamy ją *sumą podmodułów* N_1 i N_2. Podobnie określa się sumę dowolnej rodziny podmodułów $R-$modułu M (jako sumę podgrup grupy abelowej M).

W szczególności, jeśli $N_1 + N_2 = M$, to mówimy, że moduł M jest *sumą* podmodułów N_1 i N_2. Jeśli w dodatku $N_1 \cap N_2 = 0$, to mówimy, że M jest *sumą prostą* podmodułów N_1 i N_2. Piszemy wtedy $M = N_1 \oplus N_2$. Zauważmy, że tak jak dla grup abelowych, M jest sumą prostą podmodułów N_1 i N_2 wtedy i tylko wtedy gdy każdy element $m \in M$ ma *jednoznaczne* przedstawienie w postaci $m = n_1 + n_2$, gdzie $n_1 \in N_1$, $n_2 \in N_2$.

Mówimy, że podmoduł N_1 modułu M jest *składnikiem prostym* modułu M jeśli istnieje podmoduł N_2 taki, że $M = N_1 \oplus N_2$. W przestrzeni wektorowej V każda podprzestrzeń jest składnikiem prostym przestrzeni V. Jest to wysoce wyjątkowa sytuacja. Na przykład, w $\mathbb{Z}-$module $\mathbb{Z}$ (czyli w grupie liczb całkowitych) jedynymi składnikami prostymi są podmoduły 0 i $\mathbb{Z}$. Grupa $\mathbb{Z}$ nie ma bowiem nietrywialnych rozkładów na sumę prostą podgrup. Podgrupy $\mathbb{Z}$ są grupami cyklicznymi $a\mathbb{Z}$, gdzie $a \in \mathbb{Z}$. Jeśli $\mathbb{Z} = a\mathbb{Z} \oplus b\mathbb{Z}$, to $a\mathbb{Z} \cap b\mathbb{Z} = 0$ co jest możliwe tylko dla $a = 0$ lub $b = 0$. Wniosek 3.2.10 w dalszej części rozdziału podaje warunek konieczny i wystarczający na to by podmoduł modułu był składnikiem prostym modułu.

Mówimy, że moduł M jest *sumą prostą rodziny* swoich podmodułów $N_i,\ i \in I$, jeśli grupa abelowa M jest sumą prostą rodziny podgrup $N_i,\ i \in I$. Piszemy wtedy

$$M = \bigoplus \{N_i,\ i \in I\}.$$

Niech M i M' będą $R-$modułami. Na iloczynie kartezjańskim $M \times M'$ grup abelowych M i M' określamy działanie zewnętrzne z pierścieniem skalarów R kładąc

$$a(m, m') = (am, am')$$

dla $a \in R, m \in M, m' \in M'$. Łatwo sprawdza się, że w ten sposób grupa abelowa $M \times M'$ staje się $R-$modułem. Nazywamy go *iloczynem prostym* (lub kartezjańskim) modułów M i M'. Podobnie określa się iloczyn prosty dowolnej rodziny $R-$modułów $M_i, i \in I$.

Jeśli N jest podmodułem $R-$modułu M, to grupę ilorazową M/N można w sposób naturalny traktować jako $R-$moduł. Wystarczy zauważyć, że iloczyn kompleksowy warstwy $m + N$ przez element $a \in R$ (jednoelementowy podzbiór pierścienia R) zawiera się w dokładnie jednej warstwie modułu M względem podmodułu N:

$$a(m + N) = \Big\{a(m + n) : n \in N\Big\} = \Big\{am + an : n \in N\Big\} \subseteq am + N.$$

Warstwę $am + N$ nazywamy iloczynem warstwy $m + N$ przez skalar $a \in R$. W ten sposób otrzymujemy działanie zewnętrzne na grupie abelowej M/N z pierścieniem skalarów R. Łatwo sprawdza się, że grupa ilorazowa M/N staje się $R-$modułem. Moduł ten nazywamy *modułem ilorazowym* modułu M względem podmodułu N.

3.2 Homomorfizmy modułów

Niech M i M' będą $R-$modułami. *Homomorfizmem* $h : M \to M'$ nazywamy homomorfizm h grupy abelowej M w grupę abelową M' spełniający warunek

$$h(am) = ah(m) \quad \forall\ a \in R,\ m \in M.$$

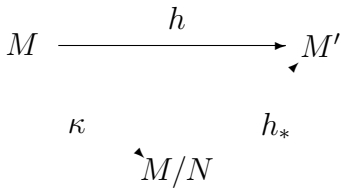
Jądro i obraz homomorfizmu modułów określamy oczywiście jako jądro i obraz homomorfizmu grup abelowych. Również takie terminy jak *epimorfizm, monomorfizm, izomorfizm* modułów interpretujemy tak jak w teorii grup (jako, odpowiednio, homomorfizm surjektywny, injektywny, bijektywny).
Niech N będzie podmodułem $R-$modułu M i niech

$$\kappa : M \to M/N, \quad \kappa(m) = m + N$$

będzie homomorfizmem kanonicznym grup abelowych. Wtedy $\kappa(am) = am + N = a(m + N) = a\kappa(m)$ dla $a \in R, m \in M$. Zatem κ jest homomorfizmem modułów. Nazywamy go homomorfizmem *kanonicznym* modułów.

Sformułujemy teraz podstawowe twierdzenia o homomorfizmach modułów. Są one analogonami twierdzeń o homomorfizmach grup z rozdziału 1.

Twierdzenie **3.2.1.** (Twierdzenie o faktoryzacji.)
Jeśli $h : M \to M'$ jest homomorfizmem $R-$modułów, $N = \ker h$ oraz $\kappa : M \to M/N$ jest homomorfizmem kanonicznym, to istnieje dokładnie jeden injektywny homomorfizm $h_* : M/N \to M'$ taki, że $h = h_* \circ \kappa$, to znaczy taki, że następujący diagram jest przemienny:



Twierdzenie **3.2.2.** (Twierdzenie o odpowiedniości.)
Jeśli $h : M \to M'$ jest epimorfizmem $R-$modułów, to przyporządkowanie $N \mapsto h(N)$ jest bijekcją rodziny podmodułów N modułu M zawierających $\ker h$ *na rodzinę wszystkich podmodułów modułu M'. Odwzorowaniem odwrotnym jest $N' \mapsto h^{-1}(N')$. Ponadto, dla każdego podmodułu N modułu M zawierającego jądro* $\ker h$ *homomorfizmu h mamy izomorfizm*

$$M/N \cong M'/h(N).$$

Twierdzenie **3.2.3.** (Twierdzenie o izomorfizmie.)
Niech M będzie $R-$modułem. Dla każdych podmodułów M', M'' modułu M istnieje izomorfizm

$$(M' + M'')/M'' \cong M'/M' \cap M''.$$

Jeśli ponadto $M'' < M' < M$, to

$$(M/M'')/(M'/M'') \cong M/M'.$$

Dowód. Istnienie odpowiednich homomorfizmów addytywnych grup abelowych wynika z twierdzeń o homomorfizmach grup. Sprawdzenie, że homomorfizmy te są homomorfizmami modułów pozostawiamy Czytelnikowi jako ćwiczenie. □

3.2.1 Rozszczepialne ciągi dokładne

DEFINICJA **3.2.4.** Ciąg $R-$modułów i homomorfizmów

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{3.5}$$

nazywa się ciągiem *dokładnym*, jeśli f jest monomorfizmem, g jest epimorfizmem oraz $\operatorname{im} f = \ker g$.

A więc dokładność ciągu (3.5) oznacza, że $\ker f = 0,\ \operatorname{im} f = \ker g,\ \operatorname{im} g = M''$. Zamiast pięcioczłonowych ciągów dokładnych można rozpatrywać ciągi dowolnej długości (nawet nieskończone). Mówimy, że ciąg

$$\cdots \longrightarrow M_{i-1} \xrightarrow{g_{i-1}} M_i \xrightarrow{g_i} M_{i+1} \longrightarrow \cdots$$

jest *dokładny w członie* M_i, jeśli $\operatorname{im} g_{i-1} = \ker g_i$. Ciąg nazywa się *dokładny,* jeśli jest dokładny w każdym członie. W szczególności, dokładność ciągu

$$0 \to M' \xrightarrow{f} M$$

oznacza, że f jest monomorfizmem, natomiast dokładność ciągu

$$M \xrightarrow{g} M'' \to 0$$

oznacza, że g jest epimorfizmem.

Przykład 3.2.1. Każdy homomorfizm modułów $g : M \to M''$ wyznacza ciąg dokładny

$$0 \to \ker g \xrightarrow{f} M \xrightarrow{g} \operatorname{im} g \to 0,$$

w którym $f : \ker g \to M$ jest włożeniem: $f(m) = m$ dla każdego $m \in \ker g$. W szczególności, jeśli M' jest podmodułem modułu M i $\kappa : M \to M/M'$ jest homomorfizmem kanonicznym, to mamy ciąg dokładny

$$0 \to M' \hookrightarrow M \xrightarrow{\kappa} M/M' \to 0.$$

Przykład 3.2.2. Niech moduł M będzie sumą prostą podmodułów M_1, M_2, $M = M_1 \oplus M_2$. Wtedy mamy ciąg dokładny

$$0 \to M_1 \xrightarrow{f} M \xrightarrow{g} M_2 \to 0, \tag{3.6}$$

w którym $f(m_1) = m_1$ dla $m_1 \in M_1$, oraz $g(m_1 + m_2) = m_2$, dla $m_1 \in M_1, m_2 \in M_2$. Ten ciąg dokładny ma pewną ważną dodatkową własność, mianowicie istnieją homomorfizmy $\varphi : M_2 \to M$ oraz $\psi : M \to M_1$ określone następująco:

$$\varphi(m_2) = m_2, \quad \psi(m_1 + m_2) = m_1$$

takie, że

$$\psi \circ f = \mathbf{1}_{M_1}, \quad g \circ \varphi = \mathbf{1}_{M_2}.$$

Okazuje się, że ta dodatkowa własność ciągu dokładnego (3.6) stanowi także warunek wystarczający na to, by moduł M był sumą prostą podmodułów M_1 i M_2.

TWIERDZENIE **3.2.5.** *Dla ciągu dokładnego*

$$M \xrightarrow{g} M'' \to 0$$

następujące warunki są równoważne.

(a) *Podmoduł* $\ker g$ *modułu* M *jest składnikiem prostym modułu* M.
(b) *Istnieje homomorfizm* $\varphi : M'' \to M$ *taki, że* $g \circ \varphi = \mathbf{1}_{M''}$.

Dowód. (a) $\Rightarrow$ (b) Niech $M = \ker g \oplus N$, dla pewnego podmodułu N modułu M. Definiujemy odwzorowanie $\varphi : M'' \to M$ następująco. Każdy element m'' modułu M'' jest postaci $m'' = g(m)$, gdzie $m \in M = \ker g \oplus N$. Jeśli $m = k + n$, gdzie $k \in \ker g, n \in N$, to kładziemy

$$\varphi(m'') = \varphi(g(m)) := n.$$

Zauważmy, że $\varphi(m'')$ nie zależy od przedstawienia elementu m'' w postaci $m'' = g(m)$. Jeśli bowiem $g(m) = g(m')$ dla $m, m' \in M$, to $m' = k' + n'$, gdzie $k' \in \ker g, n' \in N$ i wobec tego

$$g(n) = g(k + n) = g(m) = g(m') = g(k' + n') = g(n'),$$

skąd $n - n' \in \ker g \cap N = 0$. A więc $n = n'$.
Sprawdzamy teraz bezpośrednim rachunkiem, że φ jest homomorfizmem modułów. Ponadto, $g \circ \varphi = \mathbf{1}_{M''}$, gdyż dla każdego $m \in M$ mamy

$$g \circ \varphi(g(m)) = g(n) = g(m).$$

(b) $\Rightarrow$ (a) Dla dowolnego elementu $m \in M$ rozpatrzmy element $y := m - \varphi(g(m)) \in M$. Mamy

$$g(y) = g(m) - g(\varphi(g(m))) = g(m) - (g \circ \varphi)(g(m)) = g(m) - g(m) = 0,$$

a więc $y \in \ker g$. Zatem $m = y + \varphi(g(m)) \in \ker g + \operatorname{im} \varphi$. Wynika stąd, że $M = \ker g + \operatorname{im} \varphi$ i wobec tego wystarczy pokazać, że $\ker g \cap \operatorname{im} \varphi = 0$. Przypuśćmy, że $m \in \ker g \cap \operatorname{im} \varphi$. Wtedy $g(m) = 0$ oraz $m = \varphi(m'')$ dla pewnego $m'' \in M''$. Zatem wobec (b) otrzymujemy $m'' = (g \circ \varphi)(m'') = g(m) = 0$, skąd także wynika, że $m = \varphi(m'') = 0$. A więc $M = \ker g \oplus \operatorname{im} \varphi$. □

TWIERDZENIE **3.2.6.** *Dla ciągu dokładnego*

$$0 \to M' \xrightarrow{f} M$$

następujące warunki są równoważne.

(a) *Podmoduł* $\operatorname{im} f$ *modułu* M *jest składnikiem prostym modułu* M.
(c) *Istnieje homomorfizm* $\psi : M \to M'$ *taki, że* $\psi \circ f = \mathbf{1}_{M'}$.

Dowód. (a) $\Rightarrow$ (c). Jeśli mamy $M = f(M') \oplus L$ dla pewnego podmodułu L modułu M, to definiujemy

$$\psi : M \to M', \quad \psi(f(m') + l) = m'$$

dla $m' \in M',\ l \in L$. Wtedy ψ jest homomorfizmem $R-$modułów oraz

$$(\psi \circ f)(m') = \psi(f(m')) = m' = 1_{M'}(m')$$

dla każdego $m' \in M'$. Dowodzi to, że (a) $\Rightarrow$ (c).
(c) $\Rightarrow$ (a) Jeśli spełniony jest warunek (c), to dla każdego $m \in M$ weźmy $y := m - f(\psi(m)) \in M$. Wtedy

$$\psi(y) = \psi(m) - \psi f\psi(m) = \psi(m) - \psi(m) = 0,$$

zatem $y \in \ker\psi$. Stąd $m = f(\psi(m)) + y \in \operatorname{im} f + \ker\psi$.
Przypuśćmy, że $x \in \operatorname{im} f \cap \ker\psi$. Wtedy $x = f(m')$ dla pewnego $m' \in M'$ oraz $\psi(x) = 0$, to znaczy $\psi f(m') = 0$. Wobec (c) wynika stąd, że $m' = 0$ zatem także $x = f(m') = 0$. Pokazaliśmy więc, że $M = \operatorname{im} f \oplus \ker\psi$. □

Podsumowując twierdzenia 3.2.5 i 3.2.6 otrzymujemy następujący rezultat.

Twierdzenie **3.2.7.** *Dla ciągu dokładnego*

$$0 \ \to\ M' \ \xrightarrow{f}\ M \ \xrightarrow{g}\ M'' \ \to\ 0$$

następujące warunki są równoważne.

(a) *Podmoduł* $\operatorname{im} f = \ker g$ *modułu* M *jest składnikiem prostym modułu* M.
(b) *Istnieje homomorfizm* $\varphi : M'' \to M$ *taki, że* $g \circ \varphi = \mathbf{1}_{M''}$.
(c) *Istnieje homomorfizm* $\psi : M \to M'$ *taki, że* $\psi \circ f = \mathbf{1}_{M'}$.

Definicja **3.2.8.** (a) Mówimy, że ciąg dokładny

$$0 \ \to\ M' \ \xrightarrow{f}\ M \ \xrightarrow{g}\ M'' \ \to\ 0 \tag{3.7}$$

rozszczepia się, jeśli spełniony jest warunek (a) twierdzenia 3.2.7.
(b) Mówimy, że ciąg dokładny

$$M \ \xrightarrow{g}\ M'' \ \to\ 0 \tag{3.8}$$

rozszczepia się, gdy spełniony jest warunek (b) twierdzenia 3.2.7.
Homomorfizm φ nazywamy wtedy homomorfizmem *rozszczepiającym* ciąg dokładny (3.8).
(c) Mówimy, że ciąg dokładny

$$0 \ \to\ M' \ \xrightarrow{f}\ M \tag{3.9}$$

rozszczepia się, jeśli spełniony jest warunek (c) twierdzenia 3.2.7.
Homomorfizm ψ nazywamy wtedy homomorfizmem *rozszczepiającym* ciąg dokładny (3.9).

Twierdzenie 3.2.7 mówi więc, że jeśli ciąg (3.7) jest dokładny, to jego rozszczepialność jest równoważna rozszczepialności każdego z ciągów (3.8), (3.9).
Homomorfizmy φ i ψ nazywają się homomorfizmami *rozszczepiającymi* ciąg dokładny (3.7).

WNIOSEK **3.2.9.** *Jeśli ciąg dokładny* (3.7) *rozszczepia się i* φ, ψ *są homomorfizmami rozszczepiającymi z warunków* (b) *i* (c)*, to*

$$M = \ker g \oplus \operatorname{im} \varphi = \operatorname{im} f \oplus \ker \psi \quad \text{oraz} \quad M \cong M' \times M''.$$

Dowód. Pokazaliśmy, że warunek (b) pociąga $M = \ker g \oplus \operatorname{im} \varphi$ oraz, że warunek (c) pociąga $M = \operatorname{im} f \oplus \ker \psi$. Z dokładności ciągu (3.7) wynika równość $\ker g = \operatorname{im} f$. Ponieważ f jest monomorfizmem, mamy $\operatorname{im} f \cong M'$. Z warunku (b) wynika, że φ jest także monomorfizmem, zatem $\operatorname{im} \varphi \cong M''$. A więc

$$M = \ker g \oplus \operatorname{im} \varphi = \operatorname{im} f \oplus \operatorname{im} \varphi \cong M' \times M''. \qquad \square$$

WNIOSEK **3.2.10.** *Niech* N *będzie podmodułem modułu* M *i niech*

$$f : N \to M, \quad g : M \to M/N$$

będą odpowiednio identycznościowym włożeniem N *w* M *i homomorfizmem kanonicznym.*
Podmoduł N *modułu* M *jest składnikiem prostym modułu* M *wtedy i tylko wtedy gdy jeden z ciągów dokładnych*

$$0 \to N \xrightarrow{f} M, \qquad M \xrightarrow{g} M/N \to 0$$

rozszczepia się.

Rozszerzymy teraz pojęcie składnika prostego modułu przyjmując, że $R-$moduł M'' jest *składnikiem prostym* $R-$modułu M jeśli istnieją podmoduły N_1 i N_2 modułu M takie, że $M = N_1 \oplus N_2$ i $N_1 \cong M''$. A więc rozumieć będziemy termin *składnik prosty* z dokładnością do izomorfizmu modułów.

WNIOSEK **3.2.11.** *Dla* $R-$*modułów* M *i* M'' *następujące warunki są równoważne.*

(a) *Moduł* M'' *jest składnikiem prostym modułu* M*.*
(b) *Istnieje rozszczepialny ciąg dokładny* $M \to M'' \to 0$*.*
(c) *Istnieje rozszczepialny ciąg dokładny* $0 \to M'' \to M$*.*

Dowód. Wystarczy zauważyć, że trójczłonowy ciąg dokładny można zawsze przedłużyć do pięcioczłonowego ciągu dokładnego i skorzystać z wniosku 3.2.9. $\square$

3.3 Moduły wolne

Moduły wolne stanowią uogólnienie przestrzeni wektorowych i grup abelowych wolnych. Charakterystyczną cechą tych obiektów jest istnienie bazy, to znaczy podzbioru liniowo niezależnego generującego obiekt.

DEFINICJA **3.3.1.** $R-$moduł F nazywa się *modułem wolnym*, jeśli istnieje podzbiór $\mathcal{B}$ modułu F o następujących własnościach:
(a) $\mathcal{B}$ jest zbiorem liniowo niezależnym, to znaczy, dla każdych $x_1, \ldots, x_n \in R$ i $b_1, \ldots, b_n \in \mathcal{B}$ mamy implikację

$$x_1 b_1 + \cdots + x_n b_n = 0 \;\Rightarrow\; x_1 = \cdots = x_n = 0.$$

(b) Każdy element $m \in F$ ma przedstawienie w postaci

$$m = x_1 b_1 + \cdots + x_n b_n, \;\; b_1, \ldots, b_n \in \mathcal{B}, \; x_1, \ldots, x_n \in R, \; n \in \mathbb{N}. \tag{3.10}$$

Podzbiór $\mathcal{B}$ modułu wolnego F spełniający warunki (a) i (b) nazywa się *bazą* modułu wolnego F. Baza modułu wolnego F jest więc liniowo niezależnym (nad R) podzbiorem F generującym moduł F. Zgodnie z definicją, moduł F jest modułem wolnym wtedy i tylko wtedy gdy ma bazę.
Tak jak w algebrze liniowej stwierdzamy, że zbiór $\mathcal{B} \subseteq F$ jest bazą modułu wolnego F wtedy i tylko wtedy, gdy każdy element $m \in F$ ma i to tylko jedno przedstawienie w postaci (3.10).

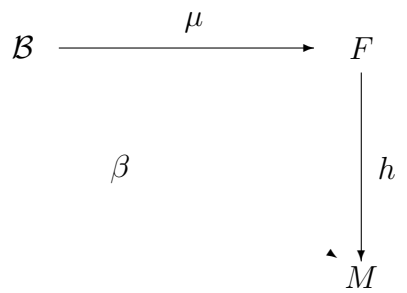
Przykład 3.3.1. $R-$moduł R jest przykładem $R-$modułu wolnego. Rzeczywiście, zbiór jednoelementowy $\mathcal{B} = \{1\}$ jest bazą $R-$modułu R. Ogólniej, suma prosta dowolnej liczby (kardynalnej) egzemplarzy $R-$modułu R jest modułem wolnym. Jeśli bowiem $F := R^{(I)} = \coprod_{i\in I} R$ to bazę F tworzy zbiór $\mathcal{B} = \{e_i : i \in I\}$, gdzie $e_i(i) = 1$ oraz $e_i(j) = 0$ dla $j \neq i$. Wynika stąd, że dla każdego zbioru I istnieje $R-$moduł wolny F z bazą mocy $|I|$. W szczególności, dla każdej liczby naturalnej n, potęga kartezjańska R^n jest wolnym $R-$modułem.

Przykład 3.3.2. $\mathbb{Z}-$moduł wolny F nazywa się *grupą abelową wolną*.
Każda przestrzeń wektorowa V nad ciałem K jest wolnym $K-$modułem. Jak bowiem wiadomo z algebry liniowej, każda przestrzeń wektorowa ma bazę.

Sformułujemy teraz kilka charakterystycznych własności wolnych $R-$modułów. Rozpoczynamy od tak zwanej własności uniwersalnej modułu wolnego, którą można byłoby przyjąć jako definicję modułu wolnego.

Twierdzenie **3.3.2.** *Niech F będzie $R-$modułem i niech $\mathcal{B}$ będzie podzbiorem modułu F. Zbiór $\mathcal{B}$ jest bazą modułu F (i F jest modułem wolnym) wtedy i tylko wtedy, gdy dla dowolnego modułu M i dowolnego odwzorowania $\beta : \mathcal{B} \to M$ istnieje dokładnie jeden homomorfizm $R-$modułów $h : F \to M$ taki, że $h(b) = \beta(b)$ dla każdego $b \in \mathcal{B}$.*

Jeśli przez $\mu : \mathcal{B} \to F$ oznaczymy włożenie $\mu(b) = b$, to występujące w twierdzeniu odwzorowania tworzą diagram przemienny



Dowód. Jeśli $\mathcal{B} = \{b_i : i \in I\}$ jest bazą $R-$modułu F oraz $\beta : \mathcal{B} \to M$ jest jakimkolwiek odwzorowaniem bazy $\mathcal{B}$ w $R-$moduł M, to β ma dokładnie jedno przedłużenie h do homomorfizmu $R-$modułów $F \to M$. Jeśli bowiem takie przedłużenie istnieje, to h, jako homomorfizm, spełnia warunek

$$h\Big(\sum_{i\in I} x_i b_i\Big) = \sum_{i\in I} x_i \beta(b_i)$$

dla każdego układu $x_i \in R$ prawie wszystkich równych zero oraz dla wszystkich $b_i \in \mathcal{B}$. Warunek ten pokazuje, że jeśli przedłużenie odwzorowania β do homomorfizmu modułów istnieje, to jest tylko jedno. Z drugiej strony, warunek ten podpowiada nam jak należy określić h na module F by pokazać istnienie przedłużenia odwzorowania β do homomorfizmu $F \to M$. Ponieważ każdy element m modułu F ma jednoznaczne przedstawienie w postaci $m = \sum_{i\in I} x_i b_i$, gdzie prawie wszystkie $x_i = 0$, wystarczy więc położyć

$$h(m) = \sum_{i\in I} x_i \beta(b_i)$$

dla każdego układu $x_i \in R$ prawie wszystkich równych zero oraz dla wszystkich $b_i \in \mathcal{B}$. Oczywiście h przedłuża β i łatwo sprawdza się, że $h : F \to M$ jest homomorfizmem modułów.
Z drugiej strony, jeśli zbiór $\mathcal{B} \subset F$ ma własność opisaną w twierdzeniu, to jest liniowo niezależny. W przeciwnym razie mamy relację

$$\sum x_i b_i = 0$$

pomiędzy elementami b_i zbioru $\mathcal{B}$ (w której prawie wszystkie współczynniki są równe 0). Gdyby tutaj $x_j \neq 0$ dla pewnego j, to określamy odwzorowanie $\beta : \mathcal{B} \to R$ kładąc $\beta(b_j) = 1$ oraz $\beta(b_i) = 0$ dla $i \neq j$. Przedłużenie β do homomorfizmu $h : F \to R$ daje teraz

$$0 = h\Big(\sum x_i b_i\Big) = \sum x_i h(b_i) = x_j,$$

sprzeczność. A więc zbiór $\mathcal{B}$ jest liniowo niezależny.
Pozostaje pokazać, że $\mathcal{B}$ generuje F. Niech więc F_1 będzie podmodułem F generowanym przez $\mathcal{B}$. Pokażemy, że $F_1 = F$. Rozpatrzmy odwzorowanie

$$\beta_1 : \mathcal{B} \to F/F_1, \quad \beta_1(b) = 0 \quad \text{dla wszystkich} \quad b \in \mathcal{B}.$$

Z jednej strony, przedłużeniem tego odwzorowania do homomorfizmu $h_1 : F \to F/F_1$ jest homomorfizm zerowy, $h_1(m) = 0$ dla wszystkich $m \in F$. Z drugiej strony, przedłużeniem odwzorowania β_1 jest także homomorfizm kanoniczny $\kappa : F \to F/F_1$. Wobec jednoznaczności przedłużenia $\kappa = h_1$ jest homomorfizmem zerowym. Ma to miejsce tylko wtedy gdy moduł ilorazowy F/F_1 jest zerowy, to znaczy wtedy, gdy $F = F_1$. □

Twierdzenie **3.3.3.** *Każdy $R-$moduł M jest homomorficznym obrazem pewnego $R-$modułu wolnego F. Jeśli moduł M jest generowany przez zbiór skończony $n-$elementowy, to M jest homomorficznym obrazem modułu wolnego z bazą $n-$elementową.*

Dowód. Niech $\{m_i : i \in I\}$ będzie zbiorem generatorów $R-$modułu M. Rozpatrujemy $R-$moduł wolny F, którego baza ma moc $|I|$ (zob. przykład 3.3.1). Niech $\mathcal{B} = \{b_i : i \in I\}$ będzie bazą modułu F. Na podstawie twierdzenia 3.3.2 przyporządkowanie $\beta : \mathcal{B} \to M,\ b_i \mapsto m_i$ można jednoznacznie przedłużyć do homomorfizmu modułów $h : F \to M$. Jest to epimorfizm $R-$modułów, gdyż

$$m_i = \beta(b_i) = h(b_i),$$

zatem wszystkie elementy z danego zbioru generatorów modułu M znajdują się w obrazie homomorfizmu h. □

TWIERDZENIE **3.3.4.** *Niech A będzie pierścieniem przemiennym. Moc bazy wolnego $A-$modułu F jest jednoznacznie wyznaczona przez moduł F. Każde dwie bazy $A-$modułu wolnego F są równoliczne.*

Dowód. Na podstawie twierdzenia 2.3.5 pierścień A ma co najmniej jeden ideał maksymalny $\mathfrak{m}$. Zatem pierścień ilorazowy $A/\mathfrak{m}$ jest ciałem. Z ideałem $\mathfrak{m}$ wiążemy podmoduł $\mathfrak{m}F$ generowany przez wszystkie iloczyny af, gdzie $a \in \mathfrak{m}$, $f \in F$ (zob. przykład 3.1.7). Rozpatrujemy teraz $A-$moduł ilorazowy $F/\mathfrak{m}F$ i zauważamy, że ma on także strukturę modułu nad ciałem $A/\mathfrak{m}$. Rzeczywiście, mnożenie warstw $f + \mathfrak{m}F$ przez skalary $a + \mathfrak{m}$ ciała $A/\mathfrak{m}$ określa się następująco:

$$(a + \mathfrak{m}) \cdot (f + \mathfrak{m}F) = af + \mathfrak{m}F.$$

Niezależność tej definicji od wyboru elementów reprezentujących warstwy wynika stąd, że jeśli $a - a' \in \mathfrak{m}$ oraz $f - f' \in \mathfrak{m}F$, to $af - a'f' = (a - a')f + a'(f - f') \in \mathfrak{m}F$. Sprawdzenie aksjomatów modułu pozostawiamy jako ćwiczenie. W ten sposób dla $A-$modułu wolnego F skonstruowaliśmy przestrzeń wektorową $F/\mathfrak{m}F$ nad ciałem $A/\mathfrak{m}$. Jeśli teraz $\mathcal{B}$ jest bazą modułu wolnego F to zbiór

$$\mathcal{B} + \mathfrak{m}F := \left\{b + \mathfrak{m}F : b \in \mathcal{B}\right\}$$

jest bazą przestrzeni wektorowej $F/\mathfrak{m}F$ nad ciałem $A/\mathfrak{m}$. Rzeczywiście, jeśli

$$\sum (x_i + \mathfrak{m})(b_i + \mathfrak{m}F) = \mathfrak{m}F \tag{3.11}$$

dla pewnych $x_i \in A$, $b_i \in B$, to $\sum x_i b_i \in \mathfrak{m}F$. Stąd wynika, że istnieją $a_k \in \mathfrak{m}$ oraz $f_k \in F$ takie, że $\sum_i x_i b_i = \sum_k a_k f_k$. Przedstawiając teraz elementy f_k jako kombinacje liniowe elementów bazy $\mathcal{B}$ otrzymamy $f_k = \sum_i z_{ki} b_i$ dla pewnych $z_{ki} \in A$ i wobec tego

$$\sum x_i b_i = \sum_k a_k f_k = \sum_k a_k \sum_i z_{ki} b_i = \sum_i (\sum_k a_k z_{ki}) b_i = \sum y_i b_i,$$

gdzie $y_i = \sum_k a_k z_{ki} \in \mathfrak{m}$. Zatem $x_i = y_i \in \mathfrak{m}$ i wobec tego wszystkie współczynniki kombinacji liniowej (3.11) są równe zero w ciele $A/\mathfrak{m}$. Dowodzi to liniowej niezależności zbioru $\mathcal{B} + \mathfrak{m}F$.
Z drugiej strony jest jasne, że zbiór $\mathcal{B} + \mathfrak{m}F$ generuje przestrzeń wektorową $F/\mathfrak{m}F$, gdyż dla dowolnej warstwy $f + \mathfrak{m}F$ z przedstawienia $f = \sum x_i b_i$ dla pewnych $x_i \in A$, $b_i \in \mathcal{B}$ wynika, że

$$f + \mathfrak{m}F = \sum (x_i + \mathfrak{m})(b_i + \mathfrak{m}F).$$

Zauważmy jeszcze, że zbiory $\mathcal{B}$ i $\mathcal{B} + \mathfrak{m}F$ są równoliczne. Rzeczywiście, gdyby dla $b_1, b_2 \in \mathcal{B}$, $b_1 \neq b_2$, zachodziła równość $b_1 + \mathfrak{m}F = b_2 + \mathfrak{m}F$, to te dwa elementy zbioru $\mathcal{B} + \mathfrak{m}F$ byłyby liniowo zależne, wbrew liniowej niezależności zbioru $\mathcal{B} + \mathfrak{m}F$. Pokazaliśmy więc, że zbiór $\mathcal{B} + \mathfrak{m}F$, równoliczny z bazą $\mathcal{B}$ modułu wolnego F, jest bazą przestrzeni wektorowej $F/\mathfrak{m}F$ nad ciałem $A/\mathfrak{m}$. Każda baza modułu wolnego F jest zatem równoliczna z pewną bazą przestrzeni wektorowej $F/\mathfrak{m}F$. Ponieważ każde dwie bazy przestrzeni wektorowej są równoliczne, więc także każde dwie bazy modułu wolnego F są równoliczne. □

Inne sformułowanie twierdzenia 3.3.4 (znane jako *invariant basis property*) brzmi następująco.

WNIOSEK **3.3.5.** *Dla każdego pierścienia przemiennego A i dla każdych liczb naturalnych n, m, jeśli $A-$moduły A^n i A^m są izomorficzne, to $n = m$.*

Twierdzenie 3.3.4 pozwala wprowadzić dla modułów wolnych nad pierścieniami przemiennymi odpowiednik pojęcia wymiaru przestrzeni wektorowej.

DEFINICJA **3.3.6.** Moc dowolnej bazy modułu wolnego F nad pierścieniem przemiennym nazywamy *rangą* modułu F i oznaczamy $\mathsf{rank}\, F$.

Tak więc, na przykład, F jest $A-$modułem wolnym rangi n wtedy i tylko wtedy gdy $F \cong A^n$. Łatwo też zauważyć, że jeśli moduł wolny nad pierścieniem przemiennym jest skończenie generowany, to ma skończoną bazę i wobec tego skończoną rangę.

Uwaga 3.3.7. Niech F będzie *skończenie generowanym* modułem wolnym i niech r będzie najmniejszą z liczb elementów w zbiorach generujących moduł F. Wtedy

$$\mathsf{rank}\, F = r.$$

Rzeczywiście, baza modułu F jest zbiorem generującym moduł F i zawiera $\mathsf{rank}\, F$ elementów, zatem $r \leqslant \mathsf{rank}\, F$. Z drugiej strony, jak pokazaliśmy w dowodzie twierdzenia 3.3.4,

$$\mathsf{rank}\, F = \dim_{A/\mathfrak{m}} F/\mathfrak{m}F.$$

Jeśli $\left\{f_1, \ldots, f_r\right\}$ jest zbiorem generującym F, to zbiór $\left\{f_1 + \mathfrak{m}F, \ldots, f_r + \mathfrak{m}F\right\}$ generuje przestrzeń wektorową $F/\mathfrak{m}F$ i wobec tego $\mathsf{rank}\, F \leqslant r$.

Okazuje się, że istnieją pierścienie nieprzemienne R takie, że $R^n \cong R^m$ dla pewnych $n \neq m$. Odpowiedni przykład można znaleźć w książce N. Bourbaki, *Elements of Mathematics, Algebra* I, *Chapters* 1–3, Springer-Verlag 1989, Exercise 16, p. 384.

Na podstawie twierdzenia 3.3.3 każdy moduł jest homomorficznym obrazem pewnego modułu wolnego. Natomiast nie każdy moduł M ma homomorficzny obraz będący (niezerowym) modułem wolnym. Jeśli to się zdarza, ma to ważne konsekwencje dla struktury modułu M.

TWIERDZENIE **3.3.8.** *Jeśli F jest modułem wolnym, to każdy ciąg dokładny*

$$0 \;\to\; M' \;\xrightarrow{\;f\;}\; M \;\xrightarrow{\;g\;}\; F \;\to\; 0$$

rozszczepia się.

Dowód. Wystarczy wskazać homomorfizm rozszczepiający $\varphi : F \to M$. Niech $\mathcal{B} = \{b_i : i \in I\}$ będzie bazą modułu F. Ponieważ homomorfizm $g : M \to F$ jest epimorfizmem, dla każdego $i \in I$ istnieje element $m_i \in M$ taki, że $g(m_i) = b_i$. Przyporządkowanie $\mathcal{B} \to M, \quad b_i \mapsto m_i$ można przedłużyć do homomorfizmu modułów $\varphi : F \to M$ takiego, że

$$\varphi(b_i) = m_i, \quad i \in I.$$

Wtedy $g \circ \varphi(b_i) = g(m_i) = b_i$, skąd wynika łatwo, że $g \circ \varphi = \mathbf{1}_F$. □

Wniosek **3.3.9.** *Jeśli moduł wolny F jest homomorficznym obrazem modułu M, to F jest składnikiem prostym modułu M.*

Dowód. Na podstawie założenia istnieje rozszczepialny ciąg dokładny $M \to F \to 0$ i wobec tego z wniosku 3.2.11 wynika, że F jest składnikiem prostym modułu M. □

Twierdzenie **3.3.10.** *Niech F będzie modułem wolnym i niech $h : F \to N$ będzie homomorfizmem modułów. Wtedy dla każdego epimorfizmu $g : M \to N$ istnieje homomorfizm $\alpha : F \to M$ taki, że $h = g \circ \alpha$.*

Dowód. Rozpatrzmy diagram

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow{\scriptstyle h} & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

w którym wiersz jest dokładny (co jest równoznaczne z surjektywnością homomorfizmu g). Niech $\mathcal{B}$ będzie bazą modułu wolnego F i niech $b \in \mathcal{B}$. Wtedy element $h(b) \in N$ jest obrazem pewnego elementu $m \in M$, gdyż g jest epimorfizmem. Obieramy jakikolwiek element $m \in M$ taki, że $g(m) = h(b)$ i kładziemy $\beta(b) = m$. Wtedy odwzorowanie $\beta : \mathcal{B} \to M$ można jednoznacznie przedłużyć do homomorfizmu modułów $\alpha : F \to M$ i homomorfizm ten spełnia warunek $g(\alpha(b)) = h(b)$ dla każdego $b \in \mathcal{B}$. Wynika stąd, że $g \circ \alpha = h$. Homomorfizm α wpisuje się w diagram

$$\begin{array}{ccccc} & & F & & \\ & \alpha \nearrow & \downarrow{\scriptstyle h} & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

który wobec $g \circ \alpha = h$ jest diagramem przemiennym. □

3.4 Moduły projektywne

Dwa ostatnie twierdzenia nasuwają pytanie, czy udowodnione w nich własności modułów wolnych są własnościami charakteryzującymi moduły wolne. Należałoby więc zbadać, czy $R-$moduł P mający jedną z następujących trzech własności jest modułem wolnym. Niech P będzie $R-$modułem.

Własność (PH)[1]. Każdy diagram $R-$modułów i homomorfizmów

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow{\scriptstyle h} & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

[1]Skrót od *podnoszenie homomorfizmów*.

z dokładnym wierszem można uzupełnić do diagramu przemiennego

$$\begin{array}{ccccc} & & P & & \\ & \alpha & \downarrow h & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

Własność (CD). Każdy ciąg dokładny

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} P \to 0$$

rozszczepia się.

Własność (SP). P jest składnikiem prostym pewnego modułu wolnego.

Zauważmy, że każdy moduł wolny P ma wszystkie trzy własności (PH), (CD), (SP). Można udowodnić, że żadna z tych własności, ani nawet wszystkie trzy razem wzięte, nie implikuje, że moduł P jest wolny. Rozpoczniemy od sprawdzenia, że własności te są równoważne w tym sensie, że jeśli moduł P ma którąkolwiek z nich, to ma także dwie pozostałe.

TWIERDZENIE **3.4.1.** *Dla $R-$modułu P,*

$$\text{(PH)} \quad \Leftrightarrow \quad \text{(CD)} \quad \Leftrightarrow \quad \text{(SP)}.$$

Dowód. (PH) $\Rightarrow$ (CD). Jeśli $M \xrightarrow{g} P \to 0$ jest ciągiem dokładnym, to na podstawie własności (PH) diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \mathbf{1}_P & & \\ M & \xrightarrow{g} & P & \longrightarrow & 0 \end{array}$$

można uzupełnić do diagramu przemiennego homomorfizmem $\alpha : P \to M$ takim, że $g \circ \alpha = \mathbf{1}_P$. Zatem ciąg dokładny występujący w warunku (CD) rozszczepia się.

(CD) $\Rightarrow$ (SP). Wiemy, że moduł P jest homomorficznym obrazem pewnego modułu wolnego F, a więc istnieje ciąg dokładny

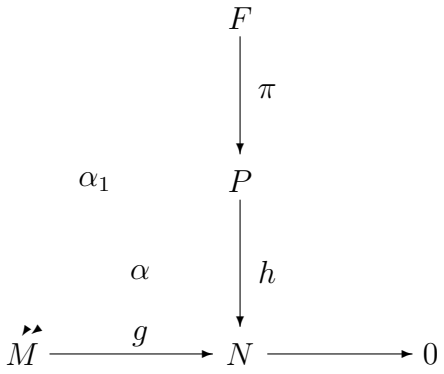
$$0 \to M' \to F \to P \to 0.$$

Ponieważ na podstawie (CD) ciąg ten rozszczepia się, moduł P jest składnikiem prostym modułu F (na podstawie wniosku 3.2.11).

(SP) $\Rightarrow$ (PH). Przypuśćmy, że $F = P \oplus Q$, gdzie F jest modułem wolnym i rozpatrzmy diagram

$$\begin{array}{ccccc} & & P & & \\ & & \downarrow h & & \\ M & \xrightarrow{g} & N & \longrightarrow & 0 \end{array}$$

występujący w warunku (PH). Niech $\pi : F \to P$ będzie rzutowaniem modułu F na składnik prosty P. Wtedy złożenie $h \circ \pi : F \to N$ jest homomorfizmem modułu wolnego F w moduł N. Na podstawie twierdzenia 3.3.10 moduł wolny F ma własność (PH), zatem istnieje homomorfizm $\alpha_1 : F \to M$ taki, że $g \circ \alpha_1 = h \circ \pi$.



Wtedy zacieśnienie α homomorfizmu α_1 do modułu P spełnia $g \circ \alpha = h$, bowiem dla $p \in P$ mamy

$$(g \circ \alpha)(p) = g(\alpha(p)) = g(\alpha_1(p)) = h(\pi(p)) = h(p).$$

A więc spełniony jest warunek (PH). □

Definicja **3.4.2.** Moduł P spełniający jeden (a więc wszystkie) z warunków (PH), (CD), (SP) nazywa się modułem *projektywnym*.

Wniosek **3.4.3.** *Każdy moduł wolny jest modułem projektywnym.*

Dowód. Moduł wolny ma własność (CD) na podstawie twierdzenia 3.3.8. □

Wniosek **3.4.4.** *Każdy moduł jest homomorficznym obrazem pewnego modułu projektywnego.*

Dowód. Wystarczy połączyć twierdzenie 3.3.3 z wnioskiem 3.4.3. □

Wniosek **3.4.5.** *Suma prosta modułów projektywnych jest modułem projektywnym.*

Dowód. Jeśli moduły projektywne P i Q są składnikami prostymi modułów wolnych F_1 i F_2, odpowiednio, to moduł $P \oplus Q$ jest składnikiem prostym modułu wolnego $F_1 \oplus F_2$. □

Wniosek **3.4.6.** *Składnik prosty modułu projektywnego jest modułem projektywnym.*

Dowód. Jeśli moduł Q jest składnikiem prostym modułu projektywnego P i P jest składnikiem prostym modułu wolnego F, to Q jest także składnikiem prostym modułu wolnego F. □

Przykład 3.4.1. Pokażemy tutaj przykład modułu projektywnego, który nie jest modułem wolnym.
Niech R_1 i R_2 będą dowolnymi pierścieniami i niech $R := R_1 \times R_2$ będzie iloczynem kartezjańskim pierścieni R_1 i R_2. Pierścień R jest wolnym $R-$modułem. Połóżmy

$$e_1 := (1_1, 0), \quad e_2 := (0, 1_2),$$

gdzie 1_1 jest jedynką R_1 oraz 1_2 jest jedynką R_2. Wtedy

$$R = R_1 \times 0 \ + \ 0 \times R_2 = Re_1 + Re_2.$$

Pierścień R traktowany jako $R-$moduł jest więc sumą dwóch ideałów głównych, a więc podmodułów modułu R. W dodatku jest to suma prosta, gdyż $Re_1 \cap Re_2 = (0, 0)$, składa się tylko z elementu zerowego pierścienia R.
$R-$moduł Re_1 jest składnikiem prostym $R-$modułu wolnego R, jest więc modułem projektywnym.
Z drugiej strony Re_1 nie ma bazy, gdyż w Re_1 każdy układ elementów jest liniowo zależny. Dla dowolnych $a_1, \ldots, a_k \in R$ elementy $a_1e_1, \ldots, a_ke_1 \in Re_1$ są liniowo zależne, gdyż

$$e_2 \cdot a_1e_1 + \cdots + e_2 \cdot a_ke_1 = 0,$$

oraz $e_2 \neq 0$. Zatem Re_1 jest $R-$modułem projektywnym ale nie jest $R-$modułem wolnym.

3.4.1 Bazy dualne modułów projektywnych

W algebrze liniowej jest dobrze znana konstrukcja bazy dualnej dla danej bazy przestrzeni wektorowej V nad ciałem K. Jeśli $\{v_1, \ldots, v_n\}$ jest bazą przestrzeni V, to rozpatrujemy funkcjonały liniowe $\varphi_i : V \to K$ takie, że

$$\varphi_i(v_j) = \delta_{ij}, \quad 1 \leqslant i, j \leqslant n,$$

gdzie $\delta_{ij} = 0$ dla $i \neq j$ oraz $\delta_{ij} = 1$ dla $i = j$. Tworzą one bazę przestrzeni dualnej $V^* = \mathsf{Hom}_K(V, K)$ (przestrzeni funkcjonałów liniowych na przestrzeni V) zwaną *bazą dualną* dla bazy $\{v_1, \ldots, v_n\}$. Zauważmy, że jeśli $v = \sum_{i=1}^n x_iv_i$, to $\varphi_i(v) = x_i$ i wobec tego mamy jednoznaczne przedstawienie

$$v = \sum_{i=1}^{n} \varphi_i(v)v_i \quad \text{dla każdego} \quad v \in V.$$

Pokażemy, że pewien wariant tej własności przestrzeni wektorowych przenosi się na moduły projektywne nad dowolnym pierścieniem przemiennym i nawet stanowi własność charakteryzującą projektywność modułu.
Dla dowolnego $R-$modułu M rozpatrujemy zbiór $M^* = \mathsf{Hom}_R(M, R)$ wszystkich funkcjonałów liniowych na M, a więc homomorfizmów $R-$modułów $M \to R$. Zbiór M^* ze zwykłym dodawaniem funkcji jest addytywną grupą abelową a jeśli R jest pierścieniem przemiennym to z działaniem zewnętrznym mnożenia funkcji przez skalary jest $R-$modułem. Nazywamy go modułem *dualnym* modułu M. W dalszym ciągu zakładamy, że R jest pierścieniem przemiennym. Można udowodnić, że jeśli

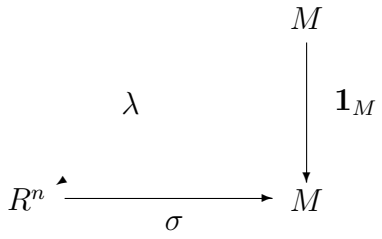
M jest modułem projektywnym, to także M^* jest modułem projektywnym (ale inaczej niż w przypadku skończenie wymiarowych przestrzeni wektorowych, M^* nie jest na ogół izomorficzny z M, nawet jeśli moduł M jest skończenie generowany).

LEMAT **3.4.7.** *Niech R będzie pierścieniem przemiennym. Dla skończenie generowanego $R-$modułu M następujące warunki są równoważne.*
(a) *M jest projektywny.*
(b) *Dla każdego zbioru generatorów $\{m_1, \ldots, m_n\}$ modułu M istnieje zbiór funkcjonałów $\{\varphi_1, \ldots, \varphi_n\} \subset M^*$ taki, że*

$$m = \sum_{i=1}^{n} \varphi_i(m) m_i \quad \text{dla każdego} \quad m \in M. \tag{3.12}$$

(c) *Istnieją zbiory generatorów $\{m_1, \ldots, m_n\}$ modułu M i funkcjonałów liniowych $\{\varphi_1, \ldots, \varphi_n\} \subset M^*$ takie, że zachodzi* (3.12).

Dowód. (a) $\Rightarrow$ (b) Z tego, że moduł M jest generowany przez n elementów wynika, że M jest homomorficznym obrazem modułu wolnego o randze n (zob. twierdzenie 3.3.3). A więc istnieje epimorfizm $\sigma : R^n \to M$ i możemy obrać σ tak, by $\sigma(e_i) = m_i$, gdzie $\{e_1, \ldots, e_n\}$ jest bazą standardową modułu wolnego R^n. Na podstawie definicji modułu projektywnego istnieje homomorfizm $\lambda : M \to R^n$ taki, że następujący diagram jest przemienny:



Rozważmy rzutowanie $\pi_i : R^n \to R$ które elementowi modułu R^n przyporządkowuje jego $i-$tą współrzędną (w bazie standardowej R^n). Zauważmy, że dla bazy standardowej $\{e_1, \ldots, e_n\}$ modułu wolnego R^n i dla $m \in M$ mamy

$$\lambda(m) = \sum_{i=1}^{n} \pi_i(\lambda(m)) e_i.$$

Odwzorowanie $\varphi_i = \pi_i \circ \lambda : M \to R$ jest funkcjonałem liniowym na M i dla każdego $m \in M$ otrzymujemy

$$\begin{aligned} m = \sigma\lambda(m) &= \sigma\Big(\sum_{i=1}^{n} \pi_i(\lambda(m)) e_i\Big) = \sum_{i=1}^{n} \pi_i(\lambda(m)) \sigma(e_i) \\ &= \sum_{i=1}^{n} \pi_i(\lambda(m)) m_i \\ &= \sum_{i=1}^{n} \varphi_i(m) m_i. \end{aligned}$$

(b) $\Rightarrow$ (c) Ta implikacja jest oczywista.
(c) $\Rightarrow$ (a) Rozpatrujemy znowu homomorfizm $\sigma : R^n \to M$ taki, że $\sigma(e_i) = m_i$, gdzie $\{e_1, \ldots, e_n\}$ jest bazą standardową modułu wolnego R^n. Ponieważ elementy m_i tworzą zbiór generatorów modułu M, homomorfizm σ jest epimorfizmem. Pokażemy, że ciąg dokładny

$$R^n \xrightarrow{\sigma} M \longrightarrow 0$$

rozszczepia się. Definiujemy homomorfizm

$$\tau : M \longrightarrow R^n, \quad \tau(m) = \sum_{i=1}^{n} \varphi_i(m) e_i$$

i dla każdego $m \in M$ obliczamy

$$\sigma\tau(m) = \sigma(\sum_{i=1}^{n} \varphi_i(m) e_i) = \sum_{i=1}^{n} \varphi_i(m)\sigma(e_i) = \sum_{i=1}^{n} \varphi_i(m) m_i = m.$$

A więc τ rozszczepia σ i wobec tego M jest składnikiem prostym R^n. To dowodzi (a). □

Zbiory elementów $\{m_1, \ldots, m_n\}$ modułu M i funkcjonałów $\{\varphi_1, \ldots, \varphi_n\}$ mające własności opisane w lemacie nazywamy *bazami dualnymi* modułów M i M^*. Oczywiście nie są to na ogół bazy modułów M i M^*, odpowiednio. Gdyby tak było, to moduły te byłyby wolne, a są tylko projektywne. Elementy $\{m_1, \ldots, m_n\}$ nie są liniowo niezależne jeśli M nie jest modułem wolnym.

Możemy teraz udowodnić dla modułów projektywnych odpowiednik elementarnego ale ważnego faktu o istnieniu funkcjonału liniowego na przestrzeni wektorowej, który nie zeruje się na wybranym wektorze. W dowodzie tego faktu wykorzystuje się zwykle istnienie bazy przestrzeni wektorowej, do której wchodzi dany wektor niezerowy.

Wniosek **3.4.8.** *Niech M będzie skończenie generowanym modułem projektywnym nad pierścieniem przemiennym. Dla każdego $m \in M$, $m \neq 0$, istnieje funkcjonał $\varphi \in M^*$ taki, że $\varphi(m) \neq 0$.*

Dowód. Ponieważ $m \neq 0$, jeden z funkcjonałów φ_i spełniających (3.12) nie znika na m. □

Wniosek 3.4.8 wykorzystuje się w dowodzie istnienia naturalnego monomorfizmu skończenie generowanego modułu projektywnego M w jego moduł bidualny $M^{**} = (M^*)^*$. Dla dowolnego $R-$modułu M określamy odwzorowanie

$$\lambda_M : M \to M^{**}, \quad \lambda_M(m) = \widehat{m},$$

gdzie $m \in M$ oraz $\widehat{m} : M^* \to R$ jest funkcjonałem liniowym na module M^* określonym następująco:

$$\widehat{m}(\varphi) = \varphi(m) \quad \text{dla} \quad \varphi \in M^*.$$

Odwzorowanie λ_M jest homomorfizmem $R-$modułów. Jeśli R jest pierścieniem przemiennym i M jest skończenie generowanym $R-$modułem projektywnym, to homomorfizm λ_M jest monomorfizmem. Rzeczywiście, jeśli $m \in \ker \lambda_M$, to $\widehat{m} = 0 \in M^{**}$. Zatem $\varphi(m) = 0$ dla każdego funkcjonału $\varphi \in M^*$. Wobec wniosku 3.4.8 wynika stąd, że $m = 0$. Zatem $\ker \lambda_M = 0$ i λ_M jest monomorfizmem.

3.4.2 Moduły projektywne nad pierścieniami lokalnymi

Przykład 3.4.1 pokazuje, że istnieją pierścienie, nad którymi nie wszystkie moduły projektywne są modułami wolnymi. Interesujące i ważne są oczywiście pierścienie nad którymi każdy moduł projektywny jest wolny. Pierścieniami takimi są, na przykład, wszystkie ciała. Rzeczywiście, jeśli K jest ciałem, to każdy $K-$ moduł jest przestrzenią wektorową i wobec tego ma bazę. Jest zatem $K-$modułem wolnym. Ten przykład jest jednak szczególny o tyle, że wszystkie $K-$moduły są wolne. Szerszą klasą pierścieni, dla których każdy skończenie generowany moduł projektywny jest wolny, są pierścienie lokalne. Przypomnijmy, że pierścień A nazywa się lokalnym, jeśli ma dokładnie jeden ideał maksymalny $\mathfrak{m}$. Wprawdzie ta definicja ma sens bez założenia przemienności pierścienia A, dla uproszczenia będziemy jednak zakładać, że pierścień lokalny A jest pierścieniem przemiennym. Rozpoczniemy od pewnego uściślenia własności definiującej moduł projektywny w przypadku modułów skończenie generowanych nad dowolnymi pierścieniami.

LEMAT **3.4.9.** *Jeśli P jest skończenie generowanym modułem projektywnym, to istnieje skończenie generowany moduł projektywny Q taki, że $P \oplus Q$ jest modułem wolnym skończonej rangi.*

Dowód. Niech N będzie modułem takim, że $F := P \oplus N$ jest wolny. Niech $\{e_i\}_{i\in I}$ będzie bazą modułu F. Zatem $F = \sum_{i\in I} Re_i$. Niech $m_1, \ldots, m_g$ będzie zbiorem generatorów modułu P. Zapiszmy każdy z generatorów m_j jako kombinację liniową elementów e_i. W tych kombinacjach liniowych wystąpi tylko skończona liczba elementów bazowych e_i. Zatem istnieje podzbiór skończony $J \subset I$ taki, że

$$P \subset \sum_{i\in J} Re_i =: F_0.$$

Zauważmy, że $F_0 = P + (N \cap F_0)$. Rzeczywiście każdy $f_0 \in F_0$ można zapisać jako $f_0 = m + n$, gdzie $m \in P$ i $n \in N$. Ale wtedy $n = f_0 - m \in F_0$. Pokazuje to, że $F_0 \subset P + (N \cap F_0)$, natomiast odwrotna inkluzja jest oczywista. Ze względu na jednoznaczność przedstawienia $f_0 = m+n$ wynika stąd, że $F_0 = P \oplus (N \cap F_0)$. Tutaj F_0 jest skończenie generowanym modułem wolnym, zatem także moduł ilorazowy F_0/P jest skończenie generowany. Ale $F_0/P \cong N \cap F_0$, zatem $N \cap F_0$ jest także skończenie generowany. Dla modułu $Q := N \cap F_0$ mamy więc

$$P \oplus Q = F_0$$

gdzie F_0 jest skończenie generowanym modułem wolnym (a więc modułem wolnym o skończonej randze) i Q jest skończenie generowanym podmodułem modułu wolnego F_0. Zatem Q jest także projektywny. □

WNIOSEK **3.4.10.** *$R-$moduł skończenie generowany P jest projektywny wtedy i tylko wtedy gdy istnieje $R-$moduł Q i liczba naturalna n takie, że*

$$P \oplus Q \cong R^n.$$

Uwaga 3.4.11. Pokażemy tutaj całkiem inną konstrukcję nazywaną *oszustwem Eilenberga* (Eilenberg's swindle). Mianowicie, jeśli P jest modułem projektywnym, to istnieje taki moduł wolny F, że

$$P \times F \cong F.$$

Jeśli bowiem $P \oplus Q$ jest modułem wolnym, to można wziąć $F = (P \oplus Q)^\infty$. Wtedy

$$F \;=\; (P \times Q)^\infty \;\cong\; P \times (Q \times P)^\infty \;\cong\; P \times F.$$

Zauważmy, że w tym przykładzie moduł wolny F nie jest skończenie generowany. Jedna z możliwych interpretacji *oszustwa* Eilenberga jest następująca. W lemacie 3.4.9, wykorzystując powyższą konstrukcję można byłoby udowodnić, że dla modułu projektywnego P istnieje moduł *wolny* F (a nie tylko projektywny) taki, że $P \oplus F$ jest modułem wolnym. Oszustwo polega na tym, że unikamy tego co najistotniejsze, mianowicie unikamy wszelkiego odwołania do skończonej generowalności rozpatrywanych modułów.

Niech teraz A będzie pierścieniem lokalnym i $\mathfrak{m}$ niech będzie jedynym ideałem maksymalnym pierścienia A. Wtedy wszystkie elementy pierścienia A nie należące do $\mathfrak{m}$ są odwracalne. Pierścień ilorazowy $A/\mathfrak{m} =: K$ jest ciałem, nazywanym ciałem reszt pierścienia lokalnego A. Warstwę $a + \mathfrak{m} \in A/\mathfrak{m}$ będziemy oznaczać $\bar{a}$. Zatem $^-\colon A \to K$ jest homomorfizmem kanonicznym. Zauważmy, że stosując homomorfizm kanoniczny do współrzędnych elementów $A-$modułu wolnego A^n otrzymamy przestrzeń wektorową K^n nad ciałem K. Ogólniej, jeśli F jest $A-$modułem wolnym z bazą $\{e_i\}$, to możemy rozpatrywać przestrzeń wektorową $\bar{F}$ nad ciałem K z bazą $\{e_i\}$ jako zbiór formalnych kombinacji liniowych elementów bazowych ze współczynnikami z ciała K. Przestrzeń $\bar{F}$ powstaje z $A-$modułu wolnego F przez zastosowanie homomorfizmu kanonicznego $^-\colon A \to K$ do współczynników kombinacji liniowych elementów bazowych modułu F. Jeśli więc $m \in F$ oraz $m = \sum a_i e_i$ to będziemy pisać $\bar{m} = \sum \bar{a}_i e_i$.

TWIERDZENIE **3.4.12.** *Jeśli A jest pierścieniem lokalnym, to każdy skończenie generowany projektywny $A-$moduł jest modułem wolnym.*

Dowód. Niech P będzie skończenie generowanym modułem projektywnym i niech Q będzie takim skończenie generowanym modułem projektywnym, że

$$F := P \oplus Q \cong A^n.$$

Niech $\{e_1, \ldots, e_n\}$ będzie bazą modułu wolnego $F = P \oplus Q$. Przez zastosowanie homomorfizmu kanonicznego do współczynników kombinacji liniowych elementów bazowych modułu F otrzymujemy przestrzeń wektorową $\bar{F} = \bar{P} \oplus \bar{Q} \cong K^n$ nad ciałem reszt pierścienia lokalnego A. W tej przestrzeni $\bar{P}$ i $\bar{Q}$ są podprzestrzeniami wektorowymi. Obierzmy $m_1, \ldots, m_\ell \in P$ oraz $m_{\ell+1}, \ldots, m_n \in Q$ tak by elementy $\bar{m}_1, \ldots, \bar{m}_\ell$ tworzyły bazę podprzestrzeni $\bar{P}$ oraz $\bar{m}_{\ell+1}, \ldots, \bar{m}_n$ tworzyły bazę podprzestrzeni $\bar{Q}$. Wtedy, wobec $\bar{F} = \bar{P} \oplus \bar{Q}$, elementy $\bar{m}_1, \ldots, \bar{m}_\ell, \bar{m}_{\ell+1}, \ldots, \bar{m}_n$ tworzą bazę przestrzeni wektorowej $\bar{F}$. Moduł wolny F ma bazę $\{e_1, \ldots, e_n\}$, mamy więc przedstawienia

$$m_i = \sum_{j=1}^{n} b_{ji} e_j, \quad i = 1, \ldots, n, \tag{3.13}$$

gdzie $B = [b_{ji}] \in M_n(A)$ jest macierzą przejścia od bazy $\{e_j\}$ modułu wolnego F do zbioru $\{m_i\}$ elementów modułu F. Zauważamy teraz, że poddając równości (3.13)

działaniu homomorfizmu kanonicznego otrzymamy

$$\bar{m}_i = \sum_{j=1}^{n} \bar{b}_{ji} e_j, \quad i = 1, \ldots, n.$$

Tym razem macierz $\bar{B} = [\bar{b}_{ji}] \in M_n(K)$ jest macierzą przejścia od bazy $\{e_1, \ldots, e_n\}$ przestrzeni $\bar{F}$ do bazy $\bar{m}_1, \ldots, \bar{m}_\ell, \bar{m}_{\ell+1}, \ldots, \bar{m}_n$ tej przestrzeni. Zatem $\det \bar{B} \neq 0$. Oczywiście $\det \bar{B} = \overline{\det B}$ i wobec tego $\det B$ nie należy do jądra $\mathfrak{m}$ homomorfizmu kanonicznego $^- : A \to K$. Ponieważ A jest pierścieniem lokalnym i $\mathfrak{m}$ jest jego jedynym ideałem maksymalnym wynika stąd, że $\det B$ jest elementem odwracalnym w pierścieniu A. Wobec tego z równości (3.13) wynika, że elementy $m_1, \ldots, m_n$ tworzą bazę modułu wolnego $F = P \oplus Q$. W szczególności, każdy element $m \in F$ ma jednoznaczne przedstawienie w postaci

$$m = a_1 m_1 + \cdots + a_\ell m_\ell + q, \quad a_i \in A,\ q \in Q.$$

Jeśli teraz $m \in P$, to w tym przedstawieniu $q = 0$ (gdyż wtedy $q \in P \cap Q = 0$) i wobec tego m ma jednoznaczne przedstawienie w postaci $m = a_1 m_1 + \cdots + a_\ell m_\ell$. Zatem $m_1, \ldots, m_\ell$ jest bazą modułu P i jest to moduł wolny. □

3.5 Bimoduły i reprezentacje pierścieni

Według definicji 3.1.1 $A-$moduł M jest addytywną grupą abelową, dla której określony jest homomorfizm $\varphi : A \to \mathsf{End}\, M$ pierścienia A w pierścień endomorfizmów $\mathsf{End}\, M$ grupy M.

Dla $a \in A$ oraz $m \in M$ obraz elementu m poprzez endomorfizm $\varphi(a)$ oznaczyliśmy $\varphi(a)(m)$, lub po prostu am. Otóż w tym miejscu pisząc znak endomorfizmu $\varphi(a)$ z *lewej* strony elementu $m \in M$ dokonaliśmy wyboru symboliki, która jest tylko jedną z dwóch możliwych.
Druga możliwość polega na pisaniu znaku endomorfizmu $\varphi(a)$ z *prawej* strony elementu $m \in M$, to znaczy $m\varphi(a)$, i oznaczaniu tego elementu ma. Wtedy na grupie abelowej M określone jest *działanie zewnętrzne* z pierścieniem skalarów A :

$$A \times M \to M, \quad (a, m) \mapsto ma$$

i ma ono następujące własności:

$$(m_1 + m_2)a = m_1 a + m_2 a \tag{3.14}$$
$$m(a_1 + a_2) = ma_1 + ma_2 \tag{3.15}$$
$$m(a_1 a_2) = (ma_1)a_2 \tag{3.16}$$
$$m1 = m \tag{3.17}$$

dla wszystkich $a, a_1, a_2 \in A,\ m_1, m_2, m \in M$. Warunki (3.1)–(3.4) charakteryzują *lewostronny* $A-$moduł M, natomiast warunki (3.9)–(3.12) charakteryzują *prawostronny* $A-$moduł M. Wszystkie pojęcia i fakty dotyczące modułów lewostronnych mają swoje naturalne odpowiedniki dla modułów prawostronnych i w związku z tym nie ma na ogół potrzeby wspominania o tej dychotomii. Jedną z wyjątkowych jest

sytuacja, gdy grupę abelową M chcemy równocześnie traktować jako lewostronny $A-$moduł i prawostronny $B-$moduł, dla różnych pierścieni A i B. Mówimy wtedy o bimodule M, lub o bimodule $A-M-B$. Dokładniej, bimodułem $A-M-B$ nazywamy addytywną grupę abelową M, która ma strukturę lewostronnego $A-$modułu i prawostronnego $B-$modułu, oraz spełniony jest następujący warunek zgodności lewo- i prawostronnego mnożenia elementów M przez elementy pierścieni A i B:

$$a(mb) = (am)b \qquad \forall\, a \in A,\ m \in M,\ b \in B. \tag{3.18}$$

Bimoduły pojawiają się w bardzo naturalny sposób w teorii reprezentacji pierścieni. Zasygnalizujemy tutaj pojęcie reprezentacji pierścienia A przez endomorfizmy $B-$modułu M.
Reprezentacją pierścienia A w pierścieniu endomorfizmów prawostronnego $B-$modułu M nazywamy każdy homomorfizm pierścieni $\varphi : A \to \mathsf{End}_B M$. Zauważmy, że każdy endomorfizm $\varphi(a) \in \mathsf{End}_B M$ jest także endomorfizmem addytywnej grupy abelowej M, zatem na podstawie definicji 3.1.1 określiliśmy na M strukturę *lewostronnego* $A-$modułu. Przypomnijmy, że lewostronne działanie zewnętrzne na M ze zbiorem skalarów A jest określone następująco:

$$am := \varphi(a)(m) \qquad \forall\, a \in A,\ m \in M.$$

Z łatwością sprawdzamy teraz, że spełniony jest warunek zgodności (3.18). Wobec $\varphi(a) \in \mathsf{End}_B M$ mamy mianowicie

$$a(mb) = \varphi(a)(mb) = \varphi(a)(m) \cdot b = (am)b$$

dla wszystkich $a \in A, m \in M, b \in B$. Tak więc każda reprezentacja pierścienia A w pierścieniu endomorfizmów prawostronnego $B-$modułu M określa na M strukturę bimodułu $A-M-B$.

Także na odwrót, jeśli mamy bimoduł $A-M-B$, to wyznacza on reprezentację pierścienia A w pierścieniu endomorfizmów prawostronnego $B-$modułu M. Dla każdego $a \in A$ rozpatrzmy bowiem odwzorowanie

$$\varphi(a) : M \to M, \qquad \varphi(a)(m) = am.$$

Z łatwością sprawdzamy, że $\varphi(a)$ jest endomorfizmem prawostronnego $B-$modułu M, zatem mamy odwzorowanie

$$\varphi : A \to \mathsf{End}_B M.$$

Ponieważ $\varphi(a_1 + a_2)(m) = (a_1 + a_2)m = a_1m + a_2m = \varphi(a_1)(m) + \varphi(a_2)(m) = (\varphi(a_1) + \varphi(a_2))(m)$ dla każdych $a_1, a_2 \in A$ oraz $m \in M$, więc

$$\varphi(a_1 + a_2) = \varphi(a_1) + \varphi(a_2) \qquad \forall\, a_1, a_2 \in A.$$

Podobnie mamy $\varphi(a_1 \cdot a_2)(m) = (a_1 \cdot a_2)m = a_1(a_2m) = \varphi(a_1)(\varphi(a_2)(m)) = (\varphi(a_1) \circ \varphi(a_2))(m)$ dla każdych $a_1, a_2 \in A$ oraz $m \in M$, skąd wynika, że

$$\varphi(a_1 \cdot a_2) = \varphi(a_1) \circ \varphi(a_2) \qquad \forall\, a_1, a_2 \in A.$$

Oczywiście mamy także $\varphi(1) = \mathbf{1}_M$.

Sprawdziliśmy więc, że odwzorowanie $\varphi : A \to \mathsf{End}_B M$ jest homomorfizmem pierścieni, jest to więc reprezentacja pierścienia A w pierścieniu endomorfizmów prawostronnego $B-$modułu M.

W ten sposób studiowanie reprezentacji pierścieni sprowadza się do studiowania struktury i własności bimodułów. Wspomnijmy jeszcze, że najbardziej klasycznym przypadkiem w teorii reprezentacji jest sytuacja, gdy M jest prawostronnym *wolnym* $B-$modułem o skończonej randze n. Wybierając w module M bazę $\mathcal{B}$ i przyporządkowując każdemu endomorfizmowi $\varphi \in \mathsf{End}_B M$ jego macierz względem bazy $\mathcal{B}$ otrzymujemy izomorfizm pierścieni $\mathsf{End}_B M \cong M_n(B)$. Możemy więc także rozpatrywać reprezentacje *macierzowe* pierścienia A nad B jako homomorfizmy $A \to M_n(B)$. Ważnym szczególnym przypadkiem są reprezentacje pierścieni w pierścieniu endomorfizmów *przestrzeni wektorowych*. Powracając do przykładu 3.1.4 zauważamy, że traktując przestrzeń wektorową V jako *prawostronny* $K-$moduł, rozpatrywany w tym przykładzie $K[X]-$moduł V_τ jest w istocie bimodułem $K[X] - V - K$.

3.6 Iloczyn tensorowy modułów

Niech M, N i P będą modułami nad pierścieniem przemiennym A. Odwzorowaniem dwuliniowym β modułów M, N w moduł P nazywamy funkcję

$$\beta : M \times N \to P$$

o własnościach

$$\beta(am + a'm', n) = a\beta(m, n) + a'\beta(m', n), \quad \beta(m, an + a'n') = a\beta(m, n) + a'\beta(m, n')$$

dla wszystkich $a, a' \in A$, $m, m' \in M$, $n, n' \in N$. Mówiąc ogólnikowo, iloczyn tensorowy $M \otimes N$ modułów M i N jest pewnym $A-$modułem, którego homomorfizmy (a więc odwzorowania *liniowe*) w moduł P są we wzajemnie jednoznacznej odpowiedniości z odwzorowaniami dwuliniowymi modułów M, N w moduł P.

Przystępujemy do konstrukcji iloczynu tensorowego modułów. Iloczyn kartezjański $M \times N$ potraktujemy jako bazę pewnego $A-$modułu wolnego, który oznaczymy $F(M \times N)$. Moduł ten składa się z wszystkich skończonych kombinacji liniowych par elementów $(m, n) \in M \times N$ ze współczynnikami z pierścienia A. W module wolnym $F(M \times N)$ rozpatrujemy podmoduł generowany przez wszystkie kombinacje liniowe elementów następujących postaci:

$$(am + a'm', n) - a(m, n) - a'(m', n), \quad (m, an + an') - a(m, n) - a'(m, n')$$

dla wszystkich $a, a' \in A$, $m, m' \in M$, $n, n' \in N$. Moduł ilorazowy $F(M \times N)/S$ nazywamy *iloczynem tensorowym* modułów M, N i oznaczamy go $M \otimes N$. Wprowadzamy także standardowe oznaczenie

$$m \otimes n := (m, n) + S.$$

Element $m \otimes n \in M \otimes N$ nazywa się tensorem prostym, natomiast elementy $M \otimes N$ nazywamy tensorami. Oczywiście tensory proste stanowią zbiór generatorów iloczynu tensorowego (gdyż pary (m, n) stanowią bazę modułu wolnego $F(M \times N)$,

a tensor prosty $m \otimes n$ jest obrazem pary (m, n) w homomorfizmie kanonicznym $F(M \times N) \to F(M \times N)/S = M \otimes N$. Zauważmy najpierw, że odwzorowanie

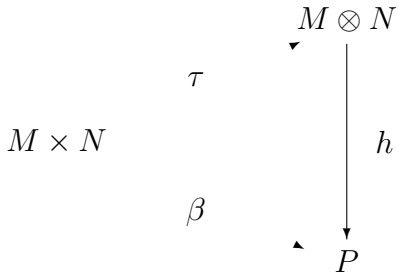
$$\tau : M \times N \to M \otimes N, \quad \tau(m, n) = m \otimes n$$

jest odwzorowaniem dwuliniowym. Rzeczywiście,

$$\begin{aligned}\tau(am + a'm', n) - a\tau(m, n) - a'\tau(m', n) &= (am + a'm') \otimes n - a(m \otimes n) - a'(m' \otimes n) \\ &= (am + a'm', n) - a(m, n) - a'(m', n) + S \\ &= 0 \in M \otimes N.\end{aligned}$$

Podobnie sprawdza się liniowość τ ze względu na drugą zmienną. Udowodnimy teraz podstawową własność iloczynu tensorowego zwaną własnością uniwersalną.

TWIERDZENIE **3.6.1.** *Niech M, N, P będą $A-$modułami. Dla dowolnego odwzorowania dwuliniowego $\beta : M \times N \to P$ istnieje dokładnie jeden homomorfizm $A-$modułów $h : M \otimes N \to P$ taki, że $h(m \otimes n) = \beta(m, n)$ dla wszystkich $m \in M, n \in N$. Następujący diagram jest więc przemienny:*



Dowód. Rozpoczynamy od określenia pomocniczego homomorfizmu

$$h' : F(M \times N) \to P,$$

który na bazie modułu wolnego $F(M \times N)$ działa następująco:

$$h'(m, n) = \beta(m, n) \quad \text{dla wszystkich} \quad (m, n) \in M \times N.$$

Zauważamy teraz, że wobec dwuliniowości odwzorowania β homomorfizm h' przeprowadza każdy generator podmodułu S na zero. Zatem $S \subset \ker h'$ i wobec tego h' indukuje homomorfizm

$$h : F(M \times N)/S \to P, \quad h(s + S) = h'(s).$$

W szczególności, jeśli $s = (m, n)$, mamy

$$h(m \otimes n) = h((m, n) + S) = h'(m, n) = \beta(m, n).$$

Pozostaje udowodnić jedyność homomorfizmu h. Zauważmy, że h spełnia warunek $h(m \otimes n) = \beta(m, n)$ dla wszystkich $m \in M, n \in N$, jest zatem jednoznacznie określony na tensorach prostych, które stanowią zbiór generatorów iloczynu tensorowego $M \otimes N$. Zatem może istnieć tylko jeden homomorfizm h o takiej własności. □

Wracając do naszej ogólnikowej zapowiedzi na temat iloczynu tensorowego możemy teraz powiedzieć nieco dokładniej, że przyporządkowując odwzorowaniu dwuliniowemu β skonstruowany w twierdzeniu homomorfizm h otrzymamy właśnie bijekcję pomiędzy odwzorowaniami dwuliniowymi $M \times N \to P$ i homomorfizmami $M \otimes N \to P$.

Konstrukcję iloczynu tensorowego dwóch modułów z łatwością przenosi się na dowolną skończoną liczbę modułów. Miejsce odwzorowań dwuliniowych zajmują odwzorowania $\ell-$liniowe,

$$M_1 \times \cdots \times M_\ell \to P,$$

które jako funkcje jednej zmiennej - przy ustalonych wartościach pozostałych zmiennych - są funkcjami $A-$liniowymi. Iloczyn tensorowy $M_1 \otimes \cdots \otimes M_\ell$ ma wtedy charakterystyczną własność uniwersalną uogólniającą twierdzenie 3.6.1 na dowolną liczbę modułów $\ell \geqslant 2$. Nietrudno sprawdzić, że konstrukcje iloczynu tensorowego dwóch i trzech modułów są ze sobą ściśle związane. Wykorzystując własność uniwersalną iloczynu tensorowego można skonstruować izomorfizm $A-$modułów $M_1 \otimes (M_2 \otimes M_3) \to M_1 \otimes M_2 \otimes M_3$ który na tensorach prostych działa następująco:

$$m_1 \otimes (m_2 \otimes m_3) \mapsto m_1 \otimes m_2 \otimes m_3.$$

3.6.1 Rozszerzenie pierścienia skalarów

Pokażemy teraz jedno z zastosowań iloczynu tensorowego modułów dające możliwość konstrukcji rozszerzenia $A-$modułu M do modułu nad rozszerzeniem A' pierścienia A. Przy tym pojęcie rozszerzenia traktujemy dość ogólnie uważając pierścień A' za rozszerzenie pierścienia A jeśli istnieje homomorfizm pierścieni $A \to A'$.

Niech $f : A \to A'$ będzie homomorfizmem pierścieni. Wtedy pierścień A' można traktować jako $A-$moduł z mnożeniem przez skalary zdefiniowanym następująco:

$$A \times A' \to A', \quad (a, a') \mapsto f(a) \cdot a'.$$

Niech M będzie $A-$modułem. Rozpatrzmy iloczyn tensorowy $A-$modułów

$$A' \otimes M =: M'.$$

Pokażemy, że M' można traktować jako $A'-$moduł z mnożeniem przez skalary z pierścienia A' określonym na tensorach prostych następująco:

$$a' \cdot (b' \otimes m) = a'b' \otimes m. \tag{3.19}$$

Formalny dowód możliwości przedłużenia tej definicji mnożenia przez skalary na dowolne tensory iloczynu $A' \otimes M$ wykorzystuje pojęcie iloczynu tensorowego trzech modułów. Rozpatrujemy odwzorowanie 3-liniowe

$$\beta : A' \times A' \times M \to A' \otimes M, \quad (a', b', m) \mapsto a'b' \otimes m.$$

Na podstawie własności uniwersalnej iloczynu tensorowego istnieje dokładnie jeden homomorfizm $A-$modułów $h : A' \otimes A' \otimes M \to A' \otimes M$ taki, że $h(a' \otimes b' \otimes m) = a'b' \otimes m$.

Identyfikujemy teraz $A' \otimes A' \otimes M$ oraz $A' \otimes (A' \otimes M)$ poprzez izomorfizm przeprowadzający $a' \otimes b' \otimes m$ na $a' \otimes (b' \otimes m)$. Homomorfizm h złożony z odwzorowaniem dwuliniowym

$$\otimes : A' \times A' \otimes M \to A' \otimes (A' \otimes M)$$

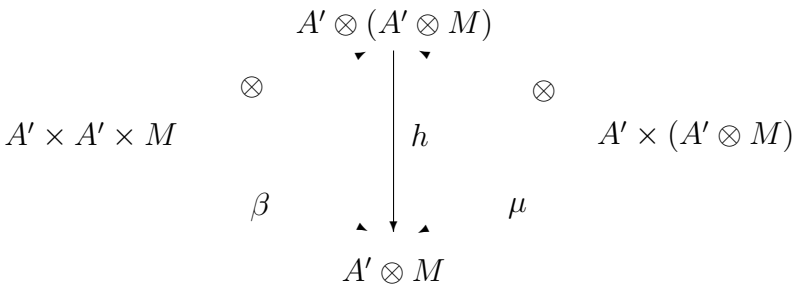
daje $A-$dwuliniowe odwzorowanie

$$\mu : A' \times (A' \otimes M) \to A' \otimes M,$$

które na szczególnych elementach $(a', (b' \otimes m)$ produktu $A' \times (A' \otimes M)$ działa następująco

$$\mu(a', (b' \otimes m)) = a'b' \otimes m.$$

Występujące w tym dowodzie moduły i odwzorowania tworzą diagram przemienny



Odwzorowanie μ pozwala traktować $A-$moduł $A' \otimes M$ jako $A'-$moduł jeśli mnożenie elementów modułu $A' \otimes M$ przez skalary z pierścienia A' określić równością

$$a' \cdot t = \mu(a', t) \quad \text{dla wszystkich} \quad a' \in A,\ t \in A' \otimes M.$$

Wystarczy sprawdzić własności (3.1) – (3.4) definicji $A-$modułu. Dla przykładu sprawdzimy pierwszą z nich i pokażemy, że

$$a' \cdot (t_1 + t_2) = a' \cdot t_1 + a' \cdot t_2$$

dla $a' \in A'$ oraz dowolnych $t_1, t_2 \in A' \otimes M$. Korzystając z dwuliniowości μ otrzymujemy

$$a' \cdot (t_1 + t_2) = \mu(a', t_1 + t_2) = \mu(a', t_1) + \mu(a', t_2) = a' \cdot t_1 + a' \cdot t_2.$$

Pokazaliśmy więc, że *dla każdego $A-$modułu M i każdego rozszerzenia A' pierścienia A iloczyn tensorowy $A-$modułów $M' = A' \otimes M$ ma naturalną strukturę $A'-$modułu.* Tak więc rozszerzeniu skalarów z A do A' towarzyszy rozszerzenie modułu M do M'.

Każdy element M' można przedstawić w postaci skończonej sumy tensorów prostych

$$\sum a'_i \otimes m_i, \quad a'_i \in A',\ m_i \in M.$$

Gdy M' traktujemy jako $A'-$moduł sumę taką możemy zapisać w postaci

$$\sum a'_i (1 \otimes m_i), \quad a'_i \in A',\ m_i \in M.$$

Zatem M' jest generowany jako $A'-$moduł przez zbiór $\{1 \otimes m : m \in M\}$.

Wprawdzie nie zawsze możemy identyfikować $A-$moduł M z pewnym $A-$podmodułem modułu M', ale jest to możliwe w sytuacji opisanej w następującym lemacie.

LEMAT **3.6.2.** *Niech M będzie $A-$modułem, i niech $f : A \to A'$ będzie homomorfizmem pierścieni. Przypuśćmy, że spełniony jest następujący warunek:*
Dla każdego niezerowego elementu $m \in M$ istnieje funkcjonał liniowy $\varphi : M \to A$ taki, że $f(\varphi(m)) \neq 0$.
Wtedy odwzorowanie $A-$liniowe

$$\tau : M \longrightarrow A' \otimes_A M, \quad m \mapsto 1 \otimes m$$

jest injektywne.

Dowód. Musimy pokazać, że $\ker \tau = 0$ a więc, że

$$0 \neq m \in M \quad \Rightarrow \quad 0 \neq 1 \otimes m \in A' \otimes M.$$

Weźmy więc $m \in M$, $m \neq 0$. Na podstawie założenia istnieje funkcjonał liniowy $\varphi : M \to A$ taki, że $f(\varphi(m)) \neq 0$. Rozpatrujemy odwzorowanie $A-$dwuliniowe

$$A' \times M \longrightarrow A', \quad (a', m) \mapsto a' f(\varphi(m)).$$

Na podstawie własności uniwersalnej iloczynu tensorowego istnieje dokładnie jedno odwzorowanie $A-$liniowe $\varphi' : A' \otimes M \to A'$ takie, że $\varphi'(a' \otimes m) = a' f(\varphi(m))$. Zatem $\varphi'(1 \otimes m) = f(\varphi(m)) \neq 0$ i wobec tego także $1 \otimes m \neq 0$. □

Jako zastosowanie lematu 3.6.2 rozpatrzmy sytuację, gdy M jest skończenie generowanym $A-$modułem projektywnym i homomorfizm $f : A \to A'$ jest włożeniem (injektywnym homomorfizmem) pierścienia A w jego rozszerzenie A'. Zatem A jest podpierścieniem pierścienia A' (jako A' można wziąć, na przykład, ciało ułamków pierścienia całkowitego A). W tej sytuacji $A-$moduł M można traktować jako $A-$podmoduł $M' = A' \otimes M$ identyfikując element $m \in M$ z tensorem prostym $1 \otimes m \in M'$. Rzeczywiście, na podstawie wniosku 3.4.8 spełnione są założenia lematu 3.6.2 i wobec tego określony w lemacie homomorfizm τ jest injektywny.

3.7 Zadania

1. Niech M będzie $A-$modułem. Udowodnić, że następujące warunki są równoważne.
(a) Istnieją podmoduły $M_1, \ldots, M_n$ modułu M takie, że $M = M_1 \oplus \cdots \oplus M_n$.
(b) Istnieją endomorfizmy $\varphi_1, \ldots, \varphi_n$ modułu M takie, że $\varphi_1 + \cdots + \varphi_n = \mathbf{1}_M$, $\varphi_i \circ \varphi_j = 0$ dla $i \neq j$ oraz $\varphi_i \circ \varphi_i = \varphi_i$ dla $i, j = 1, \ldots, n$.

2. Niech A będzie pierścieniem przemiennym i niech $a, b \in A$. Udowodnić, że następujące warunki są równoważne.

(a) $A = aA \oplus bA$ (suma prosta $A-$modułów).
(b) $ab = 0$ i istnieją $x, y \in A$ takie, że $ax + by = 1$.
(c) $ab = 0$ oraz $a + b$ jest elementem odwracalnym pierścienia A.

3. Niech $J = (X, Y) = A \cdot X + A \cdot Y$ będzie ideałem w pierścieniu $A = K[X, Y]$ wielomianów dwóch zmiennych X, Y nad ciałem K. Udowodnić, że J nie jest wolnym podmodułem $A-$modułu wolnego A.

4. Niech $R = M_2(\mathbb{R})$ będzie pierścieniem macierzy 2×2 nad ciałem $\mathbb{R}$ liczb rzeczywistych i niech

$$I = \left\{ \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix} \in R : \ x, y \in \mathbb{R} \right\}.$$

Sprawdzić, że

(a) I jest ideałem lewostronnym pierścienia R.
(b) I jest projektywnym $R-$modułem.
(c) I nie jest wolnym $R-$modułem.

5. Niech P będzie $R-$modułem projektywnym. Udowodnić, że dla każdego niezerowego elementu $p \in P$ istnieje funkcjonał liniowy φ na P taki, że $\varphi(p) \neq 0$.

6. Udowodnić, że jeśli P jest podmodułem $R-$modułu wolnego, to dla każdego niezerowego elementu $p \in P$ istnieje funkcjonał liniowy $\alpha : P \to R$ taki, że $\alpha(p) \neq 0$.

7. Niech A będzie podpierścieniem ciała K różnym od K i niech K będzie ciałem ułamków pierścienia A. Traktując K jako $A-$moduł udowodnić, że
(a) $\mathrm{Hom}_A(K, A) = 0$ (nie istnieją niezerowe funkcjonały liniowe na $A-$module K),
(b) K nie jest projektywnym $A-$modułem.

8. Niech I oraz J będą ideałami pierścienia przemiennego A.
(a) Udowodnić, że jeśli $A-$moduły A/I oraz A/J są izomorficzne, to $I = J$.
(b) Wskazać przykład pierścienia A i ideałów I, J takich, że *pierścienie* A/I oraz A/J są izomorficzne, ale $I \neq J$.

9. Udowodnić, że pierścień przemienny A jest pierścieniem całkowitym wtedy i tylko wtedy gdy ma następującą własność:
Dla każdego $A-$modułu M i dla każdego skończonego układu $m_1, \ldots, m_r \in M$, jeśli $m_1, \ldots, m_r$ są liniowo niezależne, to także $am_1, \ldots, am_r$ są liniowo niezależne dla każdego niezerowego $a \in A$.

10. Udowodnić, że jeśli nad pierścieniem przemiennym A każdy skończenie generowany $A-$moduł jest wolny, to A jest ciałem.

11. Niech A będzie pierścieniem całkowitym i niech F będzie $A-$modułem wolnym rangi 2 z bazą $\{u, v\}$. Niech $S = A(au + bv)$ będzie podmodułem wolnym rangi 1 modułu F. Udowodnić, że S jest składnikiem prostym modułu F wtedy i tylko wtedy gdy istnieją elementy $c, d \in A$ takie, że $ad - bc = 1$.

12. Niech M, N będą $R-$modułami i niech $S < M$ oraz $T < N$. Udowodnić, że

$$\frac{M \oplus N}{S \oplus T} \cong \frac{M}{S} \oplus \frac{N}{T}.$$

(Ułamki oznaczają moduły ilorazowe, $\oplus$ oznacza zewnętrzną sumę prostą (iloczyn kartezjański)).

Rozdział 4

Moduły nad pierścieniami ideałów głównych

Ostatnie zmiany 9.12.2007 r.

W tym rozdziale rozpatrujemy wyłącznie moduły nad pierścieniami przemiennymi. Przedstawimy tutaj dwa główne twierdzenia o modułach nad pierścieniami ideałów głównych: o strukturze modułów torsyjnych i o strukturze modułów skończenie generowanych. Następnie sformułujemy szczegółowo wnioski wynikające z tej teorii dla skończenie generowanych grup abelowych.

Przypomnijmy, że $A-$moduł M jest *sumą prostą* swoich podmodułów $N_1, \ldots, N_k$, jeśli każdy element $m \in M$ ma *jednoznaczne* przedstawienie w postaci

$$m = n_1 + \cdots + n_k, \quad n_i \in N_i, \quad i = 1, \ldots, k.$$

W szczególności, jeśli podmoduły N_i są cykliczne oraz N_i jest generowany przez element $m_i \in M$, to fakt, iż M jest sumą prostą podmodułów N_i oznacza dwie rzeczy: po pierwsze, każdy element $m \in M$ można przedstawić w postaci

$$m = a_1 m_1 + \cdots + a_k m_k, \quad a_1, \ldots, a_k \in A$$

oraz, po drugie, przedstawienie to jest jednoznaczne w tym sensie, że jeśli mamy inne przedstawienie

$$m = b_1 m_1 + \cdots + b_k m_k, \quad b_1, \ldots, b_k \in A,$$

to $a_1 m_1 = b_1 m_1, \ldots, a_k m_k = b_k m_k$. Nie wymagamy więc jednoznaczności współczynników $a_i \in A$ ale jednoznaczności składników $a_i m_i \in N_i$.

4.1 Moduły torsyjne

Zbadamy najpierw strukturę modułów *torsyjnych* nad całkowitymi pierścieniami ideałów głównych. Nie będziemy tu zakładać, że rozpatrywane moduły są skończenie generowane.

Definicja **4.1.1.** Niech A będzie dowolnym pierścieniem i niech M będzie $A-$modułem. Element $m \in M$ nazywamy elementem *torsyjnym*, jeśli istnieje element $a \in A,\ a \neq 0$ taki, że $am = 0$.

Moduł M nazywamy modułem *torsyjnym*, jeśli każdy element modułu M jest torsyjny.
Moduł M nazywamy modułem *ograniczonym*, jeśli istnieje element $a \in A,\ a \neq 0$ taki, że dla każdego elementu $m \in M$ mamy $am = 0$.
$A-$moduł M nazywa się modułem *beztorsyjnym*, jeśli jedynym elementem torsyjnym modułu M jest element zerowy $0 \in M$.

Przykład 4.1.1. Każdy moduł ograniczony jest modułem torsyjnym.
W grupie abelowej M element $m \in M$ jest torsyjny jeśli ma skończony rząd. Jeśli w grupie abelowej M każdy element ma rząd skończony, to M jest torsyjnym $\mathbb{Z}-$modułem. Natomiast jeśli w grupie abelowej M rzędy wszystkich elementów są wspólnie ograniczone, to M jest ograniczonym $\mathbb{Z}-$modułem. W szczególności każda skończona grupa abelowa jest ograniczonym $\mathbb{Z}-$modułem.
Przestrzenie wektorowe nie dostarczają przykładów modułów torsyjnych: każda niezerowa przestrzeń wektorowa V nad ciałem K jest beztorsyjnym $K-$modułem.
Ogólniej, każdy moduł wolny F nad pierścieniem A bez dzielników zera jest beztorsyjny.
Rzeczywiście, jeśli dla pewnego $f \in F$ oraz $0 \neq a \in A$ mamy $af = 0$, to przedstawiając f jako kombinację liniową $f = \sum x_i b_i$ elementów b_i pewnej bazy modułu F otrzymamy dla elementu af przedstawienie $0 = af = \sum a x_i b_i$. Stąd $ax_i = 0$ i wobec tego $x_i = 0$ dla każdego i. Zatem $f = 0$.
Także każdy moduł projektywny nad pierścieniem bez dzielników zera (jako składnik prosty modułu wolnego) jest beztorsyjny.
Natomiast jeśli pierścień A ma dzielniki zera, to moduł wolny nad A zawsze zawiera elementy torsyjne. Na przykład, pierścień $A = \mathbb{Z}/6\mathbb{Z}$ traktowany jako $A-$moduł jest modułem wolnym, ale element $2 + 6\mathbb{Z}$ jest elementem torsyjnym gdyż $(3 + 6\mathbb{Z})(2 + 6\mathbb{Z}) = 0 \in \mathbb{Z}/6\mathbb{Z}$.
Jeśli τ jest endomorfizmem przestrzeni wektorowej V nad ciałem K, to przestrzeń V traktowana jako $K[X]-$moduł V_τ (zob. przykład 3.1.4) jest modułem ograniczonym (a więc także torsyjnym). Rzeczywiście, jeśli $p_\tau \in K[X]$ jest wielomianem minimalnym endomorfizmu τ, to dla każdego $v \in V$ mamy

$$p_\tau v = p_\tau(\tau)(v) = 0_V(v) = 0 \in V.$$

Niech M będzie ograniczonym $A-$modułem. Zbiór

$$\mathsf{Ann}\, M = \left\{x \in A : xM = 0\right\}$$

nazywamy *anihilatorem* modułu M. Oczywiście $0 \in \mathsf{Ann}\, M$ ale wobec ograniczoności modułu M zbiór $\mathsf{Ann}\, M$ zawiera także elementy niezerowe pierścienia A. Łatwo stwierdzić, że $\mathsf{Ann}\, M$ jest niezerowym ideałem pierścienia A. Jeśli A jest pierścieniem ideałów głównych, to istnieje element $a \in A$ taki, że

$$\mathsf{Ann}\, M = (a) = aA.$$

Element a ma więc następującą własność: $aM = 0$ i jeśli $xM = 0$, to $a \mid x$. Element a nazywamy *minimalnym elementem ograniczającym* (lub *anihilującym*) modułu ograniczonego M. Element ograniczający a jest odwracalny tylko wtedy gdy M jest modułem zerowym. Zatem anihilator niezerowego modułu ograniczonego jest niezerowym ideałem właściwym pierścienia A.

Przykład 4.1.2. Jeśli τ jest endomorfizmem przestrzeni wektorowej V nad ciałem K, to wielomian minimalny p_τ endomorfizmu τ jest elementem ograniczającym $K[X]-$moduł V_τ (zob. przykład 4.1.1). Faktycznie p_τ jest *minimalnym elementem ograniczającym* $K[X]-$moduł V_τ. Jeśli bowiem $f \in K[X]$ jest jakimkolwiek wielomianem anihilującym V_τ, to dla każdego $v \in V$ mamy

$$f(\tau)(v) = fv = 0 \in V$$

i wobec tego $f(\tau) = 0_V$ jest endomorfizmem zerowym przestrzeni V. Dzielimy f przez p_τ z resztą,

$$f = gp_\tau + r,$$

gdzie $r = 0$ lub $r \neq 0$ i stopień r jest mniejszy od stopnia p_τ. Wobec $p_\tau(\tau) = 0_V$ otrzymujemy stąd $0_V = r(\tau)$, skąd wynika, że $r = 0$ (gdyż p_τ jest wielomianem najniższego stopnia zerującym się na τ). A więc $p_\tau \mid f$ oraz $\mathsf{Ann}\, V_\tau = p_\tau K[X]$.

Zanotujmy teraz bardzo prosty fakt, który okaże się użyteczny w kilku miejscach naszej dyskusji modułów torsyjnych nad pierścieniami ideałów głównych. Przyjmujemy umowę, że pierścień ideałów głównych jest automatycznie pierścieniem całkowitym (przemiennym, bez dzielników zera).

LEMAT **4.1.2.** *Niech A będzie pierścieniem ideałów głównych, $a, b \in A$,* $\mathrm{nwd}(a, b) = 1$. *Jeśli M jest $A-$modułem, $m \in M$ oraz $am = 0$, $bm = 0$, to $m = 0$.*

Dowód. Wobec naszych założeń istnieją elementy $x, y \in A$ takie, że $ax + by = 1$. Zatem

$$0 = axm + bym = 1m = m. \qquad \square$$

Następująca definicja wprowadza do rozważań podmoduły o kluczowym znaczeniu dla opisu struktury modułów torsyjnych.

DEFINICJA **4.1.3.** Niech A będzie pierścieniem ideałów głównych i niech M będzie $A-$modułem. Niech $p \in A$ będzie elementem pierwszym (nierozkładalnym) pierścienia A. Wtedy zbiór

$$T_p(M) := \{m \in M : \exists\, \ell \in \mathbb{N} \quad p^\ell m = 0\}$$

jest podmodułem modułu M. Podmoduł $T_p(M)$ nazywa się $p-$prymarną częścią modułu M lub $p-$prymarną składową modułu M.

LEMAT **4.1.4.** *Niech A będzie pierścieniem ideałów głównych i niech M będzie $A-$modułem ograniczonym. Niech $a \in A$ będzie minimalnym elementem ograniczającym modułu M i niech p będzie elementem pierwszym pierścienia A.*
(a) *Jeśli $p \nmid a$, to $T_p(M) = 0$.*
(b) *Jeśli $p \mid a$, to $T_p(M) \neq 0$.*

Dowód. (a) Niech $m \in T_p(M)$. Wtedy $p^\ell m = 0$ dla pewnej liczby naturalnej ℓ. Ponieważ $p \nmid a$ i p jest elementem pierwszym, mamy $\mathrm{nwd}(p^\ell, a) = 1$ i wobec tego na podstawie lematu 4.1.2 otrzymujemy $m = 0$.
(b) Załóżmy, że $p \mid a$. Wtedy $a = ph$ dla pewnego $h \in A$ oraz $a \nmid h$ (gdyż w przeciwnym razie p byłby elementem odwracalnym). Wobec tego h nie należy do anihilatora modułu M. Istnieje zatem taki element $m \in M$, że $m_1 := hm \neq 0$. Wtedy $pm_1 = phm = am = 0$, co oznacza, że $m_1 \in T_p(M)$. Zatem $T_p(M) \neq 0$. $\square$

A oto dwa szczególne przypadki sytuacji rozpatrywanej w lemacie 4.1.4.

Przykład 4.1.3. Jeśli M jest skończoną grupą abelową rzędu n, to n jest elementem ograniczającym grupę M, ale niekoniecznie jest *minimalnym* elementem ograniczającym M. W każdym razie minimalny element ograniczający M jest dzielnikiem liczby n i wobec tego jeśli liczba pierwsza p nie dzieli n, to nie dzieli także minimalnego elementu ograniczającego M. Wobec tego na podstawie lematu 4.1.4, jeśli liczba pierwsza p nie dzieli n, to $p-$prymarna składowa grupy M jest podgrupą zerową:

$$p \nmid n \;\Rightarrow\; T_p(M) = 0.$$

Jeśli natomiast $p \mid n$, to udowodnimy później, że $T_p(M) \neq 0$ (zob. twierdzenie 4.3.17). Wynika to wprawdzie natychmiast z twierdzenia Cauchy'ego (zob. twierdzenie 1.2.10), przypominamy jednak, że dowód twierdzenia Cauchy'ego dla grup abelowych odłożyliśmy do rozdziału 4 i właśnie jest ono konsekwencją twierdzenia 4.3.17 (zob. wniosek 4.3.18). Jeśli M jest grupą cykliczną rzędu n, to sytuacja jest prosta, gdyż n jest minimalnym elementem ograniczającym M i wobec tego dla liczby pierwszej $p \mid n$ mamy $T_p(M) \neq 0$ na podstawie lematu 4.1.4.

Przykład 4.1.4. Niech p_τ będzie wielomianem minimalnym endomorfizmu τ przestrzeni wektorowej V nad ciałem K. Wtedy p_τ jest minimalnym elementem ograniczającym $K[X]-$modułu V_τ (zob. przykład 4.1.2). Jeśli wielomian nierozkładalny $q \in K[X]$ nie dzieli p_τ, to $q-$prymarna składowa $K[X]-$modułu V_τ jest podmodułem zerowym:

$$T_q(V_\tau) = 0.$$

Natomiast jeśli wielomian nierozkładalny $q \in K[X]$ dzieli wielomian p_τ, to $q-$składowa modułu V_τ jest niezerowa. Obydwa stwierdzenia są konsekwencją lematu 4.1.4.

Zgodnie z definicją, prymarna składowa $T_p(M)$ składa się z elementów modułu M anihilowanych przez jakąkolwiek potęgę elementu pierwszego p. Pokażemy teraz, że dla modułu ograniczonego w składowej $p-$prymarnej występują tylko elementy anihilowane przez niezbyt wysokie potęgi elementu p.

LEMAT **4.1.5.** *Jeśli p^ℓ jest najwyższą potęgą elementu pierwszego p dzielącą minimalny element anihilujący a modułu ograniczonego M, to*

$$T_p(M) = \Big\{m \in M : p^\ell m = 0\Big\}.$$

Dowód. Oczywiście, zbiór $\Big\{m \in M : p^\ell m = 0\Big\}$ zawiera się w $T_p(M)$. Z drugiej strony, jeśli $m \in T_p(M)$ i $p^k m = 0$ dla pewnej liczby naturalnej $k > \ell$, to $\mathrm{nwd}(p^k, a) = p^\ell$ i wobec tego $xp^k + ya = p^\ell$ dla pewnych $x, y \in A$. Stąd $0 = xp^k m + yam = p^\ell m$. □

Przystępujemy teraz do dowodu głównego twierdzenia strukturalnego dla modułów torsyjnych.

TWIERDZENIE **4.1.6.** *Niech M będzie $A-$modułem, gdzie A jest pierścieniem ideałów głównych. Jeśli M jest modułem torsyjnym, to M jest sumą prostą wszystkich swoich składowych prymarnych:*

$$M = \bigoplus_p T_p(M),$$

gdzie p przebiega wszystkie parami niestowarzyszone elementy pierwsze pierścienia A.

Dowód. Udowodnimy najpierw, że $M = \sum_p T_p(M)$. Niech $m \in M$ oraz $am = 0$ dla $0 \neq a \in A$. Gdyby a był elementem odwracalnym, to $m = 0$ i wobec tego $m = 0 + \cdots + 0$ jest sumą elementów należących do prymarnych składowych modułu M. W przeciwnym razie

$$a = up_1^{k_1} \cdots p_r^{k_r},$$

gdzie u jest elementem odwracalnym oraz p_i są parami niestowarzyszonymi elementami pierwszymi pierścienia A. Połóżmy

$$P_i = a/p_i^{k_i}.$$

Elementy $P_1, \ldots, P_r$ są względnie pierwsze, zatem w pierścieniu (ideałów głównych) A istnieją elementy $a_1, \ldots, a_r$ takie, że

$$a_1P_1 + \cdots + a_rP_r = 1.$$

Stąd otrzymujemy

$$a_1P_1m + \cdots + a_rP_rm = m,$$

przy czym $a_iP_im \in T_{p_i}(M)$ gdyż $p_i^{k_i} \cdot a_iP_im = a_iam = 0$. Zatem $M = \sum_p T_p(M)$. Przypuśćmy teraz, że

$$m \in T_p(M) \cap \sum_{p_i} T_{p_i}(M),$$

gdzie p, p_i są parami niestowarzyszonymi elementami pierwszymi pierścienia A. Wtedy istnieją liczby naturalne $k, k_1, \ldots, k_r$ takie, że

$$p^km = 0 \quad \text{oraz} \quad p_1^{k_1} \cdots p_r^{k_r}m = 0,$$

i wobec $\operatorname{nwd}(p^k,\ p_1^{k_1} \cdots p_r^{k_r}) = 1$ z lematu 4.1.2 otrzymujemy $m = 0$. Udowodniliśmy zatem, że $T_p(M) \cap \sum_{p_i} T_{p_i}(M) = 0$ i wobec tego $M = \bigoplus_p T_p(M)$. □

4.2 Moduły skończenie generowane

Przechodzimy teraz do drugiego głównego twierdzenia o strukturze modułów nad pierścieniami ideałów głównych. Inaczej niż w przypadku modułów torsyjnych, rozpatrujemy teraz tylko moduły skończenie generowane. Twierdzenie 4.2.1 o strukturze skończenie generowanych modułów nad pierścieniami ideałów głównych udowodnimy jedynie w przypadku pierścieni euklidesowych, gdzie dowód jest nieco prostszy niż w ogólnym przypadku [1]. Przypomnijmy, że pierścień całkowity A nazywa się euklidesowy, jeśli dla A prawdziwe jest twierdzenie o dzieleniu z resztą (względem odpowiedniej normy euklidesowej N). A więc istnieje funkcja $N : A \setminus \{0\} \to \mathbb{N} \cup \{0\}$ taka, że dla każdych elementów $a, b \in A, b \neq 0$ istnieją $q, t \in A$ spełniające równość $a = bq + t$ przy czym albo $t = 0$ albo $N(t) < N(b)$. Łatwo dowodzi się, że każdy

[1] Dowód w przypadku ogólnym można znaleźć, na przykład, w książce: I. Kaplansky, *Infinite Abelian groups*, Ann Arbor 1956 (second printing), Theorem 16, p. 44.

pierścień euklidesowy jest pierścieniem ideałów głównych. Rzeczywiście, jeśli $\mathcal{I}$ jest niezerowym ideałem pierścienia euklidesowego A oraz $a \in \mathcal{I}$ jest niezerowym elementem o najmniejszej normie euklidesowej wśród elementów ideału $\mathcal{I}$, to a dzieli każdy element ideału $\mathcal{I}$, skąd wynika, że $\mathcal{I} = aA$ jest ideałem głównym. Przykładami pierścieni euklidesowych są pierścień $\mathbb{Z}$ liczb całkowitych (z normą $N(a) = |a|$) oraz pierścień $K[X]$ wielomianów jednej zmiennej nad dowolnym ciałem K (z normą $N(f) = \deg f$).

Niech M będzie modułem skończenie generowanym i niech r będzie najmniejszą z liczb elementów w zbiorach generujących moduł M. Liczbę r nazywamy *rangą* modułu M i oznaczamy ją

$$\mathsf{rank}\, M = r.$$

Zbiór generatorów modułu składający się z $r = \mathsf{rank}\, M$ elementów nazywamy *minimalnym zbiorem generatorów* modułu M. Zauważmy, że jeśli F jest skończenie generowanym modułem wolnym, to na podstawie uwagi 3.3.7 ranga $\mathsf{rank}\, F$ jest liczbą elementów w bazie modułu F.

TWIERDZENIE **4.2.1.** *Niech A będzie pierścieniem ideałów głównych i niech M będzie skończenie generowanym $A-$modułem. Wtedy M jest sumą prostą skończonego zbioru podmodułów cyklicznych. Dokładniej, jeśli $\mathsf{rank}\, M = r$, to moduł M jest sumą prostą r podmodułów cyklicznych.*

Dowód. Jak już zapowiedzieliśmy, podamy dowód w przypadku gdy A jest pierścieniem euklidesowym. Przeprowadzimy dowód indukcyjny ze względu na $\mathsf{rank}\, M$.
Jeśli $\mathsf{rank}\, M = 1$, to moduł M jest cykliczny i twierdzenie jest prawdziwe.
Załóżmy więc, że $\mathsf{rank}\, M = r > 1$ i twierdzenie jest prawdziwe dla $A-$modułów o randze $r-1$. Niech $\{m_1, \ldots, m_r\}$ będzie minimalnym zbiorem generatorów modułu M. Wtedy $M = Am_1 + \cdots + Am_r$ jest (zwykłą) sumą podmodułów cyklicznych Am_i. Jeśli dla $a_1, \ldots, a_r \in A$ równość

$$a_1 m_1 + \cdots + a_r m_r = 0 \tag{4.1}$$

zachodzi tylko wtedy gdy wszystkie jej składniki są 0 ($a_1 m_1 = \cdots = a_r m_r = 0$), to wynika stąd, że każdy element $m \in M$ ma jednoznaczne przedstawienie w postaci sumy elementów podmodułów cyklicznych $Am_1, \ldots, Am_r$ i wobec tego moduł M jest sumą prostą podmodułów cyklicznych Am_i. W tym przypadku twierdzenie jest więc prawdziwe. Pozostaje więc rozpatrzeć przypadek, gdy istnieje równość (4.1), w której nie wszystkie składniki $a_i m_i$ są równe zero. Pokażemy, że wtedy można zmodyfikować dany zbiór generatorów tak, by nowy zbiór generatorów prowadził do rozkładu modułu M na sumę prostą podmodułów cyklicznych.

Spośród wszystkich minimalnych zbiorów generatorów $\{m_1, \ldots, m_r\}$ i spośród wszystkich równości (4.1) wybieramy zbiór generatorów i równość, w której występuje *niezerowy* współczynnik a_i z najmniejszą normą euklidesową $N(a_i)$. Zmieniając ewentualnie porządek elementów w wybranym zbiorze generatorów $\{m_1, \ldots, m_r\}$ możemy zakładać, że a_1 jest niezerowym współczynnikiem o najmniejszej możliwej normie euklidesowej we wszystkich równościach postaci (4.1). Udowodnimy teraz dwa pomocnicze fakty stwierdzające własności elementu a_1.

Fakt 1. Jeśli

$$b_1 m_1 + \cdots + b_r m_r = 0 \tag{4.2}$$

dla pewnych $b_1, \ldots, b_r \in A$, to a_1 dzieli b_1.

Jeśli a_1 nie dzieli b_1, to na podstawie euklidesowości pierścienia A istnieją $q, t \in A$ takie, że

$$b_1 = a_1 q + t, \quad t \neq 0, \quad N(t) < N(a_1).$$

Wtedy z (4.1) otrzymujemy $a_1 q m_1 + \cdots + a_r q m_r = 0$ i odejmując tę równość od równości (4.2) mamy

$$(b_1 - a_1 q)m_1 + \cdots + (b_r - a_r q)m_r = 0.$$

Tutaj $b_1 - a_1 q = t \neq 0$ oraz $N(t) < N(a_1)$, co jest sprzeczne z wyborem naszego minimalnego zbioru generatorów i współczynnika a_1. A więc a_1 dzieli b_1.

Fakt 2. a_1 dzieli wszystkie współczynniki $a_2, \ldots, a_r$ występujące w wybranej równości (4.1).

Przypuśćmy, że a_1 nie dzieli a_2. Zatem istnieją $q, t \in A$ takie, że

$$a_2 = a_1 q + t, \quad t \neq 0, \quad N(t) < N(a_1).$$

Z równości (4.1) otrzymujemy wtedy

$$a_1(m_1 + q m_2) + t m_2 + a_3 m_3 + \cdots + a_r m_r = 0. \tag{4.3}$$

Zauważmy, że $\{m_1 + q m_2, m_2, \ldots, m_r\}$ jest także minimalnym zbiorem generatorów modułu M i równość (4.3), w której występuje *niezerowy* współczynnik t o normie euklidesowej mniejszej niż $N(a_1)$, jest sprzeczna z wyborem $\{m_1, \ldots, m_r\}$ oraz a_1. Zatem a_1 dzieli a_2. Zmieniając kolejność generatorów $m_2, \ldots, m_r$ pokażemy w ten sam sposób, że a_1 dzieli wszystkie pozostałe współczynniki $a_3, \ldots, a_r$.

Na podstawie Faktu 2 istnieją $q_2, \ldots, q_r \in A$ takie, że

$$a_2 = a_1 q_2, \ldots, a_r = a_1 q_r.$$

Wykorzystamy teraz elementy $q_2, \ldots, q_r \in A$ do konstrukcji następującego zbioru generatorów modułu M :

$$m_1^* = m_1 + q_2 m_2 + \cdots + q_r m_r, \; m_2, \ldots, m_r.$$

Niech $M_1 := A m_1^*$ będzie podmodułem cyklicznym generowanym przez m_1^* oraz niech $N := A m_2 + \cdots + A m_r$ będzie podmodułem generowanym przez zbiór $\{m_2, \ldots, m_r\}$. Wtedy

$$M = M_1 + N.$$

Pokażemy, że w istocie $M = M_1 \oplus N$. Wystarczy pokazać, że $M_1 \cap N = 0$. Przypuśćmy więc, że

$$m \in M_1 \cap N.$$

Wtedy istnieją $b_1, b_2, \ldots, b_r \in A$ takie, że

$$m = b_1 m_1^* = b_2 m_2 + \cdots + b_r m_r,$$

a więc także

$$b_1 m_1^* - b_2 m_2 - \cdots - b_r m_r = 0.$$

Zastępując tutaj m_1^* kombinacją liniową $m_1 + q_2 m_2 + \cdots + q_r m_r$ otrzymamy

$$b_1 m_1 + (b_1 q_2 - b_2) m_2 + \cdots + (b_1 q_r - b_r) m_r = 0.$$

Na podstawie Faktu 1 wiemy, że a_1 dzieli b_1, zatem $b_1 = q a_1$ dla pewnego $q \in A$ i w rezultacie otrzymujemy

$$\begin{aligned} m = b_1 m_1^* &= q\,(a_1 m_1^*) \\ &= q\,(a_1 m_1 + a_1 q_2 m_2 + \cdots + a_1 q_r m_r) \\ &= q\,(a_1 m_1 + a_2 m_2 + \cdots + a_r m_r) \\ &= q\,0 = 0. \end{aligned}$$

A więc $M_1 \cap N = 0$ co wraz z $M = M_1 + N$ dowodzi, że $M = M_1 \oplus N$. Ponieważ $\mathsf{rank}\, N = r - 1$, więc na podstawie założenia indukcyjnego podmoduł N jest sumą prostą $r - 1$ podmodułów cyklicznych. Zatem moduł M jest sumą prostą r podmodułów cyklicznych. □

Wniosek **4.2.2.** *Każdy skończenie generowany moduł beztorsyjny P nad pierścieniem ideałów głównych A jest $A-$modułem wolnym skończonej rangi.*

Dowód. Na podstawie twierdzenia 4.2.1, moduł P jest sumą prostą skończonej liczby r modułów cyklicznych. Natomiast moduł cykliczny Am dla $0 \neq m \in P$ jest izomorficzny z $A-$modułem A. Wynika to stąd, że P jest modułem beztorsyjnym i wobec tego $am \neq 0$ dla $0 \neq a \in A$ i $0 \neq m \in P$. Stąd $A \to Am$, $a \mapsto am$ jest izomorfizmem $A-$modułów. Zatem $P = Am_1 \oplus \cdots \oplus Am_r \cong A^r$ jest $A-$modułem wolnym rangi r. □

Wniosek **4.2.3.** *Każdy skończenie generowany moduł projektywny P nad pierścieniem ideałów głównych A jest modułem wolnym skończonej rangi.*

Dowód. Moduł projektywny P jest składnikiem prostym pewnego $A-$modułu wolnego F. Ponieważ A jest pierścieniem całkowitym, moduł F jest beztorsyjny (na podstawie przykładu 4.1.1) i wobec tego jego podmoduł P także jest beztorsyjny. Zatem P jest wolny na podstawie wniosku 4.2.2. □

Jak zauważyliśmy w przykładzie 3.1.4, jeśli τ jest endomorfizmem skończenie wymiarowej przestrzeni wektorowej V nad ciałem K, to V można traktować jako (skończenie generowany) moduł V_τ nad pierścieniem euklidesowym $K[X]$. W rozdziałach 9 i 10 zbadamy szczegółowo zastosowania twierdzeń 4.1.6 i 4.2.1 do opisu struktury modułu V_τ. Prowadzi to do dowodu istnienia postaci kanonicznych macierzy endomorfizmu τ.

4.3 Grupy abelowe

Szczególnie ważnym typem modułów są $\mathbb{Z}-$moduły, czyli grupy abelowe. Pokażemy, że twierdzenia 4.1.6 i 4.2.1 pozwalają na pełny opis struktury skończenie generowanych grup abelowych jako sum prostych grup cyklicznych. Z twierdzenia 4.2.1 wynikają następujące wnioski.

WNIOSEK **4.3.1.** *Każda skończenie generowana grupa abelowa jest sumą prostą grup cyklicznych.*

W szczególności zatem mamy następujący rezultat.

WNIOSEK **4.3.2.** *Każda skończona grupa abelowa jest sumą prostą grup cyklicznych.*

Suma prosta nieskończonych grup cyklicznych jest grupą abelową wolną. Rozpoczniemy więc od omówienia własności grup abelowych wolnych.

4.3.1 Grupy abelowe wolne

Zgodnie z definicją 3.3.1 grupa abelowa F nazywa się *grupą abelową wolną,* jeśli istnieje podzbiór $\mathcal{B} := \{b_i : i \in I\}$ grupy F taki, że każdy element $f \in F$ ma jednoznaczne przedstawienie w postaci

$$f = \sum_{i \in I} x_i b_i$$

gdzie x_i są liczbami całkowitymi oraz $x_i = 0$ dla prawie wszystkich $i \in I$. Podzbiór $\mathcal{B}$ jest wtedy bazą grupy abelowej wolnej F. Inaczej mówiąc, F jest grupą abelową wolną z bazą $\mathcal{B}$, gdy F jest sumą prostą

$$F = \bigoplus_{i \in I} F_i,$$

gdzie $F_i = \langle b_i \rangle,\ i \in I$, są nieskończonymi podgrupami cyklicznymi grupy F generowanymi przez elementy zbioru $\mathcal{B}$.

Następująca charakteryzacja grup abelowych wolnych (nazywana własnością uniwersalną) wynika z twierdzenia 3.3.2.

TWIERDZENIE **4.3.3.** *Niech F będzie grupą abelową i niech $\mathcal{B}$ będzie podzbiorem grupy F. Zbiór $\mathcal{B}$ jest bazą grupy abelowej F (i F jest grupą abelową wolną) wtedy i tylko wtedy, gdy dla dowolnej grupy abelowej M i dowolnego odwzorowania $\beta : \mathcal{B} \to M$ istnieje dokładnie jeden homomorfizm grup $h : F \to M$ taki, że $h(b) = \beta(b)$ dla każdego $b \in \mathcal{B}$.*

Przykład 4.3.1. Grupa $\mathbb{Z}$ liczb całkowitych jest grupą abelową wolną. Bazą tej grupy jest jednoelementowy podzbiór $\{1\}$. Inną bazą jest zbiór $\{-1\}$.
Addytywna grupa pierścienia wielomianów $\mathbb{Z}[X]$ jest grupą abelową wolną z bazą

$$\left\{1, X, X^2, \ldots, X^n, \ldots\right\}.$$

Zewnętrzna suma prosta (koprodukt) dowolnej rodziny nieskończonych grup cyklicznych:

$$F \cong \coprod_{i \in I} C_i, \quad C_i = \langle c_i \rangle, \quad |C_i| = \infty \tag{4.4}$$

jest grupą abelową wolną. Pokażemy mianowicie, że grupa F jest sumą prostą pewnej rodziny nieskończonych podgrup cyklicznych.
Dla każdego $j \in I$ rozpatrzmy odwzorowanie

$$\varphi_j : C_j \to F,$$

które każdemu elementowi $b_j \in C_j$ przyporządkowuje element $\varphi_j(b_j) \in F$ z wszystkimi współrzędnymi równymi zero z wyjątkiem $j-$tej współrzędnej równej b_j :

$$(\varphi_j(b_j))_i = \begin{cases} b_j & \text{dla} \quad i = j, \\ 0 & \text{dla} \quad i \neq j. \end{cases}$$

Łatwo sprawdzić, że każde odwzorowanie φ_j jest monomorfizmem grup. A więc $\varphi_j(C_j)$ jest podgrupą grupy F izomorficzną z grupą cykliczną C_j. Ponadto, każdy element grupy F ma jednoznaczne przedstawienie w postaci skończonej sumy elementów grup $\varphi_j(C_j)$. Jeśli bowiem $f = (b_i)_{i\in I} \in F$, gdzie $b_i \in C_i$, to istnieje skończony zbiór $\{i_1, \ldots, i_m\} \subseteq I$ taki, że $b_i = 0$ dla $i \notin \{i_1, \ldots, i_m\}$. Wtedy

$$f = \varphi_{i_1}(b_{i_1}) + \cdots + \varphi_{i_m}(b_{i_m}),$$

a więc $f \in F$ jest sumą obrazów swoich niezerowych współrzędnych. Stąd wynika też jednoznaczność tego przedstawienia.
Stwierdzamy zatem, że grupa F jest *wewnętrzną sumą prostą* nieskończonych podgrup cyklicznych $\varphi_i(C_i)$ grupy F,

$$F = \bigoplus_{i\in I} \varphi_i(C_i),$$

jest zatem grupą abelową wolną.

TWIERDZENIE **4.3.4.** *Każde dwie bazy grupy abelowej wolnej są równoliczne.*

Dowód. Jest to szczególny przypadek twierdzenia 3.3.4. □

DEFINICJA **4.3.5.** Moc dowolnej bazy grupy abelowej wolnej F nazywamy *rangą* grupy F i oznaczamy $\mathsf{rank}\, F$.

Przykład 4.3.2. Dla grupy abelowej wolnej $\mathbb{Z}$ mamy $\mathsf{rank}\, \mathbb{Z} = 1$.
Dla addytywnej grupy pierścienia wielomianów $\mathbb{Z}[X]$ mamy $\mathsf{rank}\, \mathbb{Z}[X] = \infty$.
Dla każdej liczby kardynalnej α istnieje grupa abelowa wolna F taka, że $\mathsf{rank}\, F = \alpha$. Wystarczy wziąć zbiór I o mocy α i położyć $F = \coprod_{i\in I} \mathbb{Z} = \mathbb{Z}^{(I)}$.

Grupa abelowa wolna jako składnik prosty grupy abelowej

Jeśli grupa abelowa M ma przedstawienie w postaci sumy prostej $M = F \oplus C$, gdzie F jest grupą abelową wolną, to opis struktury grupy M sprowadza się do opisu struktury podgrupy C, gdyż struktura składnika prostego F jest całkowicie wyjaśniona: jest on sumą prostą grup cyklicznych nieskończonych i dla pełnej charakteryzacji wystarczy wyznaczyć $\mathsf{rank}\, F$. Widzimy więc, że stwierdzenie iż grupa M ma składnik prosty będący grupą abelową wolną redukuje opis grupy do opisu pewnej podgrupy grupy M. Jak rozpoznać, że grupa M ma składnik prosty będący grupą abelową wolną? Oczywistym warunkiem koniecznym na to jest by grupa M miała homomorficzny obraz będący grupą abelową wolną (rzutowanie na składnik prosty jest epimorfizmem). Okazuje się, że ten oczywisty warunek konieczny jest także warunkiem wystarczającym.

TWIERDZENIE **4.3.6.** *Niech M będzie grupą abelową i niech G będzie grupą abelową wolną. Jeśli istnieje epimorfizm $h : M \to G$, to grupa M ma podgrupę F izomorficzną z grupą G taką, że*

$$M = F \oplus \ker h.$$

Dowód. Na podstawie twierdzenia 3.3.8 ciąg dokładny

$$0 \to \ker h \longrightarrow M \xrightarrow{h} G \to 0$$

rozszczepia się. Jeśli $\varphi : G \to M$ jest homomorfizmem rozszczepiającym, to na podstawie wniosku 3.2.9 mamy $M = \ker h \oplus \operatorname{im} \varphi$. Ponieważ $h \circ \varphi = \mathbf{1}_M$, więc φ jest monomorfizmem i wobec tego $F := \operatorname{im} \varphi$ jest podgrupą M izomorficzną z grupą G. □

A oto przykład zastosowania twierdzenia 4.3.6. Zauważmy, że poniższe twierdzenie jest szczególnym przypadkiem wniosku 4.2.2. Podamy jednak niezależny dowód oparty na twierdzeniu 4.3.6.

TWIERDZENIE **4.3.7.** *Każda podgrupa grupy abelowej wolnej jest grupą abelową wolną.*

Dowód. Rozpatrzymy tylko przypadek grup abelowych wolnych o skończonej randze i udowodnimy, że *jeśli F jest grupą abelową wolną o randze n, to każda podgrupa H grupy F jest grupą abelową wolną o randze nie większej od n*. Przeprowadzimy dowód indukcyjny ze względu na rangę grupy abelowej wolnej F. Jeśli $\mathsf{rank}\, F = 1$, to F jest nieskończoną grupą cykliczną i każda niezerowa podgrupa grupy F jest także nieskończoną grupą cykliczną, a więc grupą abelową wolną o randze 1. Natomiast podgrupę zerową możemy traktować jako grupę abelową wolną o randze 0.
Niech więc $\mathsf{rank}\, F = n > 1$ i niech twierdzenie będzie prawdziwe dla grup abelowych wolnych o randze $n-1$. Niech $\{f_1, \ldots, f_n\}$ będzie bazą grupy F i niech H będzie dowolną podgrupą grupy F. Rozpatrzmy homomorfizm grupy F na grupę cykliczną $\langle f_n \rangle$ określony następująco:

$$\pi_n : F \to \langle f_n \rangle, \quad \pi_n(x_1 f_1 + \cdots + x_n f_n) = x_n f_n,$$

dla dowolnych $x_1, \ldots, x_n \in \mathbb{Z}$. Homomorfizm π_n nazywa się *rzutowaniem* grupy F na składnik prosty $\langle f_n \rangle$. Jądrem tego rzutowania jest podgrupa $\langle f_1 \rangle \oplus \cdots \oplus \langle f_{n-1} \rangle$ grupy F, która jest grupą abelową wolną o randze $n-1$. Zacieśnienie π_n do H jest epimorfizmem grupy H na podgrupę grupy $\langle f_n \rangle$, czyli na grupę abelową wolną o randze $\leqslant 1$. Na podstawie twierdzenia 4.3.6,

$$H = F' \oplus \ker \pi_{n|H},$$

gdzie F' jest grupą abelową wolną (cykliczną nieskończoną lub zerową), natomiast $\ker \pi_{n|H}$ jest podgrupą grupy abelowej wolnej $\ker \pi_n$ o randze $n-1$. Zatem na podstawie założenia indukcyjnego $\ker \pi_{n|H}$ jest grupą abelową wolną o randze $\leqslant n-1$ i w rezultacie H jest grupą abelową wolną o randze $\leqslant n$. □

Uwaga 4.3.8. Twierdzenie 4.3.7 warto porównać z rezultatami rozdziału 3 o modułach projektywnych. Składnik prosty P grupy abelowej wolnej (wolnego $\mathbb{Z}-$modułu) F jest projektywnym $\mathbb{Z}-$modułem (na podstawie definicji 3.4.2). Jako podgrupa grupy abelowej wolnej F projektywny $\mathbb{Z}-$moduł P jest modułem wolnym (twierdzenie 4.3.7). A więc nad pierścieniem liczb całkowitych każdy moduł projektywny jest modułem wolnym. Ale twierdzenie 4.3.7 mówi znacznie więcej: nie tylko składniki proste grup abelowych wolnych są $\mathbb{Z}-$modułami wolnymi ale *każda* podgrupa grupy abelowej wolnej jest $\mathbb{Z}-$modułem wolnym.

Generatory i relacje

Znaczenie grup abelowych wolnych w teorii grup abelowych sygnalizuje następujące twierdzenie.

TWIERDZENIE **4.3.9.** *Każda grupa abelowa M jest homomorficznym obrazem pewnej grupy abelowej wolnej. Dokładniej: jeśli grupa abelowa M ma zbiór generatorów mocy α, to M jest homomorficznym obrazem grupy abelowej wolnej o randze α.*

Dowód. Jest to szczególny przypadek twierdzenia 3.3.3. □

WNIOSEK **4.3.10.** *Każda grupa abelowa M jest izomorficzna z grupą ilorazową pewnej grupy abelowej wolnej.*

Przedstawienie grupy abelowej M jako ilorazu F/H grupy abelowej wolnej F wynikające z wniosku 4.3.10 prowadzi do opisu grup abelowych za pomocą generatorów i relacji.

Niech M będzie skończenie generowaną grupą abelową. Wtedy na podstawie twierdzenia 4.3.9 istnieje grupa abelowa wolna F o skończonej randze n oraz podgrupa H grupy F takie, że $M \cong F/H$. Niech $\{f_1, \ldots, f_n\}$ będzie bazą grupy F. Na podstawie twierdzenia 4.3.7 podgrupa H jest także grupą abelową wolną i ma rangę $m \leqslant n$. Niech $\{h_1, \ldots, h_m\}$ będzie zbiorem generatorów grupy H. Mamy więc

$$h_i = a_{i1}f_1 + \cdots + a_{in}f_n, \quad i = 1, \ldots, m,$$

gdzie a_{ij} są pewnymi liczbami całkowitymi. Stąd, że elementy f_j tworzą bazę grupy F wynika, że warstwy

$$x_j = f_j + H \in F/H, \quad j = 1, \ldots, n$$

tworzą układ generatorów grupy F/H. Ponadto,

$$\sum_{j=1}^{n} a_{ij}x_j = \sum_{j=1}^{n} a_{ij}f_j + H = h_i + H = 0 \in F/H.$$

A więc

$$M \cong \langle x_1, \ldots, x_n \rangle, \quad \text{gdzie} \quad a_{i1}x_1 + \cdots + a_{in}x_n = 0 \quad \text{dla} \quad i = 1, \ldots, m.$$

To przedstawienie grupy abelowej M nazywamy przedstawieniem za pomocą generatorów i relacji.

Przykład 4.3.3. Rozpatrzymy przedstawienie grupy czwórkowej Kleina $M = V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$ za pomocą generatorów i relacji. Rozpoczynamy więc od znalezienia epimorfizmu pewnej grupy abelowej wolnej na grupę V_4. Grupa V_4 jest generowana przez dwa elementy, jest więc homomorficznym obrazem grupy abelowej wolnej o randze 2. Rzeczywiście, odwzorowanie

$$h : \mathbb{Z} \times \mathbb{Z} \to V_4, \quad (a, b) \mapsto (a \bmod 2,\ b \bmod 2)$$

jest epimorfizmem z jądrem

$$H = \ker h = \{(2a, 2b) : a, b \in \mathbb{Z}\} = \{2af_1 + 2bf_2 : a, b \in \mathbb{Z}\}$$

gdzie $f_1 = (1, 0)$, $f_2 = (0, 1)$ tworzą bazę grupy $F = \mathbb{Z} \times \mathbb{Z}$. Zatem $h_1 = 2f_1, h_2 = 2f_2$ generują podgrupę H. Dla $x_1 = f_1 + H, x_2 = f_2 + H$ mamy więc

$$V_4 \cong \langle x_1, x_2 \rangle, \quad 2x_1 = 0,\ 2x_2 = 0.$$

Uwaga 4.3.11. W rozdziale 1 dyskutowaliśmy przedstawienie grup za pomocą generatorów i relacji wynikające z faktu, że każda grupa jest homomorficznym obrazem *grupy wolnej*. Dla grup abelowych mamy zatem dwie możliwości. Pierwsza polega na przedstawieniu grupy abelowej M jako grupy ilorazowej F/H, gdzie F jest grupą abelową wolną i H jest podgrupą F, druga polega na przedstawieniu grupy abelowej M jako grupy ilorazowej F/H, gdzie F jest grupą wolną i H jest odpowiednią podgrupą normalną w F. W drugim przedstawieniu, z wyjątkiem trywialnego przypadku gdy M jest grupą cykliczną, sytuacja jest zawsze bardziej skomplikowana, gdyż grupa wolna F jest nieabelowa i podgrupa H musi zawierać relacje gwarantujące abelowość ilorazu F/H (a więc H musi zawierać komutant grupy F). Dla przykładu, kod genetyczny grupy czwórkowej Kleina, który można wyznaczyć metodą zaprezentowaną w przykładzie 1.4.5, ma postać

$$V_4 = \mathrm{gr}(\{A, B\} || A^2 = B^2 = 1,\ AB = BA).$$

4.3.2 Skończenie generowane grupy abelowe

Zauważmy najpierw, że *każda podgrupa skończenie generowanej grupy abelowej M jest skończenie generowana*. Jeśli bowiem $B < M$, to rozpatrujemy homomorfizm $h : F \to M$ pewnej grupy abelowej wolnej F o skończonej randze na grupę M (zob. twierdzenie 4.3.9). Przeciwobraz $h^{-1}(B)$ podgrupy B jest podgrupą grupy abelowej wolnej F, jest więc grupą abelową wolną o skończonej randze (twierdzenie 4.3.7). Zatem grupa $B = h(h^{-1}(B))$ jest grupą skończenie generowaną.
Zauważmy, że *skończenie generowana torsyjna grupa abelowa jest grupą skończoną*. Jeśli bowiem $\{g_1, \ldots, g_n\}$ jest zbiorem generatorów grupy torsyjnej M oraz rząd $|g_i| = r_i$, to liczba elementów dających się przedstawić w postaci $a = x_1g_1 + \cdots + x_ng_n$, gdzie $x_i \in \mathbb{Z}$, jest nie większa niż $r_1 \cdots r_n$. A więc $|M| \leqslant r_1 \cdots r_n$.
Opis struktury skończenie generowanych grup abelowych sprowadza się więc do przeanalizowania następujących przypadków:
• grupy *beztorsyjne* (nie mające elementów $\neq 0$ rzędu skończonego),
• grupy *mieszane*, zawierające zarówno elementy $\neq 0$ rzędu skończonego jak i elementy rzędu nieskończonego,
• grupy skończone.

4.3.3 Skończenie generowane beztorsyjne grupy abelowe

TWIERDZENIE **4.3.12.** *Skończenie generowana beztorsyjna grupa abelowa jest grupą abelową wolną.*

Dowód. Na podstawie wniosku 4.3.1 z twierdzenia 4.2.1, skończenie generowana grupa abelowa jest sumą prostą grup cyklicznych. Jeśli grupa ta jest beztorsyjna, to jest sumą prostą grup cyklicznych nieskończonych. Zatem jest grupą abelową wolną. □

4.3.4 Skończenie generowane mieszane grupy abelowe

Dla dowolnej grupy abelowej M podzbiór $T(M)$ wszystkich elementów rzędów skończonych jest podgrupą grupy M. Podgrupa $T(M)$ jest oczywiście grupą torsyjną.

TWIERDZENIE **4.3.13.** *Każda skończenie generowana grupa abelowa M ma rozkład na sumę prostą podgrup*

$$M = F \oplus T(M),$$

gdzie F jest grupą abelową wolną i $T(M)$ jest grupą skończoną.

Dowód. Jest to szczególny przypadek twierdzenia 4.2.1. Rzeczywiście, na podstawie tego twierdzenia grupa M jest sumą prostą skończonej liczby podgrup cyklicznych, $M = \mathbb{Z}m_1 \oplus \cdots \oplus \mathbb{Z}m_r$. Grupując oddzielnie składniki proste, które są nieskończonymi grupami cyklicznymi otrzymamy podgrupę wolną F grupy M. Suma prosta pozostałych składników, czyli skończonych grup cyklicznych, jest grupą skończoną i łatwo zauważyć, że jest ona równa $T(M)$. Zatem $M = F \oplus T(M)$.

A oto drugi dowód, niezależny od twierdzenia 4.2.1. Rozpatrzmy grupę ilorazową $G := M/T(M)$. Jest to grupa skończenie generowana, gdyż jest obrazem homomorficznym skończenie generowanej grupy M. Ponadto, jest to grupa beztorsyjna. Jeśli bowiem $n(a+T(M)) = T(M)$ dla $a \in M$ oraz $n \in \mathbb{N}$, to $na \in T(M)$, skąd wynika, że istnieje liczba $m \in \mathbb{N}$ taka, że $mna = 0$. Zatem $a \in T(M)$, oraz $a + T(M) = T(M)$. A więc jedynym elementem torsyjnym grupy G jest element zerowy.
Na podstawie twierdzenia 4.3.12 grupa G jest grupą abelową wolną. Rozpatrzmy teraz homomorfizm kanoniczny

$$h : M \to G = M/T(M),$$

którego jądrem jest grupa $T(M)$. Na podstawie twierdzenia 4.3.6 grupa M ma podgrupę F izomorficzną z G i taką, że $M = F \oplus \ker h = F \oplus T(M)$. Tutaj F jest grupą abelową wolną, gdyż jest izomorficzna z grupą abelową wolną G, natomiast grupa $T(M)$ jest podgrupą skończenie generowanej grupy abelowej M, jest więc sama skończenie generowana, a ponieważ jest torsyjna, jest grupą skończoną. □

4.3.5 Torsyjne grupy abelowe

Torsyjna grupa abelowa M jest torsyjnym $\mathbb{Z}-$modułem. Oznacza to, że każdy element grupy M ma skończony rząd. Tak jak dla wszystkich modułów nad pierścieniami ideałów głównych, dla grupy abelowej M i liczby pierwszej p symbolem $T_p(M)$

oznaczamy $p-$prymarną składową grupy M. Jest to zbiór wszystkich elementów grupy M, których rzędy są potęgami liczby p :

$$T_p(M) := \{m \in M : \exists\ \ell \in \mathbb{N} \quad p^\ell \cdot m = 0\}.$$

Jeśli grupa M nie zawiera elementów, których rzędy są potęgami liczby pierwszej p, to $T_p(M) = 0$. Następujące podstawowe twierdzenie o strukturze torsyjnych grup abelowych jest szczególnym przypadkiem twierdzenia 4.1.6.

TWIERDZENIE **4.3.14.** *Torsyjna grupa abelowa M jest sumą prostą swoich prymarnych składowych,*

$$M = \bigoplus_p T_p(M),$$

gdzie p przebiega wszystkie liczby pierwsze.

Przykład 4.3.4. Rozpatrzmy addytywną grupę $M = \mathbb{Q}/\mathbb{Z}$. Jest to grupa torsyjna gdyż dla dowolnej warstwy $q + \mathbb{Z}$ gdzie q jest liczbą wymierną o mianowniku $b \in \mathbb{N}$ mamy $b \cdot (q + \mathbb{Z}) = \mathbb{Z} = 0 \in \mathbb{Q}/\mathbb{Z}$. Grupa $\mathbb{Q}/\mathbb{Z}$ jest więc sumą prostą swoich prymarnych składowych. Zauważmy, że dla liczby pierwszej p, warstwa $q + \mathbb{Z}$ należy do składowej $T_p(\mathbb{Q}/\mathbb{Z})$ wtedy i tylko $p^\ell q \in \mathbb{Z}$ dla pewnej liczby naturalnej ℓ. A więc ma to miejsce wtedy i tylko wtedy gdy mianownik liczby q jest potęgą liczby pierwszej p. Zbiór liczb wymiernych, których mianowniki są potęgami ustalonej liczby pierwszej p oznacza się $\mathbb{Z}[\frac{1}{p}]$. Jest to podpierścień ciała liczb wymiernych (generowany przez zbiór $\mathbb{Z} \cup \left\{\frac{1}{p}\right\}$). Można także zauważyć, że $\mathbb{Z}[\frac{1}{p}]$ jest pierścieniem ułamków $S^{-1}\mathbb{Z}$ pierścienia $\mathbb{Z}$ względem zbioru multyplikatywnego $S = \left\{1, p, p^2, \ldots\right\}$ złożonego z wszystkich potęg liczby pierwszej p o wykładnikach całkowitych nieujemnych. Zbiór $\mathbb{Z}[\frac{1}{p}]$ jest zbiorem reprezentantów warstw tworzących składową $p-$prymarną $T_p(\mathbb{Q}/\mathbb{Z})$ grupy $\mathbb{Q}/\mathbb{Z}$. Traktując zbiór $\mathbb{Z}[\frac{1}{p}]$ jako grupę addytywną możemy napisać $T_p(\mathbb{Q}/\mathbb{Z}) = \mathbb{Z}[\frac{1}{p}]/\mathbb{Z}$ i wobec tego na podstawie twierdzenia 4.3.14

$$\mathbb{Q}/\mathbb{Z} = \bigoplus_p \mathbb{Z}[\tfrac{1}{p}]/\mathbb{Z}.$$

Zauważmy, że w tym przykładzie dla każdej liczby pierwszej p składowa prymarna $T_p(\mathbb{Q}/\mathbb{Z})$ jest grupą niezerową (a nawet nieskończoną).

Na podstawie twierdzenia 4.3.14 każda torsyjna grupa abelowa jest sumą prostą podgrup, w których każdy element ma rząd będący potęgą pewnej liczby pierwszej p. Dalsze badanie struktury grupy torsyjnej sprowadza się do opisu struktury prymarnych składowych $T_p(M)$. Jeśli $T_p(M)$ jest grupą skończenie generowaną, to na podstawie twierdzenia strukturalnego dla skończenie generowanych modułów nad pierścieniami euklidesowymi (zob. wniosek 4.3.1) grupa ta jest sumą prostą grup cyklicznych i znalezienie tego rozkładu opisuje zadowalająco strukturę grupy $T_p(M)$. Jeśli natomiast grupa $T_p(M)$ nie jest skończenie generowana ale jest grupą ograniczoną, to także jest sumą prostą grup cyklicznych (jest to twierdzenie Prüfera). Zajmiemy się tutaj opisem struktury grup torsyjnych w najprostszym przypadku grup skończonych.

4.3.6 Skończone grupy abelowe

Skończona grupa abelowa M jest grupą torsyjną, zatem na podstawie twierdzenia 4.3.14 mamy rozkład

$$M = \bigoplus_p T_p(M),$$

gdzie p przebiega liczby pierwsze. Tak więc pozostaje opisać strukturę skończonych grup abelowych $T_p(M)$. Na podstawie wniosku 4.3.2, każda skończona grupa abelowa jest sumą prostą grup *cyklicznych*. A więc jeśli $T_p(M) \neq 0$, to $T_p(M) = C_1 \oplus \cdots \oplus C_k$ gdzie każda grupa C_i jest niezerową grupą cykliczną. Niech c_i będzie generatorem grupy C_i. Ponieważ $c_i \in T_p(M)$, więc c_i ma rząd będący potęgą liczby pierwszej p. Zatem także C_i ma rząd będący potęgą liczby pierwszej p, powiedzmy $|C_i| = p^{s_i}$. Stąd otrzymujemy, że

$$|T_p(M)| = |C_1| \cdots |C_k| = p^{s_1+\cdots+s_k} = p^s$$

jest potęgą liczby p. Udowodniliśmy więc następujący fakt.

Wniosek **4.3.15.** *Niezerowa prymarna składowa $T_p(M)$ skończonej grupy abelowej M ma rząd będący potęgą liczby pierwszej p.*

Uwaga 4.3.16. Grupę skończoną, której rząd jest potęgą liczby pierwszej p nazywa się $p-$grupą. Udowodniliśmy więc, że $p-$prymarna składowa skończonej grupy abelowej jest $p-$grupą.

Zwracamy uwagę, że ciągle jeszcze nie jest wykluczone, że nawet dla liczby pierwszej p dzielącej rząd grupy M prymarna składowa $T_p(M)$ jest podgrupą zerową grupy M. Na podstawie przykładu 4.1.3 wiemy, że jeśli M ma rząd n oraz liczba pierwsza p nie dzieli n, to $T_p(M) = 0$. Jeśli natomiast $p \mid n$, to udowodnimy teraz, że $T_p(M) \neq 0$.

Twierdzenie **4.3.17.** *Jeśli M jest skończoną grupą abelową rzędu n,*

$$n = |M| = p_1^{n_1} \cdots p_k^{n_k},$$

gdzie $p_1, \ldots, p_k$ są różnymi liczbami pierwszymi oraz $n_i > 0$ dla $i = 1, \ldots, k$, to

$$|T_{p_i}(M)| = p_i^{n_i}, \quad i = 1, \ldots, k.$$

Dowód. Wobec rozkładu $M = \bigoplus_p T_p(M)$ mamy

$$p_1^{n_1} \cdots p_k^{n_k} = |M| = \prod_p |T_p(M)|.$$

Na podstawie wniosku 4.3.15 liczba $|T_p(M)|$ jest potęgą liczby pierwszej p (jeśli $T_p(M) = 0$, to $|T_p(M)| = p^0$). Z jednoznaczności rozkładu liczby naturalnej na iloczyn potęg liczb pierwszych wynika, że każda liczba pierwsza p występująca po prawej stronie występuje także po lewej stronie i to z tym samym wykładnikiem. Zatem $|T_{p_i}(M)| = p_i^{n_i}$ dla $i = 1, \ldots, k$. □

Przykład 4.3.5. Dla addytywnej grupy $M = \mathbb{Z}/m\mathbb{Z}$ reszt modulo $m = p_1^{n_1} \cdots p_k^{n_k}$, gdzie p_i są różnymi liczbami pierwszymi podgrupa $T_{p_i}(\mathbb{Z}/m\mathbb{Z})$ jest cykliczna (jako podgrupa grupy cyklicznej $\mathbb{Z}/m\mathbb{Z}$) i ma rząd $p_i^{n_i}$. Zatem $T_{p_i}(\mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/p_i^{n_i}\mathbb{Z}$ i wobec tego

$$\mathbb{Z}/m\mathbb{Z} = \bigoplus_{i=1}^{k} T_{p_i}(\mathbb{Z}/m\mathbb{Z}) \cong \bigoplus_{i=1}^{k} \mathbb{Z}/p_i^{n_i}\mathbb{Z}.$$

Udowodnimy teraz twierdzenie Cauchy'ego dla skończonych grup abelowych (wykorzystaliśmy je w rozdziale 1 w dowodzie twierdzenia 1.2.3).

WNIOSEK **4.3.18.** *Jeśli liczba pierwsza p dzieli rząd skończonej grupy abelowej M, to w grupie M istnieje element rzędu p.*

Dowód. Na podstawie twierdzenia 4.3.17 podgrupa $T_p(M)$ ma rząd postaci p^{n_i}, gdzie $n_i \geqslant 1$. Jest to więc nietrywialna podgrupa grupy M. Niech $a \in T_p(M)$ będzie dowolnym niezerowym elementem składowej $T_p(M)$. Wtedy rząd elementu a jest potęgą p^k liczby p, gdzie $k \geqslant 1$. A więc element $p^{k-1}\,a$ ma rząd p. □

Zauważmy jeszcze, że z twierdzenia 4.3.17 wynika, iż dla skończonej grupy abelowej M składowa prymarna $T_p(M)$ jest $p-$podgrupą Sylowa grupy M. Zatem *skończona grupa abelowa jest sumą prostą swoich $p-$podgrup Sylowa* i ponadto, *$p-$podgrupa Sylowa skończonej grupy abelowej jest sumą prostą $p-$grup cyklicznych.* A więc skończona grupa abelowa jest sumą prostą grup cyklicznych, których rzędy są potęgami liczb pierwszych.

Rozkład prymarnej składowej $T_p(M)$ na sumę prostą grup cyklicznych prowadzi do następującego izomorfizmu grup:

$$T_p(M) \cong \mathbb{Z}/p^{t_1}\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p^{t_k}\mathbb{Z},$$

gdzie można zakładać, że $t_1 \geqslant \cdots \geqslant t_k \geqslant 1$. Można udowodnić, że układ liczb $(p^{t_1}, \ldots, p^{t_k})$ jest wyznaczony jednoznacznie przez $p-$grupę $T_p(M)$. Układ ten nazywa się *typem* $p-$grupy abelowej $T_p(M)$. Dla uproszczenia oznaczeń typem $p-$grupy abelowej $T_p(M)$ nazywa się czasem układ wykładników $(t_1, \ldots, t_k)$ a liczby t_i nazywa się *niezmiennikami* grupy $T_p(M)$. Można udowodnić, że dwie skończone $p-$grupy są izomorficzne wtedy i tylko wtedy gdy mają ten sam typ. Natomiast dwie skończone grupy abelowe M i N są izomorficzne wtedy i tylko wtedy, gdy dla każdej liczby pierwszej p dzielącej rząd M lub N, typy $p-$grup $T_p(M)$ i $T_p(N)$ są równe.

4.4 Zadania

1. Niech F będzie grupą abelową wolną z bazą $\{f_1, ..., f_n\}$ i niech

$$h_i = a_{ii}f_i + \cdots + a_{in}f_n, \quad a_{ij} \in \mathbb{Z}, \quad a_{ii} > 0, \quad i = 1, \ldots, n.$$

Niech $H = \langle h_1, \ldots, h_n \rangle$ będzie podgrupą grupy F generowaną przez elementy $h_1, \ldots, h_n$. Udowodnić, że indeks $|F : H|$ podgrupy H w grupie F można obliczyć następująco:

$$|F : H| = a_{11}a_{22} \cdots a_{nn}.$$

2. Niech $\{f_1, \ldots, f_n\}$ będzie bazą grupy abelowej wolnej F i niech $a_1, \ldots, a_n$ będą liczbami naturalnymi. Udowodnić, że

$$F/\langle a_1 f_1, \ldots, a_n f_n \rangle \cong \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}.$$

3. Udowodnić, że dla dowolnych skończonych grup abelowych A, B, C zachodzi następujące *prawo skracania*:

$$A \times B \cong A \times C \;\Rightarrow\; B \cong C.$$

Wskazówka. Wykorzystać twierdzenie o istnieniu i jednoznaczności przedstawienia skończonej grupy abelowej w postaci sumy prostej $p-$grup abelowych.

Rozdział 5

Kategorie

Wersja zmieniona 22.01.2008 r.

5.1 Obiekty i morfizmy

Kategoria $\mathcal{A}$ składa się z klasy obiektów $\mathsf{Ob}(\mathcal{A})$ oraz klasy $\mathsf{Ar}(\mathcal{A})$ morfizmów. Z każdą parą obiektów $A, B \in \mathsf{Ob}(\mathcal{A})$ związany jest zbiór morfizmów

$$\mathsf{Mor}(A, B) \subseteq \mathsf{Ar}(\mathcal{A})$$

spełniający następujące warunki. Dla każdych obiektów A, B, C kategorii $\mathcal{A}$ określona jest funkcja

$$\mathsf{Mor}(B, C) \times \mathsf{Mor}(A, B) \to \mathsf{Mor}(A, C), \quad (f, g) \mapsto f \circ g$$

zwana składaniem morfizmów. Zbiory morfizmów i składanie morfizmów spełniają następujące aksjomaty: dla każdych obiektów A, B, A', B', C, D,

K1. Jeśli $A \neq A'$ lub $B \neq B'$, to $\mathsf{Mor}(A, B) \cap \mathsf{Mor}(A', B') = \emptyset$.

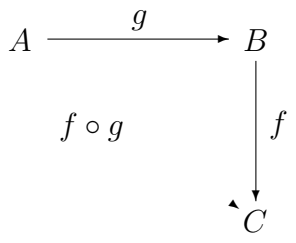
K2. Dla każdego obiektu A istnieje morfizm $\mathbf{1}_A \in \mathsf{Mor}(A, A)$ taki, że

$f \circ \mathbf{1}_A = f$ dla każdego $f \in \mathsf{Mor}(A, B)$,
$\mathbf{1}_A \circ f = f$ dla każdego $f \in \mathsf{Mor}(B, A)$.

K3. Dla każdych $h \in \mathsf{Mor}(A, B),\ g \in \mathsf{Mor}(B, C),\ f \in \mathsf{Mor}(C, D)$ zachodzi

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

Zamiast $g \in \mathsf{Mor}(A, B)$ pisze się także często $g : A \to B$ lub $A \xrightarrow{g} B$. Przy tych oznaczeniach składanie morfizmów można zapisać przy pomocy *diagramu przemiennego*



Izomorfizmem obiektów A i B nazywamy morfizm $g : A \to B$ taki, że istnieje morfizm $f : B \to A$ spełniający

$$g \circ f = \mathbf{1}_B \quad \text{i} \quad f \circ g = \mathbf{1}_A.$$

Automorfizmem obiektu A nazywamy izomorfizm $g : A \to A$. Zbiór $\mathsf{Aut}\, A$ wszystkich automorfizmów obiektu A jest grupą (ze względu na składanie morfizmów).

Przykład 5.1.1. Klasa $\mathcal{S}$ wszystkich zbiorów tworzy *kategorię zbiorów*. Zbiór morfizmów $\mathsf{Mor}(A, B)$ tworzą tu odwzorowania $f : A \to B$ zbioru A w zbiór B a operacja składania morfizmów jest superpozycją odwzorowań.
Grupa $\mathsf{Aut}\, A$ automorfizmów zbioru A w kategorii $\mathcal{S}$ jest grupą symetryczną $S(A)$ zbioru A.
Ponieważ działanie grupy G na zbiorze A utożsamiliśmy z zadaniem homomorfizmu $G \to S(A)$, sugeruje to możliwość wprowadzenia ogólnej definicji działania grupy G na dowolnym obiekcie A dowolnej kategorii $\mathcal{A}$ jako homomorfizmu $G \to \mathsf{Aut}\, A$.

Przykład 5.1.2. Klasa $\mathcal{G}$ wszystkich grup tworzy *kategorię grup*. Zbiór morfizmów $\mathsf{Mor}(A, B)$ tworzą tu homomorfizmy $f : A \to B$ grupy A w grupę B a operacja składania morfizmów jest superpozycją homomorfizmów.
Podobnie klasa $\mathcal{AG}$ wszystkich grup abelowych z homomorfizmami grup jako morfizmami, tworzy *kategorię grup abelowych*.
Również klasa $\mathcal{SG}$ wszystkich półgrup z homomorfizmami półgrup jest kategorią.
Można także rozpatrywać kategorię $\mathcal{V}(K)$ przestrzeni wektorowych nad ustalonym ciałem K, kategorię $\mathcal{R}$ pierścieni, kategorię $\mathcal{M}(R)$ modułów nad pierścieniem R, itd.

Przykłady kategorii występują nie tylko w teorii mnogości i algebrze, ale w całej matematyce. Oto przykłady pochodzące z topologii.

Przykład 5.1.3. Klasa **Top** wszystkich przestrzeni topologicznych (jako klasa obiektów) i klasa wszystkich odwzorowań ciągłych przestrzeni topologicznych (jako klasa morfizmów) tworzą kategorię.
Klasa **Metr** wszystkich przestrzeni metrycznych (jako klasa obiektów) i klasa wszystkich *kontrakcji* (jako klasa morfizmów) tworzą kategorię. Przypomnijmy, że kontrakcją przestrzeni metrycznej (X, ρ_X) w przestrzeń metryczną (Y, ρ_Y) nazywamy odwzorowanie $\varphi : X \to Y$ takie, że

$$\rho_Y(\varphi(x), \varphi(y)) \leqslant \rho_X(x, y)$$

dla każdych $x, y \in X$.

Definicja kategorii operuje pojęciem *klasy* charakterystycznym dla teorii mnogości w aksjomatycznym ujęciu pochodzącym od Bernaysa, Gödla i von Neumanna. Bez pojęcia klasy nie moglibyśmy mówić o kategorii zbiorów czy grup. Kategorię, której klasa obiektów jest zbiorem nazywa się kategorią *małą*. Wszystkie wymienione wyżej kategorie nie są małe (w potocznym języku można byłoby powiedzieć, że są niemałe ...) i nazywa się je dużymi.

We wszystkich dotychczasowych przykładach kategorii morfizmy są zwykłymi odwzorowaniami zbiorów. Oto przykład kategorii pokazujący, że natura morfizmów może być bardzo dowolna.

Przykład 5.1.4. Niech M będzie dowolnym monoidem (półgrupą z jedynką 1_M). Określimy kategorię $\mathbf{M}$ następująco. Jej jedynym obiektem jest M, to znaczy $\mathsf{Ob}(\mathbf{M}) = \{M\}$ natomiast jako zbiór morfizmów obieramy $\mathsf{Mor}(M, M) = M$, przy czym operacja składania morfizmów jest operacją mnożenia w półgrupie M.

Przykład 5.1.5. Wskażemy teraz przykład kategorii, w której obiektami są morfizmy innej kategorii. Niech więc $\mathcal{A}$ będzie kategorią. Określamy nową kategorię $\mathcal{C}$, której klasą obiektów $\mathsf{Ob}(\mathcal{C})$ jest klasa $\mathsf{Ar}(\mathcal{A})$ wszystkich morfizmów kategorii $\mathcal{A}$. Zatem obiekt kategorii $\mathcal{C}$ jest wyznaczony przez trójkę A, B, f, gdzie $A, B \in \mathsf{Ob}(\mathcal{A})$ zaś f jest morfizmem $f : A \to B$. Z każdą parą obiektów A, B kategorii $\mathcal{A}$ jest więc związany zbiór $\mathsf{Mor}(A, B)$ obiektów kategorii $\mathcal{C}$. Dla pary f, f' obiektów kategorii $\mathcal{C}$ określamy zbiór morfizmów $\mathsf{Mor}(f, f')$ w sposób następujący.
Jeśli $f : A \to B$ oraz $f' : A' \to B'$, to morfizmem μ między f i f' nazywamy każdą parę $\mu = (\varphi, \psi)$, gdzie $\varphi : A \to A'$ oraz $\psi : B \to B'$ są morfizmami kategorii $\mathcal{A}$, dla których diagram

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ A' & \xrightarrow[\ f'\ ]{} & B' \end{array}$$

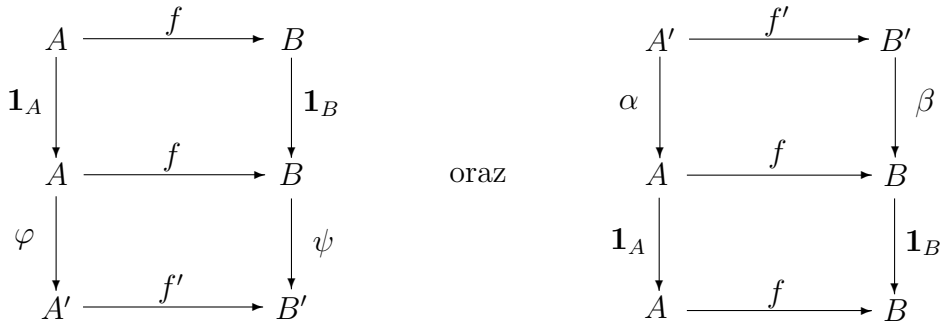
jest przemienny, to znaczy $\psi \circ f = f' \circ \varphi$ w kategorii $\mathcal{A}$.
Aby zdefiniować złożenie morfizmów $\mu = (\varphi, \psi)$ oraz $\nu = (\varphi', \psi')$ rozpatrzmy następujący diagram:

$$\begin{array}{ccc} A & \xrightarrow{\ f\ } & B \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\psi} \\ A' & \xrightarrow{\ f'\ } & B' \\ {\scriptstyle\varphi'}\downarrow & & \downarrow{\scriptstyle\psi'} \\ A'' & \xrightarrow{\ f''\ } & B'' \end{array}$$

Jest rzeczą naturalną, że złożenie $\nu \circ \mu$ określamy kładąc

$$\nu \circ \mu := (\varphi' \circ \varphi, \psi' \circ \psi).$$

Pozostaje sprawdzić, że $\mathsf{Ob}(\mathcal{C})$ i $\mathsf{Ar}(\mathcal{C})$ spełniają aksjomaty **K1**, **K2**, **K3**. Zadanie to pozostawiamy jako ćwiczenie Czytelnikowi. Zwrócimy tylko uwagę, że występujący w aksjomacie **K2** morfizm neutralny $\mathbf{1}_f$ dla obiektu $f : A \to B$ w $\mathcal{C}$ określić należy jako $\mathbf{1}_f := (\mathbf{1}_A, \mathbf{1}_B)$. Wtedy bowiem z diagramów



odczytujemy, że dla dowolnych dwóch obiektów $f : A \to B$ oraz $f' : A' \to B'$ w $\mathsf{Ob}(\mathcal{C})$ i dla dowolnych morfizmów $(\varphi, \psi) : f \to f'$ oraz $(\alpha, \beta) : f' \to f$ mamy

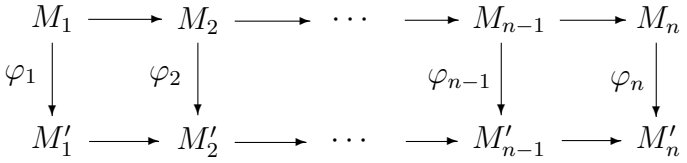
$$(\varphi, \psi) \circ (\mathbf{1}_A, \mathbf{1}_B) = (\varphi \circ \mathbf{1}_A, \psi \circ \mathbf{1}_B) = (\varphi, \psi),$$

$$(\mathbf{1}_A, \mathbf{1}_B) \circ (\alpha, \beta) = (\mathbf{1}_A \circ \alpha, \mathbf{1}_B \circ \beta) = (\alpha, \beta).$$

Istnieje wiele wariantów przykładu kategorii, której obiektami są morfizmy innej kategorii. Można, na przykład, rozważać kategorię *ciągów dokładnych* o długości n kategorii $\mathcal{M}(A)$ modułów nad pierścieniem A. Jej obiektami są $n-$członowe ciągi dokładne

$$D: \quad M_1 \longrightarrow M_2 \longrightarrow \cdots \longrightarrow M_{n-1} \longrightarrow M_n$$

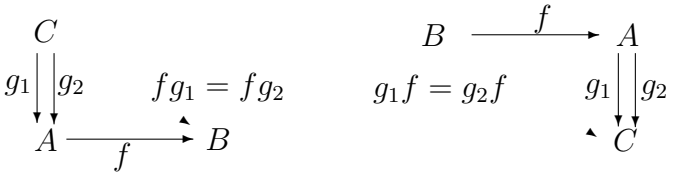
$A-$modułów i ich homomorfizmów, natomiast morfizmami pomiędzy dwoma ciągami dokładnymi D i D' są układy morfizmów $\varphi_1, \ldots, \varphi_n$ takie, że diagramy



są przemienne. Dwa inne przykłady tego typu wystąpią w dyskusji produktu i koproduktu obiektów kategorii.

5.1.1 Monomorfizmy i epimorfizmy

Definicja **5.1.1.** Morfizm $f \in \mathsf{Mor}(A, B)$ kategorii $\mathcal{A}$ nazywa się *monomorfizmem kategoryjnym*, jeśli dla każdego obiektu C tej kategorii i dla każdych morfizmów $g_1, g_2 \in \mathsf{Mor}(C, A)$ z tego, że $f \circ g_1 = f \circ g_2$ wynika $g_1 = g_2$.
Morfizm $f \in \mathsf{Mor}(B, A)$ kategorii $\mathcal{A}$ nazywa się *epimorfizmem kategoryjnym*, jeśli dla każdego obiektu C tej kategorii i dla każdych morfizmów $g_1, g_2 \in \mathsf{Mor}(A, C)$ z tego, że $g_1 \circ f = g_2 \circ f$ wynika $g_1 = g_2$.



Definicja monomorfizmu i epimorfizmu kategoryjnego jest typowym dla teorii kategorii przykładem *bezelementowego* traktowania obiektów i morfizmów kategorii. Jest to konieczność podyktowana tym, że obiekty kategorii nie muszą być zbiorami a morfizmy nie muszą być funkcjami działającymi na zbiorach (zob. przykład 5.1.5). Drugą charakterystyczną cechą tej definicji jest jej dualność: definicja epimorfizmu powstaje z definicji monomorfizmu przez odwrócenie kierunku wszystkich morfizmów (strzałek).

Dla uchwycenia zasięgu pojęć monomorfizmu i epimorfizmu kategoryjnego jest wygodnie wprowadzić pojęcie kategorii konkretnej. Z grubsza mówiąc, kategorię $\mathcal{A}$ nazywamy *konkretną* jeśli jej morfizmy $f : A \to B$ są *funkcjami* a składanie morfizmów jest składaniem (superpozycją) funkcji. Tutaj obiekty A i B nie są na ogół zbiorami (na przykład w kategorii grup są grupami), potrzebne jest zatem wyjaśnienie co rozumiemy przez *funkcję* z obiektu A do obiektu B. Posłużymy się tylko intuicją podyktowaną przykładem kategorii grup. Wprawdzie morfizm $f : A \to B$ jest tu *homomorfizmem* grup, ale f można też traktować jako funkcję określoną na *zbiorze* elementów grupy A w *zbiór* elementów grupy B (w ten sposób rozróżniamy *zbiór* A od *grupy* A). [1] Kategoriami konkretnymi są wszystkie kategorie z przykładów 5.1.1 – 5.1.3.

W kategorii konkretnej każdy morfizm injektywny jest monomorfizmem kategoryjnym a każdy morfizm surjektywny jest epimorfizmem kategoryjnym. Jeśli bowiem $f : A \to B$ jest morfizmem injektywnym oraz dla pewnego obiektu C tej kategorii i dla pewnych morfizmów $g_1, g_2 \in \mathsf{Mor}(C, A)$ mamy $f \circ g_1 = f \circ g_2$, to dla dowolnego elementu $c \in C$ mamy $f(g_1(c)) = f(g_2(c))$, skąd wobec injektywności f otrzymujemy $g_1(c) = g_2(c)$ dla każdego $c \in C$. Wobec tego $g_1 = g_2$, co dowodzi, że f jest monomorfizmem kategoryjnym.
Podobnie, jeśli $f : B \to A$ jest morfizmem surjektywnym oraz dla pewnego obiektu C tej kategorii i dla pewnych morfizmów $g_1, g_2 \in \mathsf{Mor}(A, C)$ mamy $g_1 \circ f = g_2 \circ f$, to dla dowolnego elementu $b \in B$ mamy $g_1(f(b)) = g_2(f(b))$, skąd wobec surjektywności f otrzymujemy $g_1(a) = g_2(a)$ dla każdego $a \in A$. Wobec tego $g_1 = g_2$, co dowodzi, że f jest epimorfizmem kategoryjnym.

Można pokazać, że w niektórych kategoriach konkretnych także na odwrót, każdy monomorfizm kategoryjny jest odwzorowaniem injektywnym i każdy epimorfizm kategoryjny jest odwzorowaniem surjektywnym. Ma to miejsce, na przykład, w kategoriach zbiorów, przestrzeni topologicznych, modułów i grup. Niestety, nie jest to prawdą w innych kategoriach konkretnych.

Przykład 5.1.6. Homomorfizm kanoniczny $\kappa : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ jest monomorfizmem kategoryjnym w kategorii grup abelowych podzielnych, natomiast nie jest oczywiście odwzorowaniem injektywnym. Aby sprawdzić według definicji 5.1.1, że homomorfizm κ jest monomorfizmem kategoryjnym weźmy dowolną grupę abelową podzielną C i dwa dowolne homomorfizmy $g_1, g_2 : C \to \mathbb{Q}$ takie, że $\kappa \circ g_1 = \kappa \circ g_2$. Zatem dla każdego $c \in C$ mamy

$$g_1(c) + \mathbb{Z} = (\kappa \circ g_1)(c) = (\kappa \circ g_2)(c) = g_2(c) + \mathbb{Z}.$$

[1] Czytelnika zainteresowanego kompletną definicją kategorii konkretnej odsyłamy do książki Z. Semadeniego i A. Wiwegera *Wstęp do teorii kategorii i funktorów*, PWN Warszawa 1972, str. 38.

Stąd wynika, że $g_1(c) - g_2(c) \in \mathbb{Z}$ dla każdego elementu $c \in C$. Ustalmy teraz $c \in C$. Ponieważ C jest grupą podzielną, dla każdej liczby naturalnej n istnieje element $b \in C$ taki, że $c = nb$. Wobec tego

$$g_1(c) - g_2(c) = n(g_1(b) - g_2(b)), \quad g_1(c) - g_2(c),\ g_1(b) - g_2(b) \in \mathbb{Z}$$

dla każdej liczby naturalnej n. Wynika stąd, że liczba całkowita $g_1(c) - g_2(c)$ jest podzielna przez każdą liczbę naturalną n. Zatem $g_1(c) - g_2(c) = 0$ dla każdego $c \in C$, czyli $g_1 = g_2$. Według definicji 5.1.1 homomorfizm kanoniczny $\kappa : \mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ jest monomorfizmem kategoryjnym w kategorii grup abelowych podzielnych.

Przykład 5.1.7. Homomorfizm pierścieni $f : \mathbb{Z} \to \mathbb{Q}$ jest epimorfizmem kategoryjnym w kategorii pierścieni, ale nie jest odwzorowaniem surjektywnym. Przypuśćmy bowiem, że dla pewnego pierścienia C i homomorfizmów $g_1, g_2 \in \mathsf{Mor}(\mathbb{Q}, C)$ mamy $g_1 \circ f = g_2 \circ f$. Wtedy dla każdej liczby całkowitej a mamy

$$g_1(a) = g_1(f(a)) = (g_1 \circ f)(a) = (g_2 \circ f)(a) = g_2(f(a)) = g_2(a).$$

Zatem homomorfizmy $g_1, g_2 : \mathbb{Q} \to C$ działają tak samo na liczbach całkowitych. Stąd wynika, że działają tak samo na liczbach wymiernych. Mianowicie, jeśli $a \in \mathbb{Z}$ oraz $a \neq 0$, to $g_i(a) \cdot g_i(1/a) = g_i(1) = 1$, zatem $g_i(1/a) = 1/g_i(a)$. Stąd dla dowolnej liczby całkowitej b mamy

$$g_i\Big(\frac{b}{a}\Big) = g_i(b) \cdot g_i\Big(\frac{1}{a}\Big) = \frac{g_i(b)}{g_i(a)}.$$

A więc $g_1 = g_2$.

W związku z tą sytuacją w niektórych kategoriach konkretnych należałoby rozróżniać *monomorfizmy* i *kategoryjne monomorfizmy*. Pierwsze są injektywnymi homomorfizmami, drugie monomorfizmami w sensie definicji 5.1.1. Podobnie, *epimorfizm* jest surjektywnym homomorfizmem, natomiast *kategoryjny epimorfizm* jest morfizmem spełniającym warunek definicji 5.1.1.

5.2 Iloczyny obiektów kategorii

Iloczyn kartezjański dwóch zbiorów A i B definiuje się jako zbiór par uporządkowanych (a, b), gdzie $a \in A$ oraz $b \in B$. Ta definicja odwołuje się więc bezpośrednio do elementów zbiorów A i B i określa zbiór $K = A \times B$ poprzez wskazanie elementów tego zbioru. Na pierwszy rzut oka trudno sobie wyobrazić charakteryzację iloczynu kartezjańskiego zbiorów, która nie odwołuje się w ogóle do elementów zbiorów. Jeśli jednak interesuje nas nie tyle natura elementów zbioru K ale jego własności w zestawieniu z innymi zbiorami, to taki opis w języku zbiorów i odwzorowań zbiorów jest możliwy i jest to właśnie opis w języku kategorii zbiorów.
Wraz z iloczynem $K = A \times B$ rozpatrzmy rzutowania

$$\rho_1 : K \to A, \quad \rho_1(a, b) = a \quad \text{oraz} \quad \rho_2 : K \to B, \quad \rho_2(a, b) = b.$$

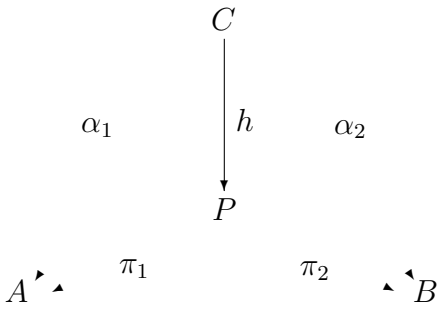
Jeśli teraz weźmiemy dowolną trójkę (C, α_1, α_2) składającą się ze zbioru C i odwzorowań $\alpha_1 : C \to A$ oraz $\alpha_2 : C \to B$, to trójka (K, ρ_1, ρ_2) ma następującą charakterystyczną własność:

istnieje dokładnie jedno odwzorowanie $g : C \to K$ takie, że $\rho_1 \circ g = \alpha_1$, $\rho_2 \circ g = \alpha_2$.

Jeśli odwzorowanie g o takiej własności istnieje, to dla każdego $c \in C$ mamy $\rho_i(g(c)) = \alpha_i(c)$ i z definicji rzutowań ρ_i wynika, że $g(c) = (\alpha_1(c), \alpha_2(c))$. A więc jeśli g istnieje, to jest jedyne. Z drugiej strony, odwzorowanie $g : C \to P$ określone wzorem $g(c) = (\alpha_1(c), \alpha_2(c))$ dla każdego $c \in C$ spełnia $\rho_i(g(c)) = \rho_i(\alpha_1(c), \alpha_2(c)) = \alpha_i(c)$.

Tę własność iloczynu kartezjańskiego wykorzystamy dla wprowadzenia pojęcia produktu dwóch obiektów dowolnej kategorii $\mathcal{A}$.

DEFINICJA **5.2.1.** *Iloczynem* lub *produktem* obiektów A i B kategorii $\mathcal{A}$ nazywamy trójkę (P, π_1, π_2), gdzie P jest obiektem kategorii $\mathcal{A}$ natomiast $\pi_1 : P \to A$ oraz $\pi_2 : P \to B$ są morfizmami kategorii $\mathcal{A}$, takimi, że dla każdego obiektu C kategorii $\mathcal{A}$ i każdych morfizmów $\alpha_1 : C \to A$, $\alpha_2 : C \to B$ istnieje dokładnie jeden morfizm $h : C \to P$ taki, że następujący diagram jest przemienny:



Przykład 5.2.1. Objaśnijmy najpierw czym jest produkt dwóch obiektów w kategorii zbiorów. Dla zbiorów A i B rozpatrujemy iloczyn kartezjański $K = A \times B$ oraz rzutowania $\rho_1 : K \to A$, $\rho_2 : K \to B$ oraz produkt (P, π_1, π_2) zbiorów A, B traktowanych jako obiekty w kategorii zbiorów. Na podstawie definicji produktu istnieje dokładnie jedno odwzorowanie $h : K \to P$ takie, że $\pi_i \circ h = \rho_i$, $i = 1, 2$. Wobec tego dla każdej pary $(a, b) \in K$ mamy

$$\pi_1 h(a, b) = \rho_1(a, b) = a, \quad \pi_2 h(a, b) = \rho_2(a, b) = b. \tag{5.1}$$

Z drugiej strony na podstawie własności iloczynu kartezjańskiego istnieje odwzorowanie $g : P \to K$ takie, że $\rho_i \circ g = \pi_i$, $i = 1, 2$. Zatem dla dowolnego $x \in P$ mamy

$$\rho_1 g(x) = \pi_1(x), \quad \rho_2 g(x) = \pi_2(x)$$

i wobec tego mamy

$$g(x) = (\pi_1(x), \pi_2(x)).$$

Stąd też wynika, że dla każdego elementu $(a, b) \in K$ mamy

$$g \circ h\,(a, b) = g(h(a, b)) = (\pi_1(h(a, b)), \pi_2(h(a, b))) = (a, b),$$

gdzie ostatnia równość jest konsekwencją (5.1). Zatem złożenie odwzorowań $g \circ h$ jest identycznością na zbiorze K, skąd wynika, że $h : K \to P$ jest odwzorowaniem

injektywnym. Pokażemy teraz, że także złożenie $h \circ g$ jest identycznością na zbiorze P, a więc dla każdego $x \in P$,

$$h(\pi_1(x), \pi_2(x)) = h \circ g\,(x) = x.$$

Przypuśćmy, że $h(g(x)) = y$ dla pewnego $y \in P$. Wtedy

$$g(x) = (g \circ h)(g(x)) = g(h(g(x))) = g(y),$$

a więc także

$$(\pi_1(x), \pi_2(x)) = (\pi_1(y), \pi_2(y)).$$

Jeśli teraz $x = h(a, b), y = h(c, d)$, gdzie $a, c \in A, b, d \in B$, to na podstawie (5.1) mamy

$$a = \rho_1(a, b) = \pi_1 h(a, b) = \pi_1(x) = \pi_1(y) = \pi_1 h(c, d) = \rho_1(c, d) = c$$

i podobnie $b = d$. Zatem $(a, b) = (c, d)$ skąd

$$x = h(a, b) = h(c, d) = y.$$

Pokazaliśmy więc, że $h(g(x)) = x$ dla każdego $x \in P$, skąd wynika, że h jest odwzorowaniem surjektywnym. Podsumowując możemy stwierdzić, że jeśli (P, π_1, π_2) jest produktem zbiorów A, B w sensie definicji 5.2.1, to istnieje bijekcja $h : A \times B \to P$ taka, że jeśli $h(a, b) = x$, to $\pi_1(x) = a = \rho_1(a, b)$ oraz $\pi_2(x) = b = \rho_2(a, b)$. Bijekcja h ustala więc odpowiedniość pomiędzy elementami zbiorów $A \times B$ oraz P, w której rzutowania ρ_i działają na elemencie $(a, b) \in A \times B$ tak samo jak odwzorowania π_i na obrazie elementu (a, b) poprzez h. Można więc powiedzieć, że trójki $(A \times B, \rho_1, \rho_2)$ i (P, π_1, π_2) różnią się właściwie tylko oznaczeniami.

Definicję 5.2.1 produktu dwóch obiektów kategorii można oczywiście rozszerzyć na dowolne rodziny obiektów kategorii.

Definicja **5.2.2.** *Iloczynem* lub *produktem* rodziny obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ nazywamy układ $(P, \{\pi_i : i \in I\})$, gdzie P jest obiektem kategorii $\mathcal{A}$ natomiast $\pi_i : P \to A_i,\ i \in I$, są morfizmami kategorii $\mathcal{A}$, takimi, że dla każdego obiektu C kategorii $\mathcal{A}$ i każdej rodziny morfizmów $\alpha_i : C \to A_i,\ \ i \in I$, istnieje dokładnie jeden morfizm $h : C \to P$, dla którego

$$\pi_i \circ h = \alpha_i \quad \forall\, i \in I.$$

Definicja produktu pozostawia otwartą kwestię *istnienia* produktu obiektów danej kategorii $\mathcal{A}$. W kategorii zbiorów $\mathcal{S}$ produkt kartezjański K rodziny zbiorów $\{A_i : i \in I\}$ wraz z rzutowaniami $\pi_i : K \to A_i$ jest jej produktem w sensie powyższej definicji. A więc w kategorii zbiorów istnieją produkty dowolnych rodzin zbiorów. Ta sama konstrukcja pozwala także udowodnić istnienie produktów w kategorii grup i w kategorii modułów. Dla przykładu podamy szczegółowy dowód tego faktu dla kategorii grup. Zamieniając w nim słowo *grupa* przez *zbiór* (lub odpowiednio przez *moduł*) oraz słowo *homomorfizm* przez *odwzorowanie* (i zachowując słowo homomorfizm) otrzymamy dowód istnienia produktów w kategorii zbiorów (i kategorii modułów nad ustalonym pierścieniem R).

TWIERDZENIE **5.2.3.** *Produkty istnieją w kategorii grup.*

Dowód. Niech $\{G_i : i \in I\}$ będzie dowolną rodziną grup i niech $P = \prod\{G_i : i \in I\}$ będzie produktem kartezjańskim rodziny grup G_i (zob. §1.3). Dla każdego $j \in I$ rozpatrujemy rzutowanie

$$\pi_j : P \to G_j, \quad \pi_j((g_i)_{i\in I}) = g_j.$$

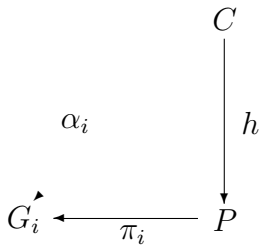
Każde rzutowanie π_j jest oczywiście homomorfizmem grup, czyli jest morfizmem w kategorii grup. Twierdzimy, że

$$(P, \{\pi_i : i \in I\}) \text{ jest produktem rodziny } \{G_i : i \in I\} \text{ w kategorii grup.}$$

Niech więc C będzie grupą i niech dla każdego $i \in I$ odwzorowania $\alpha_i : C \to G_i$ będą homomorfizmami grup. Określamy odwzorowanie

$$h : C \to P, \quad h(c) = (\alpha_i(c))_{i\in I}.$$

Jest to homomorfizm grup i dla każdego $i \in I$ diagram



jest przemienny, gdyż $\pi_i(h(c)) = \pi_i((\alpha_j(c))_{j\in I}) = \alpha_i(c)$, to znaczy $\pi_i \circ h = \alpha_i$ dla każdego $i \in I$. Pozostaje pokazać, że h jest jedynym homomorfizmem spełniającym warunek $\pi_i \circ h = \alpha_i$ dla każdego $i \in I$. Dla każdego homomorfizmu $h : C \to P$ spełniającego ten warunek i dla każdego $c \in C$ mamy $\pi_i(h(c)) = \alpha_i(c)$, skąd wynika, że

$$h(c) = (\alpha_i(c))_{i\in I}.$$

A więc h jest jednoznacznie wyznaczony przez rodzinę homomorfizmów α_i. □

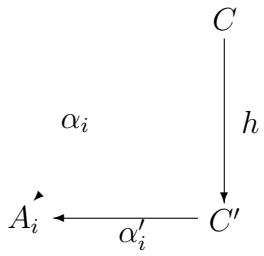
Definicję produktu obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ można także przedstawić w bardziej abstrakcyjnej formie używając konstrukcji kategorii, której obiektami są niektóre morfizmy kategorii $\mathcal{A}$. Dla ustalonej rodziny obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ rozpatrujemy kategorię $\mathcal{P}$, której obiektami są pary

$$T = \big(C, \{\alpha_i : i \in I\}\big),$$

w których C jest dowolnym obiektem kategorii $\mathcal{A}$, zaś $\alpha_i : C \to A_i$ są morfizmami kategorii $\mathcal{A}$. Morfizmem $h : T \to T'$ pomiędzy obiektami T oraz

$$T' = \big(C', \{\alpha'_i : i \in I\}\big)$$

w kategorii $\mathcal{P}$ jest każdy morfizm $h : C \to C'$ taki, że każdy diagram



jest przemienny. Produkt rodziny obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ jest tak zwanym *obiektem końcowym* kategorii $\mathcal{P}$. Jest to mianowicie taki obiekt

$$\Pi = \left(P, \{\pi_i : i \in I\}\right)$$

kategorii $\mathcal{P}$, że z każdego obiektu T tej kategorii istnieje dokładnie jeden morfizm $h : T \to \Pi$. Łatwo zauważyć, że produkt $\Pi = \left(P, \{\pi_i : i \in I\}\right)$ rodziny obiektów $\{A_i : i \in I\}$, jeśli istnieje, jest wyznaczony jednoznacznie z dokładnością do izomorfizmu. Rzeczywiście, przypuśćmy, że Π oraz $\Pi' = \left(P', \{\pi'_i : i \in I\}\right)$ są dwoma produktami rodziny obiektów $\{A_i : i \in I\}$. Wtedy Π i Π' są obiektami końcowymi kategorii $\mathcal{P}$ i wobec tego istnieją morfizmy $h : \Pi' \to \Pi$ oraz $h' : \Pi \to \Pi'$. Stąd

$$h' \circ h : \Pi' \to \Pi', \qquad h \circ h' : \Pi \to \Pi$$

są morfizmami kategorii $\mathcal{P}$. Z drugiej strony mamy także morfizmy identycznościowe

$$\mathbf{1}_{\Pi'} : \Pi' \to \Pi', \qquad \mathbf{1}_{\Pi} : \Pi \to \Pi$$

i wobec jedyności morfizmów w obiekt końcowy kategorii $\mathcal{P}$ mamy

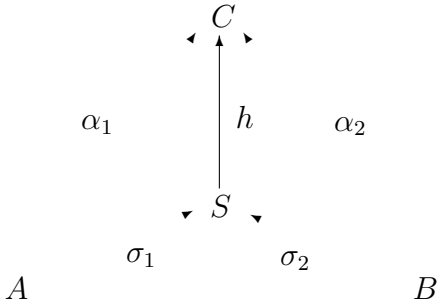
$$h' \circ h = \mathbf{1}_{\Pi'}, \qquad h \circ h' = \mathbf{1}_{\Pi}.$$

A więc h' i h są izomorfizmami.

5.3 Sumy obiektów kategorii

Pojęcie sumy obiektów kategorii jest dualne do iloczynu obiektów w tym sensie, że definicja sumy powstaje z definicji iloczynu przez zmianę kierunku wszystkich morfizmów. Wprawdzie można byłoby także pozostawić te same oznaczenia morfizmów, decydujemy się jednak na zamianę π_i, które kojarzą się przeważnie z rzutowaniami, na σ_i, które powinny kojarzyć się z włożeniami. W poniższej definicji naśladujemy w dowolnej kategorii własności sumy mnogościowej $S = A \cup B$ dwóch *rozłącznych* zbiorów A, B oraz włożeń $\sigma_1 : A \hookrightarrow S$, $\sigma_2 : B \hookrightarrow S$ zbiorów A i B w zbiór S.

Definicja **5.3.1.** *Sumą* lub *koproduktem* obiektów A i B kategorii $\mathcal{A}$ nazywamy trójkę (S, σ_1, σ_2), gdzie S jest obiektem a $\sigma_1 : A \to S$ oraz $\sigma_2 : B \to S$ są morfizmami kategorii $\mathcal{A}$, mającą następującą własność:
dla każdego obiektu C kategorii $\mathcal{A}$ i każdych morfizmów $\alpha_1 : A \to C$, $\alpha_2 : B \to C$ istnieje dokładnie jeden morfizm $h : S \to C$ taki, że następujący diagram jest przemienny:



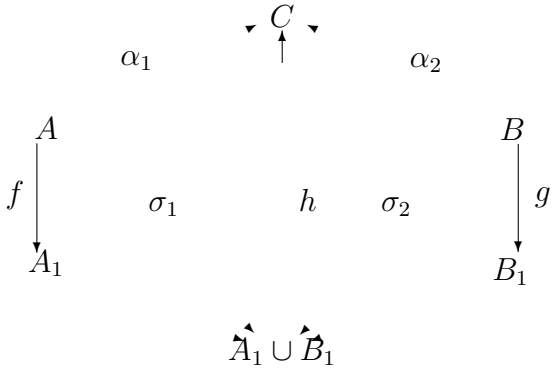
Przykład 5.3.1. Pokażemy, że w kategorii zbiorów istnieje koprodukt dowolnych dwóch zbiorów A i B. Nie jest nim jednak na ogół zwykła suma mnogościowa, chyba, że zbiory te są rozłączne. Dla danych dwóch zbiorów A i B obieramy więc zbiór A_1 równoliczny z A oraz zbiór B_1 równoliczny z B tak, by zbiory A_1 i B_1 były rozłączne: $A_1 \cap B_1 = \emptyset$. Niech

$$f : A \to A_1, \quad g : B \to B_1$$

będą bijekcjami i niech $S := A_1 \cup B_1$. Definiujemy σ_1 i σ_2 jako złożenia:

$$\sigma_1 : A \xrightarrow{f} A_1 \hookrightarrow S, \quad \sigma_2 : B \xrightarrow{g} B_1 \hookrightarrow S.$$

Twierdzimy, że (S, σ_1, σ_2) jest koproduktem zbiorów A i B.
Niech bowiem $\alpha_1 : A \to C$ i $\alpha_2 : B \to C$ będą dowolnymi odwzorowaniami. Rozpatrzmy diagram



w którym odwzorowanie h określimy następująco. Ponieważ zbiory A_1 i B_1 są rozłączne, więc każdy element $s \in S = A_1 \cup B_1$ należy tylko do jednego ze zbiorów A_1, B_1. Jeśli $s = a_1 \in A_1$, to $a_1 = f(a)$ dla pewnego $a \in A$ i kładziemy

$$h(s) = h(a_1) = h(f(a)) := \alpha_1(a).$$

Podobnie, jeśli $s = b_1 \in B_1$, to $b_1 = g(b)$ dla pewnego $b \in B$ i kładziemy

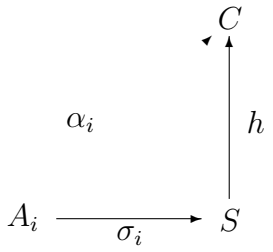
$$h(s) = h(b_1) = h(g(b)) := \alpha_2(b).$$

W ten sposób diagram uzupełniony poprzez określenie odwzorowania h staje się diagramem przemiennym, skąd odczytujemy, że

$$h \circ \sigma_i = \alpha_i \quad \text{dla} \quad i = 1, 2.$$

Z drugiej strony, odwzorowanie h spełniające te warunki jest jednoznacznie określone na elementach zbioru $S = A_1 \cup B_1$, zatem trójka (S, σ_1, σ_2) spełnia wszystkie wymagania jakie stawiamy koproduktowi obiektów w kategorii zbiorów.

DEFINICJA **5.3.2.** *Sumą* lub *koproduktem* rodziny obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ nazywamy parę $(S, \{\sigma_i : i \in I\})$, gdzie S jest obiektem kategorii $\mathcal{A}$ natomiast $\sigma_i : A_i \to S,\ i \in I$, są morfizmami kategorii $\mathcal{A}$, takimi, że dla każdego obiektu C kategorii $\mathcal{A}$ i każdej rodziny morfizmów $\alpha_i : A_i \to C,\ i \in I$, istnieje dokładnie jeden morfizm $h : S \to C$ taki, że następujący diagram jest przemienny:



to znaczy taki, że $h \circ \sigma_i = \alpha_i$ dla każdego $i \in I$.

Łatwa modyfikacja przykładu 5.3.1 pokazuje, że w kategorii zbiorów istnieją koprodukty dowolnych rodzin zbiorów. Można też udowodnić, że koprodukty istnieją w kategorii grup (zob. S. Lang, *Algebra*, rozdz. I, §8). Udowodnimy tutaj tylko prostszy fakt, że koprodukty istnieją w kategorii $\mathcal{AG}$ grup abelowych. Ponieważ ten sam dowód pokazuje istnienie koproduktu w kategorii modułów, pokażemy go w tej ogólniejszej wersji.

TWIERDZENIE **5.3.3.** *Koprodukty istnieją w kategorii $\mathcal{M}(R)$ modułów nad pierścieniem R.*

Dowód. Niech $\{M_i : i \in I\}$ będzie dowolną rodziną $R-$modułów i niech $S = \coprod\{M_i : i \in I\}$ będzie zewnętrzną sumą prostą rodziny modułów M_i. A więc S jest podmodułem produktu kartezjańskiego rodziny modułów M_i złożonym z tych elementów $(m_i)_{i\in I}$ dla których prawie wszystkie m_i są równe 0. Dla każdego $j \in I$ rozpatrujemy włożenie

$$\sigma_j : M_j \to S, \quad \sigma_j(m) = (m_i)_{i\in I}$$

gdzie $m_j = m$ oraz $m_i = 0$ dla $i \neq j$. Każde włożenie σ_j jest oczywiście homomorfizmem modułów, czyli jest morfizmem w kategorii modułów. Twierdzimy, że

$(S, \{\sigma_i : i \in I\})$ jest koproduktem rodziny $\{M_i : i \in I\}$ w kategorii modułów.

Niech więc C będzie $R-$modułem i niech dla każdego $i \in I$ odwzorowania $\alpha_i : M_i \to C$ będą homomorfizmami modułów. Określamy odwzorowanie

$$h : S \to C, \quad h((m_i)_{i\in I}) = \sum_{i\in I} \alpha_i(m_i).$$

Suma występująca po prawej stronie ma skończoną liczbę składników, gdyż wobec $(m_i)_{i\in I} \in S$ prawie wszystkie m_i są równe zero. Odwzorowanie h jest homomorfizmem modułów (tutaj wykorzystujemy fakt, że dodawanie w module C jest przemienne). Ponadto, $h \circ \sigma_i = \alpha_i$, gdyż dla $m \in M_i$ element $\sigma_i(m)$ modułu S ma $i-$tą

współrzędną równą m natomiast wszystkie pozostałe współrzędne równe zero, więc

$$h(\sigma_i(m)) = \alpha_i(m) \quad \forall m \in M_i \quad \forall i \in I.$$

Jedyność h wynika z warunku, który ma spełniać h : $h \circ \sigma_i = \alpha_i$ dla każdego $i \in I$. Warunek ten wymusza bowiem działanie homomorfizmu h na obrazach modułów M_i poprzez $h(\sigma_i(m)) = \alpha_i(m)$ dla $m \in M_i$, stąd także wynika, że h jest jednoznacznie określone na każdym elemencie modułu S. Dla $s = (m_i)_{i\in I} \in S$ mamy bowiem przedstawienie w postaci sumy $s = \sum \sigma_i(m_i)$ ze skończoną liczbą składników różnych od zera, wobec tego element

$$h(s) = \sum h(\sigma_i(m_i)) = \sum \alpha_i(m_i),$$

jest określony jednoznacznie przez rodzinę homomorfizmów $\alpha_i : M_i \to C$. □

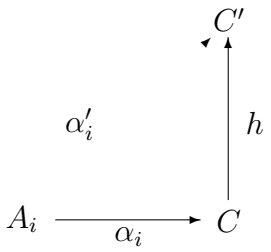
Podobnie jak w przypadku produktu, także definicję koproduktu rodziny obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ można przedstawić używając konstrukcji kategorii, której obiektami są niektóre morfizmy kategorii $\mathcal{A}$. Dla ustalonej rodziny obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ rozpatrujemy kategorię $\mathcal{K}$, której obiektami są pary

$$T = \big(C, \{\alpha_i : i \in I\}\big),$$

gdzie C jest dowolnym obiektem kategorii $\mathcal{A}$, zaś $\alpha_i : A_i \to C$ są morfizmami kategorii $\mathcal{A}$. Morfizmem $h : T \to T'$ pomiędzy obiektami T oraz

$$T' = \big(C', \{\alpha'_i : i \in I\}\big)$$

w kategorii $\mathcal{K}$ jest każdy morfizm $h : C \to C'$ taki, że każdy diagram



jest przemienny. Koprodukt rodziny obiektów $\{A_i : i \in I\}$ kategorii $\mathcal{A}$ jest tak zwanym *obiektem początkowym* kategorii $\mathcal{K}$. Jest to mianowicie taki obiekt

$$\Sigma = \big(S, \{\sigma_i : i \in I\}\big)$$

kategorii $\mathcal{K}$, że dla każdego obiektu T tej kategorii istnieje dokładnie jeden morfizm $h : \Sigma \to T$. Podobnie jak w przypadku produktu obiektów dowodzimy, że koprodukt rodziny obiektów $\{A_i : i \in I\}$, jeśli istnieje, jest wyznaczony jednoznacznie z dokładnością do izomorfizmu obiektów.

Uwaga 5.3.4. Następujące obiekty, których własności uniwersalne ustaliliśmy w poprzednich rozdziałach, są obiektami początkowymi odpowiednio określonych kategorii:

• grupa ilorazowa, pierścień ilorazowy, moduł ilorazowy;
• grupa wolna $F(X)$ z wolnym zbiorem generatorów X;
• pierścień ułamków $S^{-1}A$ względem zbioru multyplikatywnego S pierścienia przemiennego A;
• $R-$moduł wolny z bazą $\mathcal{B}$;
• iloczyn tensorowy modułów $M \otimes N$.
Pokażemy jak zinterpretować grupę ilorazową jako obiekt początkowy pewnej kategorii. Określenie obiektów i morfizmów w odpowiednich kategoriach dla pozostałych przypadków pozostawiamy jako ćwiczenie.
Dla podgrupy normalnej H grupy G rozpatrujemy wszystkie trójki (G, G', h) gdzie $h : G \to G'$ jest homomorfizmem takim, że $H \subseteq \ker h$. Trójki takie będą obiektami nowej kategorii $\mathcal{C}$. Morfizmem $\varphi : (G, G', h) \to (G, G'_1, h_1)$ pomiędzy obiektami kategorii $\mathcal{C}$ nazywamy homomorfizm $\varphi : G' \to G'_1$ taki, że $\varphi \circ h = h_1$ (o ile taki homomorfizm istnieje). Na podstawie wersji twierdzenia o faktoryzacji sformułowanej w uwadze 1.1.6, w kategorii $\mathcal{C}$ trójka $(G, G/H, \kappa)$, gdzie $\kappa : G \to G/H$ jest homomorfizmem kanonicznym, jest obiektem początkowym.

5.4 Funktory

Funktory grają w teorii kategorii rolę podobną do homomorfizmów w teorii grup. Formalna definicja funktora jest następująca.
Funktorem kowariantnym $F : \mathcal{A} \to \mathcal{B}$ z kategorii $\mathcal{A}$ do kategorii $\mathcal{B}$ nazywamy parę odwzorowań $F = (F_1, F_2)$, gdzie

$$F_1 : \mathsf{Ob}(\mathcal{A}) \to \mathsf{Ob}(\mathcal{B}) \quad \text{oraz} \quad F_2 : \mathsf{Ar}(\mathcal{A}) \to \mathsf{Ar}(\mathcal{B}),$$

spełniającą następujące warunki:

1. Dla każdego $A \in \mathsf{Ob}(\mathcal{A})$ i dla $B = F_1(A) \in \mathsf{Ob}(\mathcal{B})$ mamy $F_2(1_A) = 1_B$.
2. Dla każdego $g \in \mathsf{Ar}(\mathcal{A})$, jeśli $g \in \mathsf{Mor}(A, B)$ dla pewnych obiektów A, B kategorii $\mathcal{A}$, to $F_2(g) \in \mathsf{Mor}(F_1(A), F_1(B))$.
3. Jeśli $f : B \to C$ oraz $g : A \to B$ są morfizmami w kategorii $\mathcal{A}$, to

$$F_2(f \circ g) = F_2(f) \circ F_2(g).$$

Zastępując w definicji funktora kowariantnego warunki 2. i 3. przez

2'. Dla każdego $g \in \mathsf{Ar}(\mathcal{A})$, jeśli $g \in \mathsf{Mor}(A, B)$ dla pewnych obiektów A, B kategorii $\mathcal{A}$, to $F_2(g) \in \mathsf{Mor}(F_1(B), F_1(A))$.
3'. Jeśli $f : B \to C$ oraz $g : A \to B$ są morfizmami w kategorii $\mathcal{A}$, to

$$F_2(f \circ g) = F_2(g) \circ F_2(f),$$

otrzymujemy definicję *funktora kontrawariantnego* z kategorii $\mathcal{A}$ do kategorii $\mathcal{B}$.

Dla uproszczenia symboliki będziemy pomijać wskaźniki w oznaczeniach odwzorowań F_1 i F_2. Zatem dla funktora kowariantnego F z kategorii $\mathcal{A}$ do kategorii $\mathcal{B}$ i dla obiektów A i B kategorii $\mathcal{A}$ oraz morfizmu $g : A \to B$ będziemy pisać $F(g) : F(A) \to F(B)$ dla odpowiedniego morfizmu kategorii $\mathcal{B}$. W tej symbolice warunek zachowywania operacji składania morfizmów mówi, że funktor F przeprowadza pierwszy z następujących diagramów na drugi:

Przykład 5.4.1. Z każdą kategorią $\mathcal{A}$ jest związany funktor $I_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ taki, że $I_{\mathcal{A}}(A) = A$ dla każdego obiektu A oraz $I_{\mathcal{A}}(g) = g$ dla każdego morfizmu kategorii $\mathcal{A}$. Funktor $I_{\mathcal{A}}$ nazywa się funktorem *identycznościowym*. Jest to funktor kowariantny.

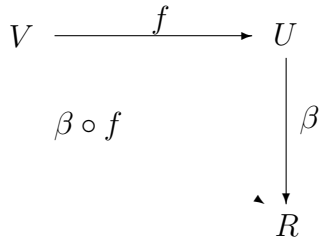
Przykład 5.4.2. Najprostszymi przykładami funktorów są tak zwane *funktory zapominania*. Rozpatrzmy, na przykład, kategorię $\mathcal{G}$ wszystkich grup oraz kategorię $\mathcal{S}$ wszystkich zbiorów. Określamy odwzorowanie $\Phi : \mathcal{G} \to \mathcal{S}$ przyporządkowując każdej grupie G zbiór $\Phi(G) = G$ oraz każdemu homomorfizmowi grup $h : G \to K$ to samo odwzorowanie $\Phi(h) = h$ pomiędzy zbiorami G i K. Odwzorowanie Φ zapomina więc strukturę grupy G i traktuje ją jako zbiór a także zapomina, że $h : G \to K$ jest homomorfizmem i traktuje h jako zwykłe odwzorowanie zbioru G w zbiór K. Jest jasne, że Φ jest funktorem kowariantnym z kategorii grup do kategorii zbiorów.
Istnieje wiele wariantów funktorów zapominania. Na przykład, przyporządkowanie każdemu pierścieniowi jego addytywnej grupy i każdemu homomorfizmowi pierścieni tego samego odwzorowania traktowanego jako homomorfizm grup addytywnych, określa funktor kowariantny z kategorii pierścieni w kategorię grup abelowych. Podobnie, przyporządkowanie $R-$modułowi jego grupy addytywnej i homomorfizmowi $R-$modułów tego samego odwzorowania traktowanego jako homomorfizm grup addytywnych określa funktor kowariantny z kategorii $R-$modułów w kategorię grup abelowych.

Przykład 5.4.3. Znacznie ważniejszym przykładem niż funktor zapominania $\Phi : \mathcal{G} \to \mathcal{S}$ jest funktor tworzenia grupy wolnej z zadanym wolnym zbiorem generatorów. Określamy $F : \mathcal{S} \to \mathcal{G}$ następująco. Zbiorowi X przyporządkowujemy grupę wolną $F(X)$ z wolnym zbiorem generatorów X. Natomiast odwzorowaniu $f : X_1 \to X_2$ zbioru X_1 w zbiór X_2 przyporządkowujemy jedyny homomorfizm $F(f) : F(X_1) \to F(X_2)$ będący przedłużeniem odwzorowania f (istnienie takiego homomorfizmu udowodniliśmy w twierdzeniu 1.4.5 dla zbiorów niepustych; jeśli X_1 jest zbiorem pustym, to z definicji $F(X_1)$ jest grupą jednoelementową). Jest rzeczą oczywistą, że $F : \mathcal{S} \to \mathcal{G}$ jest funktorem kowariantnym.

Przykład 5.4.4. W kategorii **Metr** przestrzeni metrycznych przejście od przestrzeni metrycznej M do jej uzupełnienia $\overline{M}$ jest przykładem funktora kowariantnego F tej kategorii w siebie. Mianowicie, dla dowolnych przestrzeni metrycznych M_1, M_2 i dla dowolnej kontrakcji $\varphi : M_1 \to M_2$ istnieje przedłużenie $\bar{\varphi} : \overline{M_1} \to \overline{M_2}$, które także jest kontrakcją. Stąd wynika, że przyporządkowania $F(M) = \overline{M},\ F(\varphi) = \bar{\varphi}$ określają funktor kowariantny **Metr** $\to$ **Metr**.

Przykład 5.4.5. Rozpatrzmy kategorię $\mathcal{M}(R)$ modułów nad pierścieniem R. Każdemu modułowi V przyporządkujmy jego moduł *dualny* (lub *sprzężony*) V^*. Jest to

moduł wszystkich funkcjonałów liniowych $\alpha : V \to R$. Natomiast każdemu morfizmowi $f : V \to U$ (czyli homomorfizmowi $R-$modułu V w $R-$moduł U) przyporządkujmy *morfizm transponowany* f^*, który określa się następująco. Dla morfizmu $f : V \to U$ i funkcjonału $\beta : U \to R$ mamy diagram przemienny



i wobec tego kładziemy

$$f^* : U^* \to V^*, \quad f^*(\beta) = \beta \circ f.$$

Pokażemy, że przyporządkowanie

$$F : \mathcal{M}(R) \to \mathcal{M}(R), \quad F(V) = V^*, \quad F(f) = f^* \tag{5.2}$$

jest funktorem kontrawariantnym. Najpierw sprawdzimy, że $F(1_V) = 1_{F(V)}$.
Rzeczywiście, $F(1_V) = (1_V)^*$ oraz dla dowolnego $\beta \in V^*$ mamy

$$(1_V)^*(\beta) = \beta \circ 1_V = \beta.$$

Zatem $(1_V)^*$ jest identycznością na V^* i wobec tego $F(1_V) = (1_V)^* = 1_{F(V)}$.
Dalej, dla morfizmów $f : V \to U$, $g : W \to V$ ich złożenia $f \circ g : W \to U$ i ich obrazów $f^* : U^* \to V^*$, $g^* : V^* \to W^*$, $(f \circ g)^* : U^* \to W^*$ mamy

$$(f \circ g)^*(\beta) = \beta \circ (f \circ g) = (\beta \circ f) \circ g = f^*(\beta) \circ g = g^*(f^*(\beta)) = (g^* \circ f^*)(\beta).$$

Zatem $F(f \circ g) = (f \circ g)^* = g^* \circ f^* = F(g) \circ F(f)$. Pokazaliśmy więc, że (5.2) określa funktor kontrawariantny kategorii $R-$modułów w siebie.
Funktor F nazywamy funktorem *tworzenia modułu dualnego*.
Zauważmy, że w przypadku gdy pierścień $R = K$ jest ciałem rozpatrywana przez nas kategoria $\mathcal{M}(R)$ modułów nad R jest kategorią przestrzeni wektorowych $\mathcal{V}(K)$ nad ciałem K natomiast funktor F jest funktorem tworzenia przestrzeni dualnej.

Funktor tworzenia modułu dualnego ma następującą własność, którą wykorzystamy w dowodzie stwierdzenia 5.4.3. Dla dowolnych $R-$modułów U i V,

$$F(U \oplus V) \cong F(U) \oplus F(V) \quad \text{(izomorfizm modułów)}.$$

Rzeczywiście, dla dowolnego funkcjonału $f : U \oplus V \to R$ wobec równości

$$f(u, v) = f((u, 0) + (0, v)) = f(u, 0) + f(0, v) = f|_U(u, 0) + f|_V(0, v)$$

przyporządkowanie $f \mapsto (f|_U, f|_V)$ funkcjonałowi f pary jego zacieśnień do podmodułów U i V określa homomorfizm modułów $(U \oplus V)^* \to U^* \oplus V^*$. Łatwo sprawdza się, że ten homomorfizm jest izomorfizmem $R-$modułów. Ten fakt wykorzystamy w dowodzie stwierdzenia 5.4.3.

Przykład 5.4.6. Rozpatrzmy teraz odwzorowanie $G : \mathcal{M}(R) \to \mathcal{M}(R)$ określone następująco. Dla każdych $R-$modułów V, U i dla dowolnego homomorfizmu $f : V \to U$ kładziemy

$$G(V) = F(F(V)) = V^{**}, \quad G(f) = F(F(f)) = f^{**},$$

gdzie F jest funktorem tworzenia modułu dualnego.
Zatem G każdemu $R-$modułowi V przyporządkowuje moduł $(V^*)^*$ (nazywany *bidualnym* lub *drugim sprzężonym*) i każdemu homomorfizmowi $R-$modułów $f : V \to U$ jego drugą transpozycję $(f^*)^* : V^{**} \to U^{**}$. Zauważmy, że dla morfizmu jednostkowego 1_V mamy

$$G(1_V) = F(F(1_V)) = F(1_{F(V)}) = 1_{F(F(V))} = 1_{G(V)},$$

i dla dowolnych morfizmów $f : V \to U$, $g : W \to V$ i ich złożenia $f \circ g : W \to U$ mamy

$$G(f \circ g) = F(F(f \circ g)) = F(F(g) \circ F(f)) = F(F(f)) \circ F(F(g)) = G(f) \circ G(g).$$

Zatem G jest funktorem kowariantnym kategorii $\mathcal{M}(R)$ w siebie. Nazywamy go funktorem *tworzenia modułu bidualnego.*
W szczególności, gdy $R = K$ jest ciałem, funktor $G : \mathcal{V}(K) \to \mathcal{V}(K)$ z kategorii przestrzeni wektorowych nad ciałem K w siebie nazywa się funktorem tworzenia przestrzeni bidualnej.

5.4.1 Transformacja naturalna funktorów

Pojęcie transformacji naturalnej funktorów objaśnimy na przykładzie kategorii modułów $\mathcal{M}(R)$ nad pierścieniem R. Rozpoczniemy od ustalenia związku między modułem V i jego modułem bidualnym V^{**}. Dla dowolnego $R-$modułu V określamy odwzorowanie

$$\lambda_V : V \to V^{**}, \quad \lambda_V(v) = v^*, \tag{5.3}$$

gdzie $v \in V$ oraz $v^* : V^* \to R$ jest funkcjonałem liniowym na module V^* określonym następująco:

$$v^*(\alpha) = \alpha(v) \quad \text{dla} \quad \alpha \in V^*.$$

Odwzorowanie λ_V jest homomorfizmem $R-$modułów, gdyż dla dowolnych $a, b \in R$, $u, v \in V$ oraz $\alpha \in V^*$ mamy

$$(au + bv)^*(\alpha) = \alpha(au + bv) = a\alpha(u) + b\alpha(v) = au^*(\alpha) + bv^*(\alpha) = (au^* + bv^*)(\alpha),$$

skąd

$$\lambda_V(au + bv) = (au + bv)^* = au^* + bv^* = a\lambda_V(u) + b\lambda_V(v).$$

Homomorfizm $\lambda_V : V \to V^{**}$ jest określony uniwersalną formułą (5.3) dla każdego modułu V. W szczególności, homomorfizm λ_V jest określony dla każdej przestrzeni wektorowej V (gdy pierścień R jest ciałem). W algebrze liniowej standardowym sposobem określania homomorfizmów na przestrzeni wektorowej V jest zadanie homomorfizmu poprzez jego wartości na wybranej bazie przestrzeni V. W przypadku homomorfizmu λ_V niepotrzebny jest żaden wybór bazy przestrzeni V i w dodatku formuła (5.3) stosuje się do każdej przestrzeni wektorowej V. Tę nadzwyczajną uniwersalność morfizmu λ_V podkreśla następujące stwierdzenie.

STWIERDZENIE **5.4.1.** *Niech V, U będą modułami nad pierścieniem R. Dla każdego homomorfizmu modułów $f : V \to U$ mamy diagram przemienny*

$$\begin{array}{ccc} V & \xrightarrow{\lambda_V} & V^{**} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f^{**}} \\ U & \xrightarrow[\lambda_U]{} & U^{**} \end{array}$$

w którym f^{**} jest drugą transpozycją homomorfizmu f.

Dowód. Pokażemy, że $\lambda_U f(v) = f^{**}\lambda_V(v)$ dla każdego elementu $v \in V$. Przede wszystkim zauważmy, że

$$\lambda_U f(v) = f(v)^*, \quad \text{gdzie} \quad f(v)^* : U^* \to R, \quad f(v)^*(\beta) = \beta(f(v))$$

dla każdego $\beta \in U^*$, oraz

$$f^{**}\lambda_V(v) = f^{**}(v^*), \quad \text{gdzie} \quad v^* : V^* \to R, \quad v^*(\alpha) = \alpha(v)$$

dla każdego $\alpha \in V^*$. Ponieważ $f(v)^*, f^{**}(v^*) \in U^{**}$ są funkcjonałami liniowymi na module U^*, więc aby udowodnić, że są one równe bierzemy dowolny funkcjonał $\beta \in U^*$ i sprawdzamy, że

$$f(v)^*(\beta) = \beta(f(v)) = (\beta \circ f)(v),$$

$$f^{**}(v^*)(\beta) = (f^*)^*(v^*)(\beta) = (v^* \circ f^*)(\beta) = v^*(f^*(\beta)) = v^*(\beta \circ f) = (\beta \circ f)(v).$$

Dowodzi to przemienności naszego diagramu. □

Rezultat stwierdzenia 5.4.1 posłuży nam jako przykład motywujący pojęcie transformacji naturalnej funktorów. Niech więc $\mathcal{A}$ i $\mathcal{B}$ będą kategoriami i niech $F : \mathcal{A} \to \mathcal{B}$, $G : \mathcal{A} \to \mathcal{B}$ będą dwoma funktorami kowariantnymi z kategorii $\mathcal{A}$ do kategorii $\mathcal{B}$.

Transformacją naturalną λ funktora F w funktor G nazywamy klasę morfizmów

$$\lambda_A : F(A) \to G(A), \quad A \in \mathsf{Ob}(\mathcal{A})$$

kategorii $\mathcal{B}$, jeśli dla każdego morfizmu $\alpha : A \to B$ kategorii $\mathcal{A}$ następujący diagram jest przemienny:

$$\begin{array}{ccc} F(A) & \xrightarrow{\lambda_A} & G(A) \\ {\scriptstyle F(\alpha)}\downarrow & & \downarrow{\scriptstyle G(\alpha)} \\ F(B) & \xrightarrow[\lambda_B]{} & G(B) \end{array}$$

Piszemy wtedy $\lambda : F \to G$.

Przykład 5.4.7. Niech $F = I_{\mathcal{M}(R)} : \mathcal{M}(R) \to \mathcal{M}(R)$ będzie funktorem identycznościowym kategorii modułów nad pierścieniem R i niech $G : \mathcal{M}(R) \to \mathcal{M}(R)$ będzie funktorem tworzenia modułu bidualnego. Wtedy na podstawie stwierdzenia 5.4.1 klasa morfizmów λ_V, gdzie V przebiega obiekty kategorii $\mathcal{M}(R)$, jest transformacją naturalną $\lambda : F \to G$ funktora identycznościowego F w funktor G tworzenia modułu bidualnego.

W szczególności, jeśli $R = K$ jest ciałem, to homomorfizmy λ_V wyznaczają transformację naturalną funktora identycznościowego F w funktor G tworzenia przestrzeni bidualnej na kategorii $\mathcal{V}(K)$ wszystkich przestrzeni wektorowych nad ciałem K.

5.4.2 Naturalna równoważność funktorów

Niech F i G będą funktorami kowariantnymi kategorii $\mathcal{A}$ w kategorię $\mathcal{B}$ i niech $\lambda : F \to G$ będzie transformacją naturalną funktora F w funktor G. Transformacja λ nazywa się *naturalną równoważnością* jeśli każdy morfizm λ_A jest izomorfizmem w kategorii $\mathcal{B}$. Funktory F i G nazywamy wtedy *naturalnie równoważnymi.*

Dwa następujące stwierdzenia dostarczą przykładów naturalnej równoważności funktorów.

Stwierdzenie **5.4.2.** *Dla każdego modułu wolnego V o skończonej randze homomorfizm*

$$\lambda_V : V \to V^{**}, \quad \lambda_V(v) = v^*$$

jest izomorfizmem modułów.

Dowód. Niech n będzie rangą modułu wolnego V i niech $\{e_1, \ldots, e_n\}$ będzie bazą modułu V. Dla każdego $i \in \{1, \ldots, n\}$ definiujemy odwzorowanie $\beta_i : V \to R$ kładąc

$$\beta_i\Big(\sum a_i e_i\Big) = a_i.$$

Oczywiście β_i jest funkcjonałem liniowym na module V i ma on następującą własność:

$$\beta_i(e_i) = 1 \quad \text{oraz} \quad \beta_i(e_j) = 0 \quad \text{dla} \quad j \neq i.$$

Pokażemy, że funkcjonały $\beta_1, \ldots, \beta_n$ tworzą bazę modułu dualnego V^*. Rzeczywiście, jeśli $\varphi \in V^*$ oraz $\varphi(e_i) = b_i$, $i = 1, \ldots, n$, to dla dowolnego elementu $\sum a_i e_i \in V$ mamy

$$\begin{aligned}\varphi\Big(\sum a_i e_i\Big) &= \sum a_i \varphi(e_i) = \sum a_i b_i = \sum_i a_i \sum_j b_j \beta_j(e_i) \\ &= \sum_j b_j \sum_i \beta_j(a_i e_i) = \sum_j b_j \beta_j(\sum_i a_i e_i) \\ &= \Big(\sum_j b_j \beta_j\Big)(\sum_i a_i e_i).\end{aligned}$$

Stąd wynika, że $\varphi = \sum_j b_j \beta_j$. Zatem zbiór $\{\beta_1, \ldots, \beta_n\}$ jest zbiorem generatorów modułu V^*. Ponadto, jest to zbiór liniowo niezależny, gdyż jeśli $\sum c_i \beta_i = 0$, to biorąc

wartości funkcjonałów po lewej i prawej stronie na elemencie bazowym e_j modułu V otrzymujemy $c_j = 0$. Tak więc $\{\beta_1, \ldots, \beta_n\}$ jest bazą modułu V^* zwaną bazą dualną względem bazy $\{e_1, \ldots, e_n\}$ modułu wolnego V. Wynika stąd, że V^* jest także modułem wolnym i ma rangę równą randze modułu wolnego V. Wobec tego moduły V i V^* są izomorficzne.

Ten sam argument stosuje się do V^* i V^{**}. Zatem jeśli V jest modułem wolnym o randze n, to także V^* i V^{**} są modułami wolnymi o randze n i moduły V, V^*, V^{**} są parami izomorficzne.

Pokażemy teraz, że homomorfizm $\lambda_V : V \to V^{**}$ jest izomorfizmem. Zauważmy, że

$$\lambda_V(e_i) = e_i^*, \quad \text{gdzie} \quad e_i^*(\beta_j) = \beta_j(e_i) = \delta_{ji}.$$

Zatem $\{e_1^*, \ldots, e_n^*\}$ jest bazą modułu V^{**} dualną względem bazy $\{\beta_1, \ldots, \beta_n\}$ modułu V^* i homomorfizm λ_V przeprowadza bazę $\{e_1, \ldots, e_n\}$ modułu wolnego V na bazę $\{e_1^*, \ldots, e_n^*\}$ modułu wolnego V^{**}. A więc λ_V jest izomorfizmem modułów. □

Rezultat stwierdzenia 5.4.2 można także udowodnić dla modułów projektywnych, ale potrzebna jest ogólniejsza technika dowodu nie odwołująca się do istnienia baz modułów.

STWIERDZENIE **5.4.3.** *Dla każdego skończenie generowanego modułu projektywnego V odwzorowanie*

$$\lambda_V : V \to V^{**}, \quad \lambda_V(v) = v^*$$

jest izomorfizmem modułów.

Dowód. Niech V będzie skończenie generowanym $R-$modułem projektywnym. Na podstawie lematu 3.4.10 istnieje $R-$moduł Q taki, że dla pewnej liczby naturalnej n moduł $F := V \oplus Q$ jest wolny i ma rangę n. Na podstawie stwierdzenia 5.4.2 homomorfizm $\lambda_F : F \to F^{**}$ jest izomorfizmem, zatem otrzymujemy izomorfizm

$$V \oplus Q = F \xrightarrow{\lambda_F} F^{**} \xrightarrow{\Phi} V^{**} \oplus Q^{**},$$

gdzie izomorfizm Φ otrzymujemy przez dwukrotne zastosowanie izomorfizmu z przykładu 5.4.5. A więc najpierw $F^* \cong V^* \oplus Q^*$ poprzez odwzorowanie $\varphi \mapsto (\varphi|_V, \varphi|_Q)$. Następnie, stosując ten sam argument otrzymujemy izomorfizm

$$\Phi : (V^* \oplus Q^*)^* \longrightarrow V^{**} \oplus Q^{**}, \quad \Phi(f^*) = (f^*|_{V^*}, f^*|_{Q^*}).$$

Pokażemy, że izomorfizm $\Phi \circ \lambda_F$ przeprowadza moduł V na moduł V^{**}. Wprawdzie oznacza to już, że V i V^{**} są izomorficzne, ale nasze twierdzenie mówi więcej, mianowicie, że λ_V jest izomorfizmem. Tak więc naszym ostatecznym celem jest pokazać, że $(\Phi \circ \lambda_F)|_V = \lambda_V$. Najpierw udowodnimy, że

$$\Phi\lambda_F(V) \subseteq V^{**}. \tag{5.4}$$

Rozpoczniemy od ustalenia jak należy interpretować element $\varphi = (\alpha, \beta) \in V^* \oplus Q^*$ jako funkcjonał na $V \oplus Q$. Jak wiemy z przykładu 5.4.5 mamy izomorfizm

$$(V \oplus Q)^* \to V^* \oplus Q^*, \quad \varphi \mapsto (\varphi|_V, \varphi|_Q).$$

Zatem dla $(\alpha, \beta) \in V^* \oplus Q^*$ istnieje $\varphi \in (V \oplus Q)^*$ taki, że

$$\alpha = \varphi|_V, \quad \beta = \varphi|_Q.$$

Wobec tego traktując (α, β) jako funkcjonał φ na $V \oplus Q$ dla dowolnych $v \in V, q \in Q$ mamy

$$(\alpha, \beta)(v + q) = \varphi(v + q) = \varphi(v) + \varphi(q) = \alpha(v) + \beta(q).$$

Stąd także dla $f = v + q$ otrzymujemy

$$(v + q)^*(\alpha, \beta) = f^*(\varphi) = \varphi(f) = \varphi(v + q) = (\alpha, \beta)(v + q) = \alpha(v) + \beta(q). \quad (5.5)$$

Przystępujemy do dowodu 5.4. Dla $v \in V$ mamy $\lambda_F(v) = v^* \in F^{**} = (V^* \oplus Q^*)^*$. Dla $\alpha \in V^*, \beta \in Q^*$ na podstawie (5.5) otrzymujemy $v^*(\alpha, \beta) = \alpha(v)$, w szczególności więc $v^*(0, \beta) = 0(v) = 0$ co oznacza, że $v^*|_{Q^*} = 0$. Wobec tego

$$\Phi\lambda_F(v) = \Phi(v^*) = (v^*|_{V^*}, v^*|_{Q^*}) = (v^*|_{V^*}, 0) \in V^{**} \subseteq V^{**} \oplus Q^{**}. \quad (5.6)$$

Dowodzi to (5.4). Teraz pokażemy, że w (5.4) mamy faktycznie równość. Weźmy więc dowolny element modułu $V^{**} \subseteq V^{**} \oplus Q^{**}$. Jest on postaci

$$(f^*|_{V^*}, f^*|_{Q^*}) \quad \text{gdzie} \quad f^*|_{Q^*} = 0.$$

Ten ostatni warunek oznacza, że

$$f^*(0, \beta) = 0 \quad \text{dla każdego} \quad \beta \in Q^*.$$

Jeśli zatem $f = v + q$, gdzie $v \in V, q \in Q$, to na podstawie (5.5) otrzymujemy

$$0 = (v + q)^*(0, \beta) = \beta(q) \quad \text{dla każdego} \quad \beta \in Q^*.$$

A więc $q \in Q$ jest takim elementem, że każdy funkcjonał liniowy β przyjmuje na nim wartość zero. Na podstawie wniosku 3.4.8 otrzymujemy $q = 0$. Zatem $f = v \in V$ i wobec tego

$$(f^*|_{V^*}, 0) = (v^*|_{V^*}, 0) = \Phi\lambda_F(v)$$

leży w obrazie $\Phi\lambda_F$. Pokazaliśmy więc, że $\Phi\lambda_F(V) = V^{**}$. Pozostaje ustalić, że $(\Phi \circ \lambda_F)|_V = \lambda_V$. Faktycznie zrobiliśmy to już w (5.6). Rzeczywiście, utożsamiając V^{**} ze składnikiem prostym $V^{**} \times 0$ modułu F^{**}, na podstawie (5.6) dla $v \in V$ mamy

$$\Phi\lambda_F(v) = \Phi(v^*) = (v^*|_{V^*}, v^*|_{Q^*}) = (v^*|_{V^*}, 0) = v^* \in V^{**},$$

zatem $\Phi\lambda_F(v) = v^* = \lambda_V(v)$, co należało udowodnić. □

Przykład 5.4.8. Na podstawie stwierdzenia 5.4.2 transformacja naturalna λ funktora identycznościowego F w funktor G tworzenia modułu bidualnego jest naturalną równoważnością funktorów kategorii $R-$modułów wolnych o skończonych rangach na siebie.

W szczególności, jeśli R jest ciałem, to wynika stąd, że funktor identycznościowy i funktor tworzenia przestrzeni bidualnej są naturalnie równoważnymi funktorami kategorii skończenie wymiarowych przestrzeni wektorowych nad R w siebie.

Przykład 5.4.9. Niech $\lambda : F \to G$ będzie transformacją naturalną funktora identycznościowego w funktor tworzenia modułu bidualnego kategorii $\mathcal{M}(R)$ modułów w siebie. Jeśli przez F' i G' oznaczymy zacieśnienia funktorów F i G do kategorii $\mathcal{P}(R)$ *skończenie generowanych modułów projektywnych* nad pierścieniem R, natomiast przez λ' oznaczymy zacieśnienie λ do F', to na podstawie stwierdzenia 5.4.3 transformacja $\lambda' : F' \to G'$ jest naturalną równoważnością funktorów F' i G'.

Nasza dyskusja kategorii i funktorów pozwala jeszcze raz podwyższyć poziom abstrakcji rozważań. Otóż w żadnym wypadku funktory i transformacje naturalne funktorów nie są ostatnim piętrem teorii kategorii. Przeciwnie, funktory (powiedzmy kowariantne) pomiędzy kategoriami $\mathcal{A}$ i $\mathcal{B}$ można traktować jako obiekty nowej kategorii oznaczanej $\mathcal{B}^{\mathcal{A}}$. Morfizmami pomiędzy funktorami $F : \mathcal{A} \to \mathcal{B}$ i $G : \mathcal{A} \to \mathcal{B}$ są transformacje naturalne λ funktora F w funktor G. Czytelnik z łatwością określi składanie morfizmów w $\mathcal{B}^{\mathcal{A}}$ i sprawdzi, że spełnia ono aksjomaty kategorii. Nic nie stoi na przeszkodzie, by rozpatrywać funktory z kategorii $\mathcal{B}^{\mathcal{A}}$ w inną kategorię $\mathcal{C}$. Jak wiemy funktory te tworzą nową kategorię $\mathcal{C}^{\mathcal{B}^{\mathcal{A}}}$, w której morfizmami są transformacje naturalne pomiędzy funktorami z $\mathcal{B}^{\mathcal{A}}$ do $\mathcal{C}$, etc.

Pojęcia kategorii, funktora i naturalnej równoważności funktorów wprowadzili S. Eilenberg i S. MacLane w pracy *General theory of natural equivalences* opublikowanej w Transactions of the American Mathematical Society **58** (1945), 231–294.

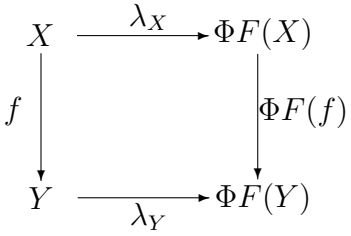
5.4.3 Funktory sprzężone

Przedstawimy tu na jednym przykładzie jedno z centralnych pojęć teorii kategorii - pojęcie funktorów sprzężonych. W przykładzie 5.4.3 rozpatrywaliśmy funktor zapominania $\Phi : \mathcal{G} \to \mathcal{S}$ oraz funktor tworzenia grupy wolnej $F : \mathcal{S} \to \mathcal{G}$. Jest rzeczą naturalną rozpatrzeć *złożenia*

$$\Phi \circ F : \mathcal{S} \to \mathcal{S}, \qquad F \circ \Phi : \mathcal{G} \to \mathcal{G}$$

tych funktorów. Natychmiast sprawdzamy, że złożenia te *nie* są funktorami identycznościowymi na $\mathcal{S}$ i $\mathcal{G}$, odpowiednio. Funktory $I_{\mathcal{S}}$ oraz $\Phi \circ F$ nie są też *naturalnie równoważne* i podobnie funktory $I_{\mathcal{G}}$ oraz $F \circ \Phi$ nie są naturalnie równoważne. Tym niemniej istnieją *transformacje naturalne* funktora $I_{\mathcal{S}}$ w funktor $\Phi \circ F$ oraz funktora $F \circ \Phi$ w funktor $I_{\mathcal{G}}$.

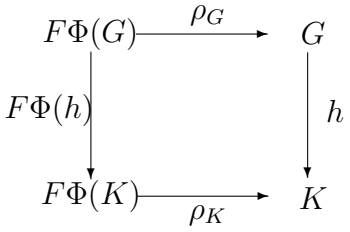
Skonstruujemy transformację naturalną $\lambda : I_{\mathcal{S}} \to \Phi F$. Dla każdego zbioru X rozpatrujemy grupę wolną $F(X)$ z wolnym zbiorem generatorów X oraz zbiór $\Phi F(X)$ elementów grupy $F(X)$. Definiujemy $\lambda_X : X \to \Phi F(X)$ jako zwykłe włożenie X w $\Phi F(X)$. Dla morfizmu $f : X \to Y$ w kategorii $\mathcal{S}$ mamy jedyny homomorfizm $F(f) : F(X) \to F(Y)$, którego istnienie wynika z uniwersalnej własności grupy wolnej (twierdzenie 1.4.5), zaś $\Phi F(f) : \Phi F(X) \to \Phi F(Y)$ jest odpowiednim odwzorowaniem zbiorów (zapominającym, że $F(f)$ jest homomorfizmem grup). Odwzorowania te tworzą diagram przemienny



co pokazuje, że klasa morfizmów $\lambda_X : X \to \Phi F(X)$ dla $X \in \mathsf{Ob}(\mathcal{S})$ jest transformacją naturalną funktora identycznościowego na kategorii zbiorów w funktor $\Phi \circ F$. Nie jest to jednak naturalna równoważność funktorów, gdyż morfizmy λ_X nie są izomorfizmami w kategorii $\mathcal{S}$ (nie są bijekcjami).

Jeśli teraz w powyższym diagramie weźmiemy $X = \Phi(G)$, $Y = \Phi(K)$, gdzie G, K są dowolnymi grupami i dla homomorfizmu $h : G \to K$ weźmiemy $f = \Phi(h)$, to klasę morfizmów $\lambda_{\Phi(G)}$ można traktować jako transformację naturalną $\lambda \circ \Phi : \Phi \to \Phi F \Phi$.

Skonstruujemy teraz naturalną transformacją funktora $F\Phi$ w funktor identycznościowy $I_{\mathcal{G}}$. Najpierw zauważmy, że dla dowolnej grupy G istnieje homomorfizm $\rho_G : F(\Phi(G)) \to G$ określony jako jedyny homomorfizm przedłużający odwzorowanie $\Phi(G) \to G$, $g \mapsto g$. Łatwo sprawdzić przemienność diagramu



dla każdej grupy K i dla każdego homomorfizmu $h : G \to K$. Klasa homomorfizmów ρ_G dla $G \in \mathsf{Ob}\,\mathcal{G}$ jest więc naturalną transformacją funktora $F\Phi$ w funktor identycznościowy $I_{\mathcal{G}}$. Poddając teraz wszystkie obiekty i morfizmy działaniu funktora zapominania Φ otrzymamy klasę morfizmów $\Phi(\rho_G)$, która jest naturalną transformacją $\Phi \circ \rho : \Phi F \Phi \to \Phi$ funktora $\Phi F \Phi$ w funktor Φ.

Nietrudno teraz zauważyć, że złożenie naturalnych transformacji $(\Phi \circ \rho) \circ (\lambda \circ \Phi) : \Phi \to \Phi$ jest identycznościową *naturalną równoważnością* funktora Φ z sobą. Sprowadza się to do sprawdzenia, że $\Phi(\rho_G)\lambda_{\Phi(G)}(g) = g$ dla każdego elementu $g \in G$.

Podobna konstrukcja pokazuje, że istnieją naturalne transformacje funktorów $F \circ \lambda : F \to F\Phi F$ oraz $\rho \circ F : F\Phi F \to F$ takie, że złożenie $(\rho \circ F) \circ (F \circ \lambda) : F \to F$ jest identycznościową naturalną równoważnością funktora F z sobą.

Ta sytuacja stanowi motywację do następującej definicji.

Niech $F : \mathcal{A} \to \mathcal{B}$ oraz $G : \mathcal{B} \to \mathcal{A}$ będą funktorami pomiędzy kategoriami $\mathcal{A}$ i $\mathcal{B}$. Funktory F i G nazywają się funktorami *sprzężonymi* jeśli istnieją naturalne transformacje $\lambda : I_{\mathcal{A}} \to GF$ oraz $\rho : FG \to I_{\mathcal{B}}$ takie, że złożenia

$$G \xrightarrow{\lambda \circ G} GFG \xrightarrow{G \circ \rho} G, \qquad F \xrightarrow{F \circ \lambda} FGF \xrightarrow{\rho \circ F} F$$

są identycznościowymi naturalnymi równoważnościami $G \to G$ oraz $F \to F$, odpowiednio.

Możemy więc powiedzieć, że funktor tworzenia grupy wolnej $F : \mathcal{S} \to \mathcal{G}$ oraz funktor zapominania $\Phi : \mathcal{G} \to \mathcal{S}$ są funktorami sprzężonymi.

5.5 Funktor K_0

5.5.1 Grupa Grothendiecka

Niech R będzie dowolnym pierścieniem. Ważnym problemem jest opisanie z dokładnością do izomorfizmu wszystkich skończenie generowanych modułów projektywnych nad pierścieniem R. W związku z tym będziemy tu rozpatrywać kategorię $\mathcal{P}(R)$ skończenie generowanych $R-$modułów projektywnych. Dla obiektu M tej kategorii (czyli skończenie generowanego $R-$modułu projektywnego) klasę obiektów izomorficznych z M oznaczymy (M). A więc $N \in (M) \iff N \cong M$. Zbiór $\mathcal{B} = \{(M) : M \in \mathsf{Ob}(\mathcal{P}(R))\}$ wszystkich klas potraktujemy jako bazę grupy abelowej wolnej F_R. Jej elementy są więc skończonymi kombinacjami liniowymi klas ze zbioru $\mathcal{B}$ postaci

$$x_1(M_1) + \cdots + x_n(M_n), \quad x_i \in \mathbb{Z}, \quad (M_i) \in \mathcal{B}.$$

W grupie F_R rozpatrujemy podgrupę H generowaną przez wszystkie elementy postaci

$$(M) - (M') - (M'') \tag{5.7}$$

gdzie moduły M, M', M'' są tak dobrane, że istnieje ciąg dokładny

$$0 \to M' \to M \to M'' \to 0$$

w kategorii $\mathcal{P}(R)$. Ponieważ jednak każdy taki ciąg dokładny rozszczepia się (na podstawie definicji modułu projektywnego), więc w sposób równoważny można powiedzieć, że podgrupa H grupy F_R jest generowana przez elementy postaci (5.7) gdzie moduły M, M', M'' spełniają warunek

$$M \cong M' \oplus M''.$$

Tutaj $\oplus$ oznacza sumę obiektów w kategorii $\mathcal{P}(R)$ (jest to więc zewnętrzna suma prosta modułów w sensie rozdziału 3).

Definiujemy teraz grupę abelową $K_0\mathcal{P}(R)$ jako grupę ilorazową

$$K_0\mathcal{P}(R) := F_R/H.$$

Grupę tę nazywamy *grupą Grothendiecka* kategorii $\mathcal{P}(R)$. Dla modułu M warstwę $(M)+H$ będziemy oznaczać $[M]$. Każdy skończenie generowany moduł projektywny nad R ma więc swój odpowiednik $[M]$ w grupie Grothendiecka $K_0\mathcal{P}(R)$. Zauważmy, że jeśli moduł M jest sumą prostą modułów M' i M'', to jego klasa $[M]$ jest w $K_0\mathcal{P}(R)$ sumą klas $[M']$ i $[M'']$. Rzeczywiście, jeśli $M \cong M' \oplus M''$, to $(M) - (M') - (M'') \in H$ zatem

$$H = (M) - (M') - (M'') + H = [M] - [M'] - [M''],$$

to znaczy $[M] = [M'] + [M'']$ w grupie $K_0\mathcal{P}(R)$, lub nieco wyraźniej,

$$[M' \oplus M''] = [M'] + [M'']. \tag{5.8}$$

Można więc powiedzieć, że grupa Grothendiecka *zapamiętuje* relację pomiędzy modułami M, M', M'' polegającą na tym, że jeden z tych modułów jest sumą prostą pozostałych.

Z tego, że grupa F_R ma bazę $\mathcal{B}$ wynika, że zbiór

$$\mathcal{B} + H = \Big\{[M] : [M] = (M) + H,\ (M) \in \mathcal{B}\Big\}$$

jest zbiorem generatorów grupy $K_0\mathcal{P}(R)$. Elementy grupy $K_0\mathcal{P}(R)$ są więc kombinacjami liniowymi ze współczynnikami całkowitymi elementów zbioru $\mathcal{B}+H$. Okazuje się jednak, że istnieje o wiele prostszy sposób prezentowania elementów grupy Grothendiecka.

Stwierdzenie **5.5.1.** *Każdy element grupy $K_0\mathcal{P}(R)$ można przedstawić w postaci $[M] - [N]$, gdzie $[M], [N] \in \mathcal{B} + H$.*

Dowód. Niech X będzie dowolnym elementem grupy $K_0\mathcal{P}(R)$. Zatem X jest kombinacją liniową elementów zbioru $\mathcal{B}+H$ ze współczynnikami całkowitymi. Grupując w tej kombinacji liniowej oddzielnie składniki ze współczynnikami dodatnimi i ujemnymi, możemy więc (dopuszczając powtórzenia składników) napisać

$$X = [M_1] + \cdots + [M_k] - ([N_1] + \cdots + [N_\ell]).$$

Zauważmy teraz, że na podstawie (5.8) mamy

$$[M_1] + \cdots + [M_k] = [M_1 \oplus \cdots \oplus M_k], \quad [N_1] + \cdots + [N_\ell] = [N_1 \oplus \cdots \oplus N_\ell].$$

Zatem $X = [M] - [N]$, gdzie $M = M_1 \oplus \cdots \oplus M_k$ oraz $N = N_1 \oplus \cdots \oplus N_\ell$. □

Przykład 5.5.1. Najprostszy przykład grupy Grothendiecka otrzymamy rozpatrując kategorię skończenie generowanych modułów projektywnych nad ciałem. Niech więc $R = L$ będzie ciałem. Moduły nad L są przestrzeniami wektorowymi i każdy moduł nad L jest wolny (ma bazę), zatem jest także projektywny. A więc $\mathcal{P}(L)$ jest kategorią skończenie wymiarowych przestrzeni wektorowych nad ciałem L. Pokażemy, że odwzorowanie

$$D : K_0\mathcal{P}(L) \to \mathbb{Z}, \quad D([U] - [V]) = \dim U - \dim V$$

jest dobrze określone na elementach grupy $K_0\mathcal{P}(L)$ i jest izomorfizmem grup.

Najpierw wykorzystamy fakt, że odwzorowanie $d : \mathcal{B} \to \mathbb{Z}$ bazy grupy abelowej wolnej F_L w grupę liczb całkowitych zadane wzorem $d_1(U) = \dim U$ ma dokładnie jedno przedłużenie do homomorfizmu $d : F_L \to \mathbb{Z}$ grupy wolnej F_L na $\mathbb{Z}$ (zob. twierdzenie 3.3.2). Jest to surjekcja, gdyż $d_1(L) = \dim L = 1$. Zauważmy ponadto, że $H \subset \ker d$. Rzeczywiście,

$$d\Big(\sum a_i\Big((M_i' \oplus M_i'') - (M_i') - (M_i'')\Big)\Big) = \sum a_i\Big(d(M_i' \oplus M_i'') - d(M_i') - d(M_i'')\Big) = 0,$$

gdyż $d(M_i' \oplus M_i'') = \dim M_i' \oplus M_i'' = \dim M_i' + \dim M_i'' = d(M_i') + d(M_i'')$. Stąd wynika, że odwzorowanie $D : F_L/H \to \mathbb{Z}$, gdzie dla $X \in F_L$ kładziemy $D(X + H) = d(X)$, jest dobrze określonym surjektywnym homomorfizmem grup. W szczególności mamy $D([U]) = d(U) = \dim U$, zatem także

$$D([U] - [V]) = D([U]) - D([V]) = \dim U - \dim V.$$

Mamy więc surjektywny homomorfizm $D : K_0\mathcal{P}(L) \to \mathbb{Z}$. Homomorfizm D jest także injektywny, gdyż

$$\begin{array}{ccccc} D([U]-[V]) = 0 & \iff & \dim U = \dim V & \iff & (U) = (V) \\ & \implies & [U] = [V] & \iff & [U] - [V] = 0. \end{array}$$

A więc grupa Grothendiecka $K_0\mathcal{P}(L)$ kategorii skończenie wymiarowych przestrzeni wektorowych nad dowolnym ciałem L jest izomorficzna z grupą liczb całkowitych.

W powyższym przykładzie wykorzystaliśmy oczywistą implikację $(U) = (V) \Rightarrow [U] = [V]$ chociaż w tej konkretnej sytuacji moglibyśmy także użyć równoważności. Wynika to z następującego faktu.

STWIERDZENIE **5.5.2.** *Dla $R-$modułów projektywnych M i N równość $[M] = [N]$ w grupie Grothendiecka $K_0\mathcal{P}(R)$ ma miejsce wtedy i tylko wtedy, gdy istnieje taki $R-$moduł projektywny P, że*

$$M \oplus P \cong N \oplus P.$$

Dowód. Jeśli $M \oplus P \cong N \oplus P$, to

$$[M] + [P] = [M \oplus P] = [N \oplus P] = [N] + [P],$$

skąd $[M] = [N]$. Wystarczalność warunku jest więc oczywista.

Dla dowodu konieczności warunku załóżmy, że $[M] = [N]$. Wtedy $(M)-(N) \in H$ i wobec tego $(M) - (N)$ jest kombinacją liniową elementów postaci (5.7). Dopuszczając powtarzające się składniki możemy oczywiście zapisać tę kombinację liniową ze współczynnikami ± 1 i wobec tego mamy przedstawienie

$$(M) - (N) = \sum \Big((M_i) - (M_i') - (M_i'') \Big) - \sum \Big((N_j) - (N_j') - (N_j'') \Big),$$

gdzie $M_i \cong M_i' \oplus M_i''$ oraz $N_j \cong N_j' \oplus N_j''$. Stąd otrzymujemy

$$(M) + \sum (M_i') + \sum (M_i'') + \sum (N_j) = (N) + \sum (N_j') + \sum (N_j'') + \sum (M_i).$$

Jest to równość w grupie abelowej wolnej F_R, a więc jednoznaczność przedstawienia elementu grupy F_R w postaci kombinacji liniowej elementów bazowych pociąga, że układ klas izomorfizmu modułów M, M_i', M_i'', N_j co najwyżej porządkiem różni się od układu klas izomorfizmu modułów N, N_j', N_j'', M_i. W szczególności otrzymujemy stąd izomorfizm modułów

$$M \oplus \bigoplus M_i' \oplus \bigoplus M_i'' \oplus \bigoplus N_j \cong N \oplus \bigoplus N_j' \oplus \bigoplus N_j'' \oplus \bigoplus M_i.$$

Niech P będzie $R-$modułem izomorficznym z każdą z powyższych sum prostych. Wtedy

$$\begin{aligned} M \oplus P &\cong M \oplus N \oplus \bigoplus N'_j \oplus \bigoplus N''_j \oplus \bigoplus M_i \\ &\cong N \oplus M \oplus \bigoplus N_j \oplus \bigoplus M'_i \oplus \bigoplus M''_i \\ &\cong N \oplus P. \end{aligned}$$

Wykorzystaliśmy tu izomorfizmy $M_i \cong M'_i \oplus M''_i$ oraz $N_j \cong N'_j \oplus N''_j$. □

Stwierdzenie 5.5.2 objaśnia dość precyzyjnie w jakim stopniu znajomość grupy Grothendiecka $K_0\mathcal{P}(R)$ może być wykorzystana do klasyfikacji skończenie generowanych modułów projektywnych nad R z dokładnością do izomorfizmu modułów. Otóż dla $R-$modułów projektywnych M i N równość $[M] = [N]$ wcale nie oznacza, że muszą one być izomorficzne. Oznacza jedynie, że dla pewnego modułu projektywnego P moduły $M \oplus P$ i $N \oplus P$ są izomorficzne. Moduł projektywny P jest składnikiem prostym pewnego modułu wolnego W, to znaczy istnieje $R-$moduł P_1 taki, że $P \oplus P_1 = W$ jest modułem wolnym. A więc $[M] = [N]$ wtedy i tylko wtedy gdy

$$M \oplus W \cong N \oplus W \quad \text{dla pewnego modułu wolnego } W. \tag{5.9}$$

Moduły M i N spełniające warunek (5.9) nazywają się *stabilnie izomorficzne*. Tak więc znajomość grupy Grothendiecka $K_0\mathcal{P}(R)$ rozwiązuje problem klasyfikacji projektywnych $R-$modułów z dokładnością do stabilnego izomorfizmu modułów.

Dla niektórych pierścieni relacje stabilnego izomorfizmu i izomorfizmu są identyczne. Jest tak na przykład dla ciał, gdyż w tym przypadku skończenie generowane moduły projektywne są skończenie wymiarowymi przestrzeniami wektorowymi i dla nich (5.9) pociąga oczywiście $M \cong N$. Również nad pierścieniami ideałów głównych $[M] = [N]$ pociąga $M \cong N$. Rzeczywiście, na podstawie wniosku 4.2.3, skończenie generowany moduł projektywny nad pierścieniem ideałów głównych jest modułem wolnym skończonej rangi, zatem (5.9) pociąga równość rang wolnych modułów M i N, zatem ich izomorfizm. W szczególności więc stabilny izomorfizm skończenie generowanych modułów projektywnych pokrywa się z izomorfizmem modułów nad pierścieniem $R = L[X]$ wielomianów jednej zmiennej nad dowolnym ciałem L. W latach 60-tych XX wieku intrygującym problemem było pytanie, czy stabilny izomorfizm pokrywa się z izomorfizmem nad pierścieniem wielomianów wielu zmiennych $R = L[X_1, \ldots, X_n]$, gdzie L jest dowolnym ciałem. Inna wersja tego pytania brzmi następująco: czy nad pierścieniem wielomianów $R-$moduł projektywny stabilnie równoważny z modułem wolnym musi być modułem wolnym? Przypuszczenie, że odpowiedź jest "tak" znane było jako *hipoteza Serre'a*. W roku 1976 opublikowano dwa niezależne dowody hipotezy Serre'a znalezione przez D. Quillena i A. A. Suslina.

Zwracamy uwagę na fakt, że istnieją przykłady pierścieni, dla których stabilny izomorfizm modułów nie pokrywa się z izomorfizmem. Można, na przykład, pokazać, że taka sytuacja ma miejsce nad pierścieniem[2]

$$R = \mathbb{R}[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1).$$

[2]Zobacz pracę Lama i Siu cytowaną w §5.5.3.

5.5.2 Funktor K_0

Konstrukcja grupy Grothendiecka $K_0\mathcal{P}(R)$ przyporządkowuje każdemu obiektowi R kategorii pierścieni $\mathcal{R}$ grupę abelową $K_0\mathcal{P}(R)$, czyli obiekt kategorii grup abelowych $\mathcal{A}$. Faktycznie jest to odwzorowanie obiektowe funktora kowariantnego $K_0 : \mathcal{R} \to \mathcal{A}$.

Dla wyjaśnienia działania tego funktora powinniśmy wskazać odpowiednie odwzorowanie morfizmowe. Jeśli $h : R \to S$ jest morfizmem w kategorii pierścieni (homomorfizmem pierścieni), to

$$K_0h : K_0\mathcal{P}(R) \to K_0\mathcal{P}(S)$$

powinien być homomorfizmem grup abelowych. Dla określenia K_0h powinniśmy więc przede wszystkim dysponować metodą przyporządkowania modułowi projektywnemu nad pierścieniem R modułu projektywnego nad pierścieniem S. Tę operację realizuje omawiana przez nas wcześniej konstrukcja iloczynu tensorowego modułów (zob. rozdział 3.6). Homomorfizm pierścieni $h : R \to S$ pozwala poprzez operację zwężenia pierścienia skalarów (omawianą w przykładzie 3.1.6) traktować S jako $R-$moduł (z działaniem zewnętrznym $a \cdot b = h(a)b$). Dla każdego $R-$modułu M rozpatrujemy teraz iloczyn tensorowy $S \otimes_R M$ dwóch $R-$modułów. Moduł ten ma jednak także strukturę $S-$modułu (z mnożeniem tensorów prostych $b \otimes m$ przez skalary $x \in S$ określonym następująco: $x \cdot (b \otimes m) = xb \otimes m$). Przejście od $R-$modułu M do $S-$modułu $S \otimes_R M$ jest podstawą do określenia homomorfizmu $F_R \to F_S$ a w konsekwencji także homomorfizmu grup abelowych $K_0h : K_0\mathcal{P}(R) \to K_0\mathcal{P}(S)$. Objaśnia to z grubsza sposób traktowania K_0 jako funktora z kategorii pierścieni do kategorii grup abelowych.

W końcu zwrócimy jeszcze uwagę, że konstrukcję grupy Grothendiecka, którą przeprowadziliśmy szczegółowo dla kategorii $\mathcal{P}(R)$ skończenie generowanych $R-$modułów projektywnych można powtórzyć dla każdej kategorii $\mathcal{A}$, w której jest określone pojęcie ciągu dokładnego. Fakt, że wykorzystaliśmy rozszczepialność ciągów dokładnych w kategorii modułów projektywnych i zastąpiliśmy je rozkładami modułów na sumy obiektów jest specyfiką kategorii $\mathcal{P}(R)$ pozwalającą uzyskać tak przejrzyste rezultaty jak, na przykład, stwierdzenie 5.5.2. W ogólnym przypadku nie można oczekiwać, że sprawy potoczą się tak dobrze, tym niemniej jest możliwa konstrukcja grupy Grothendiecka $K_0\mathcal{A}$ jako grupy ilorazowej F/H przy odpowiednim określeniu grupy abelowej wolnej F i jej podgrupy H. W ten sposób funktor K_0 staje się jednym z rutynowych pojęć teorii kategorii.

5.5.3 $K-$teoria

Funktor K_0 rozważany w latach pięćdziesiątych XX wieku przez A. Grothendiecka jest zaledwie pierwszym z ciągu funktorów K_i, które są przedmiotem badań $K-$teorii. Dla pierścienia R grupę K_1R definiuje się jako grupę ilorazową grupy macierzy $\mathbf{GL}(R)$ przez jej komutant. Przy tym $\mathbf{GL}(R)$ jest sumą mnogościową grup macierzy odwracalnych $\mathbf{GL}(n, R)$ dla wszystkich $n \geqslant 1$. Aby można było tutaj mówić o sumie mnogościowej traktuje się $\mathbf{GL}(n, R)$ jako podgrupę $\mathbf{GL}(n + 1, R)$ poprzez włożenie

$$A \mapsto \begin{bmatrix} A & 0 \\ 0 & 1 \end{bmatrix}.$$

Bardzo przystępne wprowadzenie funktorów K_0 i K_1 oraz informacje o związkach algebraicznej K-teorii z topologiczną K-teorią można znaleźć w artykule przeglądowym:

T. Y. Lam and M. K. Siu, K_0 *and* K_1 - *an introduction to algebraic* $K-$*theory.* American Mathematical Monthly **82** (1975), 329–364.

Funktor K_2 został wprowadzony przez J. Milnora w roku 1967. Dla pierścienia R grupę K_2R definiuje się jako centrum tak zwanej grupy Steinberga, określonej przy pomocy generatorów i relacji wzorowanych na relacjach spełnianych przez komutatory macierzy elementarnych w grupach $\mathbf{GL}(n, R)$. Najprzystępniejszym źródłem wiadomości na ten temat pozostaje książka Milnora:

J. Milnor, *Introduction to algebraic* $K-$*theory.* Annals of Math. Studies 72, Princeton, 1971.

Jakkolwiek grupy abelowe K_0R, K_1R, K_2R są definiowane niezależnie od siebie, są one związane pewnymi naturalnymi homomorfizmami oddającymi istotne i głębokie własności pierścieni. Ponadto, istnieje ścisła analogia pomiędzy *algebraicznymi* i *topologicznymi* $K-$funktorami, z tym, że w topologii istniała już zaawansowana teoria wyższych funktorów K_i. W związku z tym w latach sześćdziesiątych XX wieku trwała bardzo intensywna praca nad poszukiwaniem dalszych funktorów K_i, które przedłużałyby naturalne związki pomiędzy K_0R, K_1R, K_2R i utrzymały analogie z topologiczną $K-$teorią. Na początku lat siedemdziesiątych problem ten został rozwiązany przez D. Quillena, który zdefiniował *właściwe* funktory K_i dla wszystkich i sankcjonując w ten sposób powstanie algebraicznej $K-$teorii. Oficjalnym historycznym dokumentem jest referat Quillena na kongresie w Vancouver:

D. Quillen, *Higher algebraic* $K-$*theory.* Proc. ICM, Vancouver (1974), 171–176.

5.6 Zadania

1. Niech f będzie morfizmem w kategorii pierścieni przemiennych. Udowodnić, że
(a) f jest injektywnym homomorfizmem pierścieni wtedy i tylko wtedy, gdy f jest kategoryjnym monomorfizmem.
(b) Jeśli f jest surjektywnym homomorfizmem pierścieni, to f jest kategoryjnym epimorfizmem.

2. Niech f będzie morfizmem w kategorii modułów. Udowodnić, że
(a) f jest injektywnym homomorfizmem modułów wtedy i tylko wtedy, gdy f jest kategoryjnym monomorfizmem.
(b) f jest surjektywnym homomorfizmem modułów wtedy i tylko wtedy, gdy f jest kategoryjnym epimorfizmem.

3. (a) Udowodnić, że w kategorii zbiorów morfizm jest monomorfizmem wtedy i tylko wtedy gdy jest odwzorowaniem injektywnym.
(b) Udowodnić, że w kategorii zbiorów morfizm jest epimorfizmem wtedy i tylko wtedy gdy jest odwzorowaniem surjektywnym.

4. (a) Udowodnić, że w kategorii grup morfizm jest monomorfizmem wtedy i tylko

wtedy gdy jest homomorfizmem injektywnym.
(b) Udowodnić, że w kategorii grup morfizm jest epimorfizmem wtedy i tylko wtedy gdy jest homomorfizmem surjektywnym.

5. Udowodnić, że w kategorii torsyjnych grup abelowych istnieją nieskończone iloczyny proste (produkty).

6. Określić kategorie (poprzez wskazanie obiektów i morfizmów), w których następujące obiekty są obiektami początkowymi:
(a) grupa ilorazowa, pierścień ilorazowy, moduł ilorazowy;
(b) grupa wolna $F(X)$ z wolnym zbiorem generatorów X;
(c) pierścień ułamków $S^{-1}P$ względem zbioru multyplikatywnego S;
(d) $A-$moduł wolny z bazą $\mathcal{B}$;
(e) iloczyn tensorowy modułów $M \otimes N$.

Rozdział 6

Pierścienie noetherowskie

Ostatnie zmiany 17.03.2009 r.

6.1 Moduły i pierścienie noetherowskie

W tym rozdziale rozpatrywać będziemy wyłącznie moduły nad pierścieniami przemiennymi.
W związku z tym, w tym rozdziale słowo *pierścień* oznacza *pierścień przemienny*. Przypomnijmy, że w $A-$module M podzbiór S modułu M nazywamy *zbiorem generatorów* modułu M, jeśli każdy element $m \in M$ można przedstawić w postaci

$$m = x_1 m_1 + \cdots + x_r m_r, \quad \text{gdzie} \quad x_1, \ldots, x_r \in A, \quad m_1, \ldots, m_r \in S.$$

Nie wymagamy tutaj żadnej jednoznaczności tego przedstawienia. Jeśli moduł M ma skończony zbiór generatorów $S = \{m_1, \ldots, m_r\}$, to mówimy, że M jest *skończenie generowany* i piszemy

$$M = (m_1, \ldots, m_r) = Am_1 + \cdots + Am_r.$$

Przykład 6.1.1. Addytywna grupa $\mathbb{Q}$ ciała liczb wymiernych jest $\mathbb{Z}-$modułem. Dla każdej liczby całkowitej $i \geqslant 0$ oraz dla ustalonej liczby pierwszej p niech $\mathbb{Z}[1/p^i]$ będzie podgrupą cykliczną grupy $\mathbb{Q}$ (czyli podmodułem $\mathbb{Z}-$modułu $\mathbb{Q}$) generowaną przez liczbę $1/p^i$. A więc $\mathbb{Z}[1/p^i]$ składa się z wszystkich liczb wymiernych, które można zapisać w postaci a/p^i, gdzie $a \in \mathbb{Z}$. Połóżmy też

$$M(p) := \bigcup_{i \geqslant 0} \mathbb{Z}[1/p^i].$$

Oczywiście $M(p)$ jest podgrupą $\mathbb{Q}$. Łatwo sprawdzić, że grupa $M(p)$ *nie jest skończenie generowana*. A więc $\mathbb{Z}-$moduł $\mathbb{Q}$, który sam nie jest skończenie generowany, zawiera nieskończenie wiele podmodułów $M(p)$ (dla wszystkich liczb pierwszych p), które także nie są skończenie generowane.
Zauważmy też, że we wznoszącym się łańcuchu podmodułów

$$\mathbb{Z}[1/p^1] \subset \mathbb{Z}[1/p^2] \subset \cdots \subset \mathbb{Z}[1/p^i] \subset \cdots$$

mamy $\mathbb{Z}[1/p^i] \neq \mathbb{Z}[1/p^{i+1}]$ dla każdego $i \geqslant 0$. Łańcuch ten zawiera więc nieskończenie wiele różnych podmodułów $\mathbb{Z}-$modułu $\mathbb{Q}$.
Przy ustalonym p, zbiór wszystkich podmodułów $\mathbb{Z}[1/p^i]$, traktowany jako zbiór uporządkowany częściowo przez inkluzję, nie zawiera też podmodułu maksymalnego.

6.1.1 Moduły noetherowskie

Przykład 6.1.1 wskazuje że moduły nie mają na ogół pewnych własności o charakterze skończonościowym. W tym rozdziale rozpatrywać będziemy moduły, które w przeciwieństwie do $\mathbb{Z}-$modułu $\mathbb{Q}$, mają trzy własności opisane w następującej definicji.

Definicja **6.1.1.** Mówimy, że $A-$moduł M spełnia warunek *skończonej generowalności* (FG), jeśli każdy podmoduł modułu M jest skończenie generowany (ang. *finitely generated*).

Mówimy, że $A-$moduł M spełnia warunek *łańcucha wznoszącego* (ACC), (ang. *ascending chain condition*), jeśli każdy łańcuch wznoszący podmodułów modułu M

$$M_1 \subset M_2 \subset \cdots \subset M_n \subset \cdots, \quad M_i \neq M_{i+1}, \tag{6.1}$$

jest skończony.

Mówimy, że $A-$moduł M spełnia warunek *maksymalności* (MAX) jeśli każdy niepusty zbiór $\mathcal{S}$ podmodułów modułu M zawiera element maksymalny (tzn. taki $M_0 \in \mathcal{S}$, że jeśli $N \in \mathcal{S},\ M_0 \subseteq N$, to $M_0 = N$).

Twierdzenie **6.1.2.** *Dla każdego $A-$modułu M,*

$$\text{(FG)} \quad \Leftrightarrow \quad \text{(ACC)} \quad \Leftrightarrow \quad \text{(MAX)}.$$

Dowód. (FG) $\Rightarrow$ (ACC). Dla dowolnego łańcucha (6.1) podmodułów modułu M rozpatrzmy $N := \bigcup_{i\geqslant 1} M_i$. Jest to podmoduł modułu M, zatem na podstawie warunku (FG) podmoduł ten jest skończenie generowany, to znaczy $N = (n_1, \ldots, n_r)$, dla pewnych $n_1, \ldots, n_r \in N$. Każdy z elementów n_j należy do pewnego podmodułu M_i łańcucha (6.1), skąd łatwo wynika że w łańcuchu (6.1) istnieje podmoduł M_t, zawierający wszystkie elementy $n_1, \ldots, n_r$. Wtedy mamy $N = (n_1, \ldots, n_r) \subseteq M_t \subseteq N$, skąd otrzymujemy $M_t = N$. Pozostaje zauważyć, że

$$N = M_t \subseteq M_{t+1} \subseteq M_{t+2} \subseteq \cdots \quad \subseteq \bigcup_{i\geqslant 1} M_i = N,$$

skąd $M_t = M_{t+1} = M_{t+2} = \cdots$. A więc łańcuch (6.1) zawiera tylko skończoną liczbę różnych podmodułów.

(ACC) $\Rightarrow$ (MAX). Niech $\mathcal{S}$ będzie rodziną podmodułów modułu M. Obieramy dowolny podmoduł $M_1 \in \mathcal{S}$. Jeśli M_1 nie jest maksymalnym elementem $\mathcal{S}$, to istnieje $M_2 \in \mathcal{S}$ taki, że $M_1 \subset M_2$ i $M_1 \neq M_2$. Jeśli M_2 nie jest maksymalnym elementem $\mathcal{S}$, to istnieje $M_3 \in \mathcal{S}$ taki, że $M_2 \subset M_3$ i $M_2 \neq M_3$. W ten sposób konstruujemy wznoszący łańcuch (6.1) podmodułów modułu M, który na podstawie (ACC) jest skończony. Zatem ostatni element tego łańcucha jest elementem maksymalnym w $\mathcal{S}$.

(MAX) $\Rightarrow$ (FG). Niech N będzie podmodułem M. Rozważmy rodzinę $\mathcal{S}$ wszystkich skończenie generowanych podmodułów modułu N. Na podstawie (MAX), rodzina ta zawiera element maksymalny $N' = (n_1, n_2, \ldots, n_r)$. Gdyby istniał element $n \in N$, który nie należy do N', to $N' + An$ jest skończenie generowanym podmodułem

N, który ostro zawiera maksymalny skończenie generowany podmoduł N' modułu N, sprzeczność. Zatem $N = N' = (n_1, n_2, \ldots, n_r)$ jest skończenie generowanym podmodułem M. □

Definicja **6.1.3.** $A-$moduł M nazywa się modułem *noetherowskim*[1], jeśli M spełnia jeden (a więc wszystkie) z warunków (FG), (ACC), (MAX).

Przykład 6.1.2. Jeśli A jest ciałem i M jest skończenie wymiarową przestrzenią wektorową nad A, to M jest noetherowskim $A-$modułem. Wynika to z twierdzenia algebry liniowej mówiącego, że wymiar podprzestrzeni N przestrzeni M nie przekracza wymiaru przestrzeni M. Natomiast nieskończenie wymiarowe przestrzenie wektorowe nie są modułami noetherowskimi.

Podobnie, grupa abelowa wolna o skończonej randze jest noetherowskim $\mathbb{Z}-$modułem (zob. dowód twierdzenia 4.3.7). Stąd łatwo wyprowadzić wniosek, że każda skończenie generowana grupa abelowa jest noetherowskim $\mathbb{Z}-$modułem. Natomiast $\mathbb{Z}-$moduł $\mathbb{Q}$ nie jest modułem noetherowskim, jak to wynika z przykładu 6.1.1.

Twierdzenie **6.1.4.** *Każdy podmoduł modułu noetherowskiego jest modułem noetherowskim. Każdy moduł ilorazowy modułu noetherowskiego jest modułem noetherowskim.*

Dowód. Niech N będzie podmodułem modułu noetherowskiego M. Ponieważ M spełnia warunek (FG), każdy podmoduł P modułu N jest skończenie generowany (bo P jest także podmodułem modułu M). A więc N jest modułem noetherowskim. Rozważmy teraz moduł ilorazowy M/N i homomorfizm kanoniczny $\kappa : M \to M/N$. Na podstawie twierdzenia 3.2.2 o odpowiedniości każdy łańcuch wznoszący podmodułów modułu M/N ma swój przeciwobraz poprzez κ^{-1} w module M. Jeśli więc M spełnia warunek (ACC), to także M/N spełnia (ACC). □

Twierdzenie **6.1.5.** *Niech N będzie podmodułem modułu M. Jeśli N i M/N są modułami noetherowskimi, to M jest modułem noetherowskim.*

Dowód. Udowodnimy, że moduł M spełnia warunek (ACC).
Niech więc $M_1 \subseteq M_2 \subseteq \cdots$ będzie dowolnym łańcuchem podmodułów modułu M. Z tym łańcuchem wiążemy dwa następujące łańcuchy podmodułów modułów N i M/N, odpowiednio:

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots$$

$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \cdots$$

Ponieważ moduły N i M/N spełniają (ACC), można dobrać wskaźnik j tak, by

$$M_j \cap N = M_{j+1} \cap N = \cdots \tag{6.2}$$

$$(M_j + N)/N = (M_{j+1} + N)/N = \cdots \tag{6.3}$$

Pokażemy, iż stąd wynika $M_j = M_{j+1} = \cdots$. Wystarczy oczywiście pokazać, że (6.2) i (6.3) pociągają $M_j = M_{j+1}$. Z założenia mamy $M_j \subseteq M_{j+1}$, niech więc $x \in M_{j+1}$. Wtedy z (6.3) otrzymujemy $x + N \in (M_j + N)/N$. Istnieją zatem $y \in M_j$

[1]Nazwa ta pochodzi od nazwiska Emmy Noether (1882–1935).

oraz $n \in N$ takie, że $x + N = y + n + N = y + N$. A więc $x - y \in N$. Ponadto $x \in M_{j+1},\ y \in M_j \subseteq M_{j+1}$, a więc także $x - y \in M_{j+1}$. Stąd $x - y \in M_{j+1} \cap N = M_j \cap N$, to ostatnie na podstawie (6.2). Zatem $x - y \in M_j$ i wobec $y \in M_j$ otrzymujemy stąd $x \in M_j$. Pokazaliśmy więc, że $M_{j+1} \subseteq M_j$, skąd wynika już równość $M_j = M_{j+1}$. □

WNIOSEK **6.1.6.** *Niech M, M', M'' będą $A-$modułami i niech ciąg*

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$$

będzie ciągiem dokładnym. Moduł M jest noetherowski wtedy i tylko wtedy gdy moduły M' i M'' są noetherowskie.

Dowód. Jeśli $N = f(M')$, to N jest jądrem homomorfizmu g. Zatem $M'' \cong M/N$. Jeśli M jest noetherowski, to N i M/N są noetherowskie na podstawie twierdzenia 6.1.4, zatem noetherowskie są także izomorficzne z nimi moduły M' i M''. Na odwrót, jeśli M' i M'' są noetherowskie, to noetherowskie są także N i M/N, a więc M jest noetherowski na podstawie twierdzenia 6.1.5. □

6.1.2 Pierścienie noetherowskie

Pierścień A nazywa się pierścieniem *noetherowskim*, jeśli $A-$moduł A jest noetherowski.

Ta zwięzła definicja wymaga komentarza. Przede wszystkim przypomnijmy, że podmodułami $A-$modułu A są ideały pierścienia A. Pierścień A spełnia więc warunek (FG), gdy każdy ideał pierścienia A jest skończenie generowany. Podobnie, pierścień A spełnia warunek (ACC) gdy każdy łańcuch wznoszący ideałów pierścienia A

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots \subset \mathfrak{a}_n \subset \cdots , \quad \mathfrak{a}_i \neq \mathfrak{a}_{i+1}$$

jest skończony. Wreszcie pierścień A spełnia warunek (MAX) gdy każdy niepusty zbiór $\mathcal{S}$ ideałów pierścienia A zawiera ideał maksymalny w zbiorze $\mathcal{S}$ (nie musi to oczywiście być ideał maksymalny pierścienia A). Na podstawie twierdzenia 6.1.2 te trzy własności pierścienia A są równoważne.
Wynika stąd w szczególności, że pierścienie ideałów głównych, takie jak $\mathbb{Z}$ i $K[X]$, gdzie K jest ciałem, są pierścieniami noetherowskimi (gdyż każdy ideał jest generowany przez zbiór jednoelementowy, zatem spełniony jest warunek (FG)). Ponadto pierścienie ideałów głównych mają własności (ACC) i (MAX). Okazuje się, że także pierścień $\mathbb{Z}[X]$ wielomianów o współczynnikach całkowitych, mimo że nie jest pierścieniem ideałów głównych, jest pierścieniem noetherowskim. Wynika to z twierdzenia Hilberta o bazie, które udowodnimy poniżej.

TWIERDZENIE **6.1.7.** (Twierdzenie Hilberta o bazie.)
Jeśli pierścień A jest noetherowski, to pierścień $A[X]$ wielomianów jednej zmiennej o współczynnikach z pierścienia A, jest pierścieniem noetherowskim.

Dowód. Pokażemy, że pierścień $A[X]$ spełnia warunek (FG). Niech więc $\mathfrak{a}$ będzie ideałem pierścienia $A[X]$. Ideał $\mathfrak{a}$ jest sumą mnogościową podzbiorów złożonych z wielomianów tego samego stopnia należących do $\mathfrak{a}$. Dla każdej liczby całkowitej $i \geqslant 0$

rozważmy zbiór $\mathfrak{a}_i$ złożony z zera pierścienia A oraz tych wszystkich elementów pierścienia A, które są najwyższymi współczynnikami wielomianów stopnia i należących do ideału $\mathfrak{a}$. Tak więc

$$\mathfrak{a}_i := \{a \in A : \exists\, a_0, \ldots, a_{i-1} \in A \quad aX^i + a_{i-1}X^{i-1} + \cdots + a_1X + a_0 \in \mathfrak{a}\}.$$

Łatwo sprawdza się, że $\mathfrak{a}_i$ jest ideałem w pierścieniu A oraz $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$ dla każdego $i \geqslant 0$. To ostatnie wynika z faktu, że jeśli $f \in \mathfrak{a}$ jest wielomianem stopnia i z najwyższym współczynnikiem a, to $Xf \in \mathfrak{a}$ jest wielomianem stopnia $i+1$ z najwyższym współczynnikiem a.
Mamy więc łańcuch wznoszący ideałów $\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots$ pierścienia A i wobec założenia, że A jest pierścieniem noetherowskim, łańcuch ten zawiera jedynie skończoną liczbę różnych ideałów. Istnieje więc liczba naturalna r taka, że $\mathfrak{a}_r = \mathfrak{a}_{r+1} = \cdots$.
Skorzystamy jeszcze raz z faktu, że A jest pierścieniem noetherowskim obierając dla każdego z ideałów $\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_r$ skończony układ generatorów. Niech n będzie największą spośród liczb generatorów tych ideałów. Dopuszczając generatory równe $0 \in A$ możemy założyć, że *każdy* z ideałów $\mathfrak{a}_0, \mathfrak{a}_1, \ldots, \mathfrak{a}_r$ ma $n-$elementowy układ generatorów. Dla każdego $i = 0, 1, \ldots, r$ niech więc

$$a_{i1}, a_{i2}, \ldots, a_{in}$$

będzie układem generatorów ideału $\mathfrak{a}_i$. Dla każdego niezerowego a_{ij} obieramy wielomian $f_{ij} \in \mathfrak{a}$ stopnia i, którego najwyższym współczynnikiem jest element a_{ij}, jeśli zaś $a_{ij} = 0$, to jako f_{ij} obieramy wielomian zerowy. Udowodnimy, że wielomiany f_{ij} tworzą zbiór generatorów ideału $\mathfrak{a}$.

Niech $\mathfrak{b}$ będzie ideałem pierścienia $A[X]$ generowanym przez wszystkie wielomiany f_{ij}. Zatem $\mathfrak{b} \subseteq \mathfrak{a}$ i należy udowodnić, że $\mathfrak{b} = \mathfrak{a}$. Niech więc $f \in \mathfrak{a}$ i niech d będzie stopniem wielomianu f. Dla dowodu, że

$$f \in \mathfrak{a} \quad \Rightarrow \quad f \in \mathfrak{b} \tag{6.4}$$

posłużymy się indukcją ze względu na d.
Jeśli $d = 0$, to f jest wielomianem stałym, zatem należy do ideału $\mathfrak{a}_0$ generowanego przez $f_{01} = a_{01}, \ldots, f_{0n} = a_{0n}$. Ponieważ wszystkie te generatory należą do $\mathfrak{b}$, więc $\mathfrak{a}_0 \subseteq \mathfrak{b}$, skąd $f \in \mathfrak{b}$.

Załóżmy teraz, że $0 < d \leqslant r$ oraz (6.4) zachodzi dla wszystkich wielomianów stopnia $< d$. Niech $f \in \mathfrak{a}$ będzie wielomianem stopnia d. Wtedy istnieją $e_1, \ldots, e_n \in A$ takie, że wielomian

$$h := f \ - \ (e_1 f_{d1} + \cdots + e_n f_{dn})$$

ma stopień mniejszy od d i także należy do ideału $\mathfrak{a}$. Na podstawie założenia indukcyjnego $h \in \mathfrak{b}$, skąd także $f \in \mathfrak{b}$.

W końcu załóżmy, że $d > r$. Wtedy każdy z wielomianów

$$X^{d-r} f_{r1}, \ldots, X^{d-r} f_{rn}$$

ma stopień d oraz najwyższe współczynniki tych wielomianów generują ideał $\mathfrak{a}_r$. Ponieważ jednak $\mathfrak{a}_r = \mathfrak{a}_d$ i najwyższy współczynnik wielomianu f należy do $\mathfrak{a}_d$, więc

współczynnik ten da się przedstawić jako kombinacja liniowa generatorów ideału $\mathfrak{a}_r$. Istnieją więc $c_1, \ldots, c_n \in A$ takie, że wielomian

$$g := f \ - \ (c_1 X^{d-r} f_{r1} + \cdots + c_n X^{d-r} f_{rn}) \tag{6.5}$$

ma stopień mniejszy od d. Ponadto z (6.5) wynika, że $g \in \mathfrak{a}$. Zatem na podstawie założenia indukcyjnego $g \in \mathfrak{b}$. Zauważmy jednak, że z równości (6.5) wynika, iż $f \in \mathfrak{b}$ wtedy i tylko wtedy gdy $g \in \mathfrak{b}$. A więc $f \in \mathfrak{b}$. Kończy to dowód (6.4). Zatem $\mathfrak{a} = \mathfrak{b}$ jest ideałem generowanym przez skończony układ wielomianów f_{ij}. □

Wniosek **6.1.8.** *Pierścienie $\mathbb{Z}[X]$ i $\mathbb{Z}[X_1, \ldots, X_n]$ wielomianów jednej i wielu zmiennych o współczynnikach całkowitych są pierścieniami noetherowskimi.*

Dowód. Dla pierścienia $\mathbb{Z}[X]$ wynika to bezpośrednio z twierdzenia Hilberta o bazie. Natomiast dla pierścienia wielu zmiennych zauważamy, że

$$\mathbb{Z}[X_1, \ldots, X_n] = \mathbb{Z}[X_1, \ldots, X_{n-1}][X_n],$$

i stosujemy indukcję ze względu na liczbę zmiennych. □

Wniosek **6.1.9.** *Jeśli K jest ciałem, to pierścień wielomianów $K[X_1, \ldots, X_n]$ wielomianów wielu zmiennych o współczynnikach z ciała K jest pierścieniem noetherowskim.*

Dowód. Indukcja ze względu na liczbę zmiennych. □

Twierdzenie Hilberta można uzupełnić uwagą, że twierdzenie do niego odwrotne jest także prawdziwe. Otrzymujemy w ten sposób następujący warunek konieczny i wystarczający na to by pierścień A był noetherowski.

Twierdzenie **6.1.10.** *Dla dowolnego pierścienia A, pierścień A jest noetherowski wtedy i tylko wtedy gdy pierścień wielomianów $A[X]$ jest noetherowski.*

Dowód. Wobec twierdzenia Hilberta wystarczy udowodnić, że jeśli pierścień $A[X]$ jest noetherowski, to A jest noetherowski. Niech $\mathfrak{a}$ będzie ideałem w pierścieniu A i rozpatrzmy ideał $\mathfrak{a}A[X]$ pierścienia $A[X]$ generowany przez podzbiór $\mathfrak{a}$ pierścienia $A[X]$. Mamy zatem

$$\mathfrak{a}A[X] = \Big\{ a_1 h_1 + \cdots + a_r h_r \in A[X] : a_i \in \mathfrak{a},\ h_i \in A[X],\ r \in \mathbb{N} \Big\}.$$

Ponieważ $A[X]$ jest noetherowski, więc ideał ten jest skończenie generowany, powiedzmy

$$\mathfrak{a}A[X] = (f_1, \ldots, f_k)$$

dla pewnych wielomianów $f_i \in A[X]$. Dla dowolnego elementu $a \in \mathfrak{a}$ wobec $\mathfrak{a} \subset \mathfrak{a}A[X]$ mamy przedstawienie

$$a = g_1 f_1 + \cdots + g_k f_k$$

dla pewnych $g_i \in A[X]$ i stąd $a = g_1(0) f_1(0) + \cdots + g_k(0) f_k(0)$. Zatem

$$\mathfrak{a} \subseteq (f_1(0), \ldots, f_k(0)).$$

Z drugiej strony każdy generator f_i ideału $\mathfrak{a}A[X]$ ma przedstawienie postaci

$$f_i = a_{i1}h_{i1} + \cdots + a_{ir}h_{ir}$$

dla pewnych $a_{ij} \in \mathfrak{a}$, $h_{ij} \in A[X]$, $r \in \mathbb{N}$. Stąd wynika, że

$$f_i(0) = a_{i1}h_{i1}(0) + \cdots + a_{ir}h_{ir}(0) \in \mathfrak{a}.$$

Wobec tego $(f_1(0), \ldots, f_k(0)) \subseteq \mathfrak{a}$ i w rezultacie otrzymujemy równość

$$\mathfrak{a} = (f_1(0), \ldots, f_k(0)).$$

Pokazaliśmy więc, że każdy ideał $\mathfrak{a}$ pierścienia A jest skończenie generowany i wobec tego A jest pierścieniem noetherowskim. □

Twierdzenie 6.1.10 pokazuje, że podpierścień A pierścienia noetherowskiego $A[X]$ jest także noetherowski. Nie jest jednak prawdą, że każdy podpierścień każdego pierścienia noetherowskiego jest noetherowski. Pokazuje to następujący przykład.

Przykład 6.1.3. Niech A będzie podpierścieniem pierścienia $\mathbb{Z}[X]$ składającym się z wszystkich wielomianów, których wszystkie współczynniki potęg X^i, dla $i > 0$, są liczbami parzystymi. Można więc napisać, że

$$A = \mathbb{Z} + 2X\mathbb{Z}[X]$$

jest sumą podpierścienia $\mathbb{Z}$ i ideału $2X\mathbb{Z}[X]$ pierścienia $\mathbb{Z}[X]$, skąd łatwo wynika, że A jest istotnie podpierścieniem $\mathbb{Z}[X]$. W pierścieniu A rozpatrujemy następujący łańcuch wznoszący ideałów:

$$\mathfrak{a}_1 = (2X) \ \subset \ \mathfrak{a}_2 = (2X, 2X^2) \ \subset \ \mathfrak{a}_3 = (2X, 2X^2, 2X^3) \ \subset \cdots .$$

Najpierw sprawdzimy, że jest to ostro wznoszący łańcuch ideałów. Pokażemy mianowicie, że dla każdego $n \geqslant 1$ wielomian $2X^{n+1}$ nie należy do $\mathfrak{a}_n$. Przypuśćmy, że tak nie jest. Wtedy istnieją wielomiany $f_1, \ldots, f_n \in A$ takie, że

$$2X^{n+1} = 2Xf_1 + 2X^2f_2 + \cdots + 2X^nf_n.$$

Stąd otrzymujemy tożsamość wielomianową

$$X^n = f_1 + Xf_2 + \cdots + X^{n-1}f_n, \quad f_i \in A. \tag{6.6}$$

Wielomian po prawej stronie można zapisać w postaci

$$\Big(f_1(0)+Xf_2(0)+\cdots+X^{n-1}f_n(0)\Big)+\Big(f_1-f_1(0)+X(f_2-f_2(0))+\cdots+X^{n-1}(f_n-f_n(0))\Big).$$

Zauważamy, że pierwsza grupa składników tworzy wielomian stopnia $< n$ i wobec tego nie ma wpływu na współczynnik stojący przy X^n. Natomiast druga grupa składników zawiera wyłącznie wielomiany o współczynnikach parzystych. Wobec tego tożsamość (6.6) nie może mieć miejsca. W pierścieniu A wskazaliśmy więc nieskończony łańcuch różnych ideałów co oznacza, że pierścień A nie jest noetherowski. Pierścień noetherowski $\mathbb{Z}[X]$ zawiera więc podpierścień A, który nie jest noetherowski.

Twierdzenie Hilberta jest pierwszym źródłem przykładów pierścieni noetherowskich. Drugim źródłem takich przykładów jest następujące twierdzenie.

TWIERDZENIE **6.1.11.** *Homomorficzny obraz pierścienia noetherowskiego jest pierścieniem noetherowskim.*

Dowód. Jeśli $h : A \to B$ jest epimorfizmem pierścieni, to na podstawie twierdzenia 2.2.3 o odpowiedniości każdy wznoszący łańcuch ideałów pierścienia B ma swój przeciwobraz w A. Zatem jeśli A spełnia (ACC), to B także spełnia (ACC). □

Przykład 6.1.4. Niech $m \neq 0, 1$ będzie bezkwadratową liczbą całkowitą i niech

$$\mathbb{Z}[\sqrt{m}\,] = \Big\{x + y\sqrt{m} \,:\, x, y \in \mathbb{Z}\Big\}.$$

Odwzorowanie

$$h : \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{m}\,], \quad h(f) = f(\sqrt{m}\,)$$

jest epimorfizmem pierścieni. Ponieważ $\mathbb{Z}[X]$ jest noetherowski, także każdy pierścień $\mathbb{Z}[\sqrt{m}\,]$ jest noetherowski.

Można także łatwo udowodnić, że dla dowolnego pierścienia noetherowskiego A i dla dowolnego podzbioru multyplikatywnego S w A pierścień ułamków AS^{-1} jest także pierścieniem noetherowskim. W szczególności, dla każdego ideału pierwszego $\mathfrak{p}$ pierścienia noetherowskiego A lokalizacja $A_{\mathfrak{p}}$ jest pierścieniem noetherowskim.

6.1.3 Moduły i pierścienie artinowskie

Bardzo naturalnym pomysłem jest zbadanie *warunku łańcucha opadającego* (DCC) (ang. *descending chain condition*), który powstaje z (ACC) przez odwrócenie inkluzji. Mówimy, że $A-$moduł M spełnia warunek *łańcucha opadającego* (DCC), jeśli każdy łańcuch opadający podmodułów modułu M

$$M_1 \supset M_2 \supset \cdots \supset M_n \supset \cdots, \quad M_i \neq M_{i+1},$$

jest skończony. Moduł spełniający (DCC) nazywa się modułem *artinowskim*[2]. Natomiast pierścień A nazywa się artinowski, jeśli $A-$moduł A jest artinowski (każdy opadający łańcuch ideałów pierścienia A jest skończony). Łatwo stwierdzić, że pierścień $\mathbb{Z}$ nie jest pierścieniem artinowskim. Dla każdej liczby całkowitej $a \neq 0, \pm 1$ mamy bowiem nieskończony opadający łańcuch ideałów głównych:

$$(a) \supset (a^2) \supset \cdots \supset (a^n) \supset \cdots \ .$$

Tak więc pierścień noetherowski $\mathbb{Z}$ nie jest pierścieniem artinowskim. Można zauważyć, że jeśli pierścień bez dzielników zera nie jest ciałem, to nie jest pierścieniem artinowskim.
Można natomiast udowodnić, że *każdy pierścień artinowski jest pierścieniem noetherowskim*. Jest przy tym rzeczą ciekawą, że to twierdzenie nie przenosi się na moduły:

[2]Nazwa ta pochodzi od nazwiska Emila Artina (1898–1962).

istnieją moduły artinowskie, które nie są noetherowskie. Przykłady tego typu występują już wśród $\mathbb{Z}-$modułów, czyli grup abelowych. Rozpatrzmy, na przykład, podgrupę

$$\mathbb{C}(p^\infty) = \{x \in \mathbb{C} \ : \ \exists_{n\in\mathbb{N}} \quad x^{p^n} = 1\}$$

multyplikatywnej grupy liczb zespolonych złożoną z tych wszystkich pierwiastków z jedynki, których stopnie są potęgami ustalonej liczby pierwszej p. Ta grupa abelowa nie jest noetherowskim $\mathbb{Z}-$modułem, gdyż zawiera nieskończony łańcuch wznoszący podgrup $\mathbb{C}(p) \subset \mathbb{C}(p^2) \subset \cdots$. Natomiast jest to $\mathbb{Z}-$moduł artinowski, gdyż każda podgrupa właściwa grupy $\mathbb{C}(p^\infty)$ jest skończona !

Informacje o pierścieniach artinowskich można znaleźć w rozdziale II książki S. Balcerzyka i T. Józefiaka, *Pierścienie przemienne*. PWN Warszawa, 1985.

6.2 Rozkład prymarny

W tym rozdziale opiszemy klasyczne uogólnienia twierdzenia o jednoznaczności rozkładu na czynniki pierwsze w pierścieniu $\mathbb{Z}$ liczb całkowitych. Każda liczba całkowita $a \neq 0, \pm 1$ ma jednoznaczne przedstawienie w postaci iloczynu potęg różnych liczb pierwszych,

$$a = \pm p_1^{e_1} \cdots p_s^{e_s},$$

i przedstawienie to jest równoważne przedstawieniu ideału głównego (a) w postaci iloczynu – lub przekroju – ideałów generowanych przez potęgi liczb pierwszych:

$$(a) = (p_1^{e_1}) \cdots (p_s^{e_s}) = (p_1^{e_1}) \cap \cdots \cap (p_s^{e_s}).$$

Ideał w $\mathbb{Z}$ generowany przez potęgę liczby pierwszej nazywa się ideałem *prymarnym*. Twierdzenie o jednoznaczności rozkładu w $\mathbb{Z}$ można więc sformułować następująco: każdy niezerowy ideał właściwy pierścienia $\mathbb{Z}$ ma jednoznaczne przedstawienie w postaci przekroju skończonej liczby ideałów prymarnych (tutaj i poniżej ideałem właściwym pierścienia nazywamy ideał różny od całego pierścienia).

Okazuje się, że uogólnienia tego twierdzenia funkcjonują we wszystkich pierścieniach noetherowskich. Udowodnimy tutaj twierdzenie o istnieniu rozkładu prymarnego w pierścieniach noetherowskich, natomiast bardziej subtelną i obszerną teorię jednoznaczności rozkładu prymarnego przedstawimy jedynie w zarysie. Rozpoczynamy od wprowadzenia pojęcia ideału prymarnego w dowolnym pierścieniu A.

6.2.1 Ideały prymarne

Definicja **6.2.1.** Ideał $\mathfrak{q}$ pierścienia A nazywa się ideałem *prymarnym*, jeśli $\mathfrak{q} \neq A$ i dla każdych $a, b \in A$,

$$ab \in \mathfrak{q} \quad \text{i} \quad b \notin \mathfrak{q} \quad \Rightarrow \quad \exists\, n \in \mathbb{N} \quad a^n \in \mathfrak{q}. \tag{6.7}$$

Przykład 6.2.1. W dowolnym pierścieniu A każdy ideał pierwszy $\mathfrak{q}$ jest oczywiście ideałem prymarnym. Łatwo sprawdzić, że w pierścieniu $\mathbb{Z}$ liczb całkowitych każdy ideał $\mathfrak{q} = (p^m)$, generowany przez potęgę dowolnej liczby pierwszej p, jest ideałem prymarnym.

Ogólniej, jeśli A jest pierścieniem ideałów głównych, to ideał $\mathfrak{q}$ pierścienia A *jest prymarny wtedy i tylko wtedy, gdy jest potęgą ideału pierwszego* (lub równoważnie, gdy jest generowany przez potęgę elementu pierwszego pierścienia A). Rzeczywiście, jeśli $\mathfrak{q} = (p)^n = (p^n)$, gdzie p jest elementem pierwszym w A oraz $p^n|ab$ i $p^n \nmid b$, to z jednoznaczności rozkładu w A wynika, że $p|a$ i wobec tego $p^n|a^n$. Z drugiej strony, jeśli $\mathfrak{q} = (c) \neq A$ i element c nie jest stowarzyszony z potęgą elementu pierwszego, to c dzieli się przez dwa niestowarzyszone elementy pierwsze p i q. Weźmy rozkład $c = ab$ taki, że $p|a$ i $q|b$. Wtedy $c|ab$ i $c \nmid b$ ale również c nie dzieli żadnej potęgi elementu a. Wobec tego $\mathfrak{q} = (c)$ nie jest ideałem prymarnym.

LEMAT **6.2.2.** *Niech $\mathfrak{q} \neq A$ będzie ideałem w pierścieniu A. Następujące warunki są równoważne.*

(a) *Ideał $\mathfrak{q}$ jest prymarny.*
(b) *W pierścieniu ilorazowym $A/\mathfrak{q}$ każdy dzielnik zera jest elementem nilpotentnym.*
(c) *Ideał zerowy pierścienia $A/\mathfrak{q}$ jest prymarny.*

Dowód. Warunek (6.7) definiujący prymarność ideału $\mathfrak{q}$ jest równoważny warunkowi

$$(a+\mathfrak{q})(b+\mathfrak{q}) = \mathfrak{q}, \quad b+\mathfrak{q} \neq \mathfrak{q} \quad \Rightarrow \quad \exists\, n \in \mathbb{N} \quad (a+\mathfrak{q})^n = \mathfrak{q}.$$

Stąd wynika równoważność warunków (a), (b) i (c). □

Przykład 6.2.2. Pokażemy, że w pierścieniu $A = K[X,Y]$ wielomianów dwóch zmiennych nad ciałem K ideał $\mathfrak{q} = (X, Y^2)$ jest prymarny, ale nie jest potęgą ideału pierwszego.
Rozpoczniemy od uwagi, że każdy wielomian $f \in A$ można przedstawić w postaci

$$f = X \cdot g(X,Y) + h(Y) = X \cdot g(X,Y) + Y^2 \cdot h_1(Y) + aY + b,$$

gdzie $g(X,Y) \in A, h(Y), h_1(Y) \in K[Y],\ a, b \in K$. Łatwo sprawdzić, że przyporządkowanie

$$A/\mathfrak{q} \to K[Y]/(Y^2), \quad f+\mathfrak{q} \mapsto aY + b + (Y^2)$$

jest dobrze określone na warstwach i jest izomorfizmem pierścieni. A więc

$$A/\mathfrak{q} \cong K[Y]/(Y^2).$$

Pierścień $K[Y]$ jest pierścieniem ideałów głównych i Y jest elementem pierwszym tego pierścienia, zatem na podstawie przykładu 6.2.1 ideał (Y^2) jest prymarny. Wobec tego (na podstawie lematu 6.2.2) w pierścieniu $K[Y]/(Y^2)$ każdy dzielnik zera jest elementem nilpotentnym i w takim razie w izomorficznym z $K[Y]/(Y^2)$ pierścieniu $A/\mathfrak{q}$ także każdy dzielnik zera jest elementem nilpotentnym. Na podstawie lematu 6.2.2 ideał $\mathfrak{q}$ jest prymarny.
Zauważmy, że ideał $\mathfrak{q}$ nie jest ideałem pierwszym, gdyż pierścień ilorazowy $A/\mathfrak{q}$ ma dzielniki zera (w $K[Y]/(Y^2)$ mamy, na przykład, $(Y+\mathfrak{q})^2 = \mathfrak{q}$ oraz $Y+\mathfrak{q} \neq \mathfrak{q}$). Pokażemy, że nie jest on potęgą żadnego ideału pierwszego pierścienia A. Przypuśćmy zatem, że $\mathfrak{q} = \mathfrak{p}^m$, gdzie $\mathfrak{p}$ jest ideałem pierwszym w A. Wtedy

$$(X, Y^2) = \mathfrak{q} = \mathfrak{p}^m \subseteq \mathfrak{p}$$

pociąga, że $X, Y^2 \in \mathfrak{p}$, zatem także $X, Y \in \mathfrak{p}$. Wobec tego $(X, Y) \subseteq \mathfrak{p}$ i wobec maksymalności ideału (X, Y) otrzymujemy $(X, Y) = \mathfrak{p}$. A więc jeśli $\mathfrak{q}$ jest potęgą ideału pierwszego, to $\mathfrak{q} = (X, Y)^m$. Ponieważ jednak

$$\cdots \subset (X, Y)^3 \subset (X, Y)^2 \subset \mathfrak{q} \subset (X, Y)$$

i wszystkie inkluzje są ostre, wynika stąd, że $\mathfrak{q}$ nie jest potęgą ideału (X, Y), a więc nie jest także potęgą żadnego ideału pierwszego w A.

DEFINICJA **6.2.3.** Ideał $\mathfrak{n}$ pierścienia A nazywa się *nieprzywiedlny*, jeśli $\mathfrak{n} \neq A$ i dla każdych ideałów $\mathfrak{a}$ i $\mathfrak{b}$ pierścienia A,

$$\mathfrak{n} = \mathfrak{a} \cap \mathfrak{b} \quad \Rightarrow \quad \mathfrak{n} = \mathfrak{a} \ \text{ lub } \ \mathfrak{n} = \mathfrak{b}.$$

Przykład 6.2.3. W każdym pierścieniu każdy ideał maksymalny $\mathfrak{n}$ jest nieprzywiedlny, gdyż w przedstawieniu $\mathfrak{n} = \mathfrak{a} \cap \mathfrak{b}$ mamy oczywiście $\mathfrak{n} \subseteq \mathfrak{a}$ i $\mathfrak{n} \subseteq \mathfrak{b}$ i wobec maksymalności $\mathfrak{n}$ mamy $\mathfrak{n} = \mathfrak{a} = \mathfrak{b}$.
Ogólniej, każdy ideał pierwszy jest nieprzywiedlny. Jeśli bowiem dla ideału pierwszego $\mathfrak{p}$ pierścienia A mamy $\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}$ dla pewnych ideałów $\mathfrak{a}$ i $\mathfrak{b}$ pierścienia A, to zakładając, że $\mathfrak{p} \subsetneq \mathfrak{a}$ i $\mathfrak{p} \subsetneq \mathfrak{b}$ możemy wybrać elementy $a \in \mathfrak{a} \setminus \mathfrak{p}$ oraz $b \in \mathfrak{b} \setminus \mathfrak{p}$. Wtedy $ab \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{p}$, skąd wynika, że $a \in \mathfrak{p}$ lub $b \in \mathfrak{p}$, sprzeczność.
W szczególności, w pierścieniu całkowitym ideał zerowy jest nieprzywiedlny.
Nieprzywiedlność ideału $\mathfrak{n}$ pierścienia A można także rozpoznać przez przejście do pierścienia ilorazowego $A/\mathfrak{n}$: *Ideał $\mathfrak{n}$ pierścienia A jest nieprzywiedlny wtedy i tylko wtedy, gdy ideał zerowy pierścienia $A/\mathfrak{n}$ jest nieprzywiedlny.*
Jeśli bowiem $\mathfrak{n}$ jest ideałem nieprzywiedlnym pierścienia A oraz w pierścieniu $A/\mathfrak{n}$ mamy $0 = \mathfrak{n} = \mathfrak{a}' \cap \mathfrak{b}'$, gdzie $\mathfrak{a}'$ i $\mathfrak{b}'$ są ideałami pierścienia $A/\mathfrak{n}$, to biorąc przeciwobrazy $\mathfrak{a} := \kappa^{-1}(\mathfrak{a}')$, $\mathfrak{b} := \kappa^{-1}(\mathfrak{b}')$ poprzez homomorfizm kanoniczny $\kappa : A \to A/\mathfrak{n}$ otrzymamy

$$\mathfrak{n} = \kappa^{-1}(\mathfrak{n}) = \kappa^{-1}(\mathfrak{a}') \cap \kappa^{-1}(\mathfrak{b}') = \mathfrak{a} \cap \mathfrak{b}$$

skąd wobec nieprzywiedlności $\mathfrak{n}$ w A wynika, że $\mathfrak{n} = \mathfrak{a}$ lub $\mathfrak{n} = \mathfrak{b}$. A więc także $\mathfrak{n} = \kappa(\mathfrak{n}) = \kappa(\mathfrak{a}) = \mathfrak{a}'$ lub $\mathfrak{n} = \kappa(\mathfrak{n}) = \kappa(\mathfrak{b}) = \mathfrak{b}'$, co dowodzi nieprzywiedlności ideału zerowego $\mathfrak{n}$ w pierścieniu $A/\mathfrak{n}$.
Podobnie pokazuje się, że nieprzywiedlność ideału zerowego w $A/\mathfrak{n}$ pociąga nieprzywiedlność ideału $\mathfrak{n}$ w pierścieniu A.

LEMAT **6.2.4.** *W pierścieniu noetherowskim każdy ideał nieprzywiedlny jest prymarny.*

Dowód. Niech $\mathfrak{n}$ będzie ideałem nieprzywiedlnym pierścienia noetherowskiego A. Wobec lematu 6.2.2 wystarczy udowodnić, że w pierścieniu ilorazowym $A/\mathfrak{n}$ każdy dzielnik zera jest nilpotentem.
Niech więc $x, y \in A/\mathfrak{n}$, $xy = 0$, $y \neq 0$. Pokażemy, że x jest elementem nilpotentnym pierścienia $A/\mathfrak{n}$. W pierścieniu $A/\mathfrak{n}$ rozważamy wznoszący łańcuch ideałów

$$\mathsf{Ann}\, x \subseteq \mathsf{Ann}\, x^2 \subseteq \cdots \subseteq \mathsf{Ann}\, x^n \subseteq \cdots$$

gdzie $\mathsf{Ann}\, x$ jest *anihilatorem* elementu x, to znaczy, $\mathsf{Ann}\, x = \{z \in A/\mathfrak{n} : zx = 0\}$. Ponieważ A jest pierścieniem noetherowskim, pierścień ilorazowy $A/\mathfrak{n}$ jest także

noetherowski (na podstawie twierdzenia 6.1.11), a więc spełnia warunek (ACC). Istnieje zatem liczba naturalna n taka, że

$$\mathsf{Ann}\, x^n = \mathsf{Ann}\, x^{n+1} = \cdots$$

Stąd wynika, że

$$(x^n) \cap (y) = (0). \tag{6.8}$$

Niech bowiem $a \in (x^n) \cap (y)$. Wtedy $a = bx^n$ i $a = cy$ dla pewnych $b, c \in A/\mathfrak{n}$. Mamy więc

$$bx^{n+1} = bx^n \cdot x = ax = cyx = cxy = c \cdot 0 = 0.$$

Stąd $b \in \mathsf{Ann}\, x^{n+1} = \mathsf{Ann}\, x^n$, a więc $a = bx^n = 0$. Dowodzi to (6.8).
Na podstawie przykładu 6.2.3 ideał zerowy pierścienia $A/\mathfrak{n}$ jest nieprzywiedlny, zatem z (6.8) wynika, że $(x^n) = (0)$ (gdyż $y \in (y)$ oraz $y \neq 0$). A więc $x^n = 0$, i element x jest nilpotentem w $A/\mathfrak{n}$. Dowodzi to prymarności ideału $\mathfrak{n}$. □

Przykład 6.2.4. Ideał prymarny pierścienia noetherowskiego nie musi być nieprzywiedlny. Można pokazać, że w pierścieniu $\mathbb{Z}[X]$ ideał $\mathfrak{q} = (4, 2X, X^2) = (2, X)^2$ jest prymarny (jako potęga ideału maksymalnego, zob. przykład 6.2.8), ale nie jest nieprzywiedlny, gdyż $\mathfrak{q} = (4, X) \cap (2, X^2)$.

LEMAT **6.2.5.** *W pierścieniu noetherowskim każdy ideał właściwy jest przekrojem skończonej liczby ideałów nieprzywiedlnych.*

Dowód. Przypuśćmy, że w pierścieniu noetherowskim A istnieją ideały właściwe nie będące przekrojem skończonej liczby ideałów nieprzywiedlnych. W rodzinie wszystkich takich ideałów pierścienia A istnieje więc element maksymalny $\mathfrak{c}$. Ideał $\mathfrak{c}$ nie jest w szczególności ideałem nieprzywiedlnym. Oczywiście ideał $\mathfrak{c}$ daje się przedstawić jako przekrój dwóch ideałów $\mathfrak{a}$ i $\mathfrak{b}$, na przykład, $\mathfrak{a} = \mathfrak{c}$, $\mathfrak{b} = \mathfrak{c}+(a)$, gdzie a jest dowolnym elementem pierścienia A. Ponieważ jednak $\mathfrak{c}$ nie jest ideałem nieprzywiedlnym musi być przekrojem dwóch ideałów ostro zawierających $\mathfrak{c}$,

$$\mathfrak{c} = \mathfrak{a} \cap \mathfrak{b}, \quad \mathfrak{c} \neq \mathfrak{a}, \ \mathfrak{c} \neq \mathfrak{b}.$$

W takim razie ideały $\mathfrak{a}$ i $\mathfrak{b}$ nie należą do rozpatrywanej rodziny (skoro ostro zawierają maksymalny ideał tej rodziny) i wobec tego każdy z ideałów $\mathfrak{a}$ i $\mathfrak{b}$ jest przekrojem skończonej liczby ideałów nieprzywiedlnych. Wobec tego także $\mathfrak{c} = \mathfrak{a} \cap \mathfrak{b}$ jest przekrojem skończonej liczby ideałów nieprzywiedlnych, co jest sprzeczne z wyborem ideału $\mathfrak{c}$. Przypuszczenie, że lemat jest nieprawdziwy prowadzi więc do sprzeczności. □

TWIERDZENIE **6.2.6.** *W pierścieniu noetherowskim każdy ideał właściwy $\mathfrak{a}$ można przedstawić jako przekrój skończonej liczby ideałów prymarnych:*

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n.$$

Dowód. Lemat 6.2.5 gwarantuje istnienie przedstawienia w postaci przekroju ideałów nieprzywiedlnych, natomiast lemat 6.2.4 pokazuje, że jest to przedstawienie w postaci przekroju ideałów prymarnych. □

Przedstawienie ideału $\mathfrak{a}$ jako przekroju skończonej liczby ideałów prymarnych nazywa się *rozkładem prymarnym* ideału $\mathfrak{a}$. A więc w pierścieniu noetherowskim każdy ideał właściwy ma rozkład prymarny. Przejdziemy teraz do kwestii jednoznaczności rozkładu prymarnego.

6.2.2 Radykał ideału

DEFINICJA **6.2.7.** *Radykałem* $\mathsf{rad}(\mathfrak{a})$ ideału $\mathfrak{a}$ pierścienia A nazywamy zbiór wszystkich elementów pierścienia A, których pewna potęga należy do ideału $\mathfrak{a}$:

$$\mathsf{rad}(\mathfrak{a}) := \{a \in A : \exists\, n \in \mathbb{N} \quad a^n \in \mathfrak{a}\}.$$

Łatwo sprawdza się, że radykał $\mathsf{rad}(\mathfrak{a})$ ideału $\mathfrak{a}$ jest ideałem w pierścieniu A. Jeśli bowiem $a, b \in \mathsf{rad}(\mathfrak{a})$, to istnieją liczby naturalne n, m takie, że $a^n, b^m \in \mathfrak{a}$. Wtedy także $(a-b)^{n+m-1} \in \mathfrak{a}$ i wobec tego $a - b \in \mathsf{rad}(\mathfrak{a})$. Ponadto, jeśli $a \in \mathsf{rad}(\mathfrak{a})$ oraz $x \in A$, to $a^n \in \mathfrak{a}$ dla pewnej liczby naturalnej n i mamy $(ax)^n = a^n x^n \in \mathfrak{a}$. Wobec tego $ax \in \mathsf{rad}(\mathfrak{a})$.

Zauważmy, że dla ideału zerowego (0) dowolnego pierścienia A mamy $\mathsf{rad}((0)) = \mathsf{Nil}\, A$. A więc radykał ideału zerowego pierścienia A jest nilradykałem pierścienia A.

Przykład 6.2.5. Uzasadnimy tutaj następujące własności radykału ideału:

$$\begin{aligned}
\mathfrak{a} &\subseteq \mathsf{rad}(\mathfrak{a}). && (6.9)\\
\mathfrak{a} \subseteq \mathfrak{b} &\Rightarrow \mathsf{rad}(\mathfrak{a}) \subseteq \mathsf{rad}(\mathfrak{b}). && (6.10)\\
\mathsf{rad}(\mathsf{rad}(\mathfrak{a})) &= \mathsf{rad}(\mathfrak{a}). && (6.11)\\
\mathsf{rad}(\mathfrak{a} \cdot \mathfrak{b}) &= \mathsf{rad}(\mathfrak{a} \cap \mathfrak{b}). && (6.12)\\
\mathsf{rad}(\mathfrak{a} \cap \mathfrak{b}) &= \mathsf{rad}(\mathfrak{a}) \cap \mathsf{rad}(\mathfrak{b}). && (6.13)\\
\mathsf{rad}(\mathfrak{a}) = (1) &\Leftrightarrow \mathfrak{a} = (1). && (6.14)\\
\mathsf{rad}(\mathfrak{a} + \mathfrak{b}) &= \mathsf{rad}(\mathsf{rad}(\mathfrak{a}) + \mathsf{rad}(\mathfrak{b})). && (6.15)\\
\mathfrak{a} + \mathfrak{b} = (1) &\Leftrightarrow \mathsf{rad}(\mathfrak{a}) + \mathsf{rad}(\mathfrak{b}) = (1). && (6.16)
\end{aligned}$$

(6.9) i (6.10) wynikają bezpośrednio z definicji radykału. Wykorzystując (6.9) redukujemy dowód (6.11) do dowodu inkluzji $\mathsf{rad}(\mathsf{rad}(\mathfrak{a})) \subseteq \mathsf{rad}(\mathfrak{a})$.
Jeśli $a \in \mathsf{rad}(\mathsf{rad}(\mathfrak{a}))$, to $a^n \in \mathsf{rad}(\mathfrak{a})$ dla pewnej liczby naturalnej n, stąd zaś $(a^n)^m \in \mathfrak{a}$ dla pewnej liczby naturalnej m. Wobec tego $a \in \mathsf{rad}(\mathfrak{a})$.
Dowód (6.12). Ponieważ $\mathfrak{a}\cdot\mathfrak{b} \subseteq \mathfrak{a}\cap\mathfrak{b}$, więc wystarczy pokazać, że $\mathsf{rad}(\mathfrak{a}\cdot\mathfrak{b}) \supseteq \mathsf{rad}(\mathfrak{a}\cap\mathfrak{b})$. Jeśli $a \in \mathsf{rad}(\mathfrak{a} \cap \mathfrak{b})$, to $a^n \in \mathfrak{a} \cap \mathfrak{b}$ dla pewnej liczby naturalnej n. Wtedy $a^{2n} \in \mathfrak{a} \cdot \mathfrak{b}$ i wobec tego $a \in \mathsf{rad}(\mathfrak{a} \cdot \mathfrak{b})$.
Dowód (6.13). $\mathsf{rad}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathsf{rad}(\mathfrak{a}) \cap \mathsf{rad}(\mathfrak{b})$ wynika stąd, że $\mathfrak{a} \cap \mathfrak{b}$ jest podzbiorem zarówno $\mathfrak{a}$ jak i $\mathfrak{b}$. Z drugiej strony, jeśli $a \in \mathsf{rad}(\mathfrak{a}) \cap \mathsf{rad}(\mathfrak{b})$, to $a^n \in \mathfrak{a}$ oraz $a^m \in \mathfrak{b}$ dla pewnych liczb naturalnych n, m. Wobec tego $a^{n+m} \in \mathfrak{a} \cap \mathfrak{b}$, oraz $a \in \mathsf{rad}(\mathfrak{a} \cap \mathfrak{b})$.
Dowód (6.14). $1 \in \mathsf{rad}(\mathfrak{a}) \Leftrightarrow 1^n \in \mathfrak{a}$.
Dowód (6.15). $\mathsf{rad}(\mathfrak{a}+\mathfrak{b}) \subseteq \mathsf{rad}(\mathsf{rad}(\mathfrak{a})+\mathsf{rad}(\mathfrak{b}))$ gdyż $\mathfrak{a}+\mathfrak{b}$ jest podzbiorem $\mathsf{rad}(\mathfrak{a})+\mathsf{rad}(\mathfrak{b})$. Z drugiej strony, jeśli $a \in \mathsf{rad}(\mathsf{rad}(\mathfrak{a}) + \mathsf{rad}(\mathfrak{b}))$, to $a^n \in \mathsf{rad}(\mathfrak{a}) + \mathsf{rad}(\mathfrak{b})$ oraz $a^n = b + c$, gdzie $b^m \in \mathfrak{a}$, $c^k \in \mathfrak{b}$ dla pewnych liczb naturalnych n, m, k. Wtedy $a^{n(m+k)} = (b+c)^{m+k} = b^m x + c^k y$ dla pewnych $x, y \in A$. Wobec tego $a^{n(m+k)} \in \mathfrak{a}+\mathfrak{b}$ oraz $a \in \mathsf{rad}(\mathfrak{a} + \mathfrak{b})$.
Dowód (6.16). Jeśli $1 \in \mathfrak{a} + \mathfrak{b}$, to wobec $\mathfrak{a} + \mathfrak{b} \subseteq \mathsf{rad}(\mathfrak{a}) + \mathsf{rad}(\mathfrak{b})$, mamy także $1 \in \mathsf{rad}(\mathfrak{a}) + \mathsf{rad}(\mathfrak{b})$. Załóżmy teraz, że radykały ideałów $\mathfrak{a}$ i $\mathfrak{b}$ są względnie pierwsze. Wtedy na podstawie (6.15) mamy $1 \in \mathsf{rad}(\mathsf{rad}(\mathfrak{a}) + \mathsf{rad}(\mathfrak{b})) = \mathsf{rad}(\mathfrak{a} + \mathfrak{b})$, oraz $1 \in \mathfrak{a} + \mathfrak{b}$ na podstawie (6.14).

Przykład 6.2.6. Jeśli $\mathfrak{p}$ jest ideałem pierwszym, to $\mathsf{rad}(\mathfrak{p}^m) = \mathfrak{p}$ dla każdej liczby naturalnej m.
Jeśli $a \in \mathsf{rad}(\mathfrak{p}^m)$, to $a^n \in \mathfrak{p}^m$ dla pewnej liczby naturalnej n. Ponieważ $\mathfrak{p}^m \subseteq \mathfrak{p}$, więc $a^n \in \mathfrak{p}$, ponieważ zaś $\mathfrak{p}$ jest ideałem pierwszym wynika stąd, że $a \in \mathfrak{p}$. Na odwrót, jeśli $a \in \mathfrak{p}$, to $a^m \in \mathfrak{p}^m$, zatem $a \in \mathsf{rad}(\mathfrak{p}^m)$.
W szczególności, w pierścieniu $\mathbb{Z}$ liczb całkowitych, dla każdego ideału prymarnego (p^m), gdzie p jest liczbą pierwszą oraz $m \in \mathbb{N}$, mamy $\mathsf{rad}((p^m)) = (p)$.

Przykład 6.2.7. Jeśli $\mathfrak{a}$ jest ideałem pierścienia A oraz $\mathsf{rad}\,\mathfrak{a}$ jest ideałem maksymalnym pierścienia A, to $\mathfrak{a}$ jest ideałem prymarnym.
Niech $\mathfrak{m} = \mathsf{rad}\,\mathfrak{a}$ będzie ideałem maksymalnym w A. Niech $\kappa : A \to A/\mathfrak{a}$ będzie homomorfizmem kanonicznym. Wtedy dla $a \in A$ oraz $n \in \mathbb{N}$ mamy

$$(a + \mathfrak{a})^n = 0 \in A/\mathfrak{a} \iff a^n \in \mathfrak{a} \iff a \in \mathfrak{m}.$$

Stąd wynika, że $\kappa(\mathfrak{m}) = \mathsf{Nil}\left(A/\mathfrak{a}\right)$. Na podstawie twierdzenia 2.3.10, nilradykał pierścienia $A/\mathfrak{a}$ jest przekrojem wszystkich ideałów pierwszych pierścienia $A/\mathfrak{a}$. W takim razie przeciwobrazy tych ideałów pierwszych poprzez κ są ideałami w A zawierającymi $\mathfrak{m}$. Ponieważ jednak $\mathfrak{m}$ jest ideałem maksymalnym w A, przeciwobrazy ideałów pierwszych pierścienia $A/\mathfrak{a}$ są wszystkie równe $\mathfrak{m}$. Stąd wynika, że pierścień ilorazowy $A/\mathfrak{a}$ ma tylko jeden ideał pierwszy i jest nim $\mathsf{Nil}\left(A/\mathfrak{a}\right)$. Jest to zatem także jedyny ideał maksymalny pierścienia $A/\mathfrak{a}$. Wobec tego każdy element pierścienia $A/\mathfrak{a}$ leżący poza radykałem jest elementem odwracalnym (w przeciwnym razie zawierałby się w jedynym ideale maksymalnym tego pierścienia), natomiast pozostałe elementy są nilpotentami. Zatem każdy dzielnik zera w pierścieniu $A/\mathfrak{a}$ jest nilpotentem. Stąd na podstawie lematu 6.2.2 wynika, że $\mathfrak{a}$ jest ideałem prymarnym.

LEMAT **6.2.8.** *Jeśli* $\mathfrak{q}$ *jest ideałem prymarnym pierścienia* A, *to* $\mathsf{rad}(\mathfrak{q})$ *jest ideałem pierwszym w* A. *Dokładniej,* $\mathsf{rad}(\mathfrak{q})$ *jest najmniejszym ideałem pierwszym pierścienia* A *zawierającym* $\mathfrak{q}$.

Dowód. Niech $a, b \in A$ oraz $ab \in \mathsf{rad}(\mathfrak{q})$. Wtedy istnieje liczba naturalna n taka, że $a^n b^n = (ab)^n \in \mathfrak{q}$. Jeśli $a^n \in \mathfrak{q}$, to $a \in \mathsf{rad}(\mathfrak{q})$. Jeśli $a^n \notin \mathfrak{q}$, to wobec prymarności ideału $\mathfrak{q}$ istnieje liczba naturalna m taka, że $(b^n)^m \in \mathfrak{q}$. Wtedy $b \in \mathsf{rad}(\mathfrak{q})$. A więc $\mathsf{rad}(\mathfrak{q})$ jest ideałem pierwszym.
Oczywiście $\mathsf{rad}(\mathfrak{q}) \supseteq \mathfrak{q}$, jeśli zaś $\mathfrak{p}$ jest jakimkolwiek ideałem pierwszym zawierającym ideał prymarny $\mathfrak{q}$, to dla dowolnego $a \in \mathsf{rad}(\mathfrak{q})$ i odpowiedniej liczby naturalnej m mamy $a^m \in \mathfrak{q} \subseteq \mathfrak{p}$, skąd $a \in \mathfrak{p}$. A więc $\mathsf{rad}(\mathfrak{q}) \subseteq \mathfrak{p}$. □

DEFINICJA **6.2.9.** Jeśli $\mathfrak{q}$ jest ideałem prymarnym pierścienia A i $\mathfrak{p} = \mathsf{rad}(\mathfrak{q})$, to ideał $\mathfrak{q}$ nazywamy $\mathfrak{p}-$*prymarnym.*

Przykład 6.2.8. Jeśli $\mathfrak{m}$ jest ideałem maksymalnym pierścienia A, to każda potęga $\mathfrak{m}^k$ jest ideałem $\mathfrak{m}-$prymarnym.
Ideał maksymalny jest ideałem pierwszym, zatem na podstawie przykładu 6.2.6 mamy $\mathsf{rad}\,\mathfrak{m}^k = \mathfrak{m}$. Zatem radykał ideału $\mathfrak{m}^k$ jest ideałem maksymalnym i wobec tego na podstawie przykładu 6.2.7 ideał $\mathfrak{m}^k$ jest prymarny.

LEMAT **6.2.10.** *Jeśli ideały* $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ *są* $\mathfrak{p}-$*prymarne, to ideał* $\mathfrak{q} := \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ *jest także* $\mathfrak{p}-$*prymarny.*

Dowód. Najpierw sprawdzimy, że $\mathsf{rad}(\mathfrak{q}) = \mathfrak{p}$. Na podstawie (6.13) mamy mianowicie

$$\mathsf{rad}(\mathfrak{q}) = \mathsf{rad}(\mathfrak{q}_1) \cap \cdots \cap \mathsf{rad}(\mathfrak{q}_n) = \mathfrak{p} \cap \cdots \cap \mathfrak{p} = \mathfrak{p}.$$

Teraz pokażemy, że $\mathfrak{q}$ jest ideałem prymarnym. Niech więc $ab \in \mathfrak{q}$ i $b \notin \mathfrak{q}$. Wtedy istnieje wskaźnik i taki, że $b \notin \mathfrak{q}_i$. Ponieważ równocześnie $ab \in \mathfrak{q}_i$ oraz $\mathfrak{q}_i$ jest ideałem prymarnym, więc $a^k \in \mathfrak{q}_i$ dla pewnej liczby naturalnej k. Zatem $a \in \mathsf{rad}(\mathfrak{q}_i) = \mathfrak{p}$. Ponieważ $\mathfrak{p} = \mathsf{rad}(\mathfrak{q})$, wynika stąd, że $a^m \in \mathfrak{q}$ dla pewnej liczby naturalnej m. A więc $\mathfrak{q}$ jest ideałem prymarnym. □

Będziemy teraz analizować niektóre oczywiste przeszkody dla jednoznaczności rozkładu prymarnego ideału $\mathfrak{a}$ pierścienia noetherowskiego A. Jeśli

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \tag{6.17}$$

jest rozkładem prymarnym ideału $\mathfrak{a}$, to możemy z przekroju usunąć każdy ideał, który zawiera przekrój wszystkich pozostałych czynników tego przekroju. Można więc zakładać, że w przedstawieniu (6.17) mamy

$$\mathfrak{q}_i \not\supseteq \bigcap_{j \neq i} \mathfrak{q}_j \tag{6.18}$$

dla każdego ideału $\mathfrak{q}_i$. Następne uproszczenie rozkładu prymarnego (6.17) jest możliwe dzięki lematowi 6.2.10. Lemat ten pozwala uporządkować rozkład prymarny ideału $\mathfrak{a}$ poprzez zgrupowanie w jeden czynnik wszystkich ideałów prymarnych, które mają ten sam radykał. Inaczej mówiąc, możemy zakładać, że rozkład (6.17) spełnia następujący warunek:

$$\mathsf{rad}(\mathfrak{q}_i) \neq \mathsf{rad}(\mathfrak{q}_j) \quad \text{dla} \quad i \neq j. \tag{6.19}$$

Definicja **6.2.11.** Rozkład prymarny (6.17) ideału $\mathfrak{a}$ nazywa się *minimalnym rozkładem prymarnym* ideału $\mathfrak{a}$, jeśli spełnia on warunki (6.18) i (6.19).

Twierdzenie **6.2.12.** (Twierdzenie E. Laskera i E. Noether).
W pierścieniu noetherowskim każdy ideał właściwy $\mathfrak{a}$ ma minimalny rozkład prymarny (6.17). *Ponadto, ideały pierwsze $\mathfrak{p}_i := \mathsf{rad}(\mathfrak{q}_i)$ są wyznaczone jednoznacznie z dokładnością do porządku czynników.*

Twierdzenie to zostało udowodnione po raz pierwszy przez E. Laskera[3] w 1905 roku dla pierścieni wielomianów. Lasker wprowadził pojęcie ideału prymarnego. Natomiast Emmy Noether zauważyła, że twierdzenie Laskera jest prawdziwe w każdym pierścieniu spełniającym warunek (ACC).

6.2.3 Nota bibliograficzna

Kompletny wykład rozkładu prymarnego można znaleźć w następujących książkach:

M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Reading, Mass. 1969. (tłum. ros. 1972).

S. Balcerzyk, T. Józefiak, *Pierścienie przemienne*, PWN Warszawa 1985.

D. G. Northcott, *Ideal theory*, Cambridge 1953.

B. L. van der Waerden, *Algebra*, Zweiter Teil, Fünfte Aufl., Springer 1967.

[3]Emanuel Lasker (1868–1941), mistrz świata w szachach w latach 1894–1921.

6.3 Pierścienie Dedekinda

Podamy tutaj podstawowe informacje o szczególnie ważnej klasie pierścieni noetherowskich, nazywanych pierścieniami Dedekinda. Pierścienie Dedekinda są podstawowym obiektem badań w algebraicznej teorii liczb. W ich definicji oprócz wymagania, że pierścień jest noetherowski, występują jeszcze trzy inne warunki (brak dzielników zera, wymiar pierścienia równy 1, całkowita domkniętość w ciele ułamków). Objaśnimy więc najpierw pojęcia występujące w tej definicji.

6.3.1 Wymiar pierścienia

W pierścieniu A rozpatrujemy ostro wznoszące się łańcuchy ideałów pierwszych:

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n, \quad \mathfrak{p}_i \neq \mathfrak{p}_{i+1}, \quad i = 0, 1, \ldots, n-1. \tag{6.20}$$

Liczbę n nazywamy *długością* łańcucha (6.20). A więc łańcuch o długości n składa się z $n+1$ ideałów pierwszych.

Definicja **6.3.1.** Jeśli długości ostro wznoszących się łańcuchów (6.20) ideałów pierwszych pierścienia A są wspólnie ograniczone, to *wymiarem* (lub *wymiarem Krulla*) pierścienia A nazywamy maksymalną długość takich łańcuchów w A.
Jeśli długości łańcuchów (6.20) nie są wspólnie ograniczone, to mówimy, że wymiar pierścienia A jest nieskończony.
Wymiar pierścienia A oznaczamy $\dim A$.

Przykład 6.3.1. Jeśli A jest ciałem, to $\dim A = 0$.
W pierścieniu $\mathbb{Z}$ najdłuższe łańcuchy ideałów pierwszych mają postać $(0) \subset (p)$, gdzie p jest liczbą pierwszą. Zatem $\dim \mathbb{Z} = 1$.
Również $\dim K[X] = 1$, gdy K jest ciałem.
Jeśli A jest pierścieniem całkowitym (a więc ideał zerowy (0) jest ideałem pierwszym), to jest rzeczą oczywistą, że $\dim A = 1$ wtedy i tylko wtedy, gdy w pierścieniu A każdy niezerowy ideał pierwszy jest ideałem maksymalnym.
Natomiast $\dim \mathbb{Z}[X] \geqslant 2$, gdyż w $\mathbb{Z}[X]$ mamy następujący łańcuch ideałów pierwszych o długości 2:

$$(0) \subset (X) \subset (2, X).$$

Można udowodnić, że $\dim \mathbb{Z}[X] = 2$. Ogólniej, jeśli A jest pierścieniem noetherowskim, to

$$\dim A[X] = 1 + \dim A$$

(zob. S. Balcerzyk, T. Józefiak, *Pierścienie przemienne*, PWN Warszawa 1985, str. 219).

Można udowodnić, że pierścień noetherowski A ma wymiar zero wtedy i tylko wtedy, gdy jest pierścieniem artinowskim (to znaczy, gdy spełnia warunek (DCC)).

6.3.2 Elementy całkowite nad pierścieniem

Niech B będzie pierścieniem całkowitym (czyli bez dzielników zera) i niech A będzie podpierścieniem pierścienia B.

DEFINICJA **6.3.2.** Mówimy, że element $x \in B$ jest *całkowity nad pierścieniem* A (lub $A-$całkowity), jeśli istnieje liczba naturalna n i elementy $a_1, \ldots, a_n \in A$ takie, że

$$x^n + a_1 x^{n-1} + \cdots + a_n = 0.$$

Zbiór C wszystkich elementów pierścienia B całkowitych nad podpierścieniem A nazywa się *całkowitym* (lub *integralnym*) *domknięciem* pierścienia A w pierścieniu B i oznacza $C = C_B(A)$.

Jest rzeczą oczywistą, że każdy element $a \in A$ jest całkowity nad A (wystarczy wziąć $x = a, n = 1, a_1 = -a$). Zatem A zawiera się w każdym swoim całkowitym domknięciu. Fakt, że $x \in B$ jest całkowity nad A oznacza, że element x jest pierwiastkiem wielomianu $f = X^n + a_1 X^{n-1} + \cdots + a_n \in A[X]$ z tym, że wymagamy tutaj by najwyższy współczynnik wielomianu f był równy $1 \in A$, czyli, by wielomian f był wielomianem *unormowanym* o współczynnikach z A.
Pojęcie elementu całkowitego rozszerza znane z kursowego wykładu algebry pojęcie elementu *algebraicznego* nad ciałem. Jeśli bowiem A jest podciałem ciała B, to element $x \in B$ całkowity nad A jest elementem algebraicznym nad A. Bardzo często występuje problem opisu elementów ciała B całkowitych nad podpierścieniem (ale nie podciałem) A ciała B. Na przykład, gdy $A = \mathbb{Z}$ oraz $B = \mathbb{C}$, to całkowite domknięcie pierścienia $\mathbb{Z}$ w $\mathbb{C}$ nie pokrywa się z całkowitym domknięciem ciała $\mathbb{Q}$ w $\mathbb{C}$. Pierwsze składa się z wszystkich liczb algebraicznych *całkowitych*, drugie zaś z wszystkich liczb algebraicznych. Zbiory te nie są równe, gdyż na przykład, liczba $x = \frac{1}{2}\sqrt{3}$ jest algebraiczna jako pierwiastek wielomianu $X^2 - \frac{3}{4} \in \mathbb{Q}[X]$, ale nie jest liczbą algebraiczną całkowitą. Można bowiem pokazać, że każdy wielomian $f \in \mathbb{Z}[X]$ spełniający $f(x) = 0$, ma najwyższy współczynnik podzielny przez 4.

Przystępujemy teraz do dowodu podstawowej własności elementów $A-$całkowitych pierścienia B mówiącej, że całkowite domknięcie $C_B(A)$ pierścienia A w pierścieniu B jest podpierścieniem pierścienia B. Musimy więc pokazać, że suma, różnica i iloczyn dwóch $A-$całkowitych elementów pierścienia B jest elementem $A-$całkowitym. Klasyczny dowód tej własności wykorzystywał teorię wielomianów symetrycznych i jest już dzisiaj rzadko prezentowany (zob. Satz 61 w klasycznej książce: E. Hecke, *Vorlesungen über Zahlentheorie*. Leipzig 1923). Poniższy dowód ilustruje współczesną tendencję eliminując wielomiany symetryczne przez odpowiednie wykorzystanie charakteryzacji całkowitości elementu w języku teorii modułów.

Dla elementu $x \in B$ i podpierścienia A pierścienia B rozpatrujemy podpierścień $A[x]$ pierścienia B generowany przez A oraz x. Zatem

$$A[x] = \{a_0 + a_1 x + \cdots + a_m x^m \in B : a_i \in A, m \in \mathbb{N}\}.$$

Zauważmy, że zarówno B jak i $A[x]$ można traktować jako $A-$moduły.

LEMAT **6.3.3.** *Dla $x \in B$, $x \neq 0$ oraz podpierścienia A pierścienia całkowitego B następujące warunki są równoważne.*
(a) *x jest $A-$całkowity.*
(b) *$A[x]$ jest skończenie generowanym $A-$modułem.*
(c) *W $A-$module B istnieje niezerowy skończenie generowany podmoduł M taki, że*

$$xM \subseteq M.$$

Dowód. (a) $\Rightarrow$ (b). Ponieważ x jest $A-$całkowity, więc istnieje liczba naturalna n oraz elementy $a_i \in A$ takie, że

$$x^n = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}.$$

Stąd przy pomocy łatwego argumentu indukcyjnego otrzymujemy, że dla każdej liczby naturalnej m element x^m jest kombinacją liniową elementów $1, x, \ldots, x^{n-1}$ ze współczynnikami z A. A więc

$$A[x] = A \cdot 1 + A \cdot x + \cdots + A \cdot x^{n-1}$$

jest skończenie generowanym $A-$modułem.
(b) $\Rightarrow$ (c). Można wziąć $M = A[x]$.
(c) $\Rightarrow$ (a). Niech $x_1, \ldots, x_n$ będzie układem generatorów $A-$modułu M. Ponieważ $xM \subseteq M$, więc każdy iloczyn xx_i jest kombinacją liniową elementów $x_1, \ldots, x_n$

$$xx_i = a_{i1}x_1 + \cdots + a_{in}x_n, \qquad i = 1, \ldots, n,$$

gdzie $a_{ij} \in A$. Równości te można zapisać w równoważnej postaci

$$a_{i1}x_1 + \cdots + (a_{ii} - x)x_i + \cdots + a_{in}x_n = 0, \qquad i = 1, \ldots, n.$$

Ponieważ $M \neq 0$, więc nie wszystkie generatory x_i są równe zero. Zatem $x_1, \ldots, x_n$ jest niezerowym rozwiązaniem układu równań liniowych jednorodnych o macierzy współczynników $[a_{ij}]-xI_n$, gdzie I_n jest macierzą jednostkową stopnia n. Wobec tego $\det([a_{ij}]-xI_n) = 0$. Stąd wynika, że x jest pierwiastkiem unormowanego wielomianu stopnia n o współczynnikach z pierścienia A, jest więc elementem $A-$całkowitym. □

LEMAT **6.3.4.** *Jeśli $x, y \in B$ są $A-$całkowite, to $A[x, y] = A[x][y]$ jest niezerowym skończenie generowanym $A-$modułem.*

Dowód. Jeśli $x^n = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ oraz $y^m = b_0 + b_1 y + \cdots + b_{m-1}y^{m-1}$, gdzie $a_i, b_j \in A$, to $A[x, y]$ jest generowany jako $A-$moduł przez zbiór skończony

$$\{x^i y^j : 0 \leqslant i \leqslant n-1,\ 0 \leqslant j \leqslant m-1\}.$$

Ponieważ $1 \in A[x, y]$, więc $A[x, y] \neq 0$. □

Teraz możemy udowodnić zapowiedziane już twierdzenie.

TWIERDZENIE **6.3.5.** *Zbiór $C_B(A)$ wszystkich elementów pierścienia B całkowitych nad podpierścieniem A jest podpierścieniem pierścienia B zawierającym A.*

Dowód. Wystarczy pokazać, że zbiór $C_B(A)$ jest zamknięty ze względu na odejmowanie i mnożenie. Niech więc $x, y \in C_B(A)$. Weźmy $M = A[x, y]$. Jest to niezerowy skończenie generowany $A-$moduł oraz

$$(x - y)M \subseteq M, \quad (xy)M \subseteq M.$$

Zatem $x - y, xy \in C_B(A)$ na podstawie lematu 6.3.3. □

Całkowite domknięcie $C_B(A)$ pierścienia A w pierścieniu B jest więc pewnym podpierścieniem B, przy tym

$$A \subseteq C_B(A) \subseteq B.$$

Szczególnie ważny jest przypadek, gdy $A = C_B(A)$.

DEFINICJA **6.3.6.** Mówimy, że pierścień A jest *całkowicie domknięty* w B, jeśli $A = C_B(A)$ (to znaczy, gdy jedynymi elementami pierścienia B całkowitymi nad A są elementy pierścienia A).
Jeśli K jest ciałem ułamków pierścienia całkowitego A, to mówimy, że pierścień A jest *całkowicie domknięty*, gdy jest całkowicie domknięty w swoim ciele ułamków K, to znaczy, gdy $A = C_K(A)$.

Przykład 6.3.2. Pierścień $\mathbb{Z}$ jest całkowicie domknięty. Rzeczywiście, ciałem ułamków pierścienia $\mathbb{Z}$ jest ciało $\mathbb{Q}$ liczb wymiernych i jeśli $x \in C_{\mathbb{Q}}(\mathbb{Z})$, to liczba wymierna x jest pierwiastkiem unormowanego wielomianu f o współczynnikach całkowitych. Jeśli $x = a/b$ jest nieskracalnym przedstawieniem liczby x jako ilorazu liczb całkowitych, to liczba a jest dzielnikiem wyrazu wolnego wielomianu f natomiast b jest dzielnikiem najwyższego współczynnika. Stąd $b = \pm 1$ oraz $x = \pm a \in \mathbb{Z}$.
A więc $C_{\mathbb{Q}}(\mathbb{Z}) = \mathbb{Z}$.
Używając tych samych argumentów można pokazać, że każdy pierścień całkowity z jednoznacznością rozkładu na iloczyn elementów nierozkładalnych, jest całkowicie domknięty. W szczególności, każdy całkowity (to znaczy bez dzielników zera) pierścień ideałów głównych jest całkowicie domknięty.

Przykład 6.3.3. Rozważmy pierścień $A = \mathbb{Z}[\sqrt{-3}\,] = \{a + b\sqrt{-3} \in \mathbb{C} : a, b \in \mathbb{Z}\}$. Ciałem ułamków pierścienia A jest kwadratowe rozszerzenie

$$K = \mathbb{Q}(\sqrt{-3}\,) = \{a + b\sqrt{-3} \in \mathbb{C} : a, b \in \mathbb{Q}\}$$

ciała liczb wymiernych $\mathbb{Q}$. Liczba $x = (-1 + \sqrt{-3}\,)/2$ należy do K i nie należy do A. Jest ona pierwiastkiem wielomianu $X^2 + X + 1 \in A[X]$, zatem jest całkowita nad A ale nie należy do A. W takim razie $A \neq C_K(A)$ i pierścień A nie jest całkowicie domknięty. W szczególności więc, nie jest to pierścień z jednoznacznością rozkładu na iloczyn elementów nierozkładalnych. (Ten ostatni fakt można także stwierdzić bezpośrednio wskazując konkretny przykład niejednoznaczności rozkładu taki jak $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$.)
Można pokazać, że $C_K(A) = \{a + bx : a, b \in \mathbb{Z}\}$, gdzie $x = (-1 + \sqrt{-3}\,)/2$. Ponadto, pierścień $C_K(A)$ ma własność jednoznaczności rozkładu na iloczyn elementów nierozkładalnych.

6.3.3 Pierścienie Dedekinda

DEFINICJA **6.3.7.** Pierścień całkowity A nazywa się *pierścieniem Dedekinda*, jeśli ma następujące własności:
(a) A jest pierścieniem noetherowskim,
(b) $\dim A = 1$ (każdy niezerowy ideał pierwszy jest maksymalny),
(c) A jest pierścieniem całkowicie domkniętym.

Przykład 6.3.4. Najprostszym przykładem pierścienia Dedekinda jest pierścień $\mathbb{Z}$ liczb całkowitych. Ogólniej każdy całkowity pierścień ideałów głównych jest pierścieniem Dedekinda. Warunek (a) jest spełniony automatycznie, warunek (c) sprawdza się tak jak w przykładzie 6.3.2. Natomiast warunek (b) sprawdza się w kursowym wykładzie algebry (zob. A. Białynicki–Birula, *Algebra*, PWN 1971, wniosek 5.5 na str. 200). Tak więc, na przykład, pierścień wielomianów $K[X]$ jednej zmiennej nad dowolnym ciałem K jest pierścieniem Dedekinda.

Z drugiej strony, pierścień $\mathbb{Z}[X]$ wielomianów o współczynnikach całkowitych spełnia oczywiście warunki (a), (c), ale nie jest pierścieniem Dedekinda, gdyż nie spełnia warunku (b) (zob. przykład 6.3.1).

Ponieważ pierścień Dedekinda jest pierścieniem noetherowskim, więc każdy niezerowy ideał właściwy pierścienia Dedekinda ma (minimalny) rozkład prymarny (zob. twierdzenie 6.2.12). Wykorzystując dodatkowe własności pierścienia Dedekinda można ten rezultat bardzo znacznie wzmocnić i uprościć, chociaż nie jest to zadanie proste. W związku z tym ograniczymy się jedynie do objaśnienia głównego twierdzenia o rozkładach ideałów w pierścieniach Dedekinda i zasygnalizowania niektórych argumentów ogólniejszej natury.

Dla dowolnego niezerowego ideału właściwego $\mathfrak{a}$ pierścienia Dedekinda mamy rozkład

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n \tag{6.21}$$

gdzie $\mathfrak{q}_i$ są ideałami prymarnymi oraz radykały ideałów $\mathfrak{q}_i$ są parami różne. Ideał $\mathfrak{a}$ jest więc *przekrojem* ideałów prymarnych. Pokażemy teraz że w tym rozkładzie można zamienić *przekrój* ideałów *iloczynem* ideałów.

LEMAT **6.3.8.** *Jeśli ideały $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ pierścienia A są parami względnie pierwsze, to*

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n.$$

Dowód. Indukcja ze względu na n. Dla $n = 2$ własność tę zauważyliśmy już w rozdziale 2.3. Niech $n > 2$ i niech

$$\mathfrak{b} = \mathfrak{a}_1 \cdots \mathfrak{a}_{n-1} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_{n-1}.$$

Pokażemy, że ideały $\mathfrak{b}$ i $\mathfrak{a}_n$ są względnie pierwsze. Stąd, że $\mathfrak{a}_i + \mathfrak{a}_n = (1)$ dla $i < n$ wynika, że dla każdego $i < n$ istnieją $x_i \in \mathfrak{a}_i$ oraz $y_i \in \mathfrak{a}_n$ takie, że $x_i + y_i = 1$. Stąd wynika, że $x_1 \cdots x_{n-1} \in \mathfrak{b}$ oraz

$$x_1 \cdots x_{n-1} = (1 - y_1) \cdots (1 - y_{n-1}) \equiv 1 \pmod{\mathfrak{a}_n}.$$

Zatem $\mathfrak{b} + \mathfrak{a}_n = (1)$ oraz

$$\mathfrak{a}_1 \cdots \mathfrak{a}_n = \mathfrak{b} \cdot \mathfrak{a}_n = \mathfrak{b} \cap \mathfrak{a}_n = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_n,$$

przy czym środkowa równość wynika ze sprawdzonego już przypadku dwóch ideałów względnie pierwszych. □

LEMAT **6.3.9.** *Niech A będzie pierścieniem noetherowskim oraz $\dim A = 1$. Każdy niezerowy ideał właściwy $\mathfrak{a}$ pierścienia A ma rozkład prymarny* (6.21)*, w którym ideały prymarne $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ są parami względnie pierwsze.*

Dowód. Niech (6.21) będzie *minimalnym* rozkładem prymarnym ideału $\mathfrak{a}$. W szczególności radykały $\mathsf{rad}(\mathfrak{q}_i) =: \mathfrak{p}_i$ są parami różnymi ideałami pierwszymi pierścienia A. Ponieważ $\dim A = 1$, ideały $\mathfrak{p}_i$ są maksymalne w A (żaden z nich nie może być ideałem zerowym, gdyż jeśli $\mathsf{rad}(\mathfrak{q}_i) = (0)$, to wobec $\mathfrak{q}_i \subseteq \mathsf{rad}(\mathfrak{q}_i)$ także $\mathfrak{q}_i = (0)$, co pociąga $\mathfrak{a} = (0)$, wbrew założeniu).
Z drugiej strony, dla $i \neq j$ mamy $\mathfrak{p}_i \neq \mathfrak{p}_j$. Różne ideały maksymalne są względnie pierwsze, zatem na podstawie (6.16) ideały $\mathfrak{q}_i$ oraz $\mathfrak{q}_j$ są względnie pierwsze. □

Wracając teraz do rozkładu prymarnego (6.21) widzimy, że można założyć, iż czynniki tego rozkładu są parami względnie pierwsze (lemat 6.3.9) zaś na podstawie lematu 6.3.8, przekrój ideałów $\mathfrak{q}_i$ pokrywa się z ich iloczynem. A więc

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_n.$$

W pierścieniu Dedekinda każdy niezerowy ideał właściwy ma zatem przedstawienie jako iloczyn ideałów prymarnych. Faktycznie prawdziwe jest następujące znacznie dokładniejsze twierdzenie.

Twierdzenie **6.3.10.** *W pierścieniu Dedekinda każdy niezerowy ideał właściwy ma jednoznaczne przedstawienie jako iloczyn potęg ideałów pierwszych.*

Pierwszy krok w dowodzie twierdzenia 6.3.10 polega na pokazaniu, że w rozkładzie (6.21) przekroje ideałów można zastąpić *iloczynami* ideałów. Sprawdziliśmy to powyżej.

Drugi krok polega na ustaleniu, że w pierścieniu Dedekinda każdy ideał prymarny jest potęgą swojego radykału (a więc potęgą ideału pierwszego). Ten dowód pomijamy.

W trzecim kroku należy udowodnić własność jednoznaczności przedstawienia ideału $\mathfrak{a}$ w postaci iloczynu potęg ideałów pierwszych. Tutaj jest niezbędny dodatkowy argument (tak zwane *drugie twierdzenie o jednoznaczności rozkładu prymarnego*), pominięty w dyskusji rozkładu prymarnego. Pomijamy więc także dyskusję tej części dowodu twierdzenia 6.3.10.

Kompletny dowód twierdzenia 6.3.10 realizujący taki plan dowodu można znaleźć w książce: M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Reading, Mass. 1969.

Warto jeszcze zauważyć, że prawdziwe jest twierdzenie odwrotne do twierdzenia 6.3.10 i w związku z tym otrzymujemy następującą charakteryzację pierścieni Dedekinda: *Pierścień całkowity jest pierścieniem Dedekinda wtedy i tylko wtedy gdy każdy niezerowy ideał właściwy ma jednoznaczne przedstawienie jako iloczyn potęg ideałów pierwszych.* Szczegóły, a także wiele innych informacji o pierścieniach Dedekinda można znaleźć w książce: O. Zariski, P. Samuel, *Commutative algebra*, vol. I, Springer-Verlag, Berlin 1975, str. 270.

Przykład 6.3.5. Dla pierścienia Dedekinda A niech $M(A)$ oznacza monoid niezerowych ideałów pierścienia A z mnożeniem jako działaniem. Na podstawie twierdzenia 6.3.10, $M(A)$ jest monoidem z jednoznacznym rozkładem. W związku z tym dla dowolnych ideałów $\mathfrak{a}, \mathfrak{b} \in M(A)$ istnieje ich największy wspólny dzielnik $\mathrm{nwd}(\mathfrak{a}, \mathfrak{b})$ i najmniejsza wspólna wielokrotność $\mathrm{nww}(\mathfrak{a}, \mathfrak{b})$. Jeśli

$$\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_m^{a_m}, \qquad \mathfrak{b} = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_m^{b_m},$$

gdzie $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ są ideałami pierwszymi oraz $a_i \geqslant 0$, $b_i \geqslant 0$, to

$$\mathrm{nwd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m}, \qquad \mathrm{nww}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{p}_1^{f_1} \cdots \mathfrak{p}_m^{f_m},$$

gdzie dla każdego i

$$e_i = \min(a_i, b_i), \qquad f_i = \max(a_i, b_i).$$

6.3.4 Inna charakteryzacja pierścieni Dedekinda

Niech A będzie pierścieniem całkowitym i niech K będzie ciałem ułamków pierścienia A. *Ideałem ułamkowym* ciała K nazywamy każdy $A-$podmoduł $\mathfrak{a}$ ciała K dla którego istnieje różny od zera element $a \in A$ taki, że $a\mathfrak{a} \subseteq A$. W szczególności więc każdy ideał $\mathfrak{a}$ pierścienia A jest ideałem ułamkowym w K (można wziąć $a = 1$). Definiujemy *iloczyn* ideałów ułamkowych $\mathfrak{a}$ oraz $\mathfrak{b}$ ciała K podobnie jak iloczyn ideałów pierścienia jako zbiór wszystkich skończonych sum $\sum a_i b_i$, gdzie $a_i \in \mathfrak{a}$ oraz $b_i \in \mathfrak{b}$. Łatwo stwierdzić, że zbiór wszystkich ideałów ułamkowych ciała K z mnożeniem jako działaniem tworzy monoid którego jedynką jest A.

Dla każdego ideału ułamkowego $\mathfrak{a}$ ciała K kładziemy

$$\mathfrak{a}' = \{x \in K : x\mathfrak{a} \subseteq A\}.$$

Łatwo sprawdzić, że $\mathfrak{a}\mathfrak{a}' \subseteq A$ oraz $\mathfrak{a}'$ jest ideałem ułamkowym ciała K. Jeśli $\mathfrak{a}\mathfrak{a}' = A$, to ideał $\mathfrak{a}$ jest odwracalny w monoidzie ideałów ułamkowych ciała K. Można udowodnić, że *pierścień całkowity A jest pierścieniem Dedekinda wtedy i tylko wtedy gdy każdy niezerowy ideał ułamkowy ciała ułamków K pierścienia A jest odwracalny*, lub równoważnie, gdy monoid ideałów ułamkowych ciała K jest grupą (zob. J. Browkin, *Teoria ciał*, PWN Warszawa 1977, str. 259). Zauważmy jeszcze, że ideały pierścienia A nie są odwracalne w monoidzie ideałów pierścienia A. Jeśli bowiem dla ideałów $\mathfrak{a}$ i $\mathfrak{b}$ dowolnego pierścienia przemiennego A mamy $A = \mathfrak{a}\mathfrak{b}$, to wobec $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ wynika stąd, że $\mathfrak{a} = \mathfrak{b} = A$. A więc ideał właściwy $\mathfrak{a}$ pierścienia przemiennego A jest nieodwracalny w monoidzie ideałów pierścienia A.

Niech K będzie ciałem ułamków pierścienia Dedekinda A. Jeśli $\mathfrak{a}$ jest ideałem ułamkowym ciała K oraz $a\mathfrak{a} \subseteq A$ dla $a \in A$, to $a\mathfrak{a} =: \mathfrak{b}$ jest ideałem pierścienia A i wobec tego $\mathfrak{a} = \mathfrak{b} \cdot (a)^{-1}$ jest ilorazem dwóch ideałów pierścienia A. Z twierdzenia 6.3.10 wynika zatem, że każdy ideał ułamkowy ciała K ma jednoznaczne przedstawienie w postaci iloczynu potęg ideałów pierwszych (z wykładnikami całkowitymi). Inaczej mówiąc, ideały ułamkowe ciała K (z mnożeniem jako działaniem) tworzą grupę abelową wolną, której bazą jest zbiór wszystkich niezerowych ideałów pierwszych pierścienia A.

Pokażemy teraz jak można stąd uzyskać podstawową dla arytmetyki pierścieni Dedekinda informację o związku pomiędzy relacją podzielności ideałów i relacją inkluzji. Dla dowolnych niezerowych ideałów $\mathfrak{a}$ i $\mathfrak{b}$ pierścienia Dedekinda A mamy

$$\mathfrak{b} \mid \mathfrak{a} \iff \mathfrak{a} \subseteq \mathfrak{b}. \tag{6.22}$$

Jeśli $\mathfrak{b}|\mathfrak{a}$ to istnieje ideał $\mathfrak{c} \lhd A$ taki, że $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$. Ponieważ $\mathfrak{b}\mathfrak{c} \subseteq \mathfrak{b}$, więc $\mathfrak{a} \subseteq \mathfrak{b}$. Załóżmy teraz, że $\mathfrak{a} \subseteq \mathfrak{b}$. Wtedy także $\mathfrak{a}\mathfrak{b}^{-1} \subseteq \mathfrak{b}\mathfrak{b}^{-1} = A$. Zatem ideał ułamkowy

$\mathfrak{a}\mathfrak{b}^{-1}$ jest ideałem pierścienia A. Wynika stąd, że każdy ideał pierwszy $\mathfrak{p}$ występujący w rozkładzie ideału $\mathfrak{b}$ występuje także w rozkładzie ideału $\mathfrak{a}$ i to z wykładnikiem nie większym niż w $\mathfrak{a}$. Zatem $\mathfrak{b}|\mathfrak{a}$.

Jako przykład zastosowania (6.22) pokażemy, że dla niezerowych ideałów $\mathfrak{a}, \mathfrak{b}$ pierścienie Dedekinda A mamy

$$\mathrm{nwd}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}.$$

Niech bowiem $\mathfrak{d} = \mathfrak{a} + \mathfrak{b}$. Wtedy $\mathfrak{a} \subseteq \mathfrak{d}$ i $\mathfrak{b} \subseteq \mathfrak{d}$ i wobec tego $\mathfrak{d} \mid \mathfrak{a}$ i $\mathfrak{d} \mid \mathfrak{b}$. A więc $\mathfrak{d}$ jest wspólnym dzielnikiem ideałów $\mathfrak{a}$ i $\mathfrak{b}$. Jeśli teraz $\mathfrak{c}$ jest jakimkolwiek wspólnym dzielnikiem ideałów $\mathfrak{a}$ i $\mathfrak{b}$, to na podstawie (6.22) mamy $\mathfrak{a} \subseteq \mathfrak{c}$ i $\mathfrak{b} \subseteq \mathfrak{c}$. Wobec tego także $\mathfrak{d} = \mathfrak{a} + \mathfrak{b} \subseteq \mathfrak{c}$, czyli $\mathfrak{c} \mid \mathfrak{d}$. Dowodzi to, że $\mathfrak{d} = \mathrm{nwd}(\mathfrak{a}, \mathfrak{b})$. Podobnie można pokazać, że

$$\mathrm{nww}(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} \cap \mathfrak{b}.$$

Niech A będzie pierścieniem Dedekinda z ciałem ułamków K i niech $I(K)$ oznacza grupę niezerowych ideałów ułamkowych ciała K. Niech $P(K)$ oznacza podgrupę $I(K)$ złożoną z ideałów ułamkowych *głównych*, to znaczy generowanych przez jednoelementowe podzbiory ciała K. Grupa ilorazowa $\mathrm{Cl}(A) := I(K)/P(K)$ nazywa się *grupą klas ideałów* pierścienia Dedekinda A (lub ciała K). Zauważmy, że grupa klas pierścienia A jest trywialna (jednoelementowa) wtedy i tylko wtedy, gdy każdy ideał ułamkowy ciała K (a zatem także każdy ideał pierścienia A) jest ideałem głównym. Intuicyjnie rzecz biorąc, grupa klas ideałów, jeśli jest nietrywialna, wskazuje jak dalece arytmetyka pierścienia A różni się od krańcowo prostego przypadku gdy pierścień Dedekinda A jest pierścieniem ideałów głównych. W związku z tym, interesującym problemem było pytanie jakie grupy abelowe są grupami klas ideałów pierścieni Dedekinda. Pełną odpowiedź na to pytanie przyniosła praca L. Claborna z roku 1966 pod wszystko mówiącym tytułem *Every abelian group is a class group*, która ukazała się w *Pacific Journal of Mathematics* **18**, 219–222. Rezultat pracy Claborna jest więc definitywny: rozmaitość pierścieni Dedekinda jest tak wielka, że każda grupa abelowa (skończona lub nieskończona) jest grupą klas ideałów pewnego pierścienia Dedekinda.

6.4 Pierścienie liczb algebraicznych całkowitych

Wspomnieliśmy już o pierścieniu *wszystkich* liczb algebraicznych całkowitych, który jest całkowitym domknięciem $C_{\mathbb{C}}(\mathbb{Z})$ pierścienia $\mathbb{Z}$ w ciele liczb zespolonych $\mathbb{C}$. Ten pierścień nie ma interesującej arytmetyki. Nie ma w nim, na przykład elementów nierozkładalnych. Jeśli bowiem α jest liczbą algebraiczną całkowitą i nie jest to liczba odwracalna, to liczba $\sqrt{\alpha}$ też jest nieodwracalną liczbą algebraiczną całkowitą i wobec tego równość $\alpha = \sqrt{\alpha} \cdot \sqrt{\alpha}$ oznacza, że α nie jest elementem nierozkładalnym. Okazuje się, że fundamentalne znaczenie mają podpierścienie pierścienia wszystkich liczb algebraicznych całkowitych, które są całkowitymi domknięciami $C_K(\mathbb{Z})$ pierścienia liczb całkowitych $\mathbb{Z}$ w *skończonych rozszerzeniach* K ciała liczb wymiernych. Udowodnimy, że pierścienie te są pierścieniami Dedekinda.

Niech ciało K będzie skończonym rozszerzeniem ciała liczb wymiernych $\mathbb{Q}$. A więc ciało K traktowane jako przestrzeń wektorowa nad ciałem $\mathbb{Q}$ ma skończony wymiar

n. Liczbę n nazywamy *stopniem* ciała K i oznaczamy $n = [K : \mathbb{Q}]$. Z kursu algebry wiadomo, że ciało K zawiera *element pierwotny* θ. Jest to liczba ciała K taka, że

$$K = \mathbb{Q}(\theta) = \{a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} : \quad a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}.$$

W ciele K rozpatrujemy całkowite domknięcie $A := C_K(\mathbb{Z})$ pierścienia $\mathbb{Z}$ liczb całkowitych. Jest to podpierścień ciała K złożony z wszystkich liczb ciała K całkowitych nad $\mathbb{Z}$, czyli z wszystkich liczb algebraicznych całkowitych ciała K. Jeśli $n = 1$, to $K = \mathbb{Q}$ oraz $A = \mathbb{Z}$. Jeśli $n > 1$, to dla rozróżnienia liczb całkowitych ciała K od liczb całkowitych ciała $\mathbb{Q}$, te ostatnie (czyli elementy pierścienia $\mathbb{Z}$) nazywamy *wymiernymi* liczbami całkowitymi. Dla ciał wyższych stopni pierścień A będzie grał w ciele K taką rolę, jak $\mathbb{Z}$ w $\mathbb{Q}$. W szczególności,

LEMAT **6.4.1.** *K jest ciałem ułamków pierścienia A.*

Dowód. Pokażemy, że każdy element ciała K jest ilorazem dwóch liczb pierścienia A. Niech bowiem $\alpha \in K$. Wtedy liczby

$$1, \alpha, \alpha^2, \ldots, \alpha^n$$

są liniowo zależne nad $\mathbb{Q}$ ($n+1$ wektorów w $n-$wymiarowej przestrzeni wektorowej). Zatem istnieją liczby wymierne $w_0, w_1, \ldots, w_n$ nie wszystkie równe zero i takie, że

$$w_0 + w_1\alpha + \cdots + w_n\alpha^n = 0.$$

Mnożąc obie strony tej równości przez najmniejszą wspólną wielokrotność mianowników liczb $w_0, w_1, \ldots, w_n$ otrzymamy równość postaci

$$c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0,$$

gdzie $c_0, c_1, \ldots, c_n$ są liczbami całkowitymi (i nie wszystkie są równe zero). Niech $m \leqslant n$ będzie największym wskaźnikiem, dla którego $c_m \neq 0$. Połóżmy dla uproszczenia oznaczeń $c := c_m$. Liczba α jest więc pierwiastkiem wielomianu niezerowego $f = c_0 + c_1X + \cdots + c_{m-1}X^{m-1} + cX^m$ o współczynnikach całkowitych. W takim razie $0 = c^{m-1}f(\alpha) = F(c\alpha)$, gdzie

$$F = c_0c^{m-1} + c_1c^{m-2}X + \cdots + c_{m-1}X^{m-1} + X^m$$

jest wielomianem o współczynnikach całkowitych i najwyższym współczynniku 1. Liczba $\beta = c\alpha$ jest więc liczbą algebraiczną całkowitą ciała K i wobec tego $\alpha = \beta/c$ jest ilorazem dwóch liczb należących do A. □

Zauważmy, że udowodniliśmy nawet nieco silniejszą własność niż zamierzaliśmy: każda liczba ciała K jest ilorazem pewnej liczby algebraicznej całkowitej i pewnej wymiernej liczby całkowitej.
Wynika stąd także, że w ciele K można zawsze wybrać element pierwotny θ, który jest liczbą algebraiczną całkowitą.

Dowód twierdzenia, że pierścień A liczb całkowitych ciała $K = \mathbb{Q}(\theta)$ jest pierścieniem Dedekinda rozpoczniemy od ustalenia, że A jest skończenie generowaną grupą abelową. Rezultat ten sformułowany jest w stwierdzeniu 6.4.3 a w jego dowodzie wykorzystamy następujący lemat.

LEMAT **6.4.2.** *Niech $K = \mathbb{Q}(\theta)$, gdzie θ jest liczbą algebraiczną całkowitą. Jeśli $\theta_1, \ldots, \theta_n$ są wszystkimi pierwiastkami wielomianu minimalnego liczby θ, to liczba*

$$\Delta^2 = \prod_{1 \leqslant i < j \leqslant n} (\theta_i - \theta_j)^2$$

jest wymierną liczbą całkowitą.

Dowód. Rozpatrzmy ciało $L = \mathbb{Q}(\theta_1, \ldots, \theta_n)$. Jest to ciało rozkładu wielomianu minimalnego f_θ liczby θ, zatem jest to rozszerzenie Galois ciała $\mathbb{Q}$. Niech $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ będzie dowolnym automorfizmem ciała L. Wtedy σ permutuje pierwiastki wielomianu f_θ i wobec tego $\sigma(\Delta^2) = \Delta^2$. Zatem Δ^2 jest liczbą wymierną. Z drugiej strony, Δ^2 jest liczbą algebraiczną całkowitą. Zatem Δ^2 jest liczbą całkowitą wymierną. □

STWIERDZENIE **6.4.3.** *A jest grupą abelową wolną rangi $n = [K : \mathbb{Q}]$.*

Dowód. Niech $\alpha \in A$ i niech $K = \mathbb{Q}(\theta)$, gdzie θ jest liczbą algebraiczną całkowitą. Wtedy

$$\alpha = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, \quad a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}.$$

Jeśli $\theta_1, \ldots, \theta_n$ są wszystkimi pierwiastkami wielomianu minimalnego liczby θ, to liczby

$$\alpha_i = a_0 + a_1\theta_i + \cdots + a_{n-1}\theta_i^{n-1}, \quad i = 1, \ldots, n \tag{6.23}$$

nazywamy liczbami *sprzężonymi* z liczbą α. Używając wzorów Cramera możemy współczynniki a_j występujące w równościach (6.23) przedstawić w postaci

$$a_j = \frac{D_j}{\Delta},$$

gdzie $\Delta = \prod_{1 \leqslant i < j \leqslant n}(\theta_i - \theta_j)$ jest wartością wyznacznika Vandermonde'a utworzonego z liczb θ_i^j, zaś D_j jest wyznacznikiem macierzy, która powstaje z macierzy $[\theta_i^j]$ przez zastąpienie $j-$tej kolumny kolumną liczb $\alpha_1, \ldots, \alpha_n$. Ponieważ α i θ są liczbami algebraicznymi całkowitymi, także D_j i Δ są liczbami algebraicznymi całkowitymi. Stąd wynika, że liczba

$$D_j\Delta = \Delta^2 a_j$$

jest liczbą całkowitą *wymierną*. Mianowicie liczba $D_j\Delta$ jest liczbą algebraiczną całkowitą, zaś Δ^2 oraz a_j są liczbami wymiernymi. Ponieważ pierścień $\mathbb{Z}$ liczb całkowitych jest całkowicie domknięty, wynika stąd, że $D_j\Delta \in \mathbb{Z}$.

Liczbę α można więc przedstawić w postaci

$$\alpha = \sum_{j=0}^{n-1} a_j\theta^j = \sum_{j=0}^{n-1} D_j\Delta\frac{\theta^j}{\Delta^2}.$$

Wynika stąd, że liczba α należy do grupy abelowej wolnej $\mathcal{F}$ (podgrupy addytywnej grupy ciała K) z bazą

$$\frac{1}{\Delta^2}, \frac{\theta}{\Delta^2}, \ldots, \frac{\theta^{n-1}}{\Delta^2}.$$

Inaczej mówiąc A jest podgrupą $\mathcal{F}$. Wobec tego, na podstawie twierdzenia 4.3.7, A jest grupą abelową wolną i $\mathsf{rank}\, A \leqslant \mathsf{rank}\, \mathcal{F} = n$. Z drugiej jednak strony $n \leqslant \mathsf{rank}\, A$, gdyż liczby $1, \theta, \ldots, \theta^{n-1}$ należą do A i są liniowo niezależne nad $\mathbb{Z}$. Zatem $\mathsf{rank}\, A = n = [K : \mathbb{Q}]$. □

WNIOSEK **6.4.4.** *Każdy niezerowy ideał pierścienia A jest grupą abelową wolną rangi $n = [K : \mathbb{Q}]$.*

Dowód. Każdy ideał $\mathfrak{a}$ pierścienia A jest podgrupą addytywnej grupy pierścienia A, która jest grupą abelową wolną rangi n. Wobec tego na podstawie twierdzenia 4.3.7 każdy ideał w pierścieniu A jest grupą abelową wolną o randze nie większej od n. Z drugiej strony, jeśli $0 \neq \alpha \in \mathfrak{a}$, to także

$$\alpha, \alpha\theta, \ldots, \alpha\theta^{n-1} \in \mathfrak{a}$$

oraz liczby te są liniowo niezależne nad $\mathbb{Z}$. Zatem

$$n \leqslant \mathsf{rank}\,\mathfrak{a} \leqslant \mathsf{rank}\,A = n.$$

Stąd $\mathsf{rank}\,\mathfrak{a} = n$. □

STWIERDZENIE **6.4.5.** *Dla każdego ideału niezerowego $\mathfrak{a}$ pierścienia A pierścień ilorazowy $A/\mathfrak{a}$ jest skończony.*

Dowód. Najpierw zauważmy, że każdy ideał niezerowy $\mathfrak{a}$ pierścienia A zawiera pewną liczbę całkowitą wymierną. Jeśli bowiem $\alpha \in \mathfrak{a}$, $\alpha \neq 0$, to α spełnia równanie postaci $\alpha^m + a_1\alpha^{m-1} + \cdots + a_{m-1}\alpha + a_m = 0$, gdzie wszystkie $a_i \in \mathbb{Z}$ oraz $a_m \neq 0$. Z równości tej wynika jednak, że $a_m \in \mathfrak{a}$. Jeśli $a \in \mathfrak{a} \cap \mathbb{Z}$ oraz $a \neq 0$, to ideał główny $(a) = aA$ zawiera się w ideale $\mathfrak{a}$. Stąd wynika, że odwzorowanie

$$A/(a) \to A/\mathfrak{a}, \quad x + (a) \mapsto x + \mathfrak{a}$$

jest surjektywnym homomorfizmem pierścieni. Ponieważ A jest wolną grupą abelową o randze n, więc $|A/(a)| = |a|^n$. Zatem $|A/\mathfrak{a}| \leqslant |a|^n$. □

STWIERDZENIE **6.4.6.** *A jest pierścieniem noetherowskim.*

Dowód. Jeśli $\mathfrak{a}, \mathfrak{b}$ są różnymi ideałami w A oraz $\mathfrak{a} \subset \mathfrak{b}$, to $|A/\mathfrak{a}| > |A/\mathfrak{b}|$. Istnienie nieskończonego wznoszącego łańcucha różnych ideałów w A prowadziłoby więc do nieskończonego malejącego ciągu liczb naturalnych. Stąd wynika, że A spełnia (ACC). □

STWIERDZENIE **6.4.7.** $\dim A = 1$.

Dowód. Jeśli $\mathfrak{p}$ jest niezerowym ideałem pierwszym, to $A/\mathfrak{p}$ jest skończonym pierścieniem całkowitym, a więc jest ciałem. Ideał $\mathfrak{p}$ jest więc maksymalny. □

STWIERDZENIE **6.4.8.** *A jest pierścieniem całkowicie domkniętym: $C_K(A) = A$.*

Dowód. Pokażemy, że $C_K(A) \subseteq A$. Niech więc $x \in C_K(A)$ i niech

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

dla pewnych $a_0, \ldots, a_{n-1} \in A$. Rozważmy podpierścień $\bar{A} = \mathbb{Z}[a_0, \ldots, a_{n-1}]$ ciała K. Podobnie jak w dowodzie lematu 6.3.4 stwierdzamy, że $\bar{A}$ jest skończenie generowanym $\mathbb{Z}-$modułem. Zauważmy też, że x jest elementem całkowitym nad $\bar{A}$ i wobec tego z lematu 6.3.3 wynika, że podpierścień $\bar{A}[x]$ ciała K jest skończenie generowanym $\bar{A}-$modułem. W konsekwencji $M := \bar{A}[x]$ jest skończenie generowanym $\mathbb{Z}-$modułem. Ponadto, $1 \in M$, a więc $M \neq 0$, a także $xM \subseteq M$. Zatem na podstawie lematu 6.3.3 element x ciała K jest $\mathbb{Z}-$całkowity, to znaczy $x \in A$. □

Sumując rezultaty trzech ostatnich stwierdzeń otrzymujemy

TWIERDZENIE **6.4.9.** *Pierścień $A = C_K(\mathbb{Z})$ liczb algebraicznych całkowitych w skończonym rozszerzeniu K ciała liczb wymiernych jest pierścieniem Dedekinda.*

Przykład 6.4.1. Rozważmy pierścień $A = \mathbb{Z}[\sqrt{-5}\,] = \{a + b\sqrt{-5} \in \mathbb{C} : a, b \in \mathbb{Z}\}$. Ciałem ułamków pierścienia A jest kwadratowe rozszerzenie

$$K = \mathbb{Q}(\sqrt{-5}\,) = \{a + b\sqrt{-5} \in \mathbb{C} : a, b \in \mathbb{Q}\}$$

ciała liczb wymiernych $\mathbb{Q}$. Jeśli dla $a, b \in \mathbb{Q}$ liczba $\alpha = a + b\sqrt{-5}$ jest całkowita (nad $\mathbb{Z}$), to także liczba sprzężona $\bar{\alpha} = a - b\sqrt{-5}$ jest całkowita (nad $\mathbb{Z}$) (jeśli α jest pierwiastkiem wielomianu o współczynnikach całkowitych wymiernych, to $\bar{\alpha}$ jest także pierwiastkiem tego samego wielomianu). Wobec tego całkowite są także liczby $\alpha + \bar{\alpha} = 2a$ oraz $\alpha \cdot \bar{\alpha} = a^2 + 5b^2$. Liczby $2a$ oraz $a^2 + 5b^2$ są więc liczbami całkowitymi wymiernymi i stąd łatwo wynika, że $a, b \in \mathbb{Z}$. Pokazuje to, że $A = C_K(\mathbb{Z})$. Zatem na podstawie twierdzenia 6.4.9 A jest pierścieniem Dedekinda. Tymczasem A nie jest pierścieniem ideałów głównych, gdyż nie jest pierścieniem z jednoznacznym rozkładem elementów na iloczyn elementów nierozkładalnych. Mamy bowiem, na przykład,

$$9 = 3 \cdot 3 = (2 + \sqrt{-5}\,)(2 - \sqrt{-5}\,)$$

i w rozkładzie tym wszystkie czynniki są nierozkładalne oraz każde dwa różne czynniki są niestowarzyszone (to ostatnie stwierdzenie wynika stąd, że jedynymi elementami odwracalnymi pierścienia A są liczby ± 1).
Z rozkładu liczby 9 na czynniki w A otrzymujemy następujące rozkłady ideału głównego $(9) = 9A$ na iloczyn ideałów głównych

$$(9) = \mathfrak{c}^2 = \mathfrak{a} \cdot \mathfrak{b},$$

gdzie

$$\mathfrak{c} = (3), \quad \mathfrak{a} = (2 + \sqrt{-5}\,), \quad \mathfrak{b} = (2 - \sqrt{-5}\,)$$

są ideałami generowanymi odpowiednio przez 3 oraz $2 + \sqrt{-5}\,,\ 2 - \sqrt{-5}\,$.

Pokażemy teraz, jak te rozkłady ideału (9) mają się do twierdzenia o jednoznaczności rozkładu każdego ideału niezerowego pierścienia Dedekinda na iloczyn potęg ideałów pierwszych. Na pierwszy rzut oka mamy tu niejednoznaczność rozkładu gdyż ideał (9) jest z jednej strony kwadratem ideału $\mathfrak{c}$ a z drugiej iloczynem dwóch różnych ideałów $\mathfrak{a}$ i $\mathfrak{b}$.
Rozważmy ideały $\mathfrak{p}$ i $\mathfrak{q}$ określone następująco za pomocą generatorów:

$$\mathfrak{p} = (3,\ 2 + \sqrt{-5}\,), \qquad \mathfrak{q} = (3,\ 2 - \sqrt{-5}\,).$$

Można zauważyć, że $\mathfrak{p} = \mathfrak{c} + \mathfrak{a}$ oraz $\mathfrak{q} = \mathfrak{c} + \mathfrak{b}$, skąd przy pomocy (6.22) wynika, że $\mathfrak{p}$ jest największym wspólnym dzielnikiem ideałów $\mathfrak{c}$ i $\mathfrak{a}$ w multyplikatywnym monoidzie ideałów pierścienia A oraz podobnie $\mathfrak{q}$ jest największym wspólnym dzielnikiem ideałów $\mathfrak{c}$ i $\mathfrak{b}$ (zob. przykład 6.3.5).
Pokażemy najpierw, że $\mathfrak{p}$ i $\mathfrak{q}$ są ideałami pierwszymi pierścienia A. Dla dowolnych $a, b \in \mathbb{Z}$ mamy

$$a + b\sqrt{-5} \equiv a + b \bmod \mathfrak{p}$$

gdyż $\sqrt{-5} \equiv -2 \equiv 1 \bmod \mathfrak{p}$. Zatem $a + b\sqrt{-5} \equiv 0, 1, 2 \bmod \mathfrak{p}$. Stąd łatwo stwierdzamy, że

$$\mathbb{Z}[\sqrt{-5}]/\mathfrak{p} \cong \mathbb{F}_3,$$

skąd wynika, że $\mathfrak{p}$ jest ideałem maksymalnym (a więc także pierwszym) pierścienia $\mathbb{Z}[\sqrt{-5}]$. Podobnie dowodzimy, że $\mathfrak{q}$ jest ideałem pierwszym. Dalej mamy

$$\begin{aligned} \mathfrak{p} \cdot \mathfrak{q} &= (9,\ 3(2+\sqrt{-5}\,),\ 3(2-\sqrt{-5}\,),\ (2+\sqrt{-5}\,)(2-\sqrt{-5}\,)) \\ &= (3) \cdot (3,\ 2+\sqrt{-5}\,,\ 2-\sqrt{-5}\,) \\ &= (3), \end{aligned}$$

gdyż ideał $(3,\ 2+\sqrt{-5}\,,\ 2-\sqrt{-5}\,)$ jest jednostkowy, jako że zawiera jedynkę pierścienia A :

$$-3\ +\ 2+\sqrt{-5}\ +\ 2-\sqrt{-5} = 1.$$

Mamy także

$$\begin{aligned} \mathfrak{p}^2 &= (9,\ 3(2+\sqrt{-5}\,),\ (2+\sqrt{-5}\,)^2) \\ &= (2+\sqrt{-5}\,) \cdot (2-\sqrt{-5}\,,\ 3,\ 2+\sqrt{-5}\,) \\ &= (2+\sqrt{-5}\,) \end{aligned}$$

i podobnie

$$\mathfrak{q}^2 = (2-\sqrt{-5}\,).$$

Mamy więc

$$\mathfrak{c} = \mathfrak{p} \cdot \mathfrak{q}, \quad \mathfrak{a} = \mathfrak{p}^2, \quad \mathfrak{b} = \mathfrak{q}^2,$$

i wobec tego okazuje się, że dwa pozornie różne rozkłady $(9) = \mathfrak{c}^2 = \mathfrak{a} \cdot \mathfrak{b}$ ideału (9) są rezultatem różnego zgrupowania czynników *pierwszych* ideału (9) :

$$\mathfrak{c}^2 = (\mathfrak{p} \cdot \mathfrak{q})^2 = \mathfrak{p}^2 \cdot \mathfrak{q}^2 = \mathfrak{a} \cdot \mathfrak{b}.$$

Pierścienie liczb algebraicznych całkowitych w skończonych rozszerzeniach ciała liczb wymiernych są dość szczególnymi pierścieniami Dedekinda. Pierwszym sygnałem wskazującym, że nie wyczerpują one całej klasy pierścieni Dedekinda jest stwierdzenie 6.4.5. Na ogół pierścienie ilorazowe pierścienia Dedekinda nie są skończone. Na przykład, w pierścieniu wielomianów $K[X]$ nad ciałem nieskończonym K dla *każdego* ideału właściwego $\mathfrak{a}$ pierścień ilorazowy $K[X]/\mathfrak{a}$ jest nieskończony.

Innym sygnałem jest fakt, że grupa klas ideałów ułamkowych skończonego rozszerzenia ciała liczb wymiernych jest *skończona* (zob. np. J. Browkin, *Teoria ciał*, PWN Warszawa 1977, str. 274). W zestawieniu z twierdzeniem Claborna (*every abelian group is a class group*) wskazuje to miejsce pierścieni liczb algebraicznych całkowitych w ogólnej teorii pierścieni Dedekinda. Jest rzeczą ciekawą, że nie udało się dotąd rozstrzygnąć pytania, czy każda *skończona* grupa abelowa jest grupą klas ideałów jakiegoś *skończonego* rozszerzenia ciała liczb wymiernych.

6.5 Zadania

1. Niech A będzie pierścieniem noetherowskim i niech $\varphi : A \to A$ będzie homomorfizmem pierścieni. Udowodnić, że jeśli φ jest epimorfizmem, to φ jest izomorfizmem.

Wskazówka. $\ker\varphi \subseteq \ker\varphi^2 \subseteq \cdots$.

2. Niech A będzie pierścieniem noetherowskim. Pokazać, że dla każdego ideału $\mathfrak{a}$ pierścienia A istnieje liczba naturalna m taka, że

$$(\mathsf{rad}\,\mathfrak{a})^m \subseteq \mathfrak{a}.$$

Wywnioskować stąd dwa następujące stwierdzenia:

(a) W pierścieniu noetherowskim A nilradykał jest ideałem nilpotentnym, to znaczy, istnieje liczba naturalna m taka, że $(\mathsf{Nil}\,A)^m = (0)$.
(b) Jeśli $\mathfrak{q}$ jest $\mathfrak{p}-$prymarnym ideałem w pierścieniu noetherowskim A, to istnieje taka liczba naturalna m, że $\mathfrak{p}^m \subseteq \mathfrak{q} \subseteq \mathfrak{p}$.

3. Niech p będzie liczbą pierwszą i niech f będzie unormowanym wielomianem nierozkładalnym pierścienia $\mathbb{Z}[X]$ stopnia $n \geqslant 1$. Niech $\bar{f}$ oznacza wielomian pierścienia $\mathbb{Z}_p[X]$, który powstaje z f przez zastąpienie każdego współczynnika jego resztą modulo p.
(a) Sprawdzić, że (p) i (f) są ideałami pierwszymi w $\mathbb{Z}[X]$ oraz dla każdej liczby naturalnej m ideały $(p)^m$ i $(f)^m$ są prymarne w $\mathbb{Z}[X]$.
(b) Sprawdzić, że jeśli $\bar{f}$ jest nierozkładalny w $\mathbb{Z}_p[X]$, to $\mathfrak{p} = (p) + (f) = (p, f)$ jest ideałem maksymalnym w $\mathbb{Z}[X]$ i wyznaczyć liczbę elementów ciała $\mathbb{Z}[X]/\mathfrak{p}$.

4. Udowodnić, że wielomian $f = X^4 + 1$ jest nierozkładalny w $\mathbb{Q}[X]$ ale $\bar{f}$ jest rozkładalny w $\mathbb{Z}_p[X]$ dla każdej liczby pierwszej p.

5. Pokazać, że w pierścieniu $\mathbf{Z}[X]$ ideał $\mathfrak{q} = (4, X)$ jest prymarny, ale nie jest potęgą ideału pierwszego.

6. Niech $A = \{a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X] : a_1 \equiv 0 \pmod 3\}$.

(a) Pokazać, że w pierścieniu A ideał $\mathfrak{p} = (3X, X^2, X^3)$ jest ideałem pierwszym.
(b) Pokazać, że $\mathfrak{p}^2$ nie jest ideałem prymarnym.

Wskazówka. (b) Rozpatrzyć wielomian $9X^2$.

7. Niech $\mathfrak{q} = (2, X)^2 = (4, 2X, X^2)$ będzie ideałem w pierścieniu $\mathbb{Z}[X]$.

(a) Sprawdzić, że $\mathfrak{q}$ jest ideałem prymarnym.
(b) Sprawdzić, że $\mathfrak{q} = (4, X) \cap (2, X^2)$.
Ideał $\mathfrak{q}$ jest więc ideałem prymarnym w pierścieniu noetherowskim, ale nie jest nieprzywiedlny.

8. Niech A będzie pierścieniem całkowitym i niech S będzie podzbiorem multyplikatywnym w A. Udowodnić następujące stwierdzenia.
(a) Jeśli $\mathfrak{A}$ jest ideałem pierścienia ułamków AS^{-1} oraz $\mathfrak{a} = \mathfrak{A} \cap A$, to $\mathfrak{a}$ jest ideałem w A oraz $\mathfrak{A} = \mathfrak{a}S^{-1}$.

(b) Jeśli A jest pierścieniem noetherowskim, to AS^{-1} jest także pierścieniem noetherowskim.

9. Niech A będzie pierścieniem całkowitym i niech S będzie podzbiorem multyplikatywnym w A. Udowodnić następujące stwierdzenia.
(a) Jeśli $\mathfrak{A}$ jest ideałem pierwszym pierścienia AS^{-1} oraz $\mathfrak{a} = \mathfrak{A} \cap A$, to $\mathfrak{a}$ jest ideałem pierwszym w A oraz $\mathfrak{a} \subseteq A \setminus S$.
(b) Jeśli $\mathfrak{A}$ jest ideałem pierścienia AS^{-1} oraz $\mathfrak{a} = \mathfrak{A} \cap A$ jest ideałem pierwszym w A takim, że $\mathfrak{a} \subseteq A \setminus S$, to $\mathfrak{A}$ jest ideałem pierwszym w AS^{-1}.
(c) Jeśli w pierścieniu A każdy niezerowy ideał pierwszy jest maksymalny, to także w pierścieniu AS^{-1} każdy niezerowy ideał pierwszy jest maksymalny.

10. Niech A będzie pierścieniem całkowitym i niech S będzie podzbiorem multyplikatywnym w A. Udowodnić, że jeśli pierścień A jest integralnie domknięty, to pierścień ułamków AS^{-1} jest także integralnie domknięty.

Uwaga. Zadania **8**, **9**, **10** pokazują, że jeśli A jest pierścieniem Dedekinda i S jest dowolnym podzbiorem multyplikatywnym w A, to także pierścień ułamków AS^{-1} jest pierścieniem Dedekinda.

Rozdział 7

Afiniczne rozmaitości algebraiczne

Ostatnie zmiany 23.03.2009 r.

W tym rozdziale przedstawiamy podstawowe fakty o zbiorach rozwiązań układów równań wielomianowych w przestrzeni afinicznej k^n. Głównym twierdzeniem tego rozdziału jest twierdzenie Hilberta o zerach podające warunek konieczny i wystarczający istnienia rozwiązań takiego układu równań nad ciałem algebraicznie domkniętym k.

7.1 Zbiory algebraiczne i ich ideały

Rozpoczniemy od badania zbioru wspólnych zer dowolnego zbioru $\mathcal{S}$ wielomianów w pierścieniu wielomianów $k[X_1, \ldots, X_n]$, gdzie k jest dowolnym ciałem. W dalszej części rozdziału będziemy przeważnie zakładać, że k jest ciałem algebraicznie domkniętym, ale na razie nie ma potrzeby nakładać jakichkolwiek ograniczeń na ciało k.

Definicja **7.1.1.** *Zerem* wielomianu $f \in k[X_1, \ldots, X_n]$ w przestrzeni afinicznej k^n nazywamy każdy punkt $(x_1, \ldots, x_n)$ przestrzeni k^n taki, że $f(x_1, \ldots, x_n) = 0$.

Zbiorem algebraicznym V nazywamy podzbiór przestrzeni afinicznej k^n złożony z wszystkich wspólnych zer pewnego zbioru $\mathcal{S}$ wielomianów pierścienia $k[X_1, \ldots, X_n]$:

$$V = \Big\{(x_1, \ldots, x_n) \in k^n : f(x_1, \ldots, x_n) = 0 \quad \forall\, f \in \mathcal{S}\Big\}.$$

Zbiór V nazywamy zbiorem algebraicznym wyznaczonym przez zbiór $\mathcal{S}$ wielomianów (lub zbiorem wspólnych zer zbioru wielomianów $\mathcal{S}$) i oznaczamy $V = \mathcal{Z}(\mathcal{S})$.

Niech $\mathfrak{a}$ będzie ideałem pierścienia $k[X_1, \ldots, X_n]$ generowanym przez zbiór $\mathcal{S}$. Wtedy możemy także rozpatrywać zbiór algebraiczny $\mathcal{Z}(\mathfrak{a})$ wyznaczony przez ideał $\mathfrak{a}$ pierścienia $k[X_1, \ldots, X_n]$. Zauważmy, że

$$\mathcal{Z}(\mathcal{S}) = \mathcal{Z}(\mathfrak{a}).$$

Rzeczywiście, ponieważ $\mathcal{S} \subseteq \mathfrak{a}$ więc każde wspólne zero wielomianów ideału $\mathfrak{a}$ jest także wspólnym zerem wielomianów zbioru $\mathcal{S}$, to znaczy $\mathcal{Z}(\mathfrak{a}) \subseteq \mathcal{Z}(\mathcal{S})$. Z drugiej strony, jeśli punkt $x \in k^n$ jest wspólnym zerem każdego wielomianu zbioru $\mathcal{S}$, to jest także wspólnym zerem wszystkich wielomianów postaci $h_1 f_1 + \cdots + h_r f_r$,

gdzie $f_1, \ldots, f_r \in \mathcal{S}$ natomiast $h_1, \ldots, h_r$ są dowolnymi wielomianami pierścienia $k[X_1, \ldots, X_n]$. Zatem x jest wspólnym zerem wszystkich wielomianów należących do ideału $\mathfrak{a}$, skąd wynika, że $\mathcal{Z}(\mathcal{S}) \subseteq \mathcal{Z}(\mathfrak{a})$.
Tak więc *każdy zbiór algebraiczny* $V \subseteq k^n$ *jest zbiorem wspólnych zer pewnego ideału* $\mathfrak{a}$ *pierścienia* $k[X_1, \ldots, X_n]$.

Z twierdzenia Hilberta o bazie wiemy, że każdy ideał w pierścieniu $k[X_1, \ldots, X_n]$ jest skończenie generowany. A więc w pierścieniu $k[X_1, \ldots, X_n]$ istnieją wielomiany $f_1, \ldots, f_r$ takie, że $\mathfrak{a} = (f_1, \ldots, f_r)$. Jeśli więc $x = (x_1, \ldots, x_n) \in \mathcal{Z}(\mathfrak{a})$, czyli jest wspólnym zerem wszystkich wielomianów ideału $\mathfrak{a}$, to w szczególności x jest wspólnym zerem wielomianów $f_1, \ldots, f_r$. Z drugiej strony, dla $f \in \mathfrak{a}$ istnieją wielomiany $h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$ takie, że

$$f = h_1 f_1 + \cdots + h_r f_r.$$

Stąd wynika, że każdy punkt $x \in k^n$, który jest wspólnym zerem wielomianów $f_1, \ldots, f_r$ jest także zerem każdego wielomianu f ideału $\mathfrak{a}$. Wobec tego zbiór wspólnych zer wszystkich wielomianów ideału $\mathfrak{a}$ pokrywa się ze zbiorem wspólnych zer *skończonego* układu wielomianów $f_1, \ldots, f_r$ (generatorów ideału $\mathfrak{a}$).
Inaczej mówiąc, *zbiór algebraiczny* V *w przestrzeni afinicznej* k^n *jest zbiorem rozwiązań skończonego układu równań algebraicznych*

$$f_1(X_1, \ldots, X_n) = 0, \ldots, f_r(X_1, \ldots, X_n) = 0,$$

gdzie $f_1, \ldots, f_r$ są wielomianami n zmiennych o współczynnikach z ciała k. Jeśli $\mathfrak{a} = (f_1, \ldots, f_r)$, to zamiast $V = \mathcal{Z}((f_1, \ldots, f_r))$ piszemy $V = \mathcal{Z}(f_1, \ldots, f_r)$.

Uwaga 7.1.2. Przypadek szczególny, gdy wielomiany f_i są liniowe,

$$f_i = a_{i1}X_1 + \cdots + a_{in}X_n - b_i, \quad a_{ij}, b_i \in k, \tag{7.1}$$

rozpatruje się w algebrze liniowej. Istnieją definitywne metody sprawdzania, czy układ (7.1) wielomianów liniowych ma wspólne zera (to znaczy, czy odpowiedni zbiór algebraiczny jest niepusty) oraz metody wyznaczania wszystkich wspólnych zer układu (znajdowania wszystkich punktów odpowiedniego zbioru algebraicznego). Przy tym specyfiką zbiorów algebraicznych wyznaczonych przez układy równań liniowych jest fakt, że istnienie rozwiązań układu równań liniowych nie zależy od ciała, w którym poszukujemy rozwiązań. Jeśli K jest jakimkolwiek ciałem do którego należą współczynniki równań układu oraz $K \subset k$, to układ (7.1) ma wspólne zero w k^n wtedy i tylko wtedy gdy ma wspólne zero w K^n.
Natomiast w geometrii algebraicznej dopuszczamy wielomiany dowolnych stopni i istnienie zer w ciele współczynników jest rzadkością (chyba, że od razu założymy, iż ciało k jest algebraicznie domknięte). A więc na przykład wielomian $X_1^2 + X_2^2 + 1$ o współczynnikach wymiernych nie ma zera w przestrzeni afinicznej $\mathbb{Q}^2$, ani nawet w $\mathbb{R}^2$, ma natomiast zera w przestrzeni $\mathbb{C}^2$, a nawet w $\mathbb{Q}(i)^2$. W dalszym ciągu pokażemy, że jeśli k jest ciałem algebraicznie domkniętym, to każdy układ wielomianów, który generuje ideał właściwy w pierścieniu $k[X_1, \ldots, X_n]$ ma zera w przestrzeni k^n (zob. twierdzenie Hilberta o zerach). A więc nad ciałami algebraicznie domkniętymi zbiory algebraiczne ideałów właściwych są niepuste.

Przykład 7.1.1. Zbiorem algebraicznym $\mathcal{Z}(0)$ ideału zerowego (0) pierścienia $k[X_1,\ldots,X_n]$ jest cała przestrzeń k^n, to znaczy $\mathcal{Z}(0)=k^n$ (wielomian zerowy przyjmuje wartość zero w każdym punkcie przestrzeni k^n).

Zbiorem algebraicznym $\mathcal{Z}(1)$ ideału jednostkowego $(1)=k[X_1,\ldots,X_n]$ pierścienia $k[X_1,\ldots,X_n]$ jest zbiór pusty $\varnothing$, to znaczy $\mathcal{Z}(1)=\varnothing$ (wielomian stały 1 nie ma żadnego zera w k^n).

Zbiorem algebraicznym $\mathcal{Z}(f)$ ideału głównego (f) pierścienia $k[X]$ (wielomianów jednej zmiennej) jest (skończony) zbiór zer wielomianu f w ciele k.

Zbiór algebraiczny $\mathcal{Z}(f)\subset k^n$ ideału głównego generowanego przez wielomian $f\in k[X_1,\ldots,X_n]$ nazywamy *hiperpowierzchnią* w k^n o równaniu $f=0$. W szczególności, przestrzeń $k^n=\mathcal{Z}(0)$ oraz zbiór pusty $\varnothing=\mathcal{Z}(1)$ są hiperpowierzchniami. Jeśli $n=2$, hiperpowierzchnia nazywa się *krzywą algebraiczną* na płaszczyźnie afinicznej k^2.

Dla dowolnych liczb naturalnych n,m każdy ideał $\mathfrak{a}_{(n,m)}=(X_1^n,X_2^m)$ pierścienia wielomianów $k[X_1,X_2]$ ma jednopunktowy zbiór algebraiczny $V=\mathcal{Z}(\mathfrak{a}_{(n,m)})=\{(0,0)\}$ na płaszczyźnie afinicznej k^2.

Jak pokazuje ostatni przykład, różne ideały mogą mieć ten sam zbiór algebraiczny. Opisywanie zbiorów algebraicznych jako zbiorów wspólnych zer wielomianów należących do pewnego ideału pierścienia wielomianów ma więc tę niedogodność, że z danym zbiorem algebraicznym związanych jest na ogół wiele ideałów. Istnieje jednak prosty sposób na ominięcie tej trudności. Jak bowiem łatwo sprawdzić, zbiór $\mathcal{I}(V)$ *wszystkich* wielomianów pierścienia $k[X_1,\ldots,X_n]$ zerujących się we wszystkich punktach danego zbioru algebraicznego $V\subseteq k^n$ jest *ideałem* w pierścieniu $k[X_1,\ldots,X_n]$.

Definicja **7.1.3.** Niech V będzie zbiorem algebraicznym w przestrzeni afinicznej k^n. Ideał $\mathcal{I}(V)$ pierścienia $k[X_1,\ldots,X_n]$ złożony z wszystkich wielomianów pierścienia $k[X_1,\ldots,X_n]$ zerujących się w każdym punkcie zbioru V nazywamy ideałem *odpowiadającym* zbiorowi algebraicznemu V lub ideałem *stowarzyszonym* ze zbiorem algebraicznym V lub po prostu ideałem zbioru algebraicznego V:

$$\mathcal{I}(V):=\{f\in k[X_1,\ldots,X_n]: f(x_1,\ldots,x_n)=0 \quad \forall\,(x_1,\ldots,x_n)\in V\}.$$

Jeśli V jest zbiorem pustym, to można przyjąć, że warunek $f(x)=0 \quad \forall x\in V$ jest spełniony (pusto) przez wszystkie wielomiany i wobec tego $\mathcal{I}(\varnothing)=(1)$. W drugim krańcowym przypadku mamy $\mathcal{I}(k^n)=(0)$ o ile k jest ciałem nieskończonym. Natomiast dla liczby pierwszej p i ciała $p-$elementowego $\mathbb{F}_p$ mamy $\mathcal{I}(\mathbb{F}_p^1)=(X^p-X)$. Wskażemy teraz elementarne własności operacji $\mathcal{Z}$ oraz $\mathcal{I}$.

Przykład 7.1.2. Niech V, V_1 i V_2 będą zbiorami algebraicznymi w przestrzeni k^n i niech $\mathfrak{a},\mathfrak{a}_1,\mathfrak{a}_2$ będą ideałami pierścienia $k[X_1,\ldots,X_n]$. Wtedy

$$\mathfrak{a}_1\subseteq\mathfrak{a}_2 \;\Rightarrow\; \mathcal{Z}(\mathfrak{a}_1)\supseteq\mathcal{Z}(\mathfrak{a}_2). \tag{7.2}$$

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a}))\;\supseteq\;\mathfrak{a}. \tag{7.3}$$

$$\mathcal{Z}(\mathcal{I}(V))\;=\;V. \tag{7.4}$$

$$V_1\subseteq V_2 \;\Leftrightarrow\; \mathcal{I}(V_1)\supseteq\mathcal{I}(V_2). \tag{7.5}$$

$$V_1=V_2 \;\Leftrightarrow\; \mathcal{I}(V_1)=\mathcal{I}(V_2). \tag{7.6}$$

(7.2) i (7.3) są oczywiste, podobnie jak inkluzja $\mathcal{Z}(\mathcal{I}(V)) \supseteq V$ w (7.4). Dla dowodu przeciwnej inkluzji załóżmy, że $V = \mathcal{Z}(\mathfrak{a})$ dla pewnego ideału $\mathfrak{a}$. Wtedy $\mathcal{I}(V) = \mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathfrak{a}$ i na podstawie (7.2) mamy $\mathcal{Z}(\mathcal{I}(V)) \subseteq \mathcal{Z}(\mathfrak{a}) = V$.
Implikacja $V_1 \subseteq V_2 \Rightarrow \mathcal{I}(V_1) \supseteq \mathcal{I}(V_2)$ jest oczywista. Natomiast jeśli $\mathcal{I}(V_1) \supseteq \mathcal{I}(V_2)$, to na podstawie (7.2) mamy $\mathcal{Z}(\mathcal{I}(V_1)) \subseteq \mathcal{Z}(\mathcal{I}(V_2))$, skąd na podstawie (7.4) otrzymujemy $V_1 \subseteq V_2$.
W (7.6) implikacja $\Rightarrow$ jest oczywista, natomiast implikacja $\Leftarrow$ jest konsekwencją (7.4).

Występująca tutaj asymetria w (7.3) i (7.4) nie jest przypadkowa. Okazuje się, że w (7.3) nie zachodzi na ogół równość. Dokładne wyznaczenie ideału $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ (w przypadku ciała algebraicznie domkniętego k) podaje twierdzenie Hilberta o zerach, które dyskutujemy w dalszej części tego rozdziału. Podamy teraz przykłady pokazujące, że w (7.3) może zachodzić zarówno nierówność jak i równość.

Przykład 7.1.3. Niech $\mathfrak{a} = (X^2, Y)$ będzie ideałem w $k[X,Y]$. Wtedy $\mathcal{Z}(\mathfrak{a}) = \big\{(0,0)\big\}$ oraz $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(\big\{(0,0)\big\}) = (X,Y) \supsetneq (X^2,Y) = \mathfrak{a}$.

Drugi przykład pokazuje jak znaleźć ideal $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ w przypadku, gdy $\mathfrak{a} = (f)$ jest ideałem głównym w pierścieniu wielomianów $k[X,Y]$ dwóch zmiennych i o ciele k nie zakładamy, że jest algebraicznie domknięte. Rozpoczniemy od następującego lematu.

LEMAT **7.1.4.** *Niech k będzie dowolnym ciałem i niech $f, g \in k[X,Y]$. Załóżmy, że wielomian f jest nierozkładalny w $k[X,Y]$ oraz f nie dzieli wielomianu g. Wtedy układ równań algebraicznych*

$$f(X,Y) = 0, \quad g(X,Y) = 0$$

ma tylko skończoną liczbę rozwiązań w ciele k.

Dowód. Podamy tylko szkic dowodu. Niech $\deg_X f > 0$. Wtedy f można traktować jako wielomian jednej zmiennej X nad pierścieniem $k[Y]$ a także jako wielomian nad ciałem $k(Y)$ funkcji wymiernych zmiennej Y. Wykorzystamy następujące dobrze znane konsekwencje lematu Gaussa o rozkładalności wielomianów nad pierścieniami ideałów głównych (w naszym przypadku $k[Y]$) i ich ciałami ułamków ($k(Y)$).

- f jest nierozkładalny w pierścieniu $k(Y)[X]$.
- f nie dzieli g w pierścieniu $k(Y)[X]$.

Ponieważ $k(Y)[X]$ jest pierścieniem ideałów głównych, istnieją wielomiany $\alpha, \beta \in k(Y)[X]$ takie, że

$$\alpha f + \beta g = 1.$$

Mnożąc obie strony przez najmniejszą wspólną wielokrotność mianowników możemy napisać

$$A(X,Y)f(X,Y) + B(X,Y)g(X,Y) = h(Y)$$

dla pewnych $A, B \in k[X,Y],\ h \in k[Y]$. Ponieważ wielomian h ma tylko skończoną liczbę zer w ciele k, wynika stąd, że w rozwiązaniach układu równań $f(X,Y) =$

0, $g(X,Y)=0$ w ciele k niewiadoma Y przyjmuje tylko skończoną liczbę wartości. Dla każdej z tych wartości niewiadomej Y istnieje oczywiście tylko skończona liczba możliwości dla niewiadomej X w naszym układzie równań. Zatem układ ma tylko skończoną liczbę rozwiązań. □

Teraz możemy przejść do wyznaczenia ideału $\mathcal{I}(\mathcal{Z}(f))$ stowarzyszonego z krzywą algebraiczną $\mathcal{Z}(f)$. Wprawdzie formalnie na ciało k nie nakładamy żadnych ograniczeń, ale będziemy zakładać, że krzywa $\mathcal{Z}(f)$ ma nieskończenie wiele punktów, a to może mieć miejsce tylko nad ciałem nieskończonym.

STWIERDZENIE **7.1.5.** *Niech k będzie dowolnym ciałem i niech $f \in k[X,Y]$ będzie wielomianem nierozkładalnym w pierścieniu $k[X,Y]$. Jeśli krzywa $\mathcal{Z}(f)$ ma nieskończenie wiele punktów, to*

$$\mathcal{I}(\mathcal{Z}(f)) = (f).$$

Dowód. Wobec (7.3) wystarczy pokazać, że $\mathcal{I}(\mathcal{Z}(f)) \subseteq (f)$. Niech więc $g \in \mathcal{I}(\mathcal{Z}(f))$. Wtedy wielomian g zeruje się w każdym punkcie krzywej $\mathcal{Z}(f)$ i wobec tego układ równań $f(X,Y)=0,\ g(X,Y)=0$ ma nieskończenie wiele rozwiązań. W takim razie, na podstawie lematu 7.1.4, f dzieli g, czyli $g \in (f)$. □

Przykład 7.1.4. Wielomian $XY-1 \in \mathbb{R}[X,Y]$ jest nierozkładalny w pierścieniu $\mathbb{R}[X,Y]$ i krzywa $\mathcal{Z}(XY-1) \subset \mathbb{R}^2$ ma nieskończenie wiele punktów na płaszczyźnie afinicznej $\mathbb{R}^2$ (jest to hiperbola). Zatem ideałem $\mathcal{I}(\mathcal{Z}(XY-1))$ stowarzyszonym z hiperbolą $\mathcal{Z}(XY-1)$ jest ideał główny generowany przez wielomian $XY-1$.

7.2 Topologia Zariskiego

Zauważyliśmy już, że zbiór pusty i cała przestrzeń k^n są zbiorami algebraicznymi. W dwóch następnych lematach udowodnimy dalsze własności zbiorów algebraicznych analogiczne do własności zbiorów domkniętych w przestrzeni topologicznej.

LEMAT **7.2.1.** *Jeśli $V_1,\ldots,V_r$ są zbiorami algebraicznymi w przestrzeni k^n, to ich suma mnogościowa $V_1 \cup \cdots \cup V_r$ jest zbiorem algebraicznym w k^n.*

Dowód. Niech $V_i = \mathcal{Z}(\mathfrak{a}_i)$, gdzie $\mathfrak{a}_i$ jest ideałem w $k[X_1,\ldots,X_n]$. Udowodnimy, że

$$V_1 \cup \cdots \cup V_r = \mathcal{Z}(\mathfrak{a}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{a}_r) = \mathcal{Z}(\mathfrak{a}_1 \cdots \mathfrak{a}_r). \tag{7.7}$$

Rozpatrzmy najpierw przypadek $r=2$. Niech

$$\mathfrak{a}_1 = (f_1,\ldots,f_k), \quad \mathfrak{a}_2 = (g_1,\ldots,g_\ell).$$

Rozpatrzmy ideał $\mathfrak{a}_1 \cdot \mathfrak{a}_2 = (f_1g_1,\ldots,f_ig_j,\ldots,f_kg_\ell)$. Pokażemy, że

$$V_1 \cup V_2 = \mathcal{Z}(\mathfrak{a}_1) \cup \mathcal{Z}(\mathfrak{a}_2) = \mathcal{Z}(\mathfrak{a}_1 \cdot \mathfrak{a}_2). \tag{7.8}$$

Jeśli $x=(x_1,\ldots,x_n) \in V_1 \cup V_2$, to $f_i(x)=0$ dla wszystkich $i=1,\ldots,k$ lub $g_j(x)=0$ dla wszystkich $j=1,\ldots,\ell$. Zatem dla każdej pary wskaźników i,j mamy $(f_ig_j)(x) = f_i(x)g_j(x) = 0$. Oznacza to, że $x \in \mathcal{Z}(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$.

Natomiast jeśli $x \notin V_1 \cup V_2$, to $x \notin V_1$ i równocześnie $x \notin V_2$. Zatem istnieją i oraz j takie, że $f_i(x) \neq 0$ oraz $g_j(x) \neq 0$. Wtedy także $(f_i g_j)(x) \neq 0$ i wobec tego $x \notin \mathcal{Z}(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$. Dowodzi to (7.8).
Dla dowodu (7.7) przeprowadzamy dowód indukcyjny. Wykorzystując założenie indukcyjne i udowodniony już przypadek $r = 2$ otrzymujemy

$$\begin{aligned}\mathcal{Z}(\mathfrak{a}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{a}_r) &= (\mathcal{Z}(\mathfrak{a}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{a}_{r-1})) \cup \mathcal{Z}(\mathfrak{a}_r) \\ &= (\mathcal{Z}(\mathfrak{a}_1 \cdots \mathfrak{a}_{r-1})) \cup \mathcal{Z}(\mathfrak{a}_r) = \mathcal{Z}(\mathfrak{a}_1 \cdots \mathfrak{a}_{r-1} \cdot \mathfrak{a}_r).\end{aligned}$$

A więc zbiór $V_1 \cup \cdots \cup V_r$ jest zbiorem wszystkich zer ideału $\mathfrak{a}_1 \cdots \mathfrak{a}_r$, jest zatem zbiorem algebraicznym. □

Uwaga 7.2.2. Równość (7.7) można uzupełnić następująco:

$$\mathcal{Z}(\mathfrak{a}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{a}_r) = \mathcal{Z}(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r) = \mathcal{Z}(\mathfrak{a}_1 \cdots \mathfrak{a}_r).$$

Wystarczy zauważyć, że

$$\mathcal{Z}(\mathfrak{a}_1 \cdots \mathfrak{a}_r) \subseteq \mathcal{Z}(\mathfrak{a}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{a}_r) \subseteq \mathcal{Z}(\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r) \subseteq \mathcal{Z}(\mathfrak{a}_1 \cdots \mathfrak{a}_r).$$

Pierwsza inkluzja wynika z (7.7), druga wynika z $\mathfrak{a}_i \supseteq \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r$ i trzecia wynika z $\mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_r \supseteq \mathfrak{a}_1 \cdots \mathfrak{a}_r$.

LEMAT **7.2.3.** *Jeśli* $\{V_t : t \in T\}$, *jest dowolną rodziną zbiorów algebraicznych w przestrzeni afinicznej* k^n, *to ich przekrój* $\bigcap\{V_t : t \in T\}$ *jest także zbiorem algebraicznym w* k^n.

Dowód. Dla każdego $t \in T$ weźmy ideał $\mathcal{I}(V_t)$ pierścienia $k[X_1, \ldots, X_n]$ stowarzyszony ze zbiorem algebraicznym V_t. Niech $\mathfrak{a}$ będzie ideałem w pierścieniu $k[X_1, \ldots, X_n]$ generowanym przez zbiór $\bigcup\{\mathcal{I}(V_t) : t \in T\}$. A więc

$$\mathfrak{a} = \sum\Big\{\mathcal{I}(V_t) : t \in T\Big\}.$$

Udowodnimy, że

$$\mathcal{Z}(\mathfrak{a}) = \bigcap\{V_t : t \in T\}, \tag{7.9}$$

skąd wynika już, że przekrój rodziny zbiorów algebraicznych $\{V_t : t \in T\}$ jest zbiorem algebraicznym (jako zbiór wspólnych zer wielomianów ideału $\mathfrak{a}$).
Dla dowodu (7.9) zauważamy, że

$$\begin{aligned}x \in \mathcal{Z}(\mathfrak{a}) &\Leftrightarrow \forall\, f \in \mathfrak{a} \quad [\, f(x) = 0\,] \\ &\Leftrightarrow \forall\, f \in \bigcup\{\mathcal{I}(V_t) : t \in T\} \quad [\, f(x) = 0\,] \\ &\Leftrightarrow \forall\, t \in T \quad \forall\, f \in \mathcal{I}(V_t) \quad [\, f(x) = 0\,] \\ &\Leftrightarrow \forall\, t \in T \quad [\, x \in \mathcal{Z}(\mathcal{I}(V_t))\,] \\ &\Leftrightarrow \forall\, t \in T \quad [\, x \in V_t\,] \\ &\Leftrightarrow x \in \bigcap\{V_t : t \in T\}. \qquad \square\end{aligned}$$

Uwaga 7.2.4. Jeśli zbiór T jest skończony, powiedzmy $T = \Big\{1, \ldots, r\Big\}$ oraz $\mathfrak{a}_t = \mathcal{I}(V_t)$, to $\mathcal{Z}(\mathfrak{a}_t) = \mathcal{Z}(\mathcal{I}(V_t)) = V_t$. Z drugiej strony, ideał $\mathfrak{a}$ generowany przez zbiór $\bigcup\{\mathcal{I}(V_t) : t \in T\}$ jest sumą ideałów $\mathfrak{a}_i$. Zatem równość (7.9) przyjmuje postać

$$\mathcal{Z}(\mathfrak{a}_1 + \cdots + \mathfrak{a}_r) = \mathcal{Z}(\mathfrak{a}_1) \cap \cdots \cap \mathcal{Z}(\mathfrak{a}_r).$$

TWIERDZENIE **7.2.5.** *W przestrzeni k^n istnieje topologia, w której zbiorami domkniętymi są zbiory algebraiczne w k^n.*

Dowód. Wystarczy przypomnieć, że zbiór pusty i cała przestrzeń k^n są zbiorami algebraicznymi (przykład 7.1.1) i powołać się na lematy 7.2.1 i 7.2.3. □

Uwaga 7.2.6. Topologię przestrzeni afinicznej k^n wyznaczoną przez zbiory algebraiczne jako zbiory domknięte nazywa się *topologią Zariskiego* przestrzeni k^n.
Zauważmy, że zbiory jednopunktowe, a także wszystkie zbiory skończone są zbiorami algebraicznymi, a więc domkniętymi w topologii Zariskiego przestrzeni k^n. Zbiór jednopunktowy $\{x\}$, gdzie $x = (x_1, \ldots, x_n) \in k^n$, jest zbiorem rozwiązań układu równań

$$X_1 - x_1 = 0, \ \ldots, \ X_n - x_n = 0,$$

jest więc zbiorem algebraicznym. Natomiast zbiory skończone są sumami mnogościowymi skończonej liczby zbiorów jednoelementowych, są zatem algebraiczne na podstawie lematu 7.2.1. To, że zbiory jednopunktowe są domknięte oznacza w terminologii topologicznej, że przestrzeń k^n z topologią Zariskiego jest przestrzenią $\mathcal{T}_1$. Co do aksjomatu oddzielania $\mathcal{T}_2$ zob. uwagę 7.3.5.

Uwaga 7.2.7. W dowodach własności zbiorów algebraicznych ważną rolę odgrywa fakt, że pierścień wielomianów $k[X_1, \ldots, X_n]$ jest noetherowski. Bardzo przejrzystym zastosowaniem tego faktu jest dowód następującej *zasady minimum*:
W każdej niepustej rodzinie zbiorów algebraicznych istnieje minimalny zbiór algebraiczny (taki, który nie zawiera żadnego różnego od siebie zbioru tej rodziny).
Jeśli bowiem $\mathbf{V} := \{V_t : t \in T\}$ jest rodziną zbiorów algebraicznych w przestrzeni afinicznej k^n, to rozpatrujemy rodzinę stowarzyszonych ideałów

$$\mathbf{I} := \{\mathcal{I}(V_t) : t \in T\}$$

w pierścieniu $k[X_1, \ldots, X_n]$. Ponieważ pierścień ten jest noetherowski, spełnia więc warunek (MAX). Oznacza to, że w rodzinie $\mathbf{I}$ istnieje ideał $\mathcal{I}(V_{t_0})$ maksymalny w tej rodzinie. Na podstawie (7.5) wnioskujemy, ze zbiór V_{t_0} jest minimalny w rodzinie $\mathbf{V}$.

Uwaga 7.2.8. Każdy zbiór algebraiczny $V \subseteq k^n$ można traktować jako przestrzeń topologiczną z topologią Zariskiego. Zbiory jednopunktowe w V są domknięte i każdy łańcuch opadający podzbiorów domkniętych $V_1 \supset V_2 \supset \cdots$ jest skończony, gdyż odpowiada mu wznoszący łańcuch ideałów $\mathcal{I}(V_1) \subset \mathcal{I}(V_2) \subset \cdots$ w pierścieniu noetherowskim $k[X_1, \ldots, X_n]$, spełniającym zatem (ACC). W związku z tym, przechodząc do dopełnień zbiorów domkniętych w V otrzymujemy, że każdy wznoszący łańcuch podzbiorów *otwartych* zawartych w V jest także skończony. Stąd łatwo wynika, że zbiór algebraiczny V jest *zwartą* przestrzenią topologiczną. Niech bowiem $V = \bigcup_{t\in T} U_t$ będzie pokryciem zbioru V zbiorami otwartymi. Weźmy $t_1 \in T$. Jeśli $U_{t_1} \neq V$, to istnieje $t_2 \in T$ taki, że $U_{t_1} \subset U_{t_1} \cup U_{t_2}$ (ostra inkluzja). Jeśli $U_{t_1} \cup U_{t_2} \neq V$, to podobnie obieramy $t_3 \in T$ takie, że $U_{t_1} \cup U_{t_2} \subset U_{t_1} \cup U_{t_2} \cup U_{t_3}$. Ponieważ każdy łańcuch podzbiorów otwartych zawartych w V jest skończony, po skończonej liczbie kroków, powiedzmy m, otrzymamy $U_{t_1} \cup U_{t_2} \cup \cdots \cup U_{t_m} = V$. Z każdego pokrycia otwartego zbioru V można więc wybrać podpokrycie skończone.

7.3 Rozmaitości algebraiczne

DEFINICJA **7.3.1.** Niepusty zbiór algebraiczny $V \subseteq k^n$ nazywa się *rozmaitością algebraiczną*, jeśli stowarzyszony z nim ideał $\mathcal{I}(V)$ jest ideałem pierwszym w pierścieniu $k[X_1, \ldots, X_n]$.

DEFINICJA **7.3.2.** Niepusty zbiór algebraiczny $V \subseteq k^n$ nazywa się *nierozkładalny*, jeśli dla zbiorów algebraicznych A, B,

$$V = A \cup B \quad \Rightarrow \quad V = A \quad \text{lub} \quad V = B.$$

TWIERDZENIE **7.3.3.** *Niepusty zbiór algebraiczny $V \subseteq k^n$ jest nierozkładalny wtedy i tylko wtedy, gdy jest rozmaitością algebraiczną.*

Dowód. Udowodnimy najpierw, że jeśli V jest zbiorem rozkładalnym, to $\mathcal{I}(V)$ nie jest ideałem pierwszym w $k[X_1, \ldots, X_n]$. Niech więc $V = A \cup B$ oraz $V \neq A,\ V \neq B$. Wobec $A \subset V$ otrzymujemy $\mathcal{I}(A) \supset \mathcal{I}(V)$, ponadto $\mathcal{I}(A) \neq \mathcal{I}(V)$, gdyż $V \neq A$ (zobacz (7.6)). Istnieje zatem wielomian $f \in \mathcal{I}(A)$ taki, że $f \notin \mathcal{I}(V)$. Podobnie istnieje wielomian $g \in \mathcal{I}(B)$ taki, że $g \notin \mathcal{I}(V)$. Natomiast $fg \in \mathcal{I}(V)$, gdyż dla $x \in V$ mamy $x \in A$ lub $x \in B$ i wobec tego $f(x)g(x) = 0$. Ideał $\mathcal{I}(V)$ nie jest więc ideałem pierwszym.

Pozostaje pokazać, że jeśli V jest nierozkładalny, to ideał $\mathcal{I}(V)$ jest pierwszy. Przypuśćmy więc, że zbiór V jest nierozkładalny natomiast ideał $\mathcal{I}(V)$ nie jest pierwszy. Istnieją zatem wielomiany $f, g \in k[X_1, \ldots, X_n]$ takie, że $fg \in \mathcal{I}(V)$ oraz $f \notin \mathcal{I}(V),\ g \notin \mathcal{I}(V)$. Wtedy

$$A := \mathcal{Z}(f) \cap V, \quad B := \mathcal{Z}(g) \cap V$$

są zbiorami algebraicznymi. Udowodnimy, że

$$V = A \cup B \quad \text{oraz} \quad V \neq A,\ V \neq B. \tag{7.10}$$

Po pierwsze, jeśli $x \in V$, to wobec $fg \in \mathcal{I}(V)$ mamy $f(x)g(x) = 0$, i wobec tego $f(x) = 0$ lub $g(x) = 0$, czyli $x \in A$ lub $x \in B$. Zatem $V \subseteq A \cup B$. Ponieważ A i B są z definicji podzbiorami V wynika stąd równość $V = A \cup B$.
Po drugie, przypuśćmy, że $V = A$. Wtedy $\mathcal{I}(V) = \mathcal{I}(A)$, podczas gdy $f \notin \mathcal{I}(V)$ i $f \in \mathcal{I}(A)$. A więc $V \neq A$ i podobnie $V \neq B$. Dowodzi to (7.10).
Przypuszczenie, że zbiór V jest nierozkładalny i ideał $\mathcal{I}(V)$ nie jest pierwszy prowadzi więc do sprzeczności. □

Przykład 7.3.1. Niech $V = \mathcal{Z}(XY - 1) \subset \mathbb{R}^2$ będzie hiperbolą na płaszczyźnie afinicznej $\mathbb{R}^2$. Hiperbola V jest co prawda w sposób naturalny sumą mnogościową dwóch swoich gałęzi, ale gałęzie te nie są zbiorami algebraicznymi. Rzeczywiście, na podstawie przykładu 7.1.4, mamy $\mathcal{I}(V) = (XY - 1)$ i ponieważ wielomian $XY - 1$ jest nierozkładalny w pierścieniu $\mathbb{R}[X, Y]$, ideał główny $(XY - 1)$ jest ideałem pierwszym. Wobec tego hiperbola V jest rozmaitością algebraiczną a zatem także nierozkładalnym zbiorem algebraicznym.
Podobnie okrąg jednostkowy $\mathcal{Z}(X^2 + Y^2 - 1)$ czy parabola $\mathcal{Z}(Y - X^2)$ są rozmaitościami algebraicznymi na płaszczyźnie afinicznej $\mathbb{R}^2$.

TWIERDZENIE **7.3.4.** *Każdy zbiór algebraiczny A jest skończoną sumą mnogościową rozmaitości algebraicznych:*

$$A = V_1 \cup \cdots \cup V_r, \quad r \geqslant 1.$$

Jeśli w tym rozkładzie rozmaitości V_i są nieporównywalne (to znaczy, $V_i \not\subset V_j$ dla $i \neq j$), to przedstawienie jest jednoznaczne.

Dowód. Najpierw udowodnimy istnienie przedstawienia. Przypuśćmy, że istnieją zbiory algebraiczne w k^n, które nie są sumami mnogościowymi rozmaitości. Zgodnie z zasadą minimum (zobacz uwagę 7.2.7), istnieje minimalny zbiór algebraiczny Z, który nie jest skończoną sumą mnogościową rozmaitości. W szczególności więc zbiór Z nie jest rozmaitością i wobec tego nie jest nierozkładalny. Zatem $Z = A \cup B$, gdzie A i B są zbiorami algebraicznymi oraz $A \neq Z,\ B \neq Z$. Wobec minimalności Z, zbiory A i B są skończonymi sumami mnogościowymi rozmaitości, zatem także Z jest sumą rozmaitości. Przypuszczenie, że istnieją zbiory algebraiczne nie będące sumami rozmaitości prowadzi więc do sprzeczności.

Udowodnimy teraz jednoznaczność przedstawienia. Przypuśćmy, że

$$A = V_1 \cup \cdots \cup V_r = W_1 \cup \cdots \cup W_s$$

są dwoma rozkładami, w których składniki są nieporównywalne. Wtedy

$$W_j = A \cap W_j = V_1 \cap W_j \ \cup \cdots \cup \ V_r \cap W_j$$

jest rozkładem rozmaitości W_j na sumę zbiorów algebraicznych. Zatem dla pewnego i mamy

$$W_j = V_i \cap W_j,$$

skąd wynika, że $W_j \subseteq V_i$. Podobnie otrzymamy, że $V_i \subseteq W_k$ dla pewnego k. Stąd $W_j \subseteq W_k$ i wobec nieporównywalności składników przedstawienia musimy mieć $W_j = V_i = W_k$. Pokazaliśmy więc, że każda rozmaitość W_j jest równa pewnej rozmaitości V_i. W szczególności $s \leqslant r$. Podobnie jednak udowodnimy, że każda rozmaitość V_j jest równa pewnej rozmaitości W_i, skąd $r \leqslant s$. Stąd otrzymujemy, że $r = s$ oraz układ rozmaitości $V_1, \ldots, V_r$ tylko porządkiem może różnić się od układu rozmaitości $W_1, \ldots, W_r$. □

Uwaga 7.3.5. Każda rozmaitość algebraiczna V jest przestrzenią topologiczną z topologią podprzestrzeni przestrzeni topologicznej k^n (z topologią Zariskiego). Zbiorami domkniętymi w V są przekroje zbiorów domkniętych w k^n z rozmaitością V, czyli są to zbiory algebraiczne zawarte w V, natomiast zbiorami otwartymi w V są dopełnienia zbiorów domkniętych, czyli zbiory postaci $V \setminus U$, gdzie U jest zbiorem algebraicznym zawartym w V. W przestrzeni V *każde dwa niepuste zbiory otwarte mają niepusty przekrój.* Rzeczywiście, niech $A, B \subseteq V$ będą niepustymi zbiorami otwartymi w V. Wtedy $A = V \setminus V_1,\ B = V \setminus V_2$, gdzie V_1, V_2 są zbiorami algebraicznymi w V. Ponieważ A i B są niepuste więc $V \neq V_1$ i $V \neq V_2$. Zauważmy trywialną równość

$$V = V_1 \cup V_2 \cup (V \setminus V_1 \cap V \setminus V_2) = V_1 \cup V_2 \cup (A \cap B).$$

Przypuszczenie, że $A \cap B = \varnothing$ prowadzi więc do rozkładu

$$V = V_1 \cup V_2, \quad V \neq V_1,\ V \neq V_2$$

wbrew temu, że V (jako rozmaitość algebraiczna) jest nierozkładalnym zbiorem algebraicznym.
Stąd wynika, że jeśli V jest rozmaitością algebraiczną i ma więcej niż jeden punkt, to V nie jest przestrzenią Hausdorffa (nie spełnia aksjomatu oddzielania $\mathcal{T}_2$ punktów rozłącznymi zbiorami otwartymi).

Uwaga 7.3.6. Niech $\mathsf{Spec}\, k[X_1, \ldots, X_n]$ oznacza zbiór wszystkich ideałów pierwszych pierścienia $k[X_1, \ldots, X_n]$ (jest to tak zwane *spektrum* pierścienia) i niech $\mathsf{Var}\, k^n$ oznacza zbiór wszystkich rozmaitości w przestrzeni k^n. Twierdzenie 7.3.3 pozwala rozpatrywać odwzorowanie

$$\mathcal{I} : \mathsf{Var}\, k^n \longrightarrow \mathsf{Spec}\, k[X_1, \ldots, X_n], \qquad V \mapsto \mathcal{I}(V).$$

Na podstawie (7.6) odwzorowanie to jest injekcją. Zbadajmy zatem kiedy odwzorowanie $\mathcal{I}$ jest surjekcją. Jeśli ideał pierwszy $\mathfrak{p}$ pierścienia $k[X_1, \ldots, X_n]$ jest obrazem rozmaitości V, to znaczy, $\mathfrak{p} = \mathcal{I}(V)$, to także $\mathcal{Z}(\mathfrak{p}) = \mathcal{Z}(\mathcal{I}(V)) = V$, a więc

$$\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}.$$

Na odwrót, jeśli $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}$, to zbiór algebraiczny $\mathcal{Z}(\mathfrak{p})$ jest rozmaitością (na podstawie definicji) i ideał pierwszy $\mathfrak{p}$ jest obrazem rozmaitości $\mathcal{Z}(\mathfrak{p})$.
A więc odwzorowanie $\mathcal{I} : \mathsf{Var}\, k^n \longrightarrow \mathsf{Spec}\, k[X_1, \ldots, X_n]$ jest bijekcją wtedy i tylko wtedy, gdy dla każdego ideału pierwszego $\mathfrak{p}$ pierścienia $k[X_1, \ldots, X_n]$ mamy $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}$. Jak dotąd, na podstawie (7.3) wiemy tylko, że zawsze $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) \supseteq \mathfrak{p}$ oraz w stwierdzeniu 7.1.5 udowodniliśmy równość $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}$ w przypadku, gdy $\mathcal{Z}(\mathfrak{p})$ jest krzywą z nieskończenie wieloma punktami. W rozdziale 7.4 udowodnimy twierdzenie Hilberta o zerach, z którego wynika, że jeśli k jest ciałem algebraicznie domkniętym, to $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathfrak{p}$ dla każdego ideału pierwszego pierścienia $k[X_1, \ldots, X_n]$. A więc nad ciałem algebraicznie domkniętym k odwzorowanie $\mathcal{I}$ jest bijekcją. Ten fakt stanowi podstawę do interpretowania problemów geometrycznych (dotyczących rozmaitości) w języku algebraicznym (ideałów pierwszych pierścienia wielomianów).

7.4 Twierdzenie Hilberta o zerach

W przykładzie 7.1.2 zauważyliśmy, że dla dowolnego ideału $\mathfrak{a}$ pierścienia wielomianów $k[X_1, \ldots, X_n]$ mamy $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathfrak{a}$. W tym rozdziale ustalimy precyzyjnie związek pomiędzy ideałami $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ oraz $\mathfrak{a}$ w przypadku gdy k jest ciałem algebraicznie domkniętym.

Przykład 7.4.1. Pokażemy najpierw, że na ogół $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \neq \mathfrak{a}$.
Niech $\mathfrak{a} = (X, Y^2)$ będzie ideałem pierścienia $\mathbb{C}[X, Y]$. Wtedy zbiór algebraiczny ideału $\mathfrak{a}$ w przestrzeni $\mathbb{C}^n$ jest jednopunktowy: $\mathcal{Z}(\mathfrak{a}) = \{(0, 0)\}$. Rozpatrzmy wielomian $g = X + Y$. Ponieważ $g(0, 0) = 0$, więc $g \in \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$. Natomiast $g \notin \mathfrak{a}$. Gdyby bowiem $g \in \mathfrak{a}$, to wobec $X \in \mathfrak{a}$ mielibyśmy także $Y = g - X \in \mathfrak{a}$, a to jest niemożliwe

(przedstawienie $Y = Xh_1 + Y^2h_2$ prowadzi do sprzeczności po podstawieniu $X = 0$). A więc $g \in \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ oraz $g \notin \mathfrak{a}$. Z drugiej strony jednak zauważmy, że

$$g^2 = X(X + 2Y) + Y^2 \in \mathfrak{a},$$

co oznacza, że $g \in \mathsf{rad}\,\mathfrak{a}$.

Przykład 7.4.2. Punktem wyjścia do ustalenia związku między ideałami $\mathfrak{a}$ oraz $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ jest następująca uwaga. Dla każdego ideału $\mathfrak{a}$ pierścienia $k[X_1, \ldots, X_n]$,

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathsf{rad}\,\mathfrak{a} \supseteq \mathfrak{a},$$

gdzie $\mathsf{rad}\,\mathfrak{a} = \{f \in k[X_1, \ldots, X_n] : \exists\ n \in \mathbb{N} \quad f^n \in \mathfrak{a}\}$ jest *radykałem* ideału $\mathfrak{a}$ rozważanym już w rozdziale 6.2.1.
Jeśli bowiem $f \in \mathsf{rad}\,\mathfrak{a}$, to $f^n \in \mathfrak{a}$ dla pewnej liczby naturalnej n. Wtedy $f^n(x) = 0$ dla każdego punktu $x \in \mathcal{Z}(\mathfrak{a})$ i wobec tego także $f(x) = 0$ dla każdego $x \in \mathcal{Z}(\mathfrak{a})$. Zatem $f \in \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$.

Twierdzenie Hilberta o zerach (w jednej z jego wersji) udziela wyczerpującej odpowiedzi na pytanie, jaki jest dokładny związek pomiędzy ideałem $\mathfrak{a}$ i ideałem $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$. Okazuje się, że jeśli k jest ciałem algebraicznie domkniętym, to

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathsf{rad}\,\mathfrak{a}.$$

Twierdzenie Hilberta o zerach (znane jako *Nullstellensatz*), jest jednym z kluczowych punktów podstaw geometrii algebraicznej. Spośród różnych znanych dowodów tego twierdzenia zaprezentujemy dowód podany przez O. Zariskiego.[1] Wykorzystuje on następujący lemat z teorii ciał.

LEMAT **7.4.1.** *Niech K będzie podciałem pierścienia przemiennego A i niech*

$$L = K[x_1, \ldots, x_n]$$

będzie podpierścieniem pierścienia A generowanym przez K oraz elementy $x_1, \ldots, x_n$ pierścienia A. Jeśli pierścień L jest ciałem, to L jest skończonym rozszerzeniem ciała K (w szczególności więc, wszystkie elementy $x_1, \ldots, x_n$ są algebraiczne nad ciałem K).

Dowód. Przeprowadzimy dowód indukcyjny ze względu na n. Gdy $L = K[x_1]$ jest ciałem, to można założyć, że $x_1 \neq 0$, i wobec tego także $1/x_1 \in L$. Istnieje zatem niezerowy wielomian $g \in K[X]$ taki, że $1/x_1 = g(x_1)$. Wtedy mamy $x_1 g(x_1) - 1 = 0$, czyli element x_1 jest algebraiczny nad K jako zero wielomianu $Xg(X) - 1$. Zatem $L = K[x_1]$ jest skończonym rozszerzeniem K.

Niech teraz $n > 1$ i niech $L = K[x_1, \ldots, x_n]$ będzie ciałem. Zatem L zawiera ciało $K(x_1)$ i wobec tego

$$L = K(x_1)[x_2, \ldots, x_n].$$

Z założenia indukcyjnego otrzymujemy, że $x_2, \ldots, x_n$ są elementami algebraicznymi nad $K(x_1)$. Pozostaje więc udowodnić, że x_1 jest elementem algebraicznym nad K.

[1] Oscar Zariski, 1899–1986.

Przypuśćmy, że x_1 jest elementem przestępnym nad K. Ciało $K(x_1)$ możemy więc traktować jako ciało funkcji wymiernych jednej zmiennej nad K, czyli jako ciało ułamków pierścienia wielomianów $K[x_1]$. Stąd, że elementy $x_2, \ldots, x_n$ są algebraiczne nad $K(x_1)$ wynika, że istnieją wielomiany $a_2(x_1), \ldots, a_n(x_1) \in K[x_1]$ takie, że elementy $a_2(x_1)x_2, \ldots, a_n(x_1)x_n$ są całkowite nad $K[x_1]$.

Jest to konsekwencją następującej elementarnej uwagi (wykorzystanej już w dowodzie lematu 6.4.1). Jeśli element x_i jest pierwiastkiem wielomianu niezerowego $f = c_0 + c_1X + \cdots + c_{m-1}X^{m-1} + a_iX^m$ o współczynnikach z pierścienia $K[x_1]$, to a_ix_i jest pierwiastkiem wielomianu

$$c_0a_i^{m-1} + c_1a_i^{m-2}X + \cdots + c_{m-1}X^{m-1} + X^m$$

o współczynnikach z pierścienia $K[x_1]$ i najwyższym współczynniku 1. A więc a_ix_i jest całkowity nad $K[x_1]$.

Skoro $a_2(x_1)x_2, \ldots, a_n(x_1)x_n$ są całkowite nad $K[x_1]$, to także dla $a(x_1) := a_2(x_1)\cdots a_n(x_1)$ elementy $a(x_1)x_i$ są całkowite nad $K[x_1]$, $i = 2, \ldots, n$. W takim razie, dla dowolnego $\alpha = f(x_1, \ldots, x_n) \in L = K[x_1, \ldots, x_n]$, gdzie f jest wielomianem o współczynnikach z K, mnożąc α przez $a(x_1)^s$ gdzie s jest dostatecznie dużą liczbą naturalną, będziemy mogli napisać

$$a(x_1)^s\alpha = a(x_1)^s f(x_1, \ldots, x_n) = g(x_1, a(x_1)x_2, \ldots, a(x_1)x_n),$$

gdzie g jest pewnym wielomianem o współczynnikach z K. Wobec tego, dla każdego $\alpha \in L$ istnieje liczba naturalna s taka, że $a(x_1)^s\alpha$ jest elementem całkowitym nad $K[x_1]$. W szczególności, dla każdego elementu $\alpha \in K(x_1) \subset L$ istnieje liczba naturalna s taka, że $a(x_1)^s\alpha$ jest elementem całkowitym nad $K[x_1]$. Ale pierścień $K[x_1]$ jest pierścieniem ideałów głównych (jako pierścień izomorficzny z pierścieniem wielomianów jednej zmiennej nad ciałem), zatem jest całkowicie domknięty. Oznacza to że $a(x_1)^s\alpha = h(x_1) \in K[x_1]$. Otrzymaliśmy więc paradoksalny rezultat stwierdzający, że istnieje taki wielomian $a(x_1) \in K[x_1]$, że każda funkcja wymierna $\alpha \in K(x_1)$ ma przedstawienie

$$\alpha = \frac{h(x_1)}{a(x_1)^s},$$

gdzie h jest wielomianem i s jest liczbą naturalną. Jest to oczywiście niemożliwe, gdyż na przykład funkcja wymierna $1/(1 + a(x_1))$ nie ma takiego przedstawienia. Ta sprzeczność pokazuje, iż przypuszczenie że x_1 jest elementem przestępnym nad K prowadzi do sprzeczności. □

Twierdzenie **7.4.2.** (Pierwsza wersja twierdzenia Hilberta o zerach.)
Niech k będzie ciałem algebraicznie domkniętym i niech $\mathfrak{a}$ będzie dowolnym ideałem właściwym pierścienia $k[X_1, \ldots, X_n]$ (to znaczy $\mathfrak{a} \neq (1)$). Wtedy zbiór algebraiczny $\mathcal{Z}(\mathfrak{a}) \subset k^n$ ideału $\mathfrak{a}$ jest niepusty.

Dowód. Niech $\mathfrak{a}$ będzie ideałem w $k[X_1, \ldots, X_n]$ oraz $\mathfrak{a} \neq (1)$. Wtedy (na podstawie twierdzenia 2.3.5) ideał $\mathfrak{a}$ zawiera się w pewnym ideale maksymalnym $\mathfrak{m}$ pierścienia $k[X_1, \ldots, X_n]$. Inkluzja $\mathfrak{a} \subseteq \mathfrak{m}$ pociąga $\mathcal{Z}(\mathfrak{m}) \subseteq \mathcal{Z}(\mathfrak{a})$ (na podstawie przykładu 7.1.2), wystarczy więc udowodnić, że $\mathcal{Z}(\mathfrak{m})$ jest zbiorem niepustym dla każdego ideału maksymalnego $\mathfrak{m}$ pierścienia $k[X_1, \ldots, X_n]$.

Niech więc $\mathfrak{m}$ będzie ideałem maksymalnym pierścienia $k[X_1, \ldots, X_n]$. Wtedy pierścień ilorazowy $L := k[X_1, \ldots, X_n]/\mathfrak{m}$ jest ciałem. Ponadto, L jest homomorficznym obrazem pierścienia $k[X_1, \ldots, X_n]$ przez homomorfizm kanoniczny

$$\kappa : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/\mathfrak{m} = L.$$

Wynika stąd przede wszystkim, że obraz $\kappa(k)$ ciała k w L jest podciałem ciała L izomorficznym z ciałem k. W dalszym ciągu dla $a \in k$ będziemy utożsamiać obraz $\kappa(a) = a + \mathfrak{m} \in L$ z elementem $a \in k$.
Z drugiej strony, pierścień L jest homomorficznym obrazem pierścienia wielomianów $k[X_1, \ldots, X_n]$. Homomorfizm kanoniczny κ przeprowadza generatory X_i pierścienia $k[X_1, \ldots, X_n]$ na generatory x_i pierścienia L, zatem

$$L = k[x_1, \ldots, x_n], \quad \text{gdzie} \quad x_i = \kappa(X_i) = X_i + \mathfrak{m},\ i = 1, \ldots, n.$$

Ponieważ L jest ciałem, więc na podstawie Lematu 7.4.1, L jest skończonym rozszerzeniem ciała k. Ale ciało k jest algebraicznie domknięte, zatem nie ma właściwych rozszerzeń skończonych (ani algebraicznych), a więc $k = L$.
Można wobec tego zakładać, że $x_1, \ldots, x_n \in k$. Pokażemy teraz, że każdy wielomian $f \in \mathfrak{m}$ zeruje się w punkcie $x = (x_1, \ldots, x_n)$.
Wobec $x_i = \kappa(X_i)$ mamy

$$f(x) = f(\kappa(X_1), \ldots, \kappa(X_n)) = \kappa(f(X_1, \ldots, X_n)) = f + \mathfrak{m} = \mathfrak{m}.$$

Zatem $f(x) = 0 \in L$ i wobec tego $x = (x_1, \ldots, x_n) \in k^n$ jest wspólnym zerem wszystkich wielomianów w ideale $\mathfrak{m}$. Oznacza to, że $\mathcal{Z}(\mathfrak{m}) \neq \varnothing$. □

Wniosek **7.4.3.** *Jeśli $\mathfrak{a} = (f_1, \ldots, f_r)$ jest ideałem pierścienia $k[X_1, \ldots, X_n]$, to $\mathcal{Z}(\mathfrak{a}) = \varnothing$ wtedy i tylko wtedy, gdy istnieją wielomiany $h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$ takie, że*

$$f_1 h_1 + \cdots + f_r h_r = 1. \tag{7.11}$$

Dowód. Jeśli spełniony jest warunek (7.11), to $\mathfrak{a}$ jest ideałem jednostkowym i wobec tego oczywiście $\mathcal{Z}(\mathfrak{a}) = \varnothing$ (zobacz przykład 7.1.1). Jeśli natomiast warunek (7.11) nie jest spełniony, to $\mathfrak{a}$ nie jest ideałem jednostkowym i na podstawie twierdzenia 7.4.2 mamy $\mathcal{Z}(\mathfrak{a}) \neq \varnothing$. □

Uwaga 7.4.4. Istnienie tożsamości (7.11) jest dla wielomianów $n \geqslant 2$ zmiennych warunkiem silniejszym niż fakt, że $\mathrm{NWD}(f_1, \ldots, f_r) = 1$. Jeśli bowiem zachodzi tożsamość (7.11), to oczywiście wielomiany $f_1, \ldots, f_r$ nie mogą mieć wspólnego dzielnika nie będącego stałą, są więc względnie pierwsze. Natomiast jeśli wielomiany $f_1, \ldots, f_r$ są względnie pierwsze, to wielomiany te mogą mieć wspólne zero i wobec tego, na podstawie wniosku 7.4.3, nie istnieje dla nich tożsamość (7.11). Na przykład, wielomiany $f_1(X, Y) = X$, $f_2(X, Y) = Y$ mają wspólne zero $(0, 0)$ i są względnie pierwsze.

Twierdzenie **7.4.5.** (Druga wersja twierdzenia Hilberta o zerach.)
Niech k będzie ciałem algebraicznie domkniętym.

Jeśli wielomian $f \in k[X_1, \ldots, X_n]$ zeruje się w każdym wspólnym zerze wielomianów $f_1, \ldots, f_r \in k[X_1, \ldots, X_n]$, to istnieje liczba naturalna $m \geqslant 1$ oraz wielomiany $h_1, \ldots, h_r \in k[X_1, \ldots, X_n]$ takie, że

$$f^m = f_1 h_1 + \cdots + f_r h_r.$$

Inaczej mówiąc, jeśli $\mathfrak{a} = (f_1, \ldots, f_r)$ oraz $f \in \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$, to $f \in \operatorname{rad} \mathfrak{a}$.

Dowód. Dla wielomianu zerowego $f = 0$ twierdzenie jest oczywiście prawdziwe. Zakładamy więc, że $f \neq 0$. Rozpatrujemy pierścień wielomianów $n+1$ zmiennych $k[X_1, \ldots, X_n, Z]$ i w nim wielomiany

$$f_1, \ldots, f_r,\ g := 1 - Zf.$$

Wielomiany te nie mają wspólnego zera w k^{n+1}, gdyż każde wspólne zero wielomianów $f_1, \ldots, f_r$ w k^{n+1} jest także zerem wielomianu f i wobec tego wielomian g przyjmuje w takim punkcie wartość 1.
Na podstawie wniosku 7.4.3 (z pierwszej wersji twierdzenia Hilberta o zerach) istnieją więc wielomiany $g_1, \ldots, g_r, h \in k[X_1, \ldots, X_n, Z]$ takie, że

$$f_1 g_1 + \cdots + f_r g_r + (1 - Zf)h = 1.$$

Możemy tę tożsamość wielomianową traktować także jako tożsamość w ciele funkcji wymiernych $k(X_1, \ldots, X_n, Z)$. Podstawiamy teraz wszędzie w miejsce zmiennej Z funkcję wymierną $1/f$. W rezultacie otrzymujemy tożsamość w ciele funkcji wymiernych $k(X_1, \ldots, X_n)$ postaci

$$f_1 \overline{g_1} + \cdots + f_r \overline{g_r} = 1,$$

gdzie funkcje wymierne $\overline{g_1}, \ldots, \overline{g_r}$ mają mianowniki będące potęgami wielomianu f. Mnożąc obydwie strony tej tożsamości przez odpowiednio dobraną potęgę f^m wielomianu f otrzymamy tożsamość wielomianową postaci

$$f_1 h_1 + \cdots + f_r h_r = f^m,$$

gdzie $h_i = \overline{g_i} f^m \in k[X_1, \ldots, X_n]$. □

Powyższy dowód sugeruje metodę wyznaczania radykału dowolnego ideału $\mathfrak{a}$ pierścienia wielomianów $k[X_1, \ldots, X_n]$.

Wniosek **7.4.6.** *Niech $\mathfrak{a}$ będzie ideałem w $k[X_1, \ldots, X_n]$. Wielomian f należy do radykału $\operatorname{rad} \mathfrak{a}$ ideału $\mathfrak{a}$ wtedy i tylko wtedy gdy*

$$1 \in (\mathfrak{a}, 1 - Zf),$$

gdzie $(\mathfrak{a}, 1 - Zf)$ jest ideałem w $k[X_1, \ldots, X_n, Z]$ generowanym przez $\mathfrak{a}$ i wielomian $1 - Zf$.

Dowód. Niech $\mathfrak{a} = (f_1, \ldots, f_r)$. Jeśli $1 \in (\mathfrak{a}, 1 - Zf)$, to w dowodzie twierdzenia 7.4.5 pokazaliśmy, że istnieje liczba naturalna m taka, że $f^m \in \mathfrak{a}$, a więc $f \in \operatorname{rad} \mathfrak{a}$. Jeśli natomiast $f \in \operatorname{rad} \mathfrak{a}$ oraz $f^m \in \mathfrak{a}$, to z tożsamości

$$\begin{aligned} 1 &= Z^m f^m + (1 - Z^m f^m) \\ &= Z^m f^m + (1 - Zf) \cdot (1 + Zf + \cdots + Z^{m-1} f^{m-1}) \end{aligned}$$

wynika, że $1 \in (\mathfrak{a}, 1 - Zf)$. □

WNIOSEK **7.4.7.** (Twierdzenie Hilberta o zerach.)
Niech k będzie ciałem algebraicznie domkniętym. Dla każdego ideału $\mathfrak{a}$ pierścienia $k[X_1, \ldots, X_n]$ zachodzi równość

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathsf{rad}\,\mathfrak{a}.$$

Dowód. Zgodnie z twierdzeniem 7.4.5 mamy $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \subseteq \mathsf{rad}\,\mathfrak{a}$, natomiast przeciwną inkluzję zauważyliśmy już w przykładzie 7.4.2. □

7.5 Zastosowania twierdzenia Hilberta o zerach

Jako przykłady zastosowań twierdzenia Hilberta o zerach wyznaczymy wszystkie ideały maksymalne pierścienia wielomianów $k[X_1, \ldots, X_n]$, gdy k jest ciałem algebraicznie domkniętym, oraz wyjaśnimy ostatecznie związek między rozmaitościami algebraicznymi i ideałami pierwszymi pierścienia wielomianów. Ponadto, przedstawimy podstawowe własności tak zwanych ideałów radykalnych. Najpierw jednak pokażemy, że studiowany w poprzednim rozdziale rozkład prymarny ideałów w pierścieniach noetherowskich ma ważny sens geometryczny.

7.5.1 Rozkład prymarny ideałów i rozkład zbioru algebraicznego na sumę rozmaitości

Niech $\mathfrak{a}$ będzie ideałem właściwym w pierścieniu wielomianów $k[X_1, \ldots, X_n]$ nad ciałem algebraicznie domkniętym k. Na podstawie twierdzenia 6.2.12 istnieje przedstawienie ideału $\mathfrak{a}$ w postaci

$$\mathfrak{a} = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$$

gdzie $\mathfrak{q}_i$ są ideałami prymarnymi z różnym radykałami $\mathfrak{p}_i = \mathsf{rad}\,\mathfrak{q}_i$. Z tego przedstawienia ideału $\mathfrak{a}$ otrzymujemy na podstawie uwagi 7.2.2 następujące przedstawienie zbioru algebraicznego $\mathcal{Z}(\mathfrak{a})$:

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathfrak{q}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{q}_m).$$

Tutaj zbiory algebraiczne $\mathcal{Z}(\mathfrak{q}_i)$ są rozmaitościami, gdyż stowarzyszone z nimi ideały

$$\mathcal{I}\mathcal{Z}(\mathfrak{q}_i) = \mathsf{rad}\,\mathfrak{q}_i = \mathfrak{p}_i$$

są ideałami pierwszymi. Zauważmy, że wykorzystaliśmy tutaj twierdzenie Hilberta o zerach (i założenie, że k jest ciałem algebraicznie domkniętym).

A więc twierdzenie o rozkładzie prymarnym ideałów $\mathfrak{a}$ pierścienia $k[X_1, \ldots, X_n]$ ma geometryczną interpretację. Prowadzi ono natychmiast do rozkładu zbioru algebraicznego $\mathcal{Z}(\mathfrak{a})$ na sumę mnogościową rozmaitości algebraicznych.

7.5.2 Ideały maksymalne pierścienia wielomianów

Wyznaczenie wszystkich ideałów maksymalnych pierścienia $k[X_1, \ldots, X_n]$ rozpoczniemy od następującego lematu.

LEMAT **7.5.1.** *Niech $f \in A[X_1, \ldots, X_n]$ będzie wielomianem n zmiennych o współczynnikach w pierścieniu przemiennym A.*
Jeśli dla pewnych $a_1, \ldots, a_n \in A$ mamy $f(a_1, \ldots, a_n) = 0$, to istnieją wielomiany $g_1, \ldots, g_n \in A[X_1, \ldots, X_n]$ takie, że

$$f = (X_1 - a_1)g_1 + \cdots + (X_n - a_n)g_n.$$

Dowód. Gdy $n = 1$, to korzystając z tożsamości

$$X^m - a^m = (X - a)(X^{m-1} + aX^{m-2} + \cdots + a^{m-2}X + a^{m-1})$$

oraz z równości $f(a_1) = 0$ otrzymamy $f(X) = f(X) - f(a_1) = (X - a_1)g(X)$ dla odpowiednio dobranego wielomianu g. Zatem lemat jest prawdziwy dla $n = 1$.
Załóżmy teraz, że $n > 1$ i lemat jest prawdziwy dla wielomianów $n - 1$ zmiennych nad dowolnym pierścieniem przemiennym A. Jeśli $f \in A[X_1, \ldots, X_n]$ oraz $f(a_1, \ldots, a_n) = 0$ dla pewnych $a_1, \ldots, a_n \in A$, to rozważamy wielomian

$$g = g(X_1, \ldots, X_{n-1}) = f(X_1, \ldots, X_{n-1}, a_n) \in A[X_1, \ldots, X_{n-1}].$$

Wtedy $g(a_1, \ldots, a_{n-1}) = f(a_1, \ldots, a_n) = 0$, a więc na podstawie założenia indukcyjnego istnieją wielomiany $g_1, \ldots, g_{n-1} \in A[X_1, \ldots, X_{n-1}]$ takie, że

$$g = (X_1 - a_1)g_1 + \cdots + (X_{n-1} - a_{n-1})g_{n-1}.$$

Ponadto,

$$\begin{aligned} f &= f(X_1, \ldots, X_n) - f(X_1, \ldots, X_{n-1}, a_n) + f(X_1, \ldots, X_{n-1}, a_n) \\ &= (X_n - a_n)f_1(X_1, \ldots, X_n) + (X_1 - a_1)g_1 + \cdots + (X_{n-1} - a_{n-1})g_{n-1}, \end{aligned}$$

gdzie pierwszy składnik otrzymaliśmy traktując wielomian

$$f(X_1, \ldots, X_n) - f(X_1, \ldots, X_{n-1}, a_n)$$

jako wielomian jednej zmiennej X_n nad pierścieniem wielomianów $A[X_1, \ldots, X_{n-1}]$, który w punkcie $a_n \in A$ przyjmuje wartość zero. Wykorzystaliśmy więc zarówno sprawdzony już rezultat dla $n = 1$ jak i założenie indukcyjne. Wielomian f ma więc wymagane przedstawienie. □

TWIERDZENIE **7.5.2.** *Niech k będzie ciałem algebraicznie domkniętym i niech $\mathfrak{m}$ będzie ideałem pierścienia wielomianów $k[X_1, \ldots, X_n]$. Ideał $\mathfrak{m}$ jest maksymalny wtedy i tylko wtedy, gdy istnieją $a_1, \ldots, a_n \in k$ takie, że*

$$\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n).$$

Dowód. Najpierw pokażemy, że każdy ideał postaci $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ jest maksymalny. Rozważmy odwzorowanie

$$\varphi : k[X_1, \ldots, X_n] \to k, \quad \varphi(f) = f(a_1, \ldots, a_n).$$

φ jest surjektywnym homomorfizmem pierścienia $k[X_1, \ldots, X_n]$ na ciało k i wobec tego $\ker \varphi$ jest ideałem maksymalnym w $k[X_1, \ldots, X_n]$. Pokażemy, że $\ker \varphi = \mathfrak{m}$.

Jeśli $f \in \mathfrak{m}$, to mamy oczywiście $f(a_1, \ldots, a_n) = 0$, zatem $f \in \ker \varphi$. Jeśli natomiast $f \in \ker \varphi$, to na podstawie lematu 7.5.1 mamy $f \in \mathfrak{m}$. A więc $\mathfrak{m} = \ker \varphi$ jest ideałem maksymalnym.
Udowodnimy teraz, że każdy ideał maksymalny w $k[X_1, \ldots, X_n]$ jest generowany przez odpowiednio dobrane wielomiany liniowe $X_1 - a_1, \ldots, X_n - a_n$.
Załóżmy, że $\mathfrak{m}$ jest ideałem maksymalnym w $k[X_1, \ldots, X_n]$. Wtedy na podstawie twierdzenia Hilberta o zerach (twierdzenie 7.4.2) zbiór algebraiczny $\mathcal{Z}(\mathfrak{m})$ ideału $\mathfrak{m}$ jest niepusty. Załóżmy, że $a = (a_1, \ldots, a_n) \in k^n$ leży w $\mathcal{Z}(\mathfrak{m})$. Rozważmy ideał

$$\mathfrak{a} = (X_1 - a_1, \ldots, X_n - a_n)$$

pierścienia $k[X_1, \ldots, X_n]$. Na podstawie już udowodnionej części twierdzenia, $\mathfrak{a}$ jest ideałem maksymalnym w $k[X_1, \ldots, X_n]$. Udowodnimy, że $\mathfrak{m} = \mathfrak{a}$. Przede wszystkim zauważmy, że

$$\mathcal{Z}(\mathfrak{a}) = \{a\} \subseteq \mathcal{Z}(\mathfrak{m}).$$

Wobec tego, na podstawie własności (7.5) oraz (7.3) mamy

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathcal{I}(\mathcal{Z}(\mathfrak{m})) \supseteq \mathfrak{m}.$$

Zauważmy, że $\mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ jest ideałem właściwym w $k[X_1, \ldots, X_n]$ gdyż w przeciwnym razie mamy

$$a \in \mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(\mathfrak{a}))) = \mathcal{Z}(1) = \varnothing,$$

sprzeczność. Z maksymalności ideału $\mathfrak{m}$ wynika więc, że

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(\mathcal{Z}(\mathfrak{m})) = \mathfrak{m}.$$

Z drugiej strony, $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathfrak{a}$ (na podstawie (7.3)), wobec tego $\mathfrak{m} \supseteq \mathfrak{a}$. Ponieważ $\mathfrak{a}$ jest ideałem maksymalnym, wynika stąd, że $\mathfrak{m} = \mathfrak{a}$. □

Wniosek **7.5.3.** *Niech k będzie ciałem algebraicznie domkniętym.*
(a) *Jeśli $\mathfrak{m}$ jest ideałem maksymalnym pierścienia $k[X_1, \ldots, X_n]$, to jego zbiór algebraiczny $\mathcal{Z}(\mathfrak{m})$ jest jednopunktowy.*
(b) *Dla każdego punktu $a \in k^n$ ideał $\mathcal{I}(a)$ jest ideałem maksymalnym pierścienia $k[X_1, \ldots, X_n]$.*

Dowód. Pierwsza część wynika bezpośrednio z twierdzenia 7.5.2.
Dla dowodu drugiej części weźmy $a = (a_1, \ldots, a_n) \in k^n$ i rozważmy ideał

$$(X_1 - a_1, \ldots, X_n - a_n) =: \mathfrak{m}$$

pierścienia $k[X_1, \ldots, X_n]$. Wiemy, że $\mathfrak{m}$ jest ideałem maksymalnym. Jeśli wielomian $f \in \mathfrak{m}$ to także $f \in \mathcal{I}(a)$, czyli $\mathfrak{m} \subseteq \mathcal{I}(a)$. Stąd wobec maksymalności ideału $\mathfrak{m}$ wynika, że $\mathfrak{m} = \mathcal{I}(a)$. Zatem $\mathcal{I}(a)$ jest maksymalny. □

Uwaga 7.5.4. Jeśli zbiór $\mathcal{Z}(\mathfrak{m})$ jest jednopunktowy, to $\mathfrak{m}$ nie musi być ideałem maksymalnym w $k[X_1, \ldots, X_n]$. Na przykład, ideał $\mathfrak{m} = (X_1^2, X_2, \ldots, X_n)$ pierścienia $k[X_1, \ldots, X_n]$ ma jednopunktowy zbiór algebraiczny, ale nie jest ideałem maksymalnym w $k[X_1, \ldots, X_n]$.

TWIERDZENIE **7.5.5.** *Niech k będzie ciałem algebraicznie domkniętym. Przyporządkowanie*

$$\mathcal{I} : \mathsf{Var}\, k^n \longrightarrow \mathsf{Spec}\, k[X_1, \ldots, X_n], \qquad V \mapsto \mathcal{I}(V).$$

jest wzajemnie jednoznacznym odwzorowaniem pomiędzy zbiorem wszystkich rozmaitości algebraicznych $V \subseteq k^n$ i zbiorem wszystkich ideałów pierwszych pierścienia $k[X_1, \ldots, X_n]$. W tym odwzorowaniu zbiorom jednopunktowym odpowiadają ideały maksymalne pierścienia $k[X_1, \ldots, X_n]$. Odwzorowaniem odwrotnym do $\mathcal{I}$ jest

$$\mathcal{Z} : \mathsf{Spec}\, k[X_1, \ldots, X_n] \longrightarrow \mathsf{Var}\, k^n, \qquad \mathfrak{p} \mapsto \mathcal{Z}(\mathfrak{p}).$$

Dowód. Na podstawie przykładu 7.1.2 dla każdej rozmaitości algebraicznej V w k^n mamy $\mathcal{Z}(\mathcal{I}(V)) = V$ oraz na podstawie wniosku 7.4.7 dla każdego ideału pierwszego $\mathfrak{p}$ pierścienia $k[X_1, \ldots, X_n]$ mamy $\mathcal{I}(\mathcal{Z}(\mathfrak{p})) = \mathsf{rad}\,\mathfrak{p} = \mathfrak{p}$. Stąd wynika, że rozpatrywane odwzorowania są bijekcjami, których złożenia są odwzorowaniami identycznościowymi. Ponadto, na podstawie wniosku 7.5.3 zbiorowi jednopunktowemu $\{a\}$ odpowiada ideał maksymalny $\mathcal{I}(a)$ pierścienia $k[X_1, \ldots, X_n]$. □

7.5.3 Ideały radykalne

DEFINICJA **7.5.6.** Ideał $\mathfrak{a}$ pierścienia A nazywa się ideałem *radykalnym*, jeśli

$$\mathfrak{a} = \mathsf{rad}\,\mathfrak{a}.$$

Ponieważ $\mathfrak{a} \subseteq \mathsf{rad}\,\mathfrak{a}$ dla każdego ideału $\mathfrak{a}$ oraz $\mathsf{rad}(\mathfrak{a}) = (1) \Leftrightarrow \mathfrak{a} = (1)$ (na podstawie (6.14)), więc jest rzeczą oczywistą, że każdy ideał maksymalny $\mathfrak{a}$ pierścienia A jest ideałem radykalnym. Z przykładu 6.2.6 wynika także, że każdy ideał pierwszy $\mathfrak{p}$ pierścienia A jest ideałem radykalnym. Te i inne przykłady ideałów radykalnych można otrzymać przy pomocy następującej charakteryzacji ideałów radykalnych.

LEMAT **7.5.7.** *Ideał $\mathfrak{a}$ pierścienia A jest radykalny wtedy i tylko wtedy, gdy pierścień ilorazowy $A/\mathfrak{a}$ nie ma niezerowych elementów nilpotentnych.*

Dowód. Niech $\kappa : A \to A/\mathfrak{a}$ będzie homomorfizmem kanonicznym. Wtedy

$$\mathsf{rad}\,\mathfrak{a} = \kappa^{-1}(\mathsf{Nil}\, A/\mathfrak{a}),$$

gdzie $\mathsf{Nil}\, A/\mathfrak{a}$ oznacza nilradykał pierścienia $A/\mathfrak{a}$, czyli zbiór (ideał) wszystkich elementów nilpotentnych tego pierścienia. Rzeczywiście, dla $x \in A$ mamy

$$\begin{aligned} x \in \mathsf{rad}\,\mathfrak{a} &\iff x^n \in \mathfrak{a} \quad \text{dla pewnego} \quad n \in \mathbb{N} \\ &\iff x + \mathfrak{a} \in \mathsf{Nil}\, A/\mathfrak{a} \\ &\iff x \in \kappa^{-1}(\mathsf{Nil}\, A/\mathfrak{a}). \end{aligned}$$

Stąd otrzymujemy

$$\mathfrak{a} = \mathsf{rad}\,\mathfrak{a} \iff \mathfrak{a} = \kappa^{-1}(\mathsf{Nil}\, A/\mathfrak{a}) \iff \mathsf{Nil}\, A/\mathfrak{a} = \mathfrak{a}.$$

Oznacza to, że ideał $\mathfrak{a}$ jest radykalny wtedy i tylko wtedy gdy jedynym elementem nilpotentnym w $A/\mathfrak{a}$ jest zero tego pierścienia $\mathfrak{a} = 0 \in A/\mathfrak{a}$. □

Przykład 7.5.1. W pierścieniu wielomianów $k[X_1, \ldots, X_n]$ ideał główny (f) jest radykalny wtedy i tylko wtedy, gdy wielomian f w swoim rozkładzie na czynniki nierozkładalne nie ma czynników wielokrotnych (czyli gdy f jest wielomianem *bezkwadratowym*). Jeśli bowiem f jest bezkwadratowy, to potęga wielomianu g należy do ideału (f) tylko wtedy gdy $g \in (f)$ i wobec tego $\mathsf{rad}(f) = (f)$. Z drugiej strony, jeśli wielomian f ma w rozkładzie na czynniki nierozkładalne czynnik wielokrotny, $f = f_1^{\ell_1} \cdots f_r^{\ell_r}$, gdzie f_i są parami różne i nierozkładalne oraz $\ell = \max\{\ell_1, \ldots, \ell_r\} > 1$, to mamy $(f_1 \cdots f_r)^\ell \in (f)$, podczas gdy $f_1 \cdots f_r \notin (f)$. Wobec tego (f) nie jest ideałem radykalnym.

Wykorzystując twierdzenie Hilberta o zerach wyznaczymy wszystkie ideały radykalne pierścienia wielomianów nad ciałem algebraicznie domkniętym.

TWIERDZENIE **7.5.8.** *Niech k będzie ciałem algebraicznie domkniętym i niech $\mathfrak{a}$ będzie ideałem pierścienia $k[X_1, \ldots, X_n]$.*
Ideał $\mathfrak{a}$ jest radykalny wtedy i tylko wtedy, gdy istnieje zbiór algebraiczny $V \subseteq k^n$ taki, że $\mathfrak{a}$ jest ideałem stowarzyszonym ze zbiorem algebraicznym V :

$$\mathfrak{a} = \mathcal{I}(V).$$

Dowód. Jeśli $\mathfrak{a}$ jest radykalny, to $\mathsf{rad}\,\mathfrak{a} = \mathfrak{a}$ i wobec tego na podstawie twierdzenia Hilberta o zerach (wniosek 7.4.7) mamy $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathsf{rad}\,\mathfrak{a} = \mathfrak{a}$. Zatem $\mathfrak{a} = \mathcal{I}(V)$, gdzie $V = \mathcal{Z}(\mathfrak{a})$.

Z drugiej strony, jeśli $\mathfrak{a} = \mathcal{I}(V)$, to $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathcal{I}(V)) = V$, skąd na podstawie twierdzenia Hilberta o zerach otrzymujemy

$$\mathsf{rad}\,\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(V) = \mathfrak{a}.$$

A więc $\mathfrak{a}$ jest ideałem radykalnym. □

TWIERDZENIE **7.5.9.** *Niech k będzie ciałem algebraicznie domkniętym i niech $\mathfrak{a}$ będzie ideałem radykalnym pierścienia $k[X_1, \ldots, X_n]$. Wtedy ideał $\mathfrak{a}$ ma jednoznaczne przedstawienie w postaci przekroju ideałów pierwszych pierścienia $k[X_1, \ldots, X_n]$:*

$$\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r, \quad \text{gdzie} \quad \mathfrak{p}_i \not\subset \mathfrak{p}_j \quad \text{dla} \quad i \neq j.$$

Dowód. Zbiór algebraiczny $\mathcal{Z}(\mathfrak{a})$ ma przedstawienie w postaci sumy parami nieporównywalnych rozmaitości V_i :

$$\mathcal{Z}(\mathfrak{a}) = V_1 \cup \cdots \cup V_r$$

(zob. twierdzenie 7.3.4). Zauważmy oczywistą równość

$$\mathcal{I}(\mathcal{Z}(\mathfrak{a})) = \mathcal{I}(V_1 \cup \cdots \cup V_r) = \mathcal{I}(V_1) \cap \cdots \cap \mathcal{I}(V_r).$$

Tutaj każdy ideał $\mathcal{I}(V_i)$ jest ideałem pierwszym (zob. definicję 7.3.1). Ponadto, z nieporównywalności rozmaitości V_i oraz własności (7.5) wynika nieporównywalność ideałów pierwszych $\mathcal{I}(V_i)$. Z twierdzenia Hilberta o zerach (wniosek 7.4.7) wiemy, że $\mathsf{rad}\,\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$. Wobec radykalności ideału $\mathfrak{a}$ otrzymujemy więc rozkład

$$\mathfrak{a} = \mathcal{I}(V_1) \cap \cdots \cap \mathcal{I}(V_r),$$

w którym czynniki $\mathcal{I}(V_i)$ są nieporównywalnymi ideałami pierwszymi pierścienia $k[X_1, \ldots, X_n]$. Jednoznaczność tego rozkładu wynika z jednoznaczności rozkładu zbioru algebraicznego na sumę mnogościową nieporównywalnych rozmaitości (twierdzenie 7.3.4) oraz z własności (7.6).
Jeśli bowiem $\mathfrak{a} = \mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s$ są dwoma rozkładami z nieporównywalnymi czynnikami, to wynika stąd, że

$$\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(\mathfrak{p}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{p}_r) = \mathcal{Z}(\mathfrak{q}_1) \cup \cdots \cup \mathcal{Z}(\mathfrak{q}_s)$$

(zob. uwagę 7.2.2) z nieporównywalnymi składnikami. Wobec tego $r = s$ oraz po ewentualnej zmianie numeracji ideałów $\mathfrak{q}_i$ mamy $\mathcal{Z}(\mathfrak{p}_i) = \mathcal{Z}(\mathfrak{q}_i)$ dla $i = 1, \ldots, r$. Stąd $\mathfrak{p}_i = \mathfrak{q}_i$ dla $i = 1, \ldots, r$. □

Twierdzenie to można traktować jako wersję twierdzeń o rozkładzie prymarnym. Ideał radykalny w pierścieniu noetherowskim $k[X_1, \ldots, X_n]$ (nad ciałem algebraicznie domkniętym k) ma jednoznaczny rozkład prymarny i w tym rozkładzie ideały prymarne są ideałami pierwszymi. Prostota powyższego dowodu bierze się stąd, że w twierdzeniu 7.5.9 rozpatrujemy tylko ideały *radykalne*, bo tylko one są ważne z geometrycznego punktu widzenia (jako ideały stowarzyszone ze zbiorami algebraicznymi). Natomiast twierdzenia o rozkładzie prymarnym są bardziej skomplikowane, bo dotyczą *wszystkich* ideałów w dowolnym pierścieniu noetherowskim.

7.6 Ciało funkcji wymiernych na rozmaitości

W tym rozdziale podamy kilka informacji o pierścieniach funkcji wielomianowych i ciałach funkcji wymiernych na rozmaitościach algebraicznych. Zakładamy, że k jest ciałem algebraicznie domkniętym.

7.6.1 Pierścień funkcji wielomianowych na zbiorze algebraicznym

Niech $V \subseteq k^n$ będzie zbiorem algebraicznym i niech $\mathcal{I}(V)$ będzie stowarzyszonym z V ideałem pierścienia $k[X_1, \ldots, X_n]$. Pierścień ilorazowy

$$k[V] := k[X_1, \ldots, X_n]/\mathcal{I}(V)$$

nazywa się pierścieniem *funkcji wielomianowych* na zbiorze algebraicznym V. Objaśnimy najpierw tę nazwę. Każdy wielomian $f \in k[X_1, \ldots, X_n]$ wyznacza funkcję wielomianową $k^n \to k$ taką, że $a \mapsto f(a)$ dla $a \in k^n$. Będziemy interesować się zacieśnieniami f_V tych funkcji wielomianowych do zbioru algebraicznego V. A więc dla każdego wielomianu $f \in k[X_1, \ldots, X_n]$ mamy funkcję

$$f_V : V \to k, \qquad f_V(a) = f(a) \quad \text{dla} \quad a \in V.$$

Zauważmy, że dla dwóch wielomianów $f, g \in k[X_1, \ldots, X_n]$,

$$f_V = g_V \iff f + \mathcal{I}(V) = g + \mathcal{I}(V) \in k[V].$$

Rzeczywiście, $f_V = g_V$ oznacza, że $f(a) = g(a)$ dla każdego punktu $a \in V$ a to oznacza, że $f - g \in \mathcal{I}(V)$. Zatem elementy $f + \mathcal{I}(V)$ pierścienia $k[V]$ są we wzajemnie jednoznacznej odpowiedniości z funkcjami wielomianowymi f_V na zbiorze V. Identyfikując elementy pierścienia $k[V]$ z odpowiadającymi im funkcjami wielomianowymi otrzymujemy interpretację $k[V]$ jako pierścienia funkcji na zbiorze algebraicznym V.

Niech $\kappa : k[X_1, \ldots, X_n] \to k[V]$ będzie homomorfizmem kanonicznym. Wtedy elementy $\kappa(X_i) = X_i + \mathcal{I}(V) =: x_i$ generują pierścień $k[V]$,

$$k[V] = k[x_1, \ldots, x_n].$$

Zatem pierścień funkcji wielomianowych na zbiorze algebraicznym V zawiera ciało k i jest skończenie generowany nad k. Takie pierścienie nazywamy skończenie generowanymi $k-$pierścieniami (pierścień zawierający ciało k nazywamy $k-$pierścieniem). Zauważmy, że generatory $x_1, \ldots, x_n$ spełniają relacje

$$f(x_1, \ldots, x_n) = 0 \quad \text{dla każdego} \quad f \in \mathcal{I}(V).$$

Rzeczywiście, $f(x_1, \ldots, x_n) = f(X_1, \ldots, X_n) + \mathcal{I}(V) = 0 \in k[V]$ dla każdego wielomianu $f \in \mathcal{I}(V)$.

Pierścień $k[V]$ jest noetherowski, gdyż jest homomorficznym obrazem pierścienia noetherowskiego $k[X_1, \ldots, X_n]$, ale nie jest na ogół pierścieniem całkowitym. Na podstawie definicji 7.3.1 pierścień $k[V]$ jest całkowity wtedy i tylko wtedy, gdy zbiór algebraiczny V jest rozmaitością. Natomiast dla dowolnego zbioru algebraicznego V możemy tylko powiedzieć, że $k[V]$ nie ma niezerowych elementów nilpotentnych, to znaczy $\mathsf{Nil}\, k[V] = 0$. Rzeczywiście, $k[V] := k[X_1, \ldots, X_n]/\mathcal{I}(V)$, gdzie $\mathcal{I}(V)$ jest ideałem radykalnym (na podstawie twierdzenia 7.5.8) i wobec tego $\mathsf{Nil}\, k[V] = 0$ na podstawie lematu 7.5.7. Znaleźliśmy w ten sposób warunek konieczny na to by $k-$pierścień był pierścieniem funkcji wielomianowych pewnego zbioru algebraicznego.

TWIERDZENIE **7.6.1.** *Niech A będzie $k-$pierścieniem. Warunkiem koniecznym i dostatecznym na to by pierścień A był izomorficzny z pierścieniem funkcji wielomianowych na pewnym zbiorze algebraicznym w k^n jest by pierścień A był skończenie generowany nad k i nie zawierał niezerowych elementów nilpotentnych.*

Dowód. Niech $A = k[t_1, \ldots, t_n]$ będzie skończenie generowanym $k-$pierścieniem bez niezerowych elementów nilpotentnych. Zauważmy najpierw, że pierścień A jest homomorficznym obrazem pierścienia wielomianów $k[X_1, \ldots, X_n]$. Rzeczywiście, odwzorowanie

$$k[X_1, \ldots, X_n] \to k[t_1, \ldots, t_n], \quad f \mapsto f(t_1, \ldots, t_n)$$

jest surjektywnym homomorfizmem. Niech $\mathfrak{a}$ będzie jądrem tego homomorfizmu. Wtedy mamy izomorfizm pierścieni

$$k[X_1, \ldots, X_n]/\mathfrak{a} \cong k[t_1, \ldots, t_n] = A.$$

Pierścień $k[X_1, \ldots, X_n]/\mathfrak{a}$ nie ma niezerowych elementów nilpotentnych ponieważ jest izomorficzny z pierścieniem A, który nie ma niezerowych elementów nilpotentnych. Zatem na podstawie lematu 7.5.7 ideał $\mathfrak{a}$ jest radykalny. Wobec tego $\mathfrak{a} = \mathcal{I}(\mathcal{Z}(\mathfrak{a}))$ i A jest pierścieniem izomorficznym z pierścieniem funkcji wielomianowych na zbiorze algebraicznym $\mathcal{Z}(\mathfrak{a})$. □

Przykład 7.6.1. Niech $V = k^n$. Jest to zbiór algebraiczny a stowarzyszonym z nim ideałem jest ideał zerowy: $\mathcal{I}(k^n) = (0)$. Zatem pierścień funkcji wielomianowych na przestrzeni k^n,

$$k[k^n] = k[X_1, \ldots, X_n]/(0) = k[X_1, \ldots, X_n]$$

jest pierścieniem wielomianów $k[X_1, \ldots, X_n]$.
Drugim skrajnie prostym przypadkiem jest zbiór pusty: $V = \varnothing$. Tutaj $\mathcal{I}(V) = (1)$ oraz

$$k[\varnothing] = k[X_1, \ldots, X_n]/(1) = 0$$

jest pierścieniem zerowym.
Trzecim prostym przypadkiem jest jednoelementowy zbiór algebraiczny $V = \{a\}$. Wtedy $\mathcal{I}(V) = (X_1 - a_1, \ldots, X_n - a_n)$ jest ideałem maksymalnym w $k[X_1, \ldots, X_n]$ (zob. wniosek 7.5.3) oraz

$$k[\{a\}] = k[X_1, \ldots, X_n]/(X_1 - a_1, \ldots, X_n - a_n) \cong k.$$

Przykład 7.6.2. Niech V będzie hiperpowierzchnią w przestrzeni k^n. Zatem $V = \mathcal{Z}(h)$, gdzie (h) jest ideałem głównym generowanym przez pewien wielomian $h \in k[X_1, \ldots, X_n]$. Na podstawie twierdzenia Hilberta o zerach mamy $\mathcal{I}(V) = \mathcal{I}(\mathcal{Z}(h)) = \mathsf{rad}(h)$. Z przykładu 7.5.1 wiemy, że ideał (h) jest radykalny wtedy i tylko wtedy, gdy wielomian h jest bezkwadratowy. Wtedy pierścień funkcji wielomianowych na V ma postać

$$k[V] = k[X_1, \ldots, X_n]/\mathcal{I}(V) = k[X_1, \ldots, X_n]/(h).$$

Ponieważ $k[X_1, \ldots, X_n]$ jest pierścieniem z jednoznacznym rozkładem, łatwo sprawdzić, że $k[V]$ jest pierścieniem całkowitym wtedy i tylko wtedy, gdy wielomian h jest nierozkładalny w $k[X_1, \ldots, X_n]$. A więc hiperpowierzchnia $V = \mathcal{Z}(h)$ jest rozmaitością (czyli nierozkładalną hiperpowierzchnią) wtedy i tylko wtedy gdy wielomian h jest nierozkładalny w $k[X_1, \ldots, X_n]$. Ponadto, pierścień funkcji wielomianowych na hiperpowierzchni V jest skończenie generowanym $k-$pierścieniem, $k[V] = k[x_1, \ldots, x_n]$ przy czym generatory $x_1, \ldots, x_n$ spełniają relację $h(x_1, \ldots, x_n) = 0$.

Przykład 7.6.3. Niech H będzie hiperpłaszczyzną w przestrzeni k^n. A więc $H = \mathcal{Z}(h)$, gdzie $h = a_1X_1 + \cdots + a_nX_n - b \in k[X_1, \ldots, X_n]$ jest wielomianem liniowym, $a_i \neq 0$ dla co najmniej jednego i. Wtedy $\mathcal{I}(H) = \mathcal{I}\mathcal{Z}(h) = (h)$ oraz

$$k[H] = k[X_1, \ldots, X_n]/\mathcal{I}(H) = k[X_1, \ldots, X_n]/(a_1X_1 + \cdots + a_nX_n - b).$$

Pokażemy, że

$$k[H] \cong k[X_1, \ldots, X_{n-1}].$$

Wiemy, że $k[H] = k[x_1, \ldots, x_n]$, gdzie $a_1x_1 + \cdots + a_nx_n - b = 0$. Zmieniając ewentualnie numerację zmiennych w pierścieniu wielomianów możemy założyć, że $a_n \neq 0$. Faktycznie możemy założyć, że $a_n = 1$, gdyż wielomiany h i $a_n^{-1}h$ opisują tę samą hiperpłaszczyznę H. Wobec tego mamy

$$x_n = b - a_1x_1 - \cdots - a_{n-1}x_{n-1}$$

skąd wynika, że $k[H] = k[x_1, \ldots, x_{n-1}]$ jest $k-$pierścieniem generowanym przez elementy $x_1, \ldots, x_{n-1}$. Pokażemy, że są one algebraicznie niezależne. Rzeczywiście, jeśli $g(x_1, \ldots, x_{n-1}) = 0 \in k[H]$ dla pewnego wielomianu $g \in k[X_1, \ldots, X_{n-1}]$, to

$$\begin{aligned}\mathcal{I}(H) = 0_{k[H]} &= g(x_1, \ldots, x_{n-1}) = g(X_1 + \mathcal{I}(H), \ldots, X_{n-1} + \mathcal{I}(H)) \\ &= g(X_1, \ldots, X_{n-1}) + \mathcal{I}(H),\end{aligned}$$

i wobec tego $g \in \mathcal{I}(H) = (h)$, to znaczy h dzieli g w pierścieniu $k[X_1, \ldots, X_n]$. Jest to jednak niemożliwe, gdyż zmienna X_n występuje w h ze współczynnikiem niezerowym, natomiast X_n w ogóle nie występuje w żadnym jednomianie wielomianu g. Zatem $x_1, \ldots, x_{n-1}$ są algebraicznie niezależne nad k i wobec tego pierścień $k[x_1, \ldots, x_{n-1}]$ jest izomorficzny z pierścieniem wielomianów $k[X_1, \ldots, X_{n-1}]$.

Jak wynika z twierdzenia 7.6.1 pierścienie wielomianów są dość szczególnymi przykładami pierścieni funkcji wielomianowych. Następujący przykład pokazuje, że pierścienie funkcji wielomianowych na krzywych stożkowych nie są już pierścieniami wielomianów.

Przykład 7.6.4. Niech V będzie hiperbolą na płaszczyźnie zespolonej $\mathbb{C}^2$ zadaną wielomianem $XY - 1 \in \mathbb{C}[X, Y]$. Ponieważ wielomian $XY - 1$ jest nierozkładalny w $\mathbb{C}[X, Y]$, mamy

$$\mathbb{C}[V] = \mathbb{C}[X, Y]/(XY - 1).$$

Udowodnimy, że $\mathbb{C}[V]$ jest pierścieniem izomorficznym z podpierścieniem $\mathbb{C}[X, \frac{1}{X}]$ ciała funkcji wymiernych $\mathbb{C}(X)$. Oznacza to, że pierścień $\mathbb{C}[V]$ nie jest izomorficzny z pierścieniem wielomianów nad $\mathbb{C}$, gdyż w $\mathbb{C}[X, \frac{1}{X}]$ element X przestępny nad $\mathbb{C}$ jest odwracalny, co nie ma miejsca w żadnym pierścieniu wielomianów. Rozpatrzmy homomorfizm pierścieni

$$\varphi : \mathbb{C}[X, Y] \to \mathbb{C}[X, \frac{1}{X}], \quad \varphi(f) = f(X, \frac{1}{X}).$$

Zauważmy, że $\varphi(X) = X$ oraz $\varphi(Y) = \frac{1}{X}$, skąd wynika, że φ jest epimorfizmem. Pokażemy, że $\ker \varphi = (XY - 1)$. Wobec $\varphi(XY - 1) = 0$ mamy oczywiście inkluzję $(XY - 1) \subseteq \ker \varphi$. Załóżmy więc, że $g \in \ker \varphi$, to znaczy $g(X, \frac{1}{X}) = 0$. Wtedy $g(a, b) = 0$ dla każdego punktu $(a, b) \in V = \mathcal{Z}(XY - 1)$. Rzeczywiście, jeśli $ab - 1 = 0$, to $b = \frac{1}{a}$ i wobec tego $g(a, b) = g(a, \frac{1}{a}) = 0$. Wielomian g zeruje się więc w każdym wspólnym zerze ideału $(XY - 1)$ i wobec tego na podstawie twierdzenia Hilberta o zerach mamy

$$g^m \in (XY - 1)$$

dla pewnej liczby naturalnej m. Ponieważ jednak $XY - 1$ jest wielomianem nierozkładalnym, wynika stąd, że $g \in (XY - 1)$. Dowodzi to, że $\ker \varphi = (XY - 1)$. Z twierdzenia o homomorfizmach pierścieni wynika teraz, że $\mathbb{C}[X, Y]/(XY - 1) \cong \mathbb{C}[X, \frac{1}{X}]$.

Wykorzystując ten rezultat można łatwo uzyskać opis pierścienia funkcji wielomianowych na okręgu $U = \mathcal{Z}(X^2 + Y^2 - 1) \subset \mathbb{C}^2$. Najpierw rozpatrzmy homomorfizmy pierścieni

$$\varphi : \mathbb{C}[X, Y] \to \mathbb{C}[T, Z], \quad f \mapsto f\Big(\frac{1}{2}(T + Z), \frac{1}{2i}(T - Z)\Big),$$

$$\psi : \mathbb{C}[T, Z] \to \mathbb{C}[X, Y], \quad f \mapsto f(X + iY, X - iY).$$

Zauważamy, że złożenia tych homomorfizmów są identycznościami i wobec tego obydwa homomorfizmy są izomorfizmami pierścieni.
Ponieważ $X^2 + Y^2 = (X + iY)(X - iY)$, więc $\psi(TZ - 1) = X^2 + Y^2 - 1$ i wobec tego

$$\mathbb{C}[T, Z]/(TZ - 1) \cong \mathbb{C}[X, Y]/(X^2 + Y^2 - 1).$$

A więc pierścienie funkcji wielomianowych na hiperboli $\mathcal{Z}(TZ - 1) \subset \mathbb{C}^2$ oraz na okręgu $\mathcal{Z}(X^2 + Y^2 - 1) \subset \mathbb{C}^2$ są izomorficzne. Dokładniej,

$$\mathbb{C}[\mathcal{Z}(X^2 + Y^2 - 1)] \cong \mathbb{C}[T, \frac{1}{T}] = \mathbb{C}[X + iY, \frac{1}{X + iY}].$$

7.6.2 Kategoria afinicznych zbiorów algebraicznych

Obiektami tej kategorii będą afiniczne zbiory algebraiczne nad ustalonym ciałem k natomiast morfizmy $V_1 \to V_2$ określimy przy pomocy funkcji wielomianowych na zbiorze algebraicznym V_1. Niech $V_1 \subseteq k^n$ oraz $V_2 \subseteq k^m$ będą zbiorami algebraicznymi. Dla każdego układu m funkcji wielomianowych $(f_1, \ldots, f_m)$ na zbiorze V_1 mamy odwzorowanie

$$(f_1, \ldots, f_m) : V_1 \to k^m, \qquad (a_1, \ldots, a_n) \mapsto (f_1(a_1, \ldots, a_n), \ldots, f_m(a_1, \ldots, a_n)).$$

Jeśli obraz tego odwzorowania zawiera się w zbiorze algebraicznym $V_2 \subseteq k^m$, to układ $f = (f_1, \ldots, f_m)$ nazywamy morfizmem $f : V_1 \to V_2$ zbioru V_1 w zbiór V_2. Łatwo zauważyć, że odwzorowanie identycznościowe $\mathbf{1}_V$ na zbiorze algebraicznym V jest morfizmem (wystarczy przyjąć jako f_i funkcje wielomianowe określone następująco: $f_i(x_1, \ldots, x_n) = x_i$ dla $i = 1, \ldots, n$). Łatwo też sprawdzić, że składanie morfizmów jest łączne. W związku z tym klasa wszystkich zbiorów algebraicznych nad ciałem k (we wszystkich przestrzeniach afinicznych k^n) wraz z określonymi wyżej morfizmami tworzy *kategorię afinicznych zbiorów algebraicznych* nad k, którą oznaczamy $\mathcal{S}(k)$.

Zauważmy, że każdemu zbiorowi algebraicznemu $V \subseteq k^n$ przyporządkowaliśmy $k-$pierścień funkcji wielomianowych $k[V]$. Pokażemy teraz, że każdemu morfizmowi $f : V_1 \to V_2$ można w sposób naturalny przyporządkować homomorfizm $k-$pierścieni funkcji wielomianowych $k[V_2] \to k[V_1]$. Rzeczywiście, jeśli $f : V_1 \to V_2$ jest morfizmem pomiędzy zbiorami algebraicznymi V_1 i V_2, to dla dowolnej funkcji wielomianowej $\varphi \in k[V_2]$ złożenie $\varphi \circ f$ jest funkcją wielomianową na V_1, to znaczy $\varphi \circ f \in k[V_1]$. Ponadto, odwzorowanie

$$f^* : k[V_2] \to k[V_1], \qquad f^*(\varphi) = \varphi \circ f$$

jest homomorfizmem $k-$pierścieni. W ten sposób określa się funktor kontrawariantny F z kategorii $\mathcal{S}(k)$ zbiorów algebraicznych nad k w kategorię skończenie generowanych $k-$pierścieni, który na obiektach i morfizmach kategorii $\mathcal{S}(k)$ działa następująco:

$$F(V) = k[V], \qquad F(f : V_1 \to V_2) = f^*.$$

7.6.3 Zbiory algebraiczne określone nad podciałem

Zakładamy, że k jest ciałem algebraicznie domkniętym i K jest podciałem ciała k. Jeśli V jest zbiorem algebraicznym w k^n, to mówimy, że zbiór V jest *określony* nad ciałem K jeśli ideał $\mathcal{I}(V) \subset k[X_1, \ldots, X_n]$ ma zbiór generatorów w pierścieniu $K[X_1, \ldots, X_n]$. Dla zaznaczenia, że zbiór algebraiczny $V \subset k^n$ jest określony nad ciałem K piszemy $V = V/K$.
Dla zbioru algebraicznego $V = V/K$ określonego nad K rozpatrujemy ideał $\mathcal{I}(V/K)$ pierścienia $K[X_1, \ldots, X_n]$:

$$\mathcal{I}(V/K) = \Big\{ g \in K[X_1, \ldots, X_n] : g(a) = 0 \quad \forall\, a \in V \Big\} = \mathcal{I}(V) \cap K[X_1, \ldots, X_n].$$

Pierścień ilorazowy

$$K[V] := K[X_1, \ldots, X_n]/\mathcal{I}(V/K)$$

nazywa się *pierścieniem funkcji wielomianowych* nad ciałem K na zbiorze algebraicznym $V = V/K$ określonym nad K. Tak więc dla zbioru algebraicznego $V \subset k^n$ i dla każdego podciała K ciała k, nad którym jest określony zbiór algebraiczny V, mamy odrębny pierścień funkcji wielomianowych $K[V]$ nad K na $V = V/K$.
Zauważmy, że pierścień $K[V]$ można traktować jako podpierścień $k[V]$. Rzeczywiście, mamy homomorfizm pierścieni

$$K[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/\mathcal{I}(V), \quad f \mapsto f + \mathcal{I}(V),$$

którego jądrem jest $\mathcal{I}(V) \cap K[X_1, \ldots, X_n] = \mathcal{I}(V/K)$. Wobec tego mamy indukowany injektywny homomorfizm pierścieni

$$K[V] = K[X_1, \ldots, X_n]/\mathcal{I}(V/K) \to k[X_1, \ldots, X_n]/\mathcal{I}(V) = k[V],$$

który jest podstawą do utożsamienia pierścienia $K[V]$ z jego obrazem w $k[V]$.
Elementy pierścienia $K[V]$ można także interpretować jako funkcje na zbiorze V o wartościach w ciele k. Są to funkcje wielomianowe f_V wyznaczone przez wielomiany $f \in K[X_1, \ldots, X_n]$.

Przykład 7.6.5. Niech $k = \mathbb{C}$ będzie ciałem liczb zespolonych. Rozpatrzmy $f = X^2 + Y^2 \in \mathbb{C}[X, Y]$ oraz zbiór algebraiczny $V = \mathcal{Z}(f) \subset \mathbb{C}^2$. Wtedy na podstawie przykładu 7.6.2 mamy $\mathcal{I}(V) = (f)$
Rozpatrzmy pierścień funkcji wielomianowych $\mathbb{C}[V] = \mathbb{C}[X, Y]/\mathcal{I}(V) = \mathbb{C}[X, Y]/(f)$. Ponieważ $f = (X + iY)(X - iY)$ jest rozkładalny w pierścieniu $\mathbb{C}[X, Y]$, więc pierścień $\mathbb{C}[V]$ nie jest pierścieniem całkowitym. Natomiast dla każdego podciała $\mathbb{K}$ ciała $\mathbb{R}$ liczb rzeczywistych wielomian f jest nierozkładalny w pierścieniu $\mathbb{K}[X, Y]$ i wobec tego $\mathbb{K}[V] = \mathbb{K}[X, Y]/\mathcal{I}(V/\mathbb{K})$ jest pierścieniem całkowitym. Zatem injektywny homomorfizm $\mathbb{K}[V] \to \mathbb{C}[V]$ nie jest surjektywny i pierścień funkcji wielomianowych na zbiorze algebraicznym $V \subset \mathbb{C}^2$ jest istotnie większy niż jego podpierścień $\mathbb{K}[V]$ funkcji wielomianowych nad $\mathbb{K}$ na zbiorze $V = V/\mathbb{K}$ określonym nad $\mathbb{K}$.
Warto zauważyć, że jeśli elementy pierścienia $\mathbb{K}[V]$ traktujemy jako funkcje na V o wartościach w $\mathbb{C}$, to konkluzja $\mathbb{K}[V] \subsetneq \mathbb{C}[V]$ jest oczywista. Pierścień $\mathbb{K}[V]$ składa się bowiem z funkcji wielomianowych wielomianów o współczynnikach w $\mathbb{K}$ podczas gdy pierścień $\mathbb{C}[V]$ składa się z funkcji wielomianowych wszystkich wielomianów o współczynnikach zespolonych.

7.6.4 Punkty $K-$wymierne

Zbiorem punktów $K-$wymiernych zbioru algebraicznego $V \subset k^n$ nazywamy podzbiór $V(K)$ zbioru V złożony z punktów o współrzędnych w ciele K:

$$V(K) = \Big\{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0 \quad \forall\, f \in \mathcal{I}(V)\Big\} = V \cap K^n.$$

W szczególności $V(k) = V$.

Przykład 7.6.6. Niech $K = \mathbb{R}$ będzie ciałem liczb rzeczywistych oraz $k = \mathbb{C}$ ciałem liczb zespolonych. Niech $V = \mathcal{Z}(f)$, gdzie $f = X^2 + Y^2 \in \mathbb{C}[X, Y]$. Wtedy ideał (f) rozkłada się na iloczyn dwóch ideałów głównych, $(f) = (X + iY)(X - iY)$ i wobec tego na podstawie (7.8) mamy

$$V = \mathcal{Z}(f) = \mathcal{Z}(X + iY) \cup \mathcal{Z}(X - iY).$$

Zbiór algebraiczny V jest więc sumą mnogościową dwóch prostych na płaszczyźnie $\mathbb{C}^2$. Natomiast zbiór punktów $\mathbb{R}-$wymiernych $V(\mathbb{R})$ jest zbiorem jednoelementowym:

$$V(\mathbb{R}) = V \cap \mathbb{R}^2 = \Big\{(0, 0)\Big\}.$$

7.6.5 Ciało funkcji wymiernych na rozmaitości

Niech teraz $V \subseteq k^n$ będzie rozmaitością algebraiczną. Wtedy pierścień $k[V]$ funkcji wielomianowych na V jest pierścieniem całkowitym i wobec tego ma ciało ułamków, które oznaczamy $k(V)$. Ciało $k(V)$ nazywa się *ciałem funkcji wymiernych* na rozmaitości V. Zauważmy, że jeśli $\kappa : k[X_1, \ldots, X_n] \to k[V]$ jest homomorfizmem kanonicznym oraz $x_i = \kappa(X_i) = X_i + \mathcal{I}(V)$, to

$$k(V) = k(x_1, \ldots, x_n).$$

Ciało funkcji wymiernych na rozmaitości $V \subseteq k^n$ jest więc skończenie generowanym rozszerzeniem ciała k.

Przykład 7.6.7. Rozpatrzmy zbiór jednopunktowy $V = \{(a_1, \ldots, a_n)\} \subset k^n$. Wtedy na podstawie lematu 7.5.1 mamy $\mathcal{I}(V) = (X_1 - a_1, \ldots, X_n - a_n)$ a więc $k[V] = k[X_1, \ldots, X_n]/\mathcal{I}(V) \cong k$ jest ciałem. Zatem $k(V) = k$ dla każdej jednopunktowej rozmaitości V.

Przykład 7.6.8. Jeśli $V = k^n$, to $\mathcal{I}(V) = 0$ jest ideałem pierwszym, zatem k^n jest rozmaitością algebraiczną. Ciałem funkcji wymiernych na k^n jest więc ciało ułamków pierścienia $k[k^n] = k[X_1, \ldots, X_n]/0 = k[X_1, \ldots, X_n]$, czyli $k(k^n) = k(X_1, \ldots, X_n)$ jest ciałem funkcji wymiernych n zmiennych nad ciałem k.

Podobnie jak w przypadku pierścienia $k[V]$, choć z pewnymi zastrzeżeniami, także elementy ciała $k(V)$ traktujemy jako *funkcje* na V o wartościach w k. Niech $\alpha \in k(V)$. Zatem $\alpha = \frac{w_1}{w_2}$ jest ilorazem dwóch funkcji wielomianowych w_1 i w_2 na rozmaitości V, przy czym w_2 nie jest funkcją zerową na V. Takie przedstawienie elementu α ciała $k(V)$ oczywiście nie jest jednoznaczne i ta niejednoznaczność odgrywa istotną rolę w próbie traktowania α jako funkcji na V.

Niech bowiem $a = (a_1, \ldots, a_n)$ będzie punktem rozmaitości V. Jeśli $w_2(a) = 0$, to wykorzystując przedstawienie $\alpha = \frac{w_1}{w_2}$ nie możemy mówić o wartości funkcji wymiernej α w punkcie a. Może się natomiast zdarzyć, że funkcja wymierna α ma inne przedstawienie w postaci ilorazu dwóch funkcji wielomianowych, $\alpha = \frac{u_1}{u_2}$, w którym $u_2(a) \neq 0$. Wtedy element $\frac{u_1(a)}{u_2(a)}$ ciała k nazywamy *wartością* funkcji wymiernej α w punkcie a rozmaitości V a funkcję α nazywamy *określoną* w punkcie a. Ta definicja wartości funkcji wymiernej w punkcie nie zależy od sposobu przedstawienia funkcji wymiernej α jako ilorazu dwóch funkcji wielomianowych. Rzeczywiście, jeśli

$$\alpha = \frac{u_1}{u_2} = \frac{v_1}{v_2}, \quad u_i, v_i \in k[V], \quad u_2(a) \neq 0, v_2(a) \neq 0,$$

to mamy równość $u_1 v_2 = u_2 v_1$ w pierścieniu $k[V]$, skąd $u_1(a)v_2(a) = u_2(a)v_1(a)$ i wobec tego

$$\frac{u_1(a)}{u_2(a)} = \frac{v_1(a)}{v_2(a)}.$$

A więc jeśli funkcja wymierna α ma przedstawienie $\alpha = \frac{w_1}{w_2}$, gdzie $w_2(a) \neq 0$, to wartość funkcji α w punkcie $a \in V$ jest dobrze określona. Może się natomiast zdarzyć, że w każdym przedstawieniu $\alpha = \frac{w_1}{w_2}$ jako ilorazu dwóch funkcji wielomianowych mamy $w_2(a) = 0$. Wtedy funkcja α nie jest określona w punkcie a rozmaitości V. Tak więc funkcja α jest na ogół określona tylko na pewnym podzbiorze rozmaitości V. Tym niemniej, przyjęto nazywać każdy element $\alpha \in k(V)$ funkcją wymierną na rozmaitości V.

Zauważmy, że zbiór punktów rozmaitości V, na których dana funkcja wymierna α jest określona, jest niepusty. Przypuśćmy bowiem, że dla pewnego ustalonego przedstawienia funkcji wymiernej α w postaci ilorazu funkcji wielomianowych $\alpha = \frac{w_1}{w_2}$ dla wszystkich punktów $a \in V$ mamy $w_2(a) = 0$. Funkcja wielomianowa $w_2 \in k[V]$ zeruje się więc na rozmaitości V, jest zatem elementem zerowym pierścienia funkcji wielomianowych: $w_2 = 0 \in k[V]$. W takim razie w_2 nie może występować jako mianownik funkcji wymiernej w żadnym przedstawieniu funkcji wymiernej α jako ułamka. Sprzeczność.

Przykład 7.6.9. Rozpatrzmy ciało funkcji wymiernych na okręgu nad ciałem liczb zespolonych:

$$V = \mathcal{Z}(X^2 + Y^2 - 1) \subset \mathbb{C}^2, \quad \mathbb{C}(V) = \mathbb{C}(x, y), \quad \text{gdzie} \quad x^2 + y^2 = 1.$$

Weźmy funkcję wymierną $\alpha = \frac{1-y}{x} \in \mathbb{C}(x, y)$. Pokażemy, że funkcja α jest określona w punkcie $a = (0, 1)$. Wprawdzie w danym przedstawieniu funkcji α mianownik zeruje się w punkcie a, jednakże funkcja wymierna α ma inne przedstawienie jako iloraz funkcji wielomianowych, w którym mianownik nie zeruje się w punkcie a. Mamy bowiem

$$\alpha = \frac{1-y}{x} = \frac{x}{1+y}$$

i wobec tego $\alpha(a) = 0$. Oczywiście funkcja α jest także określona w każdym punkcie okręgu, którego pierwsza współrzędna jest niezerową liczbą zespoloną. Pokażemy

natomiast, że funkcja α nie jest określona w punkcie $b = (0, -1)$. Rzeczywiście, weźmy dowolne przedstawienie funkcji α w postaci ilorazu funkcji wielomianowych

$$\alpha = \frac{1-y}{x} = \frac{u(x,y)}{v(x,y)}.$$

Wtedy mamy równość funkcji wielomianowych $(1-y) \cdot v(x,y) = x \cdot u(x,y)$ i wobec tego podstawiając $x = 0$ oraz $y = -1$ otrzymujemy $v(0,-1) = 0$. Tak więc w każdym przedstawieniu funkcji α w postaci ilorazu funkcji wielomianowych mianownik zeruje się w punkcie $b = (0, -1)$.

7.6.6 Wymiar rozmaitości

Ciało funkcji wymiernych $k(V) = k(x_1, \ldots, x_n)$ na rozmaitości V jest skończenie generowanym rozszerzeniem ciała k. Ponieważ k jest ciałem algebraicznie domkniętym, każdy element $k(V)$ algebraiczny nad k należy do k. Zatem jeśli $k(V) \neq k$, to ciało $k(V)$ jest przestępnym rozszerzeniem ciała k. Zauważmy, że jeśli $V \neq k^n$, to układ $x_1, \ldots, x_n$ elementów generujących $k(V)$ jest *algebraicznie zależny* nad k. Jeśli bowiem $V = \mathcal{Z}(\mathfrak{p})$, gdzie $\mathfrak{p}$ jest niezerowym ideałem pierwszym w $k[X_1, \ldots, X_n]$ oraz $\kappa : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/\mathfrak{p} = k[V]$ jest homomorfizmem kanonicznym, to dla każdego niezerowego wielomianu $f \in \mathfrak{p}$ mamy

$$f(x_1, \ldots, x_n) = \kappa(f) = f + \mathfrak{p} = \mathfrak{p} = 0 \in k[V].$$

Maksymalną liczbę algebraicznie niezależnych elementów w zbiorze $\{x_1, \ldots, x_n\}$ nazywa się *stopniem przestępnym* ciała $k(V) = k(x_1, \ldots, x_n)$. Można udowodnić, że liczba ta nie zależy od wyboru generatorów $x_1, \ldots, x_n$ ciała $k(V)$ (zob. J. Browkin, *Teoria ciał*, PWN Warszawa, 1977, rozdz. III).

Wymiarem $\dim V$ rozmaitości $V \subseteq k^n$ nazywamy stopień przestępny ciała $k(V)$ funkcji wymiernych na V.

Przykład 7.6.10. Rozmaitość jednopunktowa $V = \{a\} \subset k^n$ ma ciało funkcji wymiernych $k(V) = k$ i wobec tego ma wymiar zero.

Przykład 7.6.11. Nierozkładalna hiperpowierzchnia $V = \mathcal{Z}(f) \subsetneq k^n$ ma wymiar $n-1$.
W szczególności, nierozkładalna krzywa $C \subsetneq k^2$ ma wymiar 1.

Niech bowiem $k(V) = k(x_1, \ldots, x_n)$ będzie ciałem ułamków pierścienia funkcji wielomianowych $k[V] = k[X_1, \ldots, X_n]/(f)$ na V, gdzie wielomian f jest nierozkładalny w $k[X_1, \ldots, X_n]$. Wtedy elementy $x_1, \ldots, x_n$ są algebraicznie zależne nad k i wobec tego $\dim V < n$.

Dla dowodu, że $\dim V \geqslant n-1$ zauważmy najpierw że wielomian f, wyznaczający hiperpowierzchnię V, nie jest stałą w k, gdyż jako wielomian nierozkładalny jest niezerowym elementem nieodwracalnym w $k[X_1, \ldots, X_n]$. Zatem w f występuje przynajmniej jedna zmienna spośród $X_1, \ldots, X_n$, powiedzmy, że jest to X_n.

Jeśli $\dim V < n-1$, to każdy układ $n-1$ elementów spośród $x_1, \ldots, x_n$ jest algebraicznie zależny nad k. W szczególności elementy $x_1, \ldots, x_{n-1}$ są algebraicznie

zależne nad k, wobec tego dla pewnego niezerowego wielomianu $g \in k[X_1, \ldots, X_{n-1}]$ mamy $g(x_1, \ldots, x_{n-1}) = 0$. Zatem dla homomorfizmu kanonicznego

$$\kappa : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/(f) = k[V]$$

mamy $\kappa(g) = g(x_1, \ldots, x_{n-1}) = 0$, skąd wynika, że $g \in \ker \kappa = (f)$. Jest to jednak niemożliwe, gdyż wielomian g nie zawiera zmiennej X_n i wobec tego nie może dzielić się przez wielomian f, w którym X_n występuje. Pokazaliśmy więc, że $\dim V < n$ oraz $\dim V \geqslant n-1$. Stąd $\dim V = n-1$.

Przykład 7.6.12. Przestrzeń k^n jest rozmaitością i ma ciało funkcji wymiernych

$$k(k^n) = k(X_1, \ldots, X_n).$$

Zatem jako rozmaitość algebraiczna przestrzeń k^n ma wymiar n.

Pojęcie wymiaru rozmaitości ma oczywiście także interpretację geometryczną. Każda rozmaitość V zawiera podrozmaitość jednopunktową i można na ogół zbudować ostro wznoszący łańcuch

$$V_0 \subset V_1 \subset \cdots \subset V_m = V$$

podrozmaitości V_i rozmaitości V. Liczbę m nazwijmy *długością* łańcucha. Można udowodnić, że maksymalna długość ostro wznoszącego łańcucha podrozmaitości rozmaitości V jest równa wymiarowi $\dim V$ rozmaitości V.

Zauważmy, że podrozmaitościom rozmaitości V odpowiadają ideały pierwsze pierścienia $k[V]$ funkcji wielomianowych na V. Rzeczywiście, jeśli $U \subset V$ jest podrozmaitością V, to $\mathcal{I}(U) \supset \mathcal{I}(V)$ i wobec tego homomorfizm kanoniczny

$$\kappa : k[X_1, \ldots, X_n] \to k[V]$$

przeprowadza ideał pierwszy $\mathcal{I}(U)$ pierścienia $k[X_1, \ldots, X_n]$ na ideał pierwszy pierścienia $k[V]$.

Zatem $\dim V$ można także interpretować jako maksymalną długość ostro opadających łańcuchów ideałów pierwszych

$$\mathfrak{p}_0 \supset \mathfrak{p}_1 \supset \cdots \supset \mathfrak{p}_m = 0$$

w pierścieniu $k[V]$. A więc w terminologii rozdziału 6.3, $\dim V = \dim k[V]$, to znaczy, wymiar rozmaitości jest równy wymiarowi Krulla pierścienia funkcji wielomianowych na rozmaitości V.

W szczególności, jeśli C jest nierozkładalną krzywą, to $\dim k[C] = 1$.

Pojęcie wymiaru można też wprowadzić dla dowolnego zbioru algebraicznego $A \subseteq k^n$. Na podstawie twierdzenia 7.3.4 zbiór algebraiczny A jest sumą mnogościową rozmaitości, $A = V_1 \cup \cdots \cup V_r$ i wobec jednoznaczności tego przedstawienia możemy określić

$$\dim A = \max\{\dim V_1, \ldots, \dim V_r\}.$$

7.6.7 Nieosobliwość rozmaitości

Dla uproszczenia rozpatrujemy tylko nierozkładalną hiperpowierzchnię $V = \mathcal{Z}(f) \subsetneq k^n$. Punkt $a = (a_1, \ldots, a_n) \in V$ nazywamy *nieosobliwym* jeśli przynajmniej jedna pochodna cząstkowa wielomianu f nie zeruje się w punkcie a:

$$\frac{\partial f}{\partial X_i}(a) \neq 0$$

dla pewnego $i \leqslant n$. W punkcie nieosobliwym $a \in V$ mamy więc hiperpłaszczyznę *styczną* do V zadaną równaniem

$$\sum_{i=1}^{n} \frac{\partial f}{\partial X_i}(a)(X_i - a_i) = 0.$$

Hiperpowierzchnia V nazywa się *gładka* jeśli każdy punkt tej hiperpowierzchni jest nieosobliwy (lub równoważnie, jeśli w każdym punkcie istnieje hiperpłaszczyzna styczna). Można udowodnić, że jeśli nierozkładalna hiperpowierzchnia V jest gładka, to pierścień funkcji wielomianowych $k[V]$ jest całkowicie domknięty. W przypadku krzywych można nawet udowodnić, że krzywa nierozkładalna C jest gładka wtedy i tylko wtedy gdy jej pierścień funkcji wielomianowych $k[C]$ jest całkowicie domknięty (zob. I. R. Shafarevich, Basic Algebraic Geometry I, Springer Verlag 1994, str. 127).

Tak więc dla krzywej nierozkładalnej C pierścień funkcji wielomianowych $k[C]$ jest pierścieniem całkowitym i ma następujące własności: jest noetherowski, całkowicie domknięty oraz $\dim k[C] = 1$.

Pierścień funkcji wielomianowych $k[C]$ na nierozkładalnej krzywej C jest więc pierścieniem Dedekinda.

7.7 Zadania

1. Niech $A \subseteq K^n$ oraz $B \subseteq K^m$ będą zbiorami algebraicznymi. Udowodnić, że produkt kartezjański $A \times B \subseteq K^{n+m}$ jest także zbiorem algebraicznym.

2. Dla dowolnych zbiorów algebraicznych $A_1, \ldots, A_n$ udowodnić, że

$$\mathcal{I}(A_1 \cup \cdots \cup A_n) = \bigcap_{i=1}^{n} \mathcal{I}(A_i).$$

3. Udowodnić, że każdy podzbiór domknięty w topologii Zariskiego przestrzeni $\mathbb{C}^n$ jest domknięty w naturalnej topologii tej przestrzeni.

4. Niech $f, g \in K[X, Y]$ gdzie K jest ciałem algebraicznie domkniętym. Udowodnić, że krzywe algebraiczne wyznaczone przez wielomiany f i g są równe (tzn. $\mathcal{Z}(f) = \mathcal{Z}(g)$) wtedy i tylko wtedy gdy istnieją liczby naturalne n, m takie, że $f \mid g^n, \quad g \mid f^m$.
Zauważyć, że warunek ten jest równoważny temu, że f i g mają te same czynniki nierozkładalne nad K.

5. Niech $f \in K[X, Y]$ gdzie K jest ciałem algebraicznie domkniętym i niech $f =$

$f_1^{e_1} \cdots f_r^{e_r}$ będzie kanonicznym rozkładem wielomianu f na czynniki nierozkładalne nad ciałem K. Udowodnić, że
(a) $\mathcal{Z}(f) = \mathcal{Z}(f_1) \cup \cdots \cup \mathcal{Z}(f_r)$ jest rozkładem zbioru algebraicznego $\mathcal{Z}(f)$ na sumę mnogościową rozmaitości.
(b) $\mathcal{I}(\mathcal{Z}(f)) = (f_1 \cdots f_r)$.

6. Udowodnić, że każdy właściwy ideał radykalny jest przekrojem zawierających go ideałów pierwszych.

Wskazówka. Jeśli $\mathfrak{a}$ jest ideałem radykalnym oraz $a \notin \mathfrak{a}$, to zbiór multyplikatywny $S = \{1, a, a^2, \ldots\}$ jest rozłączny z ideałem $\mathfrak{a}$. Rozpatrzyć ideał maksymalny w rodzinie ideałów zawierających $\mathfrak{a}$ i rozłącznych ze zbiorem S.

7. Niech $\mathsf{Spec}\, A$ będzie zbiorem wszystkich ideałów pierwszych pierścienia przemiennego A. Dla każdego ideału $\mathfrak{a} \lhd A$ definiujemy $V(\mathfrak{a}) = \left\{\mathfrak{p} \in \mathsf{Spec}\, A : \mathfrak{p} \supseteq \mathfrak{a}\right\}$. Udowodnić, że dla ideałów $\mathfrak{a}, \mathfrak{b} \lhd A$ mamy

$$V(\mathfrak{a}) \cup V(\mathfrak{b}) = V(\mathfrak{a} \cap \mathfrak{b}) = V(\mathfrak{a} \cdot \mathfrak{b}),$$

oraz dla każdej rodziny $\left\{\mathfrak{a}_i : i \in T\right\}$ ideałów pierścienia A mamy

$$\bigcap_{i \in T} V(\mathfrak{a}_i) = V(\sum_{i \in T} \mathfrak{a}_i).$$

Wywnioskować stąd, że na spektrum $\mathsf{Spec}\, A$ istnieje topologia, w której zbiorami domkniętymi są zbiory $V(\mathfrak{a})$ dla $\mathfrak{a} \lhd A$ (topologia Zariskiego na spektrum pierwszym pierścienia A).

8. Udowodnić, że $\mathsf{Spec}\, A$ jest zwartą przestrzenią topologiczną (z każdego pokrycia $\mathsf{Spec}\, A$ zbiorami otwartymi można wybrać podpokrycie skończone).

9. Udowodnić, że jeśli $\mathsf{Spec}\, A$ jest sumą dwóch rozłącznych zbiorów domkniętych, to istnieje element idempotentny $e \in A$ różny od 0 i 1.

Wskazówka. Jeśli $\mathsf{Spec}\, A = V(\mathfrak{a}) \cup V(\mathfrak{b})$ i $V(\mathfrak{a}) \cap V(\mathfrak{b}) = \emptyset$, to $\mathfrak{a} + \mathfrak{b} = A$ oraz $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathsf{Nil}\, A$.

Rozdział 8

Algebra endomorfizmów

Ostatnie zmiany 30.04.2009 r.

Głównym problemem algebry liniowej jest zrozumienie działania endomorfizmów przestrzeni wektorowych. W tym rozdziale zajmujemy się najpierw algebraicznymi własnościami zbioru wszystkich endomorfizmów ustalonej przestrzeni wektorowej a następnie rozpoczynamy analizę własności endomorfizmów uwzględniającą sposób działania endomorfizmu na przestrzeni wektorowej. Twierdzenia o postaciach kanonicznych macierzy endomorfizmów udowodnimy w następnych rozdziałach. Zakładamy znajomość podstawowych pojęć i faktów z kursowego wykładu algebry liniowej (takich jak liniowa niezależność wektorów, baza, wymiar przestrzeni, homomorfizmy).

8.1 $K-$algebry: definicje i przykłady

Niech K będzie dowolnym ciałem i niech V będzie przestrzenią wektorową nad K. *Endomorfizmem* przestrzeni V nazywamy każdy homomorfizm (przekształcenie liniowe) τ przestrzeni V w siebie. A więc

$$\tau : V \to V, \quad \tau(au + bv) = a\tau(u) + b\tau(v) \quad \text{dla wszystkich} \quad a, b \in K,\ u, v \in V.$$

Wyróżnimy *endomorfizm zerowy* $0_V : V \to V$ taki, że $0_V(u) = 0$ dla każdego $u \in V$, oraz *endomorfizm tożsamościowy* $1_V : V \to V$ taki, że $1_V(u) = u$ dla każdego $u \in V$.
Zbiór wszystkich endomorfizmów przestrzeni wektorowej V oznaczamy $\mathsf{End}\, V$ lub $\mathsf{End}_K V$, jeśli chcemy zaznaczyć, że V jest przestrzenią wektorową nad ciałem K.
Dla dowolnych $\sigma, \tau \in \mathsf{End}\, V$ określamy *sumę* $\sigma + \tau$ oraz *iloczyn* $\sigma \cdot \tau$ endomorfizmów w sposób następujący:

$$\sigma + \tau : V \to V, \quad (\sigma + \tau)(u) = \sigma(u) + \tau(u),$$

$$\sigma \cdot \tau : V \to V, \quad (\sigma \cdot \tau)(u) = \sigma(\tau(u))$$

dla każdego $u \in V$. Łatwo sprawdzić, że suma i iloczyn dwóch endomorfizmów przestrzeni V są endomorfizmami V.
W ten sposób w zbiorze $\mathsf{End}\, V$ wprowadziliśmy działania *dodawania* i *mnożenia* endomorfizmów. Rutynowe rachunki pokazują, że $\mathsf{End}_K V$ z dodawaniem i mnożeniem endomorfizmów jako działaniami jest pierścieniem.

Każdy endomorfizm przestrzeni wektorowej V jest także endomorfizmem addytywnej grupy $V^+ = (V, +)$ przestrzeni V. Z przykładu 2.1.5 wiemy, że zbiór $\mathsf{End}\, V^+$ jest pierścieniem ze względu na dodawanie i mnożenie (składanie) endomorfizmów. Zatem pierścień $\mathsf{End}\, V$ jest podpierścieniem pierścienia $\mathsf{End}\, V^+$.

W pierścieniu $\mathsf{End}\, V$ wprowadzamy jeszcze jedną operację, zwaną mnożeniem endomorfizmów przez skalary. Dla $a \in K$ oraz $\tau \in \mathsf{End}\, V$ określamy odwzorowanie

$$a\tau : V \to V, \quad (a\tau)(u) = a\tau(u) \quad \text{dla} \quad u \in V.$$

Łatwo sprawdzić, że $a\tau \in \mathsf{End}\, V$ oraz

$$\begin{aligned} a(\sigma + \tau) &= a\sigma + a\tau \\ (a+b)\tau &= a\tau + b\tau \\ (ab)\tau &= a(b\tau) \\ 1\tau &= \tau \end{aligned}$$

dla dowolnych $a, b \in K,\ \sigma, \tau \in \mathsf{End}\, V$. Widzimy więc, że działanie zewnętrzne

$$K \times \mathsf{End}\, V \to \mathsf{End}\, V, \quad (a, \tau) \mapsto a\tau$$

ma wszystkie własności wymagane od mnożenia wektorów przez skalary w przestrzeni wektorowej. Zatem $\mathsf{End}_K V$ (z dodawaniem endomorfizmów i mnożeniem endomorfizmów przez skalary) jest przestrzenią wektorową nad ciałem K.

Należy jeszcze zauważyć, że mnożenie endomorfizmów w $\mathsf{End}_K V$ oraz mnożenie endomorfizmów przez skalary są związane następującą własnością:

$$a(\sigma \cdot \tau) = a\sigma \cdot \tau = \sigma \cdot a\tau$$

dla dowolnych $\sigma, \tau \in \mathsf{End}_K V$ oraz $a \in K$. W ten sposób pierścień $\mathsf{End}_K V$ możemy traktować jako $K-$*algebrę*.

Definicja **8.1.1.** Niech E będzie przestrzenią wektorową nad ciałem K. Mówimy, że E jest K-algebrą (albo algebrą nad ciałem K) jeśli w E jest określone działanie binarne zwane mnożeniem lub mnożeniem wewnętrznym w E i spełnione są następujące warunki:

(a) E jest pierścieniem ze względu na dodawanie wektorów i mnożenie wewnętrzne.
(b) Mnożenie wewnętrzne w E i mnożenie wektorów przez skalary spełniają następujący warunek:

$$a(s \cdot t) = as \cdot t = s \cdot at \quad \text{dla wszystkich} \quad a \in K,\ s, t \in E.$$

Wymiarem $\dim_K E$ algebry E nazywamy wymiar $\dim_K E$ przestrzeni wektorowej E nad ciałem K. Jeśli mnożenie wewnętrzne w E jest przemienne, to E nazywamy $K-$algebrą przemienną.

Element zerowy algebry E oznaczamy 0_E lub 0, podobnie jedynkę algebry E oznaczamy 1_E lub 1. W algebrze endomorfizmów $\mathsf{End}_K V$ zamiast $0_{\mathsf{End}\, V}$ oraz $1_{\mathsf{End}\, V}$ piszemy 0_V i 1_V.

Jeśli E jest $K-$algebrą i $H \subseteq E$ jest podprzestrzenią wektorową przestrzeni E i równocześnie H jest podpierścieniem pierścienia E, to H także spełnia warunki (a) i (b) definicji 8.1.1 i wobec tego H jest także $K-$algebrą. Nazywamy ją *podalgebrą* algebry E.

Uwaga 8.1.2. Następująca analiza definicji $K-$algebry objaśnia rolę warunku (b) w definicji 8.1.1. Fakt, że przestrzeń wektorowa E jest pierścieniem sprowadza się do spełnienia trzech warunków:
(a_1) istnieje element $1_E \in E$ taki, że $1_E \cdot t = t \cdot 1_E = t$ dla wszystkich $t \in E$.
(a_2) mnożenie wewnętrzne w E jest działaniem łącznym,
(a_3) mnożenie wewnętrzne w E jest rozdzielne względem dodawania w E.

Niech $\beta : E \times E \to E$ będzie mnożeniem wewnętrznym w $K-$algebrze E, to znaczy $\beta(s,t) = st$ dla $s,t \in E$. Wtedy (a_3) i (b) można zapisać następująco:

$$\begin{aligned} \beta(r+s,t) &= \beta(r,t) + \beta(s,t), \\ \beta(r,s+t) &= \beta(r,s) + \beta(r,t), \\ a\beta(s,t) &= \beta(as,t) = \beta(s,at) \end{aligned}$$

dla wszystkich $r,s,t \in E$ oraz $a \in K$. Warunki te stwierdzają, że β jest operacją addytywną (warunek (a_3)) i jednorodną (warunek (b)) ze względu na każdą zmienną. Zatem β jest *odwzorowaniem dwuliniowym* przestrzeni wektorowej E w E.
Tak więc K-algebra E jest przestrzenią wektorową nad ciałem K, w której jest określone *dwuliniowe* mnożenie wewnętrzne spełniające warunki (a_1) i (a_2).

Przypomnimy teraz standardowe przykłady $K-$algebr.

Przykład 8.1.1. Przede wszystkim $\mathsf{End}_K V$ jest $K-$algebrą. Dalej, niech $M_n(K)$ będzie zbiorem wszystkich $n \times n$ macierzy (macierzy o n kolumnach i n wierszach) o elementach z ciała K. Jak już zauważyliśmy w przykładzie 2.1.4, $M_n(K)$ jest pierścieniem ze względu na dodawanie i mnożenie macierzy. Ponadto, $M_n(K)$ jest przestrzenią wektorową nad ciałem K z dodawaniem macierzy i działaniem zewnętrznym określonym następująco:

$$a \cdot [a_{ij}] := [aa_{ij}] \quad \text{dla} \quad a \in K.$$

Mnożenie macierzy jest łączne i dwuliniowe a jedynką mnożenia jest macierz jednostkowa $I \in M_n(K)$ spełniająca $I \cdot M = M \cdot I = M$ dla każdej macierzy $M \in M_n(K)$. A więc $M_n(K)$ jest K-algebrą. Zauważmy, że zbiór macierzy

$$\{M_{ij} \in M_n(K) : 1 \leqslant i,j \leqslant n\}$$

gdzie M_{ij} jest macierzą, która w $i-$tym wierszu i $j-$tej kolumnie ma 1 a na pozostałych miejscach zera, jest bazą algebry $M_n(K)$. Nazywamy ją *bazą standardową* algebry $M_n(K)$. Zarówno liniowa niezależność macierzy M_{ij} jak i fakt, że rozpinają one przestrzeń $M_n(K)$ wynika z tożsamości $[a_{ij}] = \sum_{i,j} a_{ij} M_{ij}$. Zatem

$$\dim_K M_n(K) = n^2.$$

Bezpośrednim rachunkiem sprawdzamy następującą tabelkę mnożenia macierzy M_{ij}:

$$M_{ij} \cdot M_{kl} = \begin{cases} M_{il} & \text{gdy} \quad j = k, \\ 0 & \text{gdy} \quad j \neq k. \end{cases} \tag{8.1}$$

W szczególności mamy więc $M_{12} \cdot M_{21} = M_{11} \neq M_{22} = M_{21} \cdot M_{12}$, skąd wynika, że dla $n > 1$ algebra $M_n(K)$ jest nieprzemienna.

Zauważmy jeszcze, że definicje działań w algebrze macierzy $M_n(K)$ jak również dowody odpowiednich własności tych działań nie wykorzystują faktu, że mnożenie w K jest przemienne. Wykorzystuje się jedynie fakt, że K jest K-algebrą. Wobec tego, jeśli A jest dowolną $K-$algebrą, to te same definicje działań na macierzach określają strukturę $K-$algebry na zbiorze $M_n(A)$ wszystkich $n \times n$ macierzy o elementach w K-algebrze A. Łatwo stwierdzić, że $\dim_K M_n(A) = n^2 \dim_K A$.

Przykład 8.1.2. Innym typowym przykładem $K-$algebry jest pierścień $K[X]$ wielomianów jednej zmiennej o współczynnikach w ciele K. Także pierścień $K[X_1, \ldots, X_n]$ wielomianów wielu zmiennych o współczynnikach w ciele K jest $K-$algebrą. Ciało funkcji wymiernych $K(X_1, \ldots, X_n)$ jest również $K-$algebrą. Są to przykłady $K-$algebr nieskończenie wymiarowych.
Rozpatrywany w rozdziale poprzednim pierścień $k[V]$ funkcji wielomianowych na zbiorze algebraicznym $V \subseteq k^n$ jest $k-$algebrą. Nazywa się ją także *algebrą afiniczną* zbioru algebraicznego V. Jeśli V jest rozmaitością algebraiczną, to ciało funkcji wymiernych $k(V)$ na rozmaitości V jest $k-$algebrą.

Definicja **8.1.3.** Niech E i F będą K-algebrami. *Homomorfizmem* $K-$algebry E w $K-$algebrę F nazywamy odwzorowanie $h : E \to F$ spełniające warunki

$$h(as) = ah(s), \quad h(s+t) = h(s) + h(t), \quad h(s \cdot t) = h(s) \cdot h(t), \quad h(1_E) = 1_F$$

dla wszystkich $a \in K$, $s, t \in E$. *Izomorfizmem* K-algebr nazywamy bijektywny homomorfizm K-algebr.

A więc homomorfizm algebr jest równocześnie homomorfizmem przestrzeni wektorowych i homomorfizmem pierścieni. Przypomnijmy przykład izomorfizmu $K-$algebr znany z kursu algebry liniowej.

Przykład 8.1.3. Niech V będzie n-wymiarową przestrzenią wektorową nad ciałem K. Wtedy mamy następujący izomorfizm K-algebr:

$$\mathsf{End}_K V \cong M_n(K).$$

Okazuje się, że z każdą bazą $\mathcal{B}$ przestrzeni wektorowej V związany jest pewien izomorfizm algebr $\mathsf{End}_K V$ i $M_n(K)$. Jeśli bowiem $\mathcal{B}$ jest bazą V, to każdemu endomorfizmowi τ przestrzeni V przyporządkowujemy macierz $\mathsf{m}(\tau)$ endomorfizmu τ względem bazy $\mathcal{B}$. Przypomnijmy, że jeśli $\mathcal{B} = \{v_1, \ldots, v_n\}$ jest bazą przestrzeni wektorowej V, to każdy wektor $\tau(v_j)$ przedstawiamy jako kombinację liniową wektorów bazy $\mathcal{B}$:

$$\tau(v_j) = \sum_{i=1}^{n} b_{ij} v_i,$$

gdzie b_{ij} są jednoznacznie określonymi elementami ciała K.
Macierz $\mathsf{m}(\tau, \mathcal{B}) := [b_{ij}] \in M_n(K)$ nazywa się *macierzą endomorfizmu τ w bazie $\mathcal{B}$*. Jeśli baza $\mathcal{B}$ jest ustalona to macierz $\mathsf{m}(\tau, \mathcal{B})$ oznaczamy także $\mathsf{m}(\tau)$. Łatwo stwierdzić, że przyporządkowanie $\tau \mapsto \mathsf{m}(\tau)$ jest bijekcją $\mathsf{End}_K V$ na $M_n(K)$.
Ponadto, dla dowolnych $\sigma, \tau \in \mathsf{End}_K V$ oraz dowolnego $a \in K$ mamy

$$\begin{aligned} \mathsf{m}(\sigma + \tau, \mathcal{B}) &= \mathsf{m}(\sigma, \mathcal{B}) + \mathsf{m}(\tau, \mathcal{B}), \\ \mathsf{m}(a\tau, \mathcal{B}) &= a\,\mathsf{m}(\tau, \mathcal{B}). \end{aligned}$$

Jeśli bowiem

$$\sigma(v_j) = \sum_{i=1}^{n} a_{ij} v_i, \quad \tau(v_j) = \sum_{i=1}^{n} b_{ij} v_i$$

to

$$(\sigma + \tau)(v_j) = \sum_{i=1}^{n} (a_{ij} + b_{ij}) v_i,$$

oraz

$$a\tau(v_j) = \sum_{i=1}^{n} a b_{ij} v_i$$

co oznacza, że $\mathsf{m}(\sigma + \tau, \mathcal{B}) = \mathsf{m}(\sigma, \mathcal{B}) + \mathsf{m}(\tau, \mathcal{B})$ oraz $\mathsf{m}(a\tau, \mathcal{B}) = a\,\mathsf{m}(\tau, \mathcal{B})$.
Dalej, dla dowolnych $\sigma, \tau \in \mathsf{End}_K V$ mamy także

$$\begin{aligned} (\sigma \cdot \tau)(v_j) &= \sigma(\tau(v_j)) = \sigma(\sum_{i=1}^{n} b_{ij} v_i) = \sum_{i=1}^{n} b_{ij} \sigma(v_i) = \sum_{i=1}^{n} b_{ij} \sum_{k=1}^{n} a_{ki} v_k \\ &= \sum_{k=1}^{n} (\sum_{i=1}^{n} a_{ki} b_{ij}) v_k, \end{aligned}$$

skąd wynika, że element c_{kj} macierzy endomorfizmu $\sigma \cdot \tau$ w bazie $\mathcal{B}$ ma postać

$$c_{kj} = \sum_{k=1}^{n} a_{ki} b_{ij}.$$

Jest to więc element $k-$tego wiersza i $j-$tej kolumny iloczynu macierzy $[a_{ij}] \cdot [b_{ij}]$.
Bijektywne odwzorowanie

$$\mathsf{End}_K V \to M_n(K), \quad \tau \mapsto \mathsf{m}(\tau)$$

ma więc następujące własności

$$\mathsf{m}(a\sigma) = a\mathsf{m}(\sigma), \quad \mathsf{m}(\sigma + \tau) = \mathsf{m}(\sigma) + \mathsf{m}(\tau), \quad \mathsf{m}(\sigma \cdot \tau) = \mathsf{m}(\sigma) \cdot \mathsf{m}(\tau), \quad \mathsf{m}(1_V) = I$$

dla wszystkich $a \in K,\ \sigma, \tau \in \mathsf{End}_K V$, jest więc izomorfizmem K-algebr. Izomorficzne algebry mają oczywiście równe wymiary, zatem wobec $\dim_K M_n(K) = n^2$ mamy

$$\dim_K V = n < \infty \quad \Rightarrow \quad \dim \mathsf{End}_K V = n^2.$$

Jak już wiemy, zbiór macierzy $\{M_{ij} \in M_n(K) : 1 \leqslant i, j \leqslant n\}$, gdzie M_{ij} jest macierzą, która w $i-$tym wierszu i $j-$tej kolumnie ma 1 a na pozostałych miejscach zera, jest bazą algebry $M_n(K)$. Wobec tego przeciwobraz tej bazy poprzez

izomorfizm $\mathsf{m} : \mathsf{End}_K V \to M_n(K)$ jest bazą algebry $\mathsf{End}_K V$. Opiszemy ją nieco dokładniej. Niech $\mathcal{B} = \{v_1, \ldots, v_n\}$ będzie bazą przestrzeni V. Dla każdej pary liczb naturalnych i, j niewiększych od n obieramy endomorfizm τ_{ij} przestrzeni V taki, że $\mathsf{m}(\tau_{ij}, \mathcal{B}) = M_{ij}$. Wtedy $\tau_{ij}(v_j) = v_i$, natomiast dla $k \neq j$ kolumna o numerze k macierzy M_{ij} jest zerowa, zatem $\tau_{ij}(v_k) = 0$. Możemy więc krótko opisać działanie endomorfizmu τ_{ij} na wektorach bazowych w sposób następujący:

$$\tau_{ij}(v_k) = \delta_{jk} v_i, \quad k = 1, \ldots, n,$$

gdzie δ_{jk} jest *deltą Kroneckera*, $\delta_{jk} = 1$ gdy $j = k$ oraz $\delta_{jk} = 0$ gdy $j \neq k$.
Bazę $\{\tau_{ij} : 1 \leqslant i, j \leqslant n\}$ nazywamy *bazą standardową* algebry endomorfizmów $\mathsf{End}_K V$ wyznaczoną przez bazę $\mathcal{B}$ przestrzeni V. Zatem izomorfizm m przeprowadza bazę standardową algebry $\mathsf{End}_K V$ na bazę standardową algebry $M_n(K)$.

Okazuje się, że algebry endomorfizmów przestrzeni wektorowych odgrywają w teorii algebr taką rolę jak grupy symetryczne w teorii grup. Wynika to z następującego faktu.

TWIERDZENIE **8.1.4.** *Każda $K-$algebra jest izomorficzna z podalgebrą algebry endomorfizmów $\mathsf{End}_K V$ pewnej przestrzeni wektorowej V nad ciałem K.*

Dowód. Niech E będzie $K-$algebrą. Wtedy E jest przestrzenią wektorową nad ciałem K i wobec tego możemy rozpatrywać algebrę endomorfizmów $\mathsf{End}_K E$ tej przestrzeni wektorowej. Pokażemy, że algebra E jest izomorficzna z podalgebrą algebry endomorfizmów $\mathsf{End}_K E$ przestrzeni wektorowej E.
Dla każdego $s \in E$ rozpatrujemy odwzorowanie $\tau_s : E \to E$ określone następująco: $\tau_s(v) = sv$ dla każdego $v \in E$. Tutaj sv jest iloczynem elementów algebry E. Łatwo sprawdza się, że τ_s jest endomorfizmem przestrzeni wektorowej E. Dla $u, v \in E$ mamy bowiem na podstawie rozdzielności mnożenia względem dodawania w E

$$\tau_s(u + v) = s(u + v) = su + sv = \tau_s(u) + \tau_s(v),$$

oraz dla $a \in K$, $v \in E$ mamy

$$\tau_s(av) = s(av) = a(sv) = a\tau_s(v).$$

Określamy teraz odwzorowanie

$$\varphi : E \to \mathsf{End}\, E, \quad \varphi(s) = \tau_s.$$

Rutynowe rachunki pokazują, że φ jest homomorfizmem $K-$algebr, to znaczy,

$$\varphi(as + bt) = a\varphi(s) + b\varphi(t), \quad \varphi(s \cdot t) = \varphi(s) \cdot \varphi(t), \quad \varphi(1) = 1_E$$

dla każdych $a, b \in K$, $s, t \in E$. Jądrem tego homomorfizmu jest zbiór tych $s \in E$ dla których $\varphi(s) = \tau_s$ jest endomorfizmem zerowym 0_E. A więc $s \in \ker \varphi$ pociąga, że $sv = 0$ dla każdego $v \in E$. W szczególności więc $s = s \cdot 1 = 0$, skąd wynika, że $\ker \varphi = \{0\}$. Zatem φ jest różnowartościowym homomorfizmem i wobec tego jest izomorfizmem algebry E na podalgebrę $\varphi(E)$ algebry $\mathsf{End}_K E$. □

8.2 Algebry z dzieleniem i algebry proste

Algebry z dzieleniem i algebry proste są w klasie pierścieni nieprzemiennych odpowiednikami ciał. Jedna z możliwych charakteryzacji ciał w klasie pierścieni przemiennych polega na wyodrębnieniu pierścieni, w których każdy różny od zera element jest odwracalny. Przeniesienie tej charakteryzacji do klasy wszystkich pierścieni (niekoniecznie przemiennych) prowadzi do następującej definicji.

DEFINICJA **8.2.1.** $K-$algebra E nazywa się algebrą *z dzieleniem*, jeśli każdy różny od zera element algebry E jest odwracalny w E.

Najprostszymi przykładami algebr z dzieleniem są rozszerzenia ciał: jeśli K jest podciałem ciała E, to E jest przemienną $K-$algebrą i oczywiście jest to algebra z dzieleniem. W ten sposób nad ciałem $\mathbb{R}$ liczb rzeczywistych otrzymujemy dwie przemienne $\mathbb{R}-$algebry z dzieleniem: $\mathbb{R}$ i $\mathbb{C}$. Okazuje się, że nad $\mathbb{R}$ nie ma już innych przemiennych skończenie wymiarowych algebr z dzieleniem. Każda taka algebra jest ciałem i jest skończonym rozszerzeniem ciała $\mathbb{R}$, a więc jest to jedynie $\mathbb{R}$ lub $\mathbb{C}$. Można też udowodnić, że nad $\mathbb{R}$ nie istnieje $3-$wymiarowa algebra z dzieleniem. Natomiast nad $\mathbb{R}$ istnieje $4-$wymiarowa algebra z dzieleniem $\mathbb{H}$ zwana *algebrą kwaternionów Hamiltona*.

Konstrukcję algebry $\mathbb{H}$ można opisać następująco. W dowolnej $4-$wymiarowej przestrzeni wektorowej nad $\mathbb{R}$ obieramy jakąkolwiek bazę i jej elementy oznaczamy $\mathbf{1}, i, j, k$. Definiując wewnętrzne mnożenie w $\mathbb{H}$ zakładamy, że będzie ono rozdzielne względem dodawania i wobec tego wystarczy jedynie wskazać reguły mnożenia elementów bazowych. Kluczowe są następujące definicje:

$$\mathbf{1} = 1_{\mathbb{H}}, \quad i^2 = -\mathbf{1}, \quad j^2 = -\mathbf{1}, \quad i \cdot j = k = -j \cdot i. \tag{8.2}$$

Jeśli, na przykład, chcemy znaleźć $k \cdot j$, to możemy postępować następująco:

$$k \cdot j = (i \cdot j) \cdot j = i \cdot j^2 = i \cdot (-\mathbf{1}) = -i.$$

W ten sposób używając tylko (8.2) sprawdzamy, że

$$j \cdot k = i = -k \cdot j, \quad k \cdot i = j = -i \cdot k, \quad k^2 = -\mathbf{1}.$$

Ponieważ zakładamy rozdzielność mnożenia względem dodawania, potrafimy teraz jednoznacznie obliczyć iloczyn dowolnych dwóch *kwaternionów* $(x_0\mathbf{1} + x_1 i + x_2 j + x_3 k)(y_0\mathbf{1} + y_1 i + y_2 j + y_3 k)$. W ten sposób $4-$wymiarowa przestrzeń wektorowa $\mathbb{H}$ staje się algebrą nad ciałem $\mathbb{R}$ liczb rzeczywistych.

Istnieje też bardziej geometryczne podejście do definicji algebry kwaternionów Hamiltona. W $4-$wymiarowej przestrzeni

$$\mathbb{H} = \mathbb{R}\mathbf{1} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k,$$

której wektory nazywamy kwaternionami, wyróżniamy dwie podprzestrzenie, 1-wymiarową podprzestrzeń $\mathbb{R}\mathbf{1}$ kwaternionów *skalarnych* oraz 3-wymiarową podprzestrzeń

$$\mathbb{H}_0 := \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$$

kwaternionów *czystych*. Zauważmy, że $\mathbb{H} = \mathbb{R}\mathbf{1} \oplus \mathbb{H}_0$, zatem każdy kwaternion ma jednoznaczne przedstawienie w postaci sumy kwaternionu skalarnego i kwaternionu czystego. Mnożenie kwaternionów definiujemy w dwóch krokach. Dla kwaternionów $p = x_0\mathbf{1} + p_0,\ q = y_0\mathbf{1} + q_0$, gdzie $x_0, y_0 \in \mathbb{R}$ i p_0, q_0 są kwaternionami czystymi, pierwsza reguła jest następująca:

$$p \cdot q = (x_0\mathbf{1} + p_0) \cdot (y_0\mathbf{1} + q_0) = x_0y_0\mathbf{1} + x_0q_0 + y_0p_0 + p_0 \cdot q_0, \tag{8.3}$$

gdzie iloczyn $p_0 \cdot q_0$ kwaternionów czystych będzie określony drugą regułą mnożenia. Dla wprowadzenia drugiej reguły traktujemy przestrzeń $\mathbb{H}_0$ kwaternionów czystych jako przestrzeń euklidesową ze standardowym iloczynem skalarnym

$$(p_0, q_0) = x_1y_1 + x_2y_2 + x_3y_3$$

dla $p_0 = x_1i + x_2j + x_3k,\ q_0 = y_1i + y_2j + y_3k \in \mathbb{H}_0$. W przestrzeni euklidesowej $\mathbb{H}_0$ mamy także określony *iloczyn wektorowy*

$$[p_0, q_0] := \det \begin{bmatrix} i & j & k \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{bmatrix} = (x_2y_3 - x_3y_2)i + (x_3y_1 - x_1y_3)j + (x_1y_2 - x_2y_1)k$$

z pożyteczną interpretacją geometryczną (wektor $[p_0, q_0]$ jest prostopadły do obydwu wektorów p_0 i q_0 oraz jego długość jest równa polu równoległoboku rozpiętego na p_0, q_0). Przy tym jest rzeczą istotną, że iloczyn wektorowy $[\ ,\ ] : \mathbb{H}_0 \times \mathbb{H}_0 \to \mathbb{H}_0$ jest odwzorowaniem dwuliniowym. Wykorzystamy teraz iloczyn skalarny i iloczyn wektorowy p_0 i q_0 by zdefiniować iloczyn czystych kwaternionów:

$$p_0 \cdot q_0 := -(p_0, q_0)\mathbf{1} + [p_0, q_0]. \tag{8.4}$$

Wykorzystując reguły (8.3) i (8.4), określamy zatem iloczyn dowolnych kwaternionów $p, q \in \mathbb{H}$. Jest rzeczą oczywistą, że tak określone mnożenie jest dwuliniowe. Mniej trywialnym ćwiczeniem jest sprawdzenie łączności mnożenia, które pomijamy. Natomiast łatwo stwierdzić, że $\mathbf{1}$ jest jedynką algebry $\mathbb{H}$. Rzeczywiście,

$$\mathbf{1} \cdot q = (1\mathbf{1} + 0) \cdot (y_0\mathbf{1} + q_0) = y_0\mathbf{1} + q_0 = q$$

zgodnie z (8.3) i (8.4), i podobnie $q \cdot \mathbf{1} = q$. W ten sposób skonstruowaliśmy 4-wymiarową algebrę kwaternionów Hamiltona. Łatwo sprawdzić, że ta konstrukcja daje dokładnie tę samą algebrą, którą opisaliśmy wcześniej przy pomocy reguł mnożenia (8.2). Rzeczywiście,

$$i \cdot j = -(i,j)\mathbf{1} + [i,j] = [i,j] = k \quad \text{oraz} \quad j \cdot i = -(j,i)\mathbf{1} + [j,i] = [j,i] = -k,$$
$$i^2 = -(i,i)\mathbf{1} + [i,i] = -1\mathbf{1} = -\mathbf{1} \quad \text{oraz} \quad j^2 = -(j,j)\mathbf{1} + [j,j] = -1\mathbf{1} = -\mathbf{1}.$$

Niech teraz $p = x_0\mathbf{1} + p_0 \in \mathbb{H}$, gdzie $p_0 = x_1i + x_2j + x_3k \in \mathbb{H}_0$. Kwaternion $\overline{p} := x_0\mathbf{1} - p_0$ nazywa się kwaternionem *sprzężonym* z p, natomiast iloczyn $p \cdot \overline{p}$ nazywa się *normą* kwaternionu p i oznacza $N(p)$. Zatem

$$\begin{aligned} N(p) = p \cdot \overline{p} &= x_0^2\mathbf{1} + x_0(-p_0) + x_0p_0 - p_0^2 = x_0^2\mathbf{1} - p_0^2 \\ &= x_0^2\mathbf{1} + (p_0, p_0)\mathbf{1} - [p_0, p_0] = x_0^2\mathbf{1} + (p_0, p_0)\mathbf{1} \\ &= (x_0^2 + x_1^2 + x_2^2 + x_3^2)\mathbf{1}. \end{aligned}$$

Wykorzystując tę formułę dla normy kwaternionu udowodnimy teraz z łatwością następujący fakt.

STWIERDZENIE **8.2.2.** $\mathbb{R}-$*algebra kwaternionów* $\mathbb{H}$ *jest algebrą z dzieleniem.*

Dowód. Niech $p \in \mathbb{H}$ będzie niezerowym kwaternionem. Wtedy jego norma $p \cdot \overline{p} = x\mathbf{1}$ jest niezerowym kwaternionem skalarnym, a więc x jest różną od zera liczbą rzeczywistą (sumą kwadratów współrzędnych kwaternionu p). Wobec tego

$$p \cdot x^{-1}\overline{p} = \mathbf{1},$$

co dowodzi, że p jest odwracalny (oraz $p^{-1} = x^{-1}\overline{p}$). □

Rolę algebry kwaternionów Hamiltona podkreśla udowodnione w roku 1877 twierdzenie G. Frobeniusa mówiące, że nad ciałem $\mathbb{R}$ liczb rzeczywistych jedynymi skończenie wymiarowymi algebrami z dzieleniem są (z dokładnością do izomorfizmu) $\mathbb{R}, \mathbb{C}$ oraz $\mathbb{H}$.

Przystępujemy teraz do wprowadzenia algebr *prostych*. Jak wiemy, ciała można scharakteryzować wśród pierścieni przemiennych nie tylko poprzez odwracalność wszystkich elementów niezerowych. Pierścień przemienny K jest ciałem wtedy i tylko wtedy, gdy ma tylko dwa ideały: ideał zerowy $0 = 0K$ oraz ideał jednostkowy $K = 1K$. Wykorzystamy tę charakteryzację ciał dla wprowadzenia klasy algebr *prostych*.

DEFINICJA **8.2.3.** Algebrę E nad ciałem K nazywamy *prostą* K-algebrą, jeśli ideał zerowy 0 oraz cała algebra E są jedynymi ideałami algebry E.

Przykład 8.2.1. Jeśli ciało K jest podciałem ciała E, to E jest prostą K-algebrą. Natomiast K-algebra $K[X]$ nie jest prosta, gdyż wszystkie ideały główne pierścienia $K[X]$ generowane przez wielomiany stopni dodatnich są różne od 0 i $K[X]$.

Każda algebra z dzieleniem jest prosta. Niech bowiem $\mathfrak{a}$ będzie niezerowym ideałem algebry z dzieleniem E. Niech $s \in \mathfrak{a}$ i $s \neq 0$. Wtedy s jest elementem odwracalnym w E, zatem istnieje element $t \in E$ taki, że $st = 1_E$. Wtedy $1_E = st \in \mathfrak{a}$, skąd wynika, że $E = \mathfrak{a}$. Tak więc każdy niezerowy ideał algebry z dzieleniem E jest równy całej algebrze E. Zatem E jest prostą $K-$algebrą. W szczególności więc, algebra $\mathbb{H}$ kwaternionów Hamiltona jest $\mathbb{R}-$algebrą prostą.

8.3 Centralność i prostota algebry endomorfizmów

Centrum $K-$algebry E nazywamy centrum pierścienia E,

$$\mathsf{Z}(E) := \Big\{ s \in E : st = ts \text{ dla wszystkich } t \in E \Big\}.$$

Centrum pierścienia E jest podpierścieniem pierścienia E i jest także podprzestrzenią przestrzeni wektorowej E. Rzeczywiście, jeśli $s \in \mathsf{Z}(E)$ oraz $a \in K$, to dla każdego $t \in E$ mamy

$$as \cdot t = a(s \cdot t) = a(t \cdot s) = t \cdot as,$$

zatem $as \in \mathsf{Z}(E)$. Centrum $\mathsf{Z}(E)$ jest więc podalgebrą algebry E. W szczególności, ponieważ jedynka 1_E należy do centrum, zatem także zbiór $K1_E := \{a1_E : a \in K\}$ skalarnych krotności jedynki algebry E zawiera się w centrum algebry E:

$$K1_E \subseteq \mathsf{Z}(E). \tag{8.5}$$

DEFINICJA **8.3.1.** K-algebra E nazywa się algebrą *centralną*, jeśli $K1_E = \mathsf{Z}(E)$.

Można więc powiedzieć, że nieprzemienna centralna K-algebra E jest w wysokim stopniu nieprzemienna. Jedynymi elementami centralnymi takiej algebry są elementy skalarne.

TWIERDZENIE **8.3.2.** *Algebra endomorfizmów* $\mathsf{End}_K V$ *dowolnej przestrzeni wektorowej nad dowolnym ciałem* K *jest centralną* $K-$*algebrą.*

Dowód. Jeśli $\dim_K V = 1$, to $\mathsf{End}_K V \cong M_1(K) \cong K$, zatem $\mathsf{Z}(\mathsf{End}_K V) = \mathsf{End}_K V = K1_V$. Możemy więc założyć, że $\dim V > 1$. Przy tym założeniu udowodnimy równoważność trzech następujących warunków:

(a) $\sigma \in \mathsf{Z}(\mathsf{End}_K V)$.

(b) σ zachowuje wszystkie proste w przestrzeni V (to znaczy $\sigma(Kv) = Kv$ dla każdego $v \in V$).

(c) $\sigma \in K1_V$.

(a) $\Rightarrow$ (b). Przypuśćmy, że endomorfizm σ przestrzeni V należy do centrum $\mathsf{End}_K V$ ale nie zachowuje wszystkich prostych przestrzeni V.
Dla pewnych wektorów $v, w \in V$ mamy więc $\sigma(v) = w \notin Kv$. Wtedy v i w są liniowo niezależne, istnieje więc endomorfizm ρ taki, że $\rho(v) = v$ oraz $\rho(w) \notin Kw$. Zatem

$$\sigma\rho(v) = \sigma(v) = w, \quad \rho\sigma(v) = \rho(w) \notin Kw,$$

skąd wynika, że $\sigma\rho \neq \rho\sigma$ i wobec tego σ nie należy do centrum $\mathsf{End}_K V$, sprzeczność.

(b) $\Rightarrow$ (c) Załóżmy, że σ zachowuje wszystkie proste w przestrzeni V. Niech u, v będą liniowo niezależnymi wektorami przestrzeni V oraz $\sigma(u) = au$, $\sigma(v) = bv$ dla pewnych $a, b \in K$. Wtedy istnieje także $c \in K$ takie, że $\sigma(u + v) = c(u + v)$. Wobec tego mamy

$$cu + cv = \sigma(u + v) = \sigma(u) + \sigma(v) = au + bv.$$

Wobec liniowej niezależności wektorów u, v otrzymujemy stąd $a = c = b$. Z drugiej strony, jeśli niezerowe wektory u, v są liniowo zależne, to $v = xu$ dla pewnego $x \in K$ i wobec tego $\sigma(v) = x\sigma(u) = axu = av$. Zatem dla każdego wektora $v \in V$ mamy $\sigma(v) = av$ co oznacza, że $\sigma = a1_V \in K1_V$.

(c) $\Rightarrow$ (a) zauważyliśmy już w (8.5). □

Uwaga 8.3.3. Łatwo stwierdzić, że jeśli $h : E \to F$ jest izomorfizmem K-algebr, to $h(\mathsf{Z}(E)) = \mathsf{Z}(F)$. W szczególności więc, jeśli E jest centralną K-algebrą, to $\mathsf{Z}(F) = h(K1_E) = Kh(1_E) = K1_F$, to znaczy, F jest także centralną K-algebrą. Z faktu, że algebra endomorfizmów $n-$wymiarowej przestrzeni wektorowej jest izomorficzna z algebrą macierzy $M_n(K)$ wynika, że algebra macierzy $M_n(K)$ jest centralną $K-$algebrą.

TWIERDZENIE **8.3.4.** *Niech* V *będzie skończenie wymiarową przestrzenią wektorową nad ciałem* K. *Wtedy algebra endomorfizmów* $\mathsf{End}_K V$ *jest prostą* $K-$*algebrą.*

Dowód. Niech $n = \dim_K V$ i niech $\mathcal{B} = \{v_1, \ldots, v_n\}$ będzie dowolną bazą przestrzeni V. Niech $\{\tau_{ij} : 1 \leqslant i, j \leqslant n\}$ będzie *bazą standardową* algebry endomorfizmów $\mathsf{End}_K V$ wyznaczoną przez bazę $\mathcal{B}$. Zatem

$$\tau_{ij}(v_k) = \delta_{jk} v_i, \quad k = 1, \ldots, n.$$

Z (8.1) otrzymujemy następującą tabelę mnożenia dla tej bazy:

$$\tau_{ij} \cdot \tau_{kl} = \begin{cases} \tau_{il} & \text{gdy} \quad j = k, \\ 0 & \text{gdy} \quad j \neq k. \end{cases} \tag{8.6}$$

Zauważmy, że endomorfizm tożsamościowy 1_V ma następujące jednoznaczne przedstawienie jako kombinacja liniowa endomorfizmów bazy standardowej:

$$1_V = \tau_{11} + \cdots + \tau_{nn}. \tag{8.7}$$

Niech teraz $\tau \in \mathsf{End}_K V$ będzie dowolnym endomorfizmem i niech

$$\tau = \sum_{i,j} a_{ij} \tau_{ij},$$

gdzie $a_{ij} \in K$ są współrzędnymi endomorfizmu τ w bazie standardowej algebry $\mathsf{End}_K V$. Wykorzystując (8.6) otrzymujemy następujące tożsamości:

$$\tau_{ii} \cdot \tau \cdot \tau_{jj} = a_{ij} \tau_{ij}. \tag{8.8}$$

Przypuśćmy teraz, że algebra $\mathsf{End}_K V$ ma niezerowy ideał $\mathfrak{a}$ i niech endomorfizm τ będzie niezerowym elementem $\mathfrak{a}$. Wtedy τ ma przynajmniej jedną niezerową współrzędną $a_{ij} \neq 0$. Ponieważ $\mathfrak{a}$ jest ideałem i $\tau \in \mathfrak{a}$, więc także $\tau_{ii} \cdot \tau \cdot \tau_{jj} \in \mathfrak{a}$, zatem wobec (8.8) mamy $a_{ij}\tau_{ij} \in \mathfrak{a}$. Wiemy także, że $\mathfrak{a}$ jest podprzestrzenią przestrzeni wektorowej A, zatem

$$a_{ij}^{-1} \cdot a_{ij} \tau_{ij} = \tau_{ij} \in \mathfrak{a}.$$

Pokazaliśmy więc, że jeśli $\tau \in \mathfrak{a}$ oraz współrzędna o numerze (i, j) endomorfizmu τ jest niezerowym skalarem, to $\tau_{ij} \in \mathfrak{a}$. Ponieważ $\mathfrak{a}$ jest ideałem, mamy także

$$\tau_{ki} \cdot \tau_{ij} \cdot \tau_{jk} \in \mathfrak{a}$$

dla wszystkich $k = 1, \ldots, n$. Z drugiej strony, wykorzystując dwukrotnie tożsamość (8.6) otrzymujemy

$$\tau_{ki} \cdot \tau_{ij} \cdot \tau_{jk} = \tau_{kk}.$$

Zatem $\tau_{kk} \in \mathfrak{a}$ dla $k = 1, \ldots, n$, i wobec (8.7) mamy

$$1_V = \tau_{11} + \cdots + \tau_{nn} \in \mathfrak{a}.$$

Stąd wynika, że każdy endomorfizm τ należy do $\mathfrak{a}$, gdyż $\tau = \tau \cdot 1_V \in \mathfrak{a}$. A więc każdy niezerowy ideał algebry endomorfizmów $\mathsf{End}_K V$ jest równy całej algebrze $\mathsf{End}_K V$. Wobec tego $\mathsf{End}_K V$ jest prostą $K-$algebrą. □

Algebry, które są równocześnie centralne i proste nazywają się *centralnymi prostymi* $K-$algebrami.

WNIOSEK **8.3.5.** *Algebra endomorfizmów* $\mathsf{End}_K V$ *skończenie wymiarowej przestrzeni wektorowej* V *nad ciałem* K *jest centralną prostą* $K-$*algebrą.*
Każda algebra macierzy $M_n(K)$ *jest centralną prostą* $K-$*algebrą.*

Można udowodnić, że każda skończenie wymiarowa centralna prosta $K-$algebra E jest izomorficzna z algebrą macierzy $M_n(D)$, gdzie D jest odpowiednio dobraną centralną $K-$algebrą z dzieleniem. Liczba n jest wyznaczona jednoznacznie, natomiast algebra D jest wyznaczona jednoznacznie z dokładnością do izomorfizmu $K-$algebr. Jest to słynne twierdzenie J. H. M. Wedderburna z 1908 roku (zob. np. O. T. O'Meara, *Introduction to Quadratic Forms*, Springer-Verlag, 1971, str. 125–127).

8.4 Wielomian minimalny endomorfizmu

Wprawdzie interesują nas przede wszystkim wielomiany minimalne endomorfizmów przestrzeni wektorowych, ale bez żadnego dodatkowego wysiłku można wprowadzić pojęcie wielomianu minimalnego elementu dowolnej $K-$algebry. Niech więc E będzie dowolną $K-$algebrą. Rozpatrzmy homomorfizm $K-$algebry $K[X]$ wielomianów jednej zmiennej w algebrę E, oparty na operacji podstawiania ustalonego elementu $t \in E$ w miejsce zmiennej wielomianu (zob. przykład 3.1.4, w którym rozpatrywaliśmy przypadek gdy $E = \mathsf{End}_K V$ jest algebrą endomorfizmów przestrzeni wektorowej V). Niech więc

$$f = a_0 + a_1 X + \cdots + a_n X^n$$

będzie wielomianem o współczynnikach z ciała K i niech $t \in E$ będzie dowolnym elementem algebry E. Wtedy określamy

$$f(t) := a_0 1_E + a_1 t + \cdots + a_n t^n.$$

Stąd wynika, że dla dowolnego wielomianu $f \in K[X]$ oraz $t \in E$ mamy $f(t) \in E$. Zauważamy teraz, że przy ustalonym $t \in E$, odwzorowanie

$$\varphi_t : K[X] \to E, \quad \varphi_t(f) = f(t)$$

jest homomorfizmem $K-$algebr. Dla dowolnych wielomianów $f, g \in K[X]$ mamy bowiem

$$(f+g)(t) = f(t) + g(t), \quad (fg)(t) = f(t) \cdot g(t),$$

oraz dla jedynki 1 algebry $K[X]$ mamy $\varphi_t(1) = 1_E$.
Ponadto, $\varphi_t(af) = (af)(t) = af(t) = a\varphi_t(t)$ dla każdego $a \in K$.
Ważną konsekwencją tego, że φ_t jest homomorfizmem pierścieni jest następujący fakt.

STWIERDZENIE **8.4.1.** *Dla każdego elementu* $t \in E$ *i dla dowolnych wielomianów* $f, g \in K[X]$ *elementy* $f(t)$ *i* $g(t)$ *algebry* E *są przemienne:*

$$f(t) \cdot g(t) = g(t) \cdot f(t).$$

W szczególności więc dla dowolnych wielomianów $f, g \in K[X]$ *i dla dowolnego endomorfizmu* τ *przestrzeni wektorowej* V *endomorfizmy* $f(\tau)$ *i* $g(\tau)$ *są przemienne.*

Dowód. Mamy bowiem $f(t) \cdot g(t) = \varphi_t(fg) = \varphi_t(gf) = g(t) \cdot f(t)$. □

Pokażemy teraz, że homomorfizm $\varphi_t : K[X] \to E$ nie jest na ogół monomorfizmem.

TWIERDZENIE **8.4.2.** *Jeśli E jest $n-$wymiarową algebrą nad ciałem K, to każdy element $t \in E$ jest zerem pewnego niezerowego wielomianu stopnia $\leqslant n$ o współczynnikach z ciała K.*

Dowód. W przestrzeni wektorowej E każdy układ $n+1$ elementów jest liniowo zależny. Dla każdego elementu $t \in E$ istnieją więc skalary $a_0, a_1, \ldots, a_n \in K$, nie wszystkie równe zero, takie, że

$$a_0 1_E + a_1 t + \cdots + a_n t^n = 0_E.$$

Oznacza to, że dla wielomianu $g = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ mamy $g \neq 0$ oraz $g(t) = 0_E$. □

WNIOSEK **8.4.3.** *Jeśli V jest $n-$wymiarową przestrzenią wektorową nad ciałem K, to każdy endomorfizm τ przestrzeni V jest zerem pewnego niezerowego wielomianu stopnia $\leqslant n^2$ o współczynnikach z ciała K.*

Dowód. Jeśli $\dim_K V = n$, to $\dim \mathsf{End}_K V = n^2$. □

Można pokazać, że każdy endomorfizm τ przestrzeni $n-$wymiarowej jest zerem pewnego wielomianu stopnia $\leqslant n$. Wynika to z klasycznego twierdzenia Cayleya-Hamiltona, ale w rozdziale 10 podamy inny dowód oparty na twierdzeniu o strukturze $K[X]-$modułu V_τ (zob. twierdzenie 10.1.11).

WNIOSEK **8.4.4.** *Dla każdego elementu t skończenie wymiarowej $K-$algebry E jądro homomorfizmu $\varphi_t : K[X] \to E$ jest niezerowym ideałem w pierścieniu wielomianów $K[X]$.*

Wiemy, że w pierścieniu wielomianów $K[X]$ każdy ideał jest główny. W szczególności $\ker \varphi_t = (p)$ jest ideałem głównym generowanym przez pewien wielomian $p \in K[X]$. Prowadzi to do następującej definicji *wielomianu minimalnego* elementu $t \in E$.

DEFINICJA **8.4.5.** Niech t będzie elementem skończenie wymiarowej $K-$algebry E. *Wielomianem minimalnym* p_t elementu t nazywamy unormowany generator p_t ideału $\ker \varphi_t$ pierścienia $K[X]$.

A więc $p_t \in K[X]$ jest wielomianem minimalnym elementu t wtedy i tylko wtedy, gdy p_t jest wielomianem unormowanym (to znaczy, najwyższy współczynnik wielomianu p_t jest równy 1) oraz $\ker \varphi_t = (p_t)$. Warunki te są równoważne temu, że p_t jest wielomianem unormowanym, $p_t(t) = 0_E$ oraz p_t dzieli każdy wielomian $f \in K[X]$ taki, że $f(t) = 0_E$.

W szczególności, każdy endomorfizm τ skończenie wymiarowej przestrzeni wektorowej V nad ciałem K ma swój wielomian minimalny $p_\tau \in K[X]$, a także każda macierz $A \in M_n(K)$ ma swój wielomian minimalny $p_A \in K[X]$.

Przykład 8.4.1. Wielomianem minimalnym endomorfizmu zerowego 0_V jest wielomian $p_{0_V} = X \in K[X]$, natomiast wielomianem minimalnym endomorfizmu tożsamościowego 1_V jest wielomian $p_{1_V} = X - 1 \in K[X]$. Jeśli σ jest endomorfizmem nilpotentnym stopnia m, to znaczy $\sigma^m = 0_V$ oraz $\sigma^{m-1} \neq 0_V$, to $p_\sigma = X^m$.

STWIERDZENIE **8.4.6.** *Niech $\varphi : E \to F$ będzie izomorfizmem skończenie wymiarowych $K-$algebr. Wtedy dla każdego elementu $t \in E$ mamy*

$$p_t = p_{\varphi(t)}.$$

W szczególności, jeśli τ jest endomorfizmem skończenie wymiarowej przestrzeni wektorowej nad ciałem K i A jest macierzą τ w dowolnej bazie przestrzeni V, to wielomiany minimalne endomorfizmu τ i macierzy A są równe:

$$p_\tau = p_A.$$

Dowód. Mamy $p_t(t) = 0$, zatem także $0 = \varphi(p_t(t)) = p_t(\varphi(t))$. Stąd $p_{\varphi(t)} \mid p_t$. Podobnie, biorąc φ^{-1} zamiast φ otrzymamy $p_t \mid p_{\varphi(t)}$. Zatem $p_t = p_{\varphi(t)}$. Odwzorowanie algebry endomorfizmów przestrzeni V w algebrę macierzy, które każdemu endomorfizmowi τ przyporządkowuje jego macierz A w ustalonej bazie przestrzeni wektorowej, jest izomorfizmem algebr (zob. przykład 8.1.3). Zatem $p_\tau = p_A$ na podstawie pierwszej części stwierdzenia. □

Przykład 8.4.2. Wielomian minimalny elementu t skończenie wymiarowej algebry E zawiera wiele ważnych informacji o elemencie t. Na przykład, jeśli wyraz wolny wielomianu minimalnego p_t elementu t jest równy zero (to znaczy, jeśli $p_t(0) = 0$), to element t jest dzielnikiem zera w algebrze E. Jeśli bowiem $p_t = a_1X + \cdots + a_{m-1}X^{m-1} + X^m$, to

$$0_E = p_t(t) = a_1t + \cdots + t^m = t(a_1 1_E + \cdots + t^{m-1}) = (a_1 1_E + \cdots + t^{m-1})t,$$

oraz $a_1 1_E + \cdots + t^{m-1} \neq 0_V$, gdyż w przeciwnym razie element t byłby zerem niezerowego wielomianu stopnia $m-1$ wbrew temu, że wielomian minimalny p_t elementu t ma stopień m.

W rozdziale 2.1 wprowadziliśmy pojęcie elementów pierścienia lewo- i prawostronnie odwracalnych oraz odwracalnych. Z przykładu 2.1.6 wynika, że w algebrze nieskończenie wymiarowej mogą istnieć elementy jednostronnie odwracalne, które jednak nie są obustronnie odwracalne (i w związku z tym nie są odwracalne).

Okazuje się, że w algebrze *skończenie wymiarowej* nie może istnieć element, który byłby jednostronnie odwracalny i równocześnie nie był odwracalny. Wynika to z następującej analizy związku między odwracalnością elementu a niezerowaniem się wyrazu wolnego wielomianu minimalnego tego elementu.

TWIERDZENIE **8.4.7.** *Dla elementu t skończenie wymiarowej $K-$algebry E następujące warunki są równoważne.*
(a) *Wyraz wolny wielomianu minimalnego elementu t jest różny od zera.*
(b) *t jest odwracalny w E.*
(c) *t jest lewostronnie odwracalny w E.*
(d) *t jest prawostronnie odwracalny w E.*

Dowód. Niech $p_t = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m$. Wtedy mamy tożsamość wielomianową

$$p_t = a_0 + Xq$$

gdzie $q := a_1 + \cdots + a_{m-1}X^{m-2} + X^{m-1}$.
(a) $\Rightarrow$ (b) Jeśli $a_0 \neq 0$, to z równości $p_t(t) = 0_E$ otrzymujemy $0_E = a_0 1_E + tq(t)$, skąd

$$1_E = t \cdot (-a_0^{-1}q(t)) = (-a_0^{-1}q(t)) \cdot t.$$

A więc t jest elementem odwracalnym oraz elementem odwrotnym do t jest

$$t^{-1} = -a_0^{-1}q(t).$$

(b) $\Rightarrow$ (a) Jeśli $a_0 = 0$, to jak już zauważyliśmy w przykładzie 8.4.2, t jest dzielnikiem zera w algebrze E (gdyż $t \cdot q(t) = q(t) \cdot t = 0_E$) i wobec tego t nie jest elementem odwracalnym.
Pozostaje pokazać, że (c) $\Rightarrow$ (b) oraz (d) $\Rightarrow$ (b) (gdyż przeciwne implikacje są trywialne).
Załóżmy (c). Wtedy istnieje element t_1 algebry E taki, że $t_1 t = 1_E$. Jeśli t nie jest odwracalny, to wobec już udowodnionej równoważności warunków (a) i (b) wyraz wolny wielomianu minimalnego p_t jest równy zero. Wobec tego dla $s = q(t)$ mamy $s \neq 0_E$ oraz $ts = 0_E$. Zatem

$$0_E = t_1(ts) = (t_1 t)s = 1_E s = s,$$

sprzeczność. A więc t jest odwracalny. Podobnie dowodzi się, że (d) $\Rightarrow$ (b). □

Twierdzenie **8.4.8.** *Dla elementu t skończenie wymiarowej $K-$algebry E następujące warunki są równoważne.*
(a) *Wyraz wolny wielomianu minimalnego elementu t jest równy zero.*
(b) *t jest dzielnikiem zera w E.*
(c) *t jest lewostronnym dzielnikiem zera w E.*
(d) *t jest prawostronnym dzielnikiem zera w E.*

Dowód. Każdy z warunków (b), (c), (d) pociąga (a), gdyż jednostronny a tym bardziej obustronny dzielnik zera nie jest elementem odwracalnym. Natomiast jeśli założymy (a), to w oznaczeniach dowodu twierdzenia 8.4.7 mamy $t \cdot q(t) = q(t) \cdot t = 0_E$ oraz $q(t) \neq 0_E$. Wobec tego (a) pociąga (b) i tym bardziej (c) i (d). □

Wniosek **8.4.9.** *Jeśli element t skończenie wymiarowej $K-$algebry E nie jest odwracalny w E, to jest dzielnikiem zera w E.*

Według naszej definicji dzielnika zera (w rozdziale 2.1) element t jest dzielnikiem zera w E jeśli jest równocześnie lewostronnym i prawostronnym dzielnikiem zera. Oznacza to, że istnieją $s_1, s_2 \in E$ takie, że $ts_1 = s_2 t = 0_E$. Zanotujmy zauważony już wcześniej fakt, że w tej sytuacji zawsze można dobrać $s_1 = s_2$.

Wniosek **8.4.10.** *Jeśli element t jest dzielnikiem zera w E, to istnieje taki element $s \in E$, że*

$$ts = st = 0_E.$$

Dowód. W oznaczeniach dowodu twierdzenia 8.4.7 wystarczy przyjąć $s = q(t)$. □

8.5 Endomorfizmy odwracalne

Opisane w twierdzeniach 8.4.7 i 8.4.8 charakteryzacje elementów odwracalnych i dzielników zera a także wnioski z nich stosują się oczywiście do endomorfizmów skończenie wymiarowych przestrzeni wektorowych. Charakteryzacje te mają dość formalny charakter i nie biorą pod uwagę faktu, że elementy $K-$algebry $\mathsf{End}_K V$ są funkcjami (homomorfizmami) $V \to V$. Przy tym przestrzeń wektorowa V nad ciałem K jest wolnym $K-$modułem, zatem jeśli $\mathcal{B}$ jest bazą V to endomorfizm $\tau : V \to V$ jest jednoznacznie wyznaczony poprzez swoje wartości na bazie $\mathcal{B}$.
Uwzględniając ten punkt widzenia podamy teraz dobrze znaną charakteryzację endomorfizmów odwracalnych jako bijektywnych homomorfizmów (czyli izomorfizmów) przestrzeni V na siebie. Przedtem jednak przypomnijmy terminologię stosowaną na ogół w algebrze liniowej.

Definicja **8.5.1.** Endomorfizm τ przestrzeni wektorowej V nazywa się endomorfizmem *nieosobliwym*, jeśli $\ker \tau = 0$.
Endomorfizm τ nazywa się endomorfizmem *osobliwym*, jeśli nie jest nieosobliwy, to znaczy, jeśli istnieje wektor $v \in V$ taki, że $v \neq 0$ i $\tau(v) = 0$.

A więc endomorfizm $\tau : V \to V$ jest nieosobliwy wtedy i tylko wtedy, gdy jest odwzorowaniem injektywnym (różnowartościowym), natomiast τ jest osobliwy wtedy i tylko wtedy, gdy ma niezerowe jądro.
Podstawą do powiązania nieosobliwości endomorfizmu z własnościami, które zależą od wielomianu minimalnego endomorfizmu jest następujący lemat.

Lemat **8.5.2.** *Niech $\tau : V \to V$ będzie endomorfizmem skończenie wymiarowej przestrzeni wektorowej nad ciałem K. Wtedy*

$$\dim_K V = \dim_K \ker \tau \ + \ \dim_K \operatorname{im} \tau.$$

Dowód. Rozpatrzmy przestrzeń ilorazową $V/\ker \tau$. Na podstawie twierdzenia o homomorfizmach przestrzeni wektorowych mamy izomorfizm

$$\operatorname{im} \tau \cong V/\ker \tau.$$

Z drugiej strony, dla dowolnej podprzestrzeni U przestrzeni V mamy

$$\dim_K V/U = \dim_K V - \dim_K U.$$

Jeśli bowiem $\{v_1, \ldots, v_k\}$ jest dowolną bazą podprzestrzeni U, to uzupełniamy ją do bazy

$$\{v_1, \ldots, v_k, u_1, \ldots, u_m\}$$

przestrzeni V i z łatwością dowodzimy, że warstwy $u_1 + U, \ldots, u_m + U$ tworzą bazę przestrzeni ilorazowej V/U. Zatem dla $U = \ker \tau$ otrzymujemy

$$\dim_K \operatorname{im} \tau = \dim_K V/\ker \tau = \dim_K V - \dim_K \ker \tau,$$

skąd wynika już teza naszego lematu. □

TWIERDZENIE **8.5.3.** *Dla endomorfizmu $\tau : V \to V$ skończenie wymiarowej przestrzeni wektorowej V następujące warunki są równoważne:*

(a) *τ jest nieosobliwy.*
(b) *τ jest injektywny.*
(c) *τ jest surjektywny.*
(d) *τ jest izomorfizmem.*
(e) *τ jest odwracalny w $\mathsf{End}_K V$.*
(f) *Wyraz wolny wielomianu minimalnego endomorfizmu τ jest różny od zera.*

Dowód. Równoważność warunków (a), (b), (c), (d) wynika z lematu 8.5.2 natomiast równoważność (e) i (f) wynika z twierdzenia 8.4.7. Jeśli τ jest endomorfizmem odwracalnym i τ^{-1} jest endomorfizmem odwrotnym do τ, to z $\tau\tau^{-1} = 1_V$ wynika, że $\tau(\tau^{-1}(v)) = v$ dla każdego $v \in V$. Zatem τ jest surjektywny. A więc (e) $\Rightarrow$ (c).
Wystarczy teraz pokazać, że (d) $\Rightarrow$ (e). Jeśli $\tau : V \to V$ jest izomorfizmem, to każdy wektor przestrzeni V można jednoznacznie przedstawić w postaci $\tau(v)$, gdzie $v \in V$. Wobec tego określamy odwzorowanie

$$\sigma : V \to V, \quad \sigma(\tau(v)) = v$$

dla każdego $v \in V$. Łatwe sprawdzenie pokazuje, że σ jest endomorfizmem przestrzeni V. Ponadto, z określenia endomorfizmu σ wynika, że $\sigma\tau = 1_V$. A więc endomorfizm τ jest lewostronnie odwracalny i wobec tego na podstawie twierdzenia 8.4.7 jest odwracalny. □

Uwaga 8.5.4. Można udowodnić, że dla endomorfizmu $\tau : M \to M$ skończenie generowanego modułu nad dowolnym pierścieniem, jeśli τ jest surjektywny, to τ jest injektywny i wobec tego jest izomorfizmem (zob. H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge 1986, Theorem 2.4, str. 9). Natomiast twierdzenie odwrotne nie jest prawdziwe. Jeśli A jest pierścieniem całkowitym oraz $0 \neq a \in A$ jest elementem nieodwracalnym, to ideał główny $(a) = aA$ jest różny od A oraz odwzorowanie $A \to A$, $x \mapsto ax$ jest injektywnym endomorfizmem $A-$ modułu A, który nie jest endomorfizmem surjektywnym.

8.6 Rząd endomorfizmu

DEFINICJA **8.6.1.** *Rzędem* $\mathsf{rank}\,\tau$ endomorfizmu $\tau : V \to V$ nazywamy wymiar obrazu endomorfizmu τ :

$$\mathsf{rank}\,\tau := \dim_K \operatorname{im}\tau.$$

Zauważmy, że $0 \leqslant \mathsf{rank}\,\tau \leqslant \dim_K V$. Przy tym $\mathsf{rank}\,\tau = \dim_K V$ wtedy i tylko wtedy, gdy endomorfizm τ jest nieosobliwy. Jeśli τ jest osobliwy, to $0 \leqslant \mathsf{rank}\,\tau < \dim_K V$. Widzimy więc, że rząd endomorfizmu pozwala nie tylko rozgraniczyć endomorfizmy nieosobliwe od osobliwych, ale jest także swoistą miarą osobliwości endomorfizmu. Można intuicyjnie uważać, że im większy rząd endomorfizmu osobliwego, tym bliższy jest on nieosobliwości. Z drugiej strony, jeśli $\mathsf{rank}\,\tau = 0$, to $\tau = 0_V$ jest krańcowo osobliwy. Zauważmy, że zgodnie z lematem 8.5.2,

$$\mathsf{rank}\,\tau = \dim_K V - \dim_K \ker\tau.$$

TWIERDZENIE **8.6.2.** *Niech σ, τ będą endomorfizmami skończenie wymiarowej przestrzeni wektorowej V nad ciałem K. Wtedy*
(a) $\mathsf{rank}\,\sigma\tau \leqslant \mathsf{rank}\,\tau$.
(b) $\mathsf{rank}\,\sigma\tau \leqslant \mathsf{rank}\,\sigma$.
(c) $\mathsf{rank}\,\sigma\tau \leqslant \min\{\mathsf{rank}\,\sigma, \mathsf{rank}\,\tau\}$.
(d) *Jeśli endomorfizm σ jest nieosobliwy, to*

$$\mathsf{rank}\,\sigma\tau = \mathsf{rank}\,\tau\sigma = \mathsf{rank}\,\tau.$$

Dowód. (a) Skorzystamy tu z faktu, że $\dim \sigma(U) \leqslant \dim U$ dla dowolnej podprzestrzeni U przestrzeni V. Wtedy dla $U = \tau(V)$ mamy

$$\mathsf{rank}\,\sigma\tau = \dim \operatorname{im} \sigma\tau = \dim \sigma(\tau(V)) \leqslant \dim \tau(V) = \mathsf{rank}\,\tau.$$

(b) Skorzystamy tu z faktu, że dla dowolnych podprzestrzeni U_1, U_2 przestrzeni V, jeśli $U_1 \subseteq U_2$, to $\dim \sigma(U_1) \leqslant \dim \sigma(U_2)$. Zatem dla $U_1 = \tau(V)$ oraz $U_2 = V$ mamy

$$\mathsf{rank}\,\sigma\tau = \dim \sigma(\tau(V)) \leqslant \dim \sigma(V) = \mathsf{rank}\,\sigma.$$

(c) wynika z (a) i (b).
(d) Endomorfizm nieosobliwy σ jest izomorfizmem i wobec tego przeprowadza podprzestrzeń U przestrzeni V na podprzestrzeń o takim samym wymiarze: $\dim \sigma(U) = \dim U$. Stąd dla $U = \tau(V)$ mamy

$$\mathsf{rank}\,\sigma\tau = \dim \sigma(\tau(V)) = \dim \tau(V) = \mathsf{rank}\,\tau.$$

Z drugiej strony, jeśli endomorfizm σ jest nieosobliwy, to $\sigma(V) = V$ i wobec tego

$$\mathsf{rank}\,\tau\sigma = \dim \tau(\sigma(V)) = \dim \tau(V) = \mathsf{rank}\,\tau.$$

Dowodzi to części (d) twierdzenia. □

WNIOSEK **8.6.3.** *Jeśli σ jest nieosobliwym endomorfizmem skończenie wymiarowej przestrzeni wektorowej V, to dla każdego endomorfizmu τ przestrzeni V mamy*

$$\mathsf{rank}\,\sigma^{-1}\tau\sigma = \mathsf{rank}\,\tau.$$

Dowód. Zastosujemy część (d) twierdzenia 8.6.2:

$$\mathsf{rank}\,\sigma^{-1}\tau\sigma = \mathsf{rank}\,\sigma^{-1}(\tau\sigma) = \mathsf{rank}\,\tau\sigma = \mathsf{rank}\,\tau,$$

gdyż wraz z σ także σ^{-1} jest endomorfizmem nieosobliwym. □

8.7 Podobieństwo endomorfizmów

Zbadamy teraz związek między macierzami $\mathsf{m}(\tau, \mathcal{A})$ oraz $\mathsf{m}(\tau, \mathcal{B})$ endomorfizmu τ w dwóch uporządkowanych bazach $\mathcal{A}$ i $\mathcal{B}$ przestrzeni V. Niech więc

$$\mathcal{A} = \{u_1, \ldots, u_n\} \quad \text{i} \quad \mathcal{B} = \{v_1, \ldots, v_n\}$$

będą uporządkowanymi bazami przestrzeni V i niech

$$\mathsf{m}(\tau, \mathcal{A}) = [a_{ij}] =: A \quad \text{oraz} \quad \mathsf{m}(\tau, \mathcal{B}) = [b_{ij}] =: B.$$

Zatem

$$\tau(u_j) = \sum_{i=1}^{n} a_{ij} u_i, \qquad \tau(v_j) = \sum_{i=1}^{n} b_{ij} v_i$$

dla $j = 1, \ldots, n$. Obieramy endomorfizm $\sigma \in \mathsf{End}_K V$ taki, że

$$\sigma(u_j) = v_j, \quad j = 1, \ldots, n.$$

Endomorfizm σ jest automorfizmem przestrzeni V oraz

$$\tau\sigma(u_j) = \tau(v_j) = \sum_{i=1}^{n} b_{ij} v_i = \sum_{i=1}^{n} b_{ij} \sigma(u_i) = \sigma(\sum_{i=1}^{n} b_{ij} u_i).$$

Wynika stąd, że

$$\sigma^{-1}\tau\sigma(u_j) = \sum_{i=1}^{n} b_{ij} u_i,$$

dla $j = 1, \ldots, n$. Równości te pokazują, że endomorfizm $\sigma^{-1}\tau\sigma$ ma w bazie $\mathcal{A}$ macierz B, to znaczy, $\mathsf{m}(\sigma^{-1}\tau\sigma, \mathcal{A}) = B$. Niech $S := \mathsf{m}(\sigma, \mathcal{A})$. Wtedy

$$B = \mathsf{m}(\sigma^{-1}\tau\sigma, \mathcal{A}) = \mathsf{m}(\sigma^{-1}, \mathcal{A})\, \mathsf{m}(\tau, \mathcal{A})\, \mathsf{m}(\sigma, \mathcal{A}) = S^{-1}AS.$$

Udowodniliśmy więc następujące twierdzenie.

TWIERDZENIE **8.7.1.** *Jeśli A i B są macierzami endomorfizmu τ w bazach $\mathcal{A}$ i $\mathcal{B}$ przestrzeni V i jeśli $S = \mathsf{m}(\sigma, \mathcal{A})$ jest macierzą endomorfizmu σ przeprowadzającego bazę $\mathcal{A}$ na bazę $\mathcal{B}$, to*

$$B = S^{-1}AS.$$

Uwaga 8.7.2. Macierz $S = \mathsf{m}(\sigma, \mathcal{A})$ można także interpretować jako *macierz przejścia* od uporządkowanej bazy $\mathcal{A}$ do uporządkowanej bazy $\mathcal{B}$. Jeśli bowiem $S = [s_{ij}]$, to

$$v_j = \sigma(u_j) = \sum_{i=1}^{n} s_{ij} u_i, \quad j = 1, \ldots, n.$$

W przykładzie 8.1.3 rozpatrywaliśmy już odwzorowanie

$$\mu : \mathsf{End}_K V \longrightarrow M_n(K), \quad \mu(\tau) = \mathsf{m}(\tau, \mathcal{B})$$

i stwierdziliśmy, że jest ono izomorfizmem $K-$algebr. Wobec tego odwzorowanie μ przeprowadza grupę $U(\mathsf{End}_K V)$ elementów odwracalnych algebry endomorfizmów na grupę $U(M_n(K))$ elementów odwracalnych algebry macierzy. Elementy odwracalne w obydwu algebrach nazywa się także *nieosobliwymi*. Tradycyjne oznaczenia dla grup endomorfizmów nieosobliwych i macierzy nieosobliwych (stopnia n nad ciałem K) są następujące: $\mathsf{Aut}\, V$ i $\mathbf{GL}(n, K)$. A więc $\mu(\mathsf{Aut}\, V) = \mathbf{GL}(n, K)$.

DEFINICJA **8.7.3.** Macierze $A, B \in M_n(K)$ nazywamy *podobnymi* lub *sprzężonymi*, jeśli istnieje macierz nieosobliwa $S \in \mathbf{GL}(n, K)$ taka, że

$$B = S^{-1}AS.$$

Relacja podobieństwa macierzy jest relacją równoważnościową w algebrze macierzy $M_n(K)$. Twierdzenie 8.7.1 orzeka, że macierze endomorfizmu τ w różnych bazach przestrzeni V są podobne.

DEFINICJA **8.7.4.** Endomorfizmy ρ i τ przestrzeni V nazywamy endomorfizmami *podobnymi* lub *sprzężonymi*, jeśli istnieje endomorfizm nieosobliwy σ taki, że

$$\rho = \sigma^{-1}\tau\sigma.$$

Łatwo sprawdzić, że relacja podobieństwa endomorfizmów jest relacją równoważności w algebrze $\mathsf{End}_K V$.

LEMAT **8.7.5.** *Niech ρ i τ będą podobnymi endomorfizmami przestrzeni V. Wtedy*
(a) $p_\rho = p_\tau$.
(b) *ρ jest nieosobliwy wtedy i tylko wtedy, gdy τ jest nieosobliwy.*
(c) $\mathsf{rank}\,\rho = \mathsf{rank}\,\tau$.

Dowód. (a) Niech σ będzie endomorfizmem nieosobliwym takim, że $\rho = \sigma^{-1}\tau\sigma$. Zauważmy najpierw, że dla dowolnej liczby naturalnej k mamy

$$(\sigma^{-1}\tau\sigma)^k = \sigma^{-1}\tau^k\sigma.$$

Zatem dla dowolnego wielomianu $g \in K[X]$ mamy $g(\sigma^{-1}\tau\sigma) = \sigma^{-1}g(\tau)\sigma$.
Wynika stąd, że $g(\sigma^{-1}\tau\sigma) = 0_V$ wtedy i tylko wtedy, gdy $g(\tau) = 0_V$. Stąd wynika już równość wielomianów minimalnych endomorfizmów $\rho = \sigma^{-1}\tau\sigma$ oraz τ.
Można też zauważyć, że (a) wynika ze stwierdzenia 8.4.6. Rzeczywiście, przy ustalonym endomorfizmie odwracalnym σ odwzorowanie $\tau \mapsto \sigma^{-1}\tau\sigma$ jest automorfizmem algebry endomorfizmów $\mathsf{End}_K V$. Wobec tego, na podstawie stwierdzenia 8.4.6 endomorfizmy τ i $\rho = \sigma^{-1}\tau\sigma$ mają równe wielomiany minimalne.
(b) wynika z twierdzeń 8.4.7, 8.4.8 i z (a). Zauważmy też, że (b) wynika z (c). Natomiast (c) udowodniliśmy już jako wniosek 8.6.3. □

TWIERDZENIE **8.7.6.** *Dla endomorfizmów ρ i τ przestrzeni V następujące warunki są równoważne:*
(a) *ρ i τ są podobne.*
(b) *Dla każdej uporządkowanej bazy $\mathcal{A}$ przestrzeni V macierze $\mathsf{m}(\rho, \mathcal{A})$ i $\mathsf{m}(\tau, \mathcal{A})$ są podobne.*
(b′) *Istnieje uporządkowana baza $\mathcal{A}'$ przestrzeni V taka, że macierze $\mathsf{m}(\rho, \mathcal{A}')$ i $\mathsf{m}(\tau, \mathcal{A}')$ są podobne.*
(c) *Dla każdej uporządkowanej bazy $\mathcal{A}$ przestrzeni V istnieje uporządkowana baza $\mathcal{B}$ przestrzeni V taka, że $\mathsf{m}(\rho, \mathcal{A}) = \mathsf{m}(\tau, \mathcal{B})$.*
(c′) *Istnieją uporządkowane bazy $\mathcal{A}$ i $\mathcal{B}$ przestrzeni V takie, że $\mathsf{m}(\rho, \mathcal{A}) = \mathsf{m}(\tau, \mathcal{B})$.*

Dowód. (a) $\Rightarrow$ (b) Niech $\rho = \sigma^{-1}\tau\sigma$, gdzie $\sigma \in \mathsf{Aut}\,V$ i niech $\mathcal{A}$ będzie dowolną bazą przestrzeni V. Wtedy

$$\mathsf{m}(\rho, \mathcal{A}) = \mathsf{m}(\sigma^{-1}\tau\sigma, \mathcal{A}) = S^{-1} \cdot \mathsf{m}(\tau, \mathcal{A}) \cdot S,$$

gdzie $S = \mathsf{m}(\sigma, \mathcal{A})$. A więc macierze $\mathsf{m}(\rho, \mathcal{A})$ i $\mathsf{m}(\tau, \mathcal{A})$ są podobne.

(b) $\Rightarrow$ (b$'$) jest oczywiste.
(b$'$) $\Rightarrow$ (c) Niech $\mathsf{m}(\rho, \mathcal{A}') = S^{-1} \cdot \mathsf{m}(\tau, \mathcal{A}') \cdot S$, gdzie S jest macierzą odwracalną i niech $\mathcal{A}$ będzie dowolną bazą uporządkowaną przestrzeni V. Macierz $\mathsf{m}(\rho, \mathcal{A})$ jest podobna do macierzy $\mathsf{m}(\rho, \mathcal{A}')$ (na podstawie twierdzenia 8.7.1), zatem istnieje macierz odwracalna T taka, że

$$\mathsf{m}(\rho, \mathcal{A}) = T^{-1} \cdot \mathsf{m}(\rho, \mathcal{A}') \cdot T.$$

Stąd

$$\mathsf{m}(\rho, \mathcal{A}) = T^{-1}S^{-1} \cdot \mathsf{m}(\tau, \mathcal{A}') \cdot ST = (ST)^{-1} \cdot \mathsf{m}(\tau, \mathcal{A}') \cdot (ST).$$

Obieramy automorfizm α przestrzeni V taki, że $ST = \mathsf{m}(\alpha, \mathcal{A}')$. Niech $\mathcal{B} = \alpha(\mathcal{A}')$. Wtedy $\mathcal{B}$ jest bazą przestrzeni V i na podstawie twierdzenia 8.7.1 mamy $(ST)^{-1}\mathsf{m}(\tau, \mathcal{A}')(ST) = \mathsf{m}(\tau, \mathcal{B})$. A więc $\mathsf{m}(\rho, \mathcal{A}) = \mathsf{m}(\tau, \mathcal{B})$.

(c) $\Rightarrow$ (c$'$) jest oczywiste.
(c$'$) $\Rightarrow$ (a) Niech σ będzie automorfizmem przestrzeni V przeprowadzającym bazę $\mathcal{A}$ na bazę $\mathcal{B}$. Wtedy na podstawie (c$'$) i twierdzenia 8.7.1 mamy

$$\mathsf{m}(\rho, \mathcal{A}) = \mathsf{m}(\tau, \mathcal{B}) = \mathsf{m}(\sigma, \mathcal{A})^{-1} \cdot \mathsf{m}(\tau, \mathcal{A}) \cdot \mathsf{m}(\sigma, \mathcal{A}) = \mathsf{m}(\sigma^{-1}\tau\sigma, \mathcal{A}).$$

Endomorfizmy ρ i $\sigma^{-1}\tau\sigma$ mają więc równe macierze w bazie $\mathcal{A}$ skąd wynika, że $\rho = \sigma^{-1}\tau\sigma$. A więc (c$'$) $\Rightarrow$ (a). □

Jak widzimy, endomorfizmy podobne mają te same wielomiany minimalne, równe rzędy a także identyczne macierze w odpowiednio dobranych bazach przestrzeni. Jest więc rzeczą naturalną pogrupować endomorfizmy przestrzeni wektorowej w klasy endomorfizmów podobnych i badać po jednym endomorfizmie z każdej klasy. Innymi słowy mówiąc, należy rozważyć problem klasyfikacji endomorfizmów przestrzeni V ze względu na podobieństwo endomorfizmów. Problem ten jest ściśle związany z klasyfikacją macierzy w $M_n(K)$ ze względu na podobieństwo macierzy.

Jeśli bowiem ustalimy bazę $\mathcal{A}$ przestrzeni V i każdemu endomorfizmowi τ przestrzeni V przyporządkujemy macierz $\mu(\tau) = A = \mathsf{m}(\tau, \mathcal{A})$ endomorfizmu τ względem bazy $\mathcal{A}$, to jak wiemy, otrzymujemy izomorfizm $K-$algebr

$$\mu : \mathsf{End}_K V \to M_n(K).$$

Ten izomorfizm przeprowadza klasy endomorfizmów podobnych na klasy macierzy podobnych:

$$\mu\{\sigma^{-1}\tau\sigma : \sigma \in \mathsf{Aut}\, V\} = \{S^{-1}AS : S \in \mathbf{GL}(n, k)\},$$

gdzie $\mu(\sigma) = S$ dla $\sigma \in \mathsf{Aut}\, V$. A więc μ przeprowadza klasę endomorfizmów podobnych do τ na zbiór macierzy endomorfizmu τ we wszystkich bazach przestrzeni V (lub równoważnie, na zbiór macierzy wszystkich endomorfizmów podobnych do τ, w ustalonej bazie $\mathcal{A}$ przestrzeni V).
Ta obserwacja jest podstawą klasyfikacji endomorfizmów przestrzeni wektorowej i poszukiwania postaci kanonicznych macierzy endomorfizmów. Z każdym endomorfizmem τ przestrzeni V wiążemy klasę macierzy tego endomorfizmu we wszystkich bazach przestrzeni V i znajdujemy w tej klasie macierze szczególnych postaci, które opisują przejrzyście działanie endomorfizmu τ na odpowiadających tym macierzom bazach przestrzeni wektorowej V. Są to tak zwane postaci kanoniczne macierzy endomorfizmu τ.

Uwaga 8.7.7. Można udowodnić, że dla każdego izomorfizmu $K-$algebr

$$\varphi : \mathsf{End}_K V \to M_n(K)$$

istnieje baza $\mathcal{A}$ przestrzeni V taka, że $\varphi(\tau) = \mathsf{m}(\tau, \mathcal{A})$ dla każdego $\tau \in \mathsf{End}_K V$. Inaczej mówiąc, każdy izomorfizm $\mathsf{End}_K V \to M_n(K)$ można otrzymać z jednego ustalonego izomorfizmu $\mu : \mathsf{End}_K V \to M_n(K)$ przez złożenie μ z pewnym *automorfizmem wewnętrznym* algebry macierzy $M_n(K) \to M_n(K)$, $A \mapsto S^{-1}AS$.

Znacznie ogólniejsze twierdzenie Skolema-Noether mówi, że dla dowolnych skończenie wymiarowych $K-$algebr centralnych i prostych A, B każdy homomorfizm $K-$algebr $\varphi : A \to B$ można otrzymać z jednego jakiegokolwiek homomorfizmu $\psi : A \to B$ przez złożenie ψ z odpowiednim automorfizmem wewnętrznym algebry B (zob. W. Scharlau, *Quadratic and Hermitian Forms*. Springer-Verlag 1985, str. 291). Zauważmy, że wynika stąd iż każdy automorfizm skończenie wymiarowej algebry centralnej i prostej jest automorfizmem wewnętrznym. Wystarczy bowiem wziąć dowolny automorfizm $\varphi : A \to A$ oraz $\psi = \mathrm{id}_A$. W szczególności więc każdy automorfizm algebry endomorfizmów skończenie wymiarowej przestrzeni wektorowej jest automorfizmem wewnętrznym (i podobnie dla algebry macierzy $M_n(K)$).

8.8 Zadania

Zakładamy, że V jest skończenie wymiarową przestrzenią wektorową nad ciałem K, chyba, że w zadaniu jest inne założenie o V.

1. Niech V będzie przestrzenią wektorową z bazą $\{v_1, \ldots, v_n\}$ i niech τ będzie endomorfizmem przestrzeni V takim, że

$$\tau(v_1) = v_2, \quad \tau(v_2) = v_3, \ldots, \tau(v_{n-1}) = v_n, \quad \tau(v_n) = -a_n v_1 - a_{n-1} v_2 - \cdots - a_1 v_n.$$

(a) Udowodnić, że $f(\tau) = 0 \in \mathsf{End}_K V$ dla wielomianu

$$f = X^n + a_1 X^{n-1} + \cdots + a_n \in K[X].$$

(b) Udowodnić, że f jest wielomianem minimalnym endomorfizmu τ.

2. (a) Niech V będzie skończenie wymiarową przestrzenią wektorową nad ciałem liczb rzeczywistych. Udowodnić, że nie istnieją endomorfizmy σ i τ przestrzeni V takie, że

$$\sigma\tau - \tau\sigma = \mathbf{1}_V.$$

(b) Niech K będzie ciałem o charakterystyce 2 i niech V będzie 2-wymiarową przestrzenią wektorową nad ciałem K. Wskazać endomorfizmy σ i τ przestrzeni V takie, że

$$\sigma\tau - \tau\sigma = \mathbf{1}_V.$$

(c) Niech K będzie dowolnym ciałem i niech $V = K[X]$ będzie przestrzenią wektorową wielomianów nad K. Niech σ będzie endomorfizmem różniczkowania względem X, natomiast τ niech będzie endomorfizmem mnożenia wielomianu przez X. Sprawdzić, że

$$\sigma\tau - \tau\sigma = \mathbf{1}_V.$$

3. Udowodnić, że jeśli $\tau \neq 0_V$ jest osobliwym endomorfizmem przestrzeni V, to istnieje endomorfizm σ przestrzeni V taki, że $\sigma \cdot \tau = 0_V$ ale $\tau \cdot \sigma \neq 0_V$.

4. Udowodnić, że każdy endomorfizm przestrzeni wektorowej V nad ciałem o charakterystyce $\neq 2$ można przedstawić w postaci sumy endomorfizmów odwracalnych.

5. Niech V będzie przestrzenią nieskończenie wymiarową i niech $\tau \in \mathsf{End}_K V$ będzie endomorfizmem jednoznacznie lewostronnie odwracalnym (to znaczy, istnieje dokładnie jeden endomorfizm $\sigma \in \mathsf{End}_K V$ taki, że $\sigma\tau = 1_V$). Udowodnić, że τ jest endomorfizmem odwracalnym.

6. Niech $A, B \in M_n(K)$ będą macierzami idempotentnymi, to znaczy, $A^2 = A$ oraz $B^2 = B$. Udowodnić, że macierze A i B są podobne wtedy i tylko wtedy gdy mają równe rzędy.

7. Niech $\operatorname{char} K \neq 2$. Udowodnić, że jeśli endomorfizm τ przestrzeni V spełnia tożsamość $\tau^3 = \tau$, to istnieją podprzestrzenie $U,\ W,\ Z$ przestrzeni V takie, że
(a) $V = U \oplus W \oplus Z$
(b) $\tau(u) = 0$ dla $u \in U$,
(c) $\tau(w) = w$ dla $w \in W$,
(d) $\tau(z) = -z$ dla $z \in Z$.

8. Udowodnić, że jeśli σ jest endomorfizmem nilpotentnym oraz $f \in K[X]$ jest dowolnym wielomianem takim, że $f(0) \neq 0$, to endomorfizm $f(\sigma)$ jest odwracalny.

9. Pokazać, że jeśli macierze rzeczywiste A i B są podobne nad ciałem liczb zespolonych, to są także podobne nad ciałem liczb rzeczywistych.

10. Niech $\mathcal{A}$ będzie bazą przestrzeni V i niech

$$\mu_{\mathcal{A}} : \mathsf{End}_K V \to M_n(K)$$

będzie izomorfizmem $K-$algebr, który każdemu endomorfizmowi τ przestrzeni V przyporządkowuje macierz $\mu_{\mathcal{A}}(\tau)$ endomorfizmu τ względem bazy $\mathcal{A}$. Udowodnić, że jeśli $\mathcal{A}$ i $\mathcal{B}$ są bazami przestrzeni V, to izomorfizmy $\mu_{\mathcal{A}}$ i $\mu_{\mathcal{B}}$ są równe wtedy i tylko wtedy gdy bazy $\mathcal{A}$ i $\mathcal{B}$ są proporcjonalne (to znaczy, istnieje niezerowy element $c \in K$ taki, że $\mathcal{B} = c\mathcal{A}$).

Rozdział 9

Algebra liniowa: Triangularyzacja i diagonalizacja

Ostatnie zmiany 5.05.2008 r.

W tym rozdziale V jest skończenie wymiarową przestrzenią wektorową nad dowolnym ciałem K. Rozpatrywać będziemy geometryczne aspekty działania endomorfizmu na przestrzeni wektorowej. Przede wszystkim ustalimy wzorzec przejrzystego działania endomorfizmu jaki stanowią endomorfizmy diagonalizowalne i scharakteryzujemy je kompletnie poprzez własności wielomianów minimalnych. Podamy również podobną charakteryzację endomorfizmów, które w pewnej bazie mają macierz trójkątną.

9.1 Wartości własne endomorfizmu

Najprostszym typem endomorfizmów są endomorfizmy skalarne $\alpha = a1_V$, gdzie $a \in K$. Endomorfizm skalarny α dokonuje "rozciągania" przestrzeni wektorowej w każdym kierunku w tym samym stopniu, $\alpha(v) = av$ dla każdego $v \in V$.
Jeśli endomorfizm τ nie jest skalarny, to jest rzeczą celową zbadać, jak bardzo różni się on od endomorfizmów skalarnych. Pierwsze i najważniejsze przybliżenie sugeruje następujący lemat. Opisuje on sytuację, gdy endomorfizm τ przynajmniej w jednym kierunku działa tak jak pewien endomorfizm skalarny.

LEMAT **9.1.1.** *Dla $a \in K$ oraz $\tau \in \mathsf{End}_K V$ następujące warunki są równoważne.*

(a) *Endomorfizm $\tau - a1_V$ jest osobliwy.*
(b) *Istnieje $v \in V$ taki, że $v \neq 0$ oraz $\tau(v) = av$.*
(c) *Istnieje $v \in V$ taki, że $v \neq 0$ oraz $\tau(u) = au$ dla każdego $u \in Kv$.*

Dowód. Mamy oczywiste implikacje (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (a). □

DEFINICJA **9.1.2.** Element $a \in K$ nazywa się *wartością własną* endomorfizmu τ przestrzeni wektorowej V, jeśli endomorfizm $\tau - a1_V$ jest osobliwy.

Jeśli $a \in K$ jest wartością własną endomorfizmu τ, to *wektorem własnym* endomorfizmu τ *należącym do wartości własnej* a nazywamy każdy wektor $v \in V$ taki, że

$$v \neq 0 \quad \text{i} \quad \tau(v) = av.$$

Jeśli $v \in V$ jest wektorem własnym endomorfizmu τ należącym do wartości własnej a, to endomorfizm τ na prostej Kv działa tak jak endomorfizm skalarny $a1_V$, to znaczy, $\tau(u) = au$ dla każdego $u \in Kv$.

Dla każdej wartości własnej endomorfizmu τ istnieje oczywiście wektor własny należący do tej wartości własnej. Natomiast istnienia wartości własnych endomorfizmu można oczekiwać tylko w szczególnych sytuacjach. Jedną z nich opisujemy poniżej. Zwykle istnienia wartości własnych endomorfizmu dowodzi się przy użyciu wielomianu charakterystycznego endomorfizmu, którego definicja wymaga pojęcia wyznacznika. Przytoczony tu dowód omija te metody i drastycznie upraszcza klasyczne podejście do problemu istnienia wartości własnych.

TWIERDZENIE **9.1.3.** *Jeśli K jest ciałem algebraicznie domkniętym, to każdy endomorfizm $\tau \in \mathsf{End}_K V$ ma przynajmniej jedną wartość własną.*

Dowód.[1] Niech $p_\tau \in K[X]$ będzie wielomianem minimalnym endomorfizmu τ. Ponieważ K jest ciałem algebraicznie domkniętym, wielomian p_τ rozkłada się nad K na iloczyn czynników liniowych:

$$p_\tau = (X - a_1) \cdots (X - a_m), \quad a_1, \ldots, a_m \in K.$$

W takim razie

$$0_V = p_\tau(\tau) = (\tau - a_1 1_V) \cdots (\tau - a_m 1_V).$$

Oznacza to, że przynajmniej jeden z endomorfizmów $\tau - a_1 1_V, \ldots, \tau - a_m 1_V$, powiedzmy $\tau - a_i 1_V$, jest osobliwy (gdyby wszystkie były nieosobliwe, to także ich iloczyn byłby nieosobliwy, a jest endomorfizmem zerowym). W takim razie a_i jest wartością własną endomorfizmu τ. □

Podejście użyte w powyższym dowodzie prowadzi do znacznie bardziej precyzyjnego i ogólnego rezultatu.

TWIERDZENIE **9.1.4.** *Niech K będzie dowolnym ciałem i niech $\tau \in \mathsf{End}_K V$. Załóżmy, że wielomian minimalny p_τ endomorfizmu τ ma pierwiastek a w ciele K. Wtedy a jest wartością własną endomorfizmu τ.*

Dowód. Z założenia mamy rozkład $p_\tau = (X - a) \cdot g$, gdzie $g \in K[X]$ ma stopień mniejszy niż wielomian p_τ. Stąd

$$0 = 0_V(v) = p_\tau(\tau)(v) = (\tau - a1_V)(g(\tau)(v))$$

dla każdego wektora $v \in V$. Zauważmy, że endomorfizm $g(\tau)$ nie może być endomorfizmem zerowym, gdyż przeczyłoby to minimalności wielomianu p_τ. Zatem istnieje $v \in V$ taki, że $u := g(\tau)(v) \neq 0$. Ponieważ $(\tau - a1_V)(u) = 0$, endomorfizm $\tau - a1_V$ jest osobliwy i wobec tego a jest wartością własną endomorfizmu τ. □

W dowodzie twierdzenia 9.1.3 stwierdziliśmy, że *jeden* z pierwiastków wielomianu p_τ jest wartością własną endomorfizmu τ. Wykorzystując twierdzenie 9.1.4 możemy wzmocnić ten rezultat i stwierdzić, że *dla endomorfizmu τ przestrzeni wektorowej*

[1] Zobacz Sh. Axler, Down with determinants. *Amer. Math. Monthly* **102** (1995), 139–154.

nad ciałem algebraicznie domkniętym każdy pierwiastek wielomianu minimalnego p_τ endomorfizmu τ jest wartością własną endomorfizmu τ.
Rozpatrywać teraz będziemy endomorfizm τ przestrzeni wektorowej V nad *dowolnym* ciałem K.

LEMAT **9.1.5.** *Niech $a \in K$ będzie wartością własną endomorfizmu τ i niech $v \in V$ będzie wektorem własnym należącym do wartości własnej a. Wtedy dla każdego wielomianu $g \in K[X]$ endomorfizm $g(\tau)$ ma wartość własną $g(a)$ oraz v jest wektorem własnym endomorfizmu $g(\tau)$ należącym do wartości własnej $g(a)$.*

Dowód. Zauważmy najpierw, że dla każdej liczby naturalnej k,

> jeśli v jest wektorem własnym endomorfizmu τ należącym do wartości własnej a, to v jest wektorem własnym endomorfizmu τ^k należącym do wartości własnej a^k.

Rzeczywiście, jeśli $\tau(v) = av$ dla pewnego niezerowego wektora $v \in V$, to $\tau^2(v) = \tau(\tau(v)) = \tau(av) = a\tau(v) = a^2v$ i łatwa indukcja pokazuje, że $\tau^k(v) = a^kv$.
Stąd dla wielomianu $g = c_0X^m + c_1X^{m-1} + \cdots + c_m$ mamy

$$\begin{aligned} g(\tau)(v) &= c_0\tau^m(v) + c_1\tau^{m-1}(v) + \cdots + c_m 1_V(v) \\ &= c_0a^mv + c_1a^{m-1}v + \cdots + c_mv \\ &= g(a)v. \end{aligned}$$

A więc $g(a)$ jest wartością własną endomorfizmu $g(\tau)$ oraz v jest wektorem własnym należącym do wartości własnej $g(a)$. □

TWIERDZENIE **9.1.6.** *Niech $\tau \in \mathsf{End}_K V$. Element $a \in K$ jest wartością własną endomorfizmu τ wtedy i tylko wtedy gdy a jest pierwiastkiem wielomianu minimalnego endomorfizmu τ.*

Dowód. Jeśli a jest pierwiastkiem p_τ to a jest wartością własną τ to na podstawie twierdzenia 9.1.4. Z drugiej strony, jeśli a jest wartością własną endomorfizmu τ, niech $v \in V$ będzie wektorem własnym endomorfizmu τ należącym do a. Zatem $\tau(v) = av$ oraz $v \neq 0$. Na podstawie lematu dla wielomianu minimalnego p_τ endomorfizmu τ mamy $p_\tau(\tau)(v) = p_\tau(a)v$. Ponieważ $p_\tau(\tau) = 0_V$, więc wynika stąd, że $p_\tau(a)v = 0$. Ponieważ zaś wektor v jest niezerowy, otrzymujemy $p_\tau(a) = 0$. □

A więc endomorfizm $\tau \in \mathsf{End}_K V$ ma wartość własną wtedy i tylko wtedy, gdy jego wielomian minimalny p_τ ma pierwiastek w ciele K.

WNIOSEK **9.1.7.** *Każdy endomorfizm τ ma tylko skończoną $\geqslant 0$ liczbę wartości własnych.*

Wynika to stąd, że wielomian minimalny endomorfizmu τ ma skończoną $\geqslant 0$ liczbę pierwiastków w ciele K.

Ciągle jeszcze nie mamy zadowalającej odpowiedzi na pytanie ile wartości własnych może mieć endomorfizm przestrzeni $n-$wymiarowej. Liczba wartości własnych endomorfizmu nie przekracza stopnia wielomianu minimalnego tego endomorfizmu (bo

wszystkie wartości własne endomorfizmu są pierwiastkami jego wielomianu minimalnego). Jednakże z dowodu twierdzenia 8.4.3 wynika jedynie, że stopień wielomianu minimalnego endomorfizmu przestrzeni $n-$wymiarowej jest niewiększy od n^2. Później udowodnimy, że stopień ten jest niewiększy od n, teraz jednak uzyskamy inną drogą zadowalającą informację o liczbie wartości własnych endomorfizmu.

TWIERDZENIE **9.1.8.** *Jeśli $a_1, \ldots, a_k \in K$ są różnymi wartościami własnymi endomorfizmu τ oraz $v_1, \ldots, v_k \in V$ są wektorami własnymi endomorfizmu τ należącymi odpowiednio do wartości własnych $a_1, \ldots, a_k$, to wektory $v_1, \ldots, v_k$ są liniowo niezależne w przestrzeni V.*

Dowód. Jeśli $v_1, \ldots, v_k$ są liniowo zależne, to istnieją skalary $c_1, \ldots, c_k$ nie wszystkie równe zero takie, że

$$c_1 v_1 + \cdots + c_k v_k = 0. \tag{9.1}$$

Biorąc wartości endomorfizmu τ otrzymujemy

$$c_1 a_1 v_1 + \cdots + c_k a_k v_k = 0.$$

Mnożąc pierwszą z tych równości przez a_1 i odejmując stronami otrzymamy

$$c_2(a_1 - a_2)v_2 + \cdots + c_k(a_1 - a_k)v_k = 0.$$

Równość ta pokazuje liniową zależność wektorów $v_2, \ldots, v_k$ (gdyż jeśli $c_i \neq 0$, to $c_i(a_1 - a_i) \neq 0$). Podobnie z liniowej zależności wektorów $v_2, \ldots, v_k$ wydedukujemy liniową zależność wektorów $v_3, \ldots, v_k$. Kontynuując dochodzimy do wniosku, że układ jednoelementowy złożony z wektora v_k jest liniowo zależny, sprzeczność (gdyż $v_k \neq 0$). □

Drugi dowód. Zauważmy, że

$$\begin{aligned}(\tau - a_j 1_V)(c_1 v_1 + \cdots + c_k v_k) &= \sum_{i=1}^{k} \tau(c_i v_i) - \sum_{i=1}^{k} a_j c_i v_i \\ &= \sum_{i=1}^{k} (a_i c_i v_i - a_j c_i v_i) = \sum_{i=1}^{k} c_i(a_i - a_j)v_i \\ &= \sum_{i=1,\ i\neq j}^{k} c_i(a_i - a_j)v_i.\end{aligned}$$

Wobec tego biorąc obraz obu stron równości (9.1) przez endomorfizm $(\tau - a_2 1_V) \cdots (\tau - a_k 1_V)$ otrzymujemy

$$c_1(a_1 - a_2) \cdots (a_1 - a_k)v_1 = 0.$$

Stąd wynika, że $c_1 = 0$. Podobnie dowodzi się, że $c_j = 0$ dla $j = 2, \ldots, k$. □

WNIOSEK **9.1.9.** *Każdy endomorfizm τ przestrzeni $n-$wymiarowej ma co najwyżej n różnych wartości własnych.*

WNIOSEK **9.1.10.** *Jeśli $\dim_K V = n$ i endomorfizm τ ma n różnych wartości własnych, to istnieje baza przestrzeni V złożona z wektorów własnych endomorfizmu τ.*

9.2 Endomorfizmy diagonalizowalne

Przypomnijmy, że jeśli $\mathcal{B} = \{v_1, \ldots, v_n\}$ jest uporządkowaną bazą przestrzeni wektorowej V to każdemu endomorfizmowi $\tau \in \mathsf{End}_K V$ odpowiada *macierz endomorfizmu τ w bazie $\mathcal{B}$*. Mianowicie, każdy wektor $\tau(v_j)$ przedstawiamy jako kombinację liniową wektorów bazy $\mathcal{B}$:

$$\tau(v_j) = \sum_{i=1}^{n} b_{ij} v_i,$$

gdzie $b_{ij} \in K$ i kładziemy $\mathsf{m}(\tau, \mathcal{B}) := [b_{ij}] \in M_n(K)$. Zatem $j-$tą kolumnę macierzy $\mathsf{m}(\tau, \mathcal{B})$ tworzą współrzędne wektora $\tau(v_j)$ w bazie $\mathcal{B}$.
Można uważać, że znalezienie macierzy endomorfizmu τ względem jakiejś bazy $\mathcal{B}$ przestrzeni V rozwiązuje już problem opisania działania endomorfizmu τ na przestrzeni wektorowej V. Jeśli bowiem znamy obrazy elementów bazy $\mathcal{B}$ przestrzeni V, to potrafimy już znaleźć obraz każdego wektora v tej przestrzeni (jeśli tylko znamy współrzędne wektora v w bazie $\mathcal{B}$). Jednakże, jeśli baza $\mathcal{B}$ jest obrana całkowicie przypadkowo, to nie można na ogół z macierzy endomorfizmu odczytać żadnych informacji o geometrycznym charakterze działania endomorfizmu τ. A więc, na przykład, nie można stwierdzić czy endomorfizm zachowuje jakieś proste przestrzeni V, lub ogólniej, czy ma jakieś podprzestrzenie niezmiennicze. Natomiast wybierając bazę przestrzeni V "dopasowaną" do endomorfizmu τ można takie informacje odczytać jednym rzutem oka na macierz endomorfizmu. Nasze główne zadanie polega na tym, żeby dla jak najszerszej klasy przestrzeni wektorowych i ich endomorfizmów wskazać sposób dobierania baz przestrzeni gwarantujący najprostszą postać macierzy endomorfizmu.
A oto przykład takiej sytuacji, kiedy macierz endomorfizmu ma szczególnie prostą postać pozwalającą na pełne zrozumienie działania endomorfizmu na przestrzeni wektorowej.

TWIERDZENIE **9.2.1.** *Jeśli $\dim_K V = n$ oraz endomorfizm τ ma n różnych wartości własnych, to istnieje baza przestrzeni V, względem której endomorfizm τ ma macierz diagonalną.*

Dowód. Niech $a_1, \ldots, a_n$ będą wartościami własnymi endomorfizmu τ. Dla każdej wartości własnej a_j obieramy wektor własny v_j należący do a_j. Na podstawie wniosku 9.1.10, wektory własne $v_1, \ldots, v_n$ tworzą bazę $\mathcal{B}$ przestrzeni V. Zatem z równości $\tau(v_j) = a_j v_j$ wynika, że

$$\mathsf{m}(\tau, \mathcal{B}) = \begin{bmatrix} a_1 & 0 & \ldots & 0 \\ 0 & a_2 & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & a_n \end{bmatrix}.$$

A więc macierz endomorfizmu τ w bazie $\mathcal{B}$ jest diagonalna. □

Endomorfizm τ przestrzeni wektorowej V nazywamy *diagonalizowalnym*, jeśli istnieje baza $\mathcal{B}$ przestrzeni V taka, że macierz $\mathsf{m}(\tau, \mathcal{B})$ jest diagonalna. Twierdzenie 9.2.1 podaje więc warunek wystarczający diagonalizowalności endomorfizmu, który

można sformułować następująco: jeśli wielomian minimalny endomorfizmu τ przestrzeni $n-$wymiarowej ma n różnych pierwiastków w ciele K, to endomorfizm τ jest diagonalizowalny. Okazuje się jednak, że wymaganie by wielomian minimalny miał $n = \dim V$ różnych pierwiastków w ciele K jest zbędne. Istotne jest tylko by wielomian ten rozkładał się na iloczyn *różnych* czynników liniowych nad K. Poniższe twierdzenie podaje warunek konieczny diagonalizowalności, o którym udowodnimy w końcu rozdziału 9.4 (zob. twierdzenie 9.4.1), że jest także wystarczający.

TWIERDZENIE **9.2.2.** *Jeśli endomorfizm $\tau \in \mathsf{End}_K V$ jest diagonalizowalny, to wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn parami różnych czynników liniowych:*

$$p_\tau = (X - b_1) \cdots (X - b_k), \quad b_1, \ldots, b_k \in K, \quad b_i \neq b_j \quad \text{dla} \quad i \neq j.$$

Dowód. Niech $\mathcal{B}$ będzie bazą V taką, że $D = \mathsf{m}(\tau, \mathcal{B})$ jest macierzą diagonalną. Wśród elementów ciała K występujących na przekątnej macierzy D niektóre mogą występować więcej niż jeden raz. Niech $b_1, \ldots, b_k$ będą wszystkimi parami różnymi elementami ciała K występującymi na przekątnej macierzy D. Wtedy wielomian

$$f := (X - b_1) \cdots (X - b_k)$$

rozkłada się nad ciałem K na iloczyn parami różnych czynników liniowych. Udowodnimy, że $f = p_\tau$.
Przede wszystkim $b_1, \ldots, b_k$ jako elementy przekątnej diagonalnej macierzy endomorfizmu τ są wartościami własnymi endomorfizmu τ. Na podstawie twierdzenia 9.1.6 elementy $b_1, \ldots, b_k$ są pierwiastkami wielomianu minimalnego p_τ i wobec tego f dzieli p_τ.
Z drugiej strony $f(\tau) = 0_V$. Rzeczywiście, weźmy dowolny wektor $v \in \mathcal{B}$ i odpowiadającą mu wartość własną b_i. Zatem $(\tau - b_i 1_V)(v) = 0$ oraz

$$f(\tau)(v) = (\tau - b_1 1_V) \cdots (\tau - b_k 1_V)(v) = 0,$$

gdyż endomorfizmy $\tau - b_1 1_V, \ldots, \tau - b_k 1_V$ są przemienne. A więc $f(\tau)(v) = 0$ dla każdego $v \in \mathcal{B}$ i wobec tego $f(\tau) = 0_V$. Stąd wynika, że p_τ dzieli f. Ponieważ obydwa wielomiany f i p_τ są unormowane, wynika stąd, że $f = p_\tau$. □

9.3 Postać kanoniczna trójkątna

Postacie kanoniczne macierzy endomorfizmu $\tau \in \mathsf{End}_K V$ zależą w decydującej mierze od wielomianu minimalnego p_τ endomorfizmu τ. Rozpatrzyliśmy już przypadek, gdy wielomian p_τ rozkłada się nad ciałem K na iloczyn $n = \dim V$ *różnych* czynników liniowych. Wtedy endomorfizm τ ma n różnych wartości własnych i na podstawie twierdzenia 9.2.1 istnieje baza przestrzeni V, w której τ ma macierz *diagonalną*. W tym rozdziale rozpatrzymy przypadek, gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn czynników liniowych, ale niekoniecznie różnych. Innymi słowy, dopuszczamy by wielomian minimalny p_τ miał pierwiastki wielokrotne, ale wymagamy, by wszystkie one należały do ciała K. Nie wymagamy też, by wielomian minimalny p_τ miał stopień $n = \dim V$. Okazuje się, że w takim

przypadku istnieje baza przestrzeni V, w której τ ma macierz *trójkątną*.

Macierz $A = [a_{ij}] \in M_n(K)$ nazywamy macierzą *trójkątną*, jeśli wszystkie elementy pod główną przekątną są równe zero ($a_{ij} = 0$ dla $i > j$, macierz górna trójkątna), lub gdy wszystkie elementy nad główną przekątną są równe zero ($a_{ij} = 0$ dla $i < j$, macierz dolna trójkątna). Jeśli endomorfizm τ ma w bazie $\{v_1, \ldots, v_n\}$ macierz górną trójkątną, to w bazie $\{v_n, \ldots, v_1\}$ ma macierz dolną trójkątną. Żadna z tych postaci macierzy trójkątnej nie ma więc przewagi nad drugą.

Przypomnimy najpierw pojęcie podprzestrzeni niezmienniczej endomorfizmu.

Definicja **9.3.1.** Podprzestrzeń U przestrzeni V nazywamy podprzestrzenią *niezmienniczą* endomorfizmu $\tau \in \mathsf{End}_K V$ (lub $\tau-$niezmienniczą) jeśli $\tau(U) \subseteq U$, to znaczy, jeśli dla każdego $u \in U$ także $\tau(u) \in U$.

Przykład 9.3.1. Jeśli $u \in V$ jest wektorem własnym endomorfizmu τ, to prosta $U = Ku$ jest 1–wymiarową podprzestrzenią niezmienniczą endomorfizmu τ. Ogólniej, jeśli $u_1, \ldots, u_k$ są wektorami własnymi endomorfizmu τ, to podprzestrzeń $\mathsf{lin}\{u_1, \ldots, u_k\} = Ku_1 + \cdots + Ku_k$ jest podprzestrzenią niezmienniczą endomorfizmu τ. Podprzestrzeń $\tau-$niezmiennicza nie musi jednak być rozpięta na wektorach własnych endomorfizmu τ. Na przykład, dla dowolnych wektorów $v_1, v_2 \in V$ i dla endomorfizmu τ przestrzeni V takiego, że $\tau(v_1) = v_2, \tau(v_2) = v_1$ podprzestrzeń $Kv_1 + Kv_2$ jest $\tau-$niezmiennicza.

Lemat **9.3.2.** *Niech U będzie podprzestrzenią niezmienniczą endomorfizmu τ przestrzeni V. Wtedy:*
(a) *Odwzorowanie $\bar{\tau} : V/U \to V/U$, $\bar{\tau}(v + U) = \tau(v) + U$ jest dobrze określonym endomorfizmem przestrzeni ilorazowej V/U.*
(b) *Jeśli endomorfizm τ jest zerem wielomianu $q \in K[X]$, to endomorfizm $\bar{\tau}$ jest także zerem wielomianu q.*
(c) *Wielomian minimalny $\bar{p} \in K[X]$ endomorfizmu $\bar{\tau} \in \mathsf{End}_K V/U$ jest dzielnikiem wielomianu minimalnego p endomorfizmu τ.*

Dowód. (a) pozostawiamy jako ćwiczenie. Dla dowodu (b) połóżmy $q = \sum c_i X^i$. Wtedy dla dowolnej warstwy $v + U \in V/U$ mamy

$$\begin{aligned} q(\bar{\tau})(v + U) &= \sum c_i \bar{\tau}^i(v + U) = \sum c_i(\tau^i(v) + U) \\ &= \sum c_i \tau^i(v) + U = q(\tau)(v) + U = U. \end{aligned}$$

A więc $q(\bar{\tau})$ jest endomorfizmem zerowym przestrzeni V/U.
(c) Ponieważ $p(\tau) = 0_V$, więc na podstawie (b) mamy także $p(\bar{\tau}) = 0_{V/U}$. Zatem wielomian minimalny $\bar{p}$ endomorfizmu $\bar{\tau}$ dzieli wielomian p. □

Endomorfizm $\bar{\tau} : V/U \to V/U$ opisany w lemacie 9.3.2 nazywa się endomorfizmem *indukowanym* przez endomorfizm τ.

Twierdzenie **9.3.3.** *Niech τ będzie endomorfizmem przestrzeni wektorowej V nad ciałem K. Jeśli wielomian minimalny endomorfizmu τ rozkłada się nad ciałem K na iloczyn czynników liniowych, to przestrzeń V ma bazę, w której macierz endomorfizmu τ jest trójkątna.*

Dowód. Przeprowadzimy dowód indukcyjny ze względu na wymiar n przestrzeni V. Jeśli $n = 1$, to twierdzenie jest trywialnie prawdziwe. Załóżmy więc, że $n > 1$ oraz twierdzenie jest prawdziwe dla endomorfizmów wszystkich przestrzeni wektorowych nad ciałem K o wymiarze $n - 1$.
Niech $\tau \in \mathsf{End}_K V$, $\dim_K V = n$ oraz niech wielomian minimalny $p = p_\tau$ endomorfizmu τ rozkłada się na czynniki liniowe nad ciałem K. Niech $a \in K$ będzie pierwiastkiem wielomianu p. Wtedy, na podstawie twierdzenia 9.1.4, a jest wartością własną endomorfizmu τ i wobec tego jeśli u jest wektorem własnym należącym do wartości własnej a, to prosta $U = Ku$ jest 1–wymiarową podprzestrzenią niezmienniczą endomorfizmu τ.
Rozpatrujemy teraz przestrzeń ilorazową V/U i endomorfizm indukowany $\bar{\tau}$ tej przestrzeni. Ponieważ na podstawie lematu 9.3.2 wielomian minimalny $\bar{p}$ endomorfizmu indukowanego $\bar{\tau}$ jest dzielnikiem wielomianu p, więc wielomian $\bar{p}$ rozkłada się na czynniki liniowe nad ciałem K. Przestrzeń V/U ma wymiar $n - 1$, wobec tego na podstawie założenia indukcyjnego istnieje baza $\{\bar{v}_2, \ldots, \bar{v}_n\}$ przestrzeni V/U, w której endomorfizm $\bar{\tau}$ ma macierz trójkątną. Istnieją więc $a_{ij} \in K$ takie, że

$$\bar{\tau}(\bar{v}_j) = a_{2j}\bar{v}_2 + \cdots + a_{jj}\bar{v}_j \quad \text{dla} \quad j = 2, \ldots, n.$$

Obieramy teraz wektory $v_j \in V$ tak, by $\bar{v}_j = v_j + U$ dla $j = 2, \ldots, n$. Wtedy wektory $u, v_2, \ldots, v_n$ tworzą bazę przestrzeni V i macierz endomorfizmu τ w tej bazie jest trójkątna. Rzeczywiście,

$$\begin{aligned} \tau(v_j) + U &= \bar{\tau}(\bar{v}_j) \\ &= a_{2j}\bar{v}_2 + \cdots + a_{jj}\bar{v}_j \\ &= a_{2j}v_2 + \cdots + a_{jj}v_j \ + \ U. \end{aligned}$$

Stąd $\tau(v_j) - (a_{2j}v_2 + \cdots + a_{jj}v_j) \in U = Ku$. Istnieje więc $a_{1j} \in K$ taki, że

$$\tau(v_j) = a_{1j}u + a_{2j}v_2 + \cdots + a_{jj}v_j$$

dla każdego $j = 2, \ldots, n$, a to oznacza, że endomorfizm τ ma w bazie $\{u, v_2, \ldots, v_n\}$ macierz trójkątną. □

Endomorfizm τ przestrzeni V będziemy nazywać *triangularyzowalnym*, jeśli istnieje baza przestrzeni V, w której τ ma macierz trójkątną. Okazuje się, że dla endomorfizmów triangularyzowalnych problem znalezienia wartości własnych sprowadza się do znalezienia ich macierzy trójkątnych. Wynika to z następującej obserwacji.

STWIERDZENIE **9.3.4.** *Jeśli endomorfizm $\tau \in \mathsf{End}_K V$ ma macierz trójkątną $[a_{ij}]$ w pewnej bazie przestrzeni V, to każdy element diagonalny a_{jj} tej macierzy jest wartością własną endomorfizmu τ.*

Dowód. Niech $\mathcal{B} = \{v_1, \ldots, v_n\}$ będzie bazą V taką, że $\mathsf{m}(\tau, \mathcal{B}) = [a_{ij}]$ jest macierzą trójkątną. Ponieważ

$$\tau(v_j) = a_{1j}v_1 + a_{2j}v_2 + \cdots + a_{jj}v_j$$

dla każdego $j = 1, \ldots, n$, więc $\tau(v_1) = a_{11}v_1$ co oznacza, że a_{11} jest wartością własną endomorfizmu τ. Niech teraz $j > 1$ i niech $U = \mathsf{lin}\{v_1, \ldots, v_{j-1}\}$. Wtedy $\tau(U) \subseteq U$

i wobec tego możemy rozpatrzyć endomorfizm indukowany $\bar{\tau} : V/U \to V/U$ taki, że $\bar{\tau}(v + U) = \tau(v) + U$. Mamy zatem

$$\bar{\tau}(v_j + U) = \tau(v_j) + U = a_{jj}v_j + U = a_{jj}(v_j + U),$$

co oznacza, że a_{jj} jest wartością własną endomorfizmu $\bar{\tau}$. Na podstawie twierdzenia 9.1.6 skalar a_{jj} jest pierwiastkiem wielomianu minimalnego endomorfizmu $\bar{\tau}$, zaś na podstawie lematu 9.3.2(c) wynika stąd, że a_{jj} jest pierwiastkiem wielomianu minimalnego endomorfizmu τ. Zatem a_{jj} jest wartością własną endomorfizmu τ (na podstawie twierdzenia 9.1.6). □

Możemy teraz udowodnić twierdzenie charakteryzujące endomorfizmy triangularyzowalne poprzez własności ich wielomianów minimalnych.

TWIERDZENIE **9.3.5.** *Endomorfizm $\tau \in \mathsf{End}_K V$ ma macierz trójkątną w pewnej bazie przestrzeni V wtedy i tylko wtedy, gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn czynników liniowych:*

$$p_\tau = (X - b_1) \cdots (X - b_k), \quad b_1, \ldots, b_k \in K.$$

Dowód. Jedną część tego twierdzenia już udowodniliśmy (twierdzenie 9.3.3). Dla dowodu drugiej części załóżmy, że $\mathcal{B} = \{v_1, \ldots, v_n\}$ jest bazą V w której $\mathsf{m}(\tau, \mathcal{B}) = [a_{ij}]$ jest macierzą trójkątną. Rozpatrzmy wielomian

$$f := (X - a_{11}) \cdots (X - a_{nn}).$$

Jest to iloczyn czynników liniowych nad ciałem K. Udowodnimy, że p_τ dzieli f. Wystarczy zatem pokazać, że $f(\tau) = 0_V$, czyli $f(\tau)(v_j) = 0$ dla każdego $v_j \in \mathcal{B}$. Ponieważ

$$\tau(v_j) = a_{1j}v_1 + a_{2j}v_2 + \cdots + a_{jj}v_j$$

dla każdego $j = 1, \ldots, n$, więc dla każdego $j > 1$ mamy

$$(\tau - a_{jj}1_V)(v_j) \in \mathsf{lin}\{v_1, \ldots, v_{j-1}\}.$$

Ogólniej

$$(\tau - a_{jj}1_V)(\mathsf{lin}\{v_1, \ldots, v_j\}) \subseteq \mathsf{lin}\{v_1, \ldots, v_{j-1}\}.$$

Stąd wynika, że dla dowolnego $v_j \in \mathcal{B}$ mamy

$$(\tau - a_{22}1_V) \cdots (\tau - a_{j-1\,j-1}1_V)(\tau - a_{jj}1_V)(v_j) \in \mathsf{lin}\{v_1\}.$$

Ponieważ $(\tau - a_{11}1_V)(v_1) = 0$, więc wobec przemienności endomorfizmów $\tau - a_{ii}1_V$ otrzymujemy stąd

$$f(\tau)(v_j) = (\tau - a_{11}1_V) \cdots (\tau - a_{nn}1_V)(v_j) = 0.$$

A więc $f(\tau)(v_j) = 0$ dla każdego $v_j \in \mathcal{B}$ i wobec tego $f(\tau) = 0_V$. Stąd wynika, że p_τ dzieli f i wobec tego rozkłada się na czynniki liniowe nad ciałem K. □

WNIOSEK **9.3.6.** *Endomorfizm triangularyzowalny τ z macierzą trójkątną $A = [a_{ij}]$ jest nieosobliwy wtedy i tylko wtedy gdy $a_{11}a_{22} \cdots a_{nn} \neq 0$.*

Dowód. Na podstawie twierdzenia 9.3.4 wielomian minimalny p_τ ma pierwiastek 0 wtedy i tylko wtedy gdy jeden z elementów diagonalnych macierzy A jest równy 0. Zatem

$$p_\tau(0) = 0 \iff a_{11}a_{22}\cdots a_{nn} = 0.$$

Wobec twierdzenia 8.5.3 endomorfizm τ jest odwracalny wtedy i tylko wtedy gdy $a_{11}a_{22}\cdots a_{nn} \neq 0$. □

Wniosek 9.3.6 pokazuje jak bez użycia pojęcia wyznacznika można uzyskać rezultat klasycznie nierozerwalnie związany z teorią wyznaczników.

Z twierdzenia 9.3.5 wynika w szczególności, że każdy endomorfizm nilpotentny przestrzeni V ma macierz trójkątną w odpowiedniej bazie przestrzeni V. Prowadzi to do następującej charakteryzacji endomorfizmów nilpotentnych.

Wniosek **9.3.7.** *Endomorfizm σ przestrzeni V jest nilpotentny wtedy i tylko wtedy gdy jest triangularyzowalny i w każdej macierzy trójkątnej $A = [a_{ij}]$ tego endomorfizmu wszystkie elementy diagonalne są równe zero:*

$$a_{jj} = 0, \quad \text{dla} \quad j = 1, \ldots, n.$$

Dowód. Endomorfizm nilpotentny σ ma wielomian minimalny postaci $p_\sigma = X^m$. Zatem jest triangularyzowalny i na podstawie stwierdzenia 9.3.4 każdy element diagonalny a_{jj} macierzy A jest pierwiastkiem p_σ. Zatem $a_{jj} = 0$ dla $j = 1, \ldots, n$.

Na odwrót, jeśli istnieje baza $\mathcal{B} = \{v_1, \ldots, v_n\}$ przestrzeni V taka, że $\sigma(v_1) = 0$ oraz

$$\sigma(v_j) = a_{1j}v_1 + a_{2j}v_2 + \cdots + a_{j-1\,j-1}v_{j-1}$$

dla $j > 1$, to łatwy rachunek pokazuje, że $\sigma^n(v_j) = 0$ dla każdego $j = 1, \ldots, n$. Zatem $\sigma^n = 0_V$. □

Wniosek **9.3.8.** *Niech A będzie macierzą endomorfizmu τ przestrzeni V nad ciałem K w pewnej bazie przestrzeni V. Macierz A jest podobna do macierzy trójkątnej wtedy i tylko wtedy gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn czynników liniowych.*

Dowód. Niech $\mathcal{A}$ będzie bazą przestrzeni V taką, że $\mathsf{m}(\tau, \mathcal{A}) = A$. Rozkładalność p_τ na czynniki liniowe nad K jest równoważna istnieniu bazy $\mathcal{B}$ przestrzeni V takiej, że macierz $B = \mathsf{m}(\tau, \mathcal{B})$ jest trójkątna (na podstawie twierdzenia 9.3.5). Jeśli S jest macierzą automorfizmu przeprowadzającego bazę $\mathcal{A}$ na bazę $\mathcal{B}$, to na podstawie twierdzenia 8.7.1 mamy $B = S^{-1}AS$. A więc macierz A jest podobna do macierzy trójkątnej B. Z drugiej strony, jeśli macierz $A = \mathsf{m}(\tau, \mathcal{A})$ jest podobna do macierzy trójkątnej B oraz ρ jest endomorfizmem przestrzeni V, który w bazie $\mathcal{A}$ ma macierz $B = \mathsf{m}(\rho, \mathcal{A})$, to endomorfizmy ρ i τ są podobne (twierdzenie 8.7.6). Wobec tego, na podstawie lematu 8.7.5, endomorfizmy ρ i τ mają równe wielomiany minimalne. Ale p_ρ rozkłada się nad K na iloczyn czynników liniowych (na podstawie twierdzenia 9.3.5), zatem p_τ także ma taki rozkład. □

Wniosek **9.3.9.** *Niech $A \in M_n(K)$. Macierz A jest podobna do macierzy trójkątnej wtedy i tylko wtedy gdy wielomian minimalny p_A macierzy A rozkłada się nad ciałem K na iloczyn czynników liniowych.*

Dowód. Niech τ będzie endomorfizmem $n-$wymiarowej przestrzeni wektorowej V nad ciałem K, który w pewnej bazie przestrzeni V ma macierz A. Wtedy $p_A = p_\tau$ na podstawie stwierdzenia 8.4.6 i rezultat wynika z wniosku 9.3.8. □

9.4 Diagonalizacja

Pokażemy teraz, że technikę dowodu twierdzenia 9.3.3 można także użyć do charakteryzacji endomorfizmów diagonalizowalnych. W następnym rozdziale podamy jeszcze jeden, znacznie prostszy, dowód tego twierdzenia wykorzystujący ogólne twierdzenie o rozkładzie.

TWIERDZENIE **9.4.1.** *Endomorfizm $\tau \in \mathsf{End}_K V$ jest diagonalizowalny wtedy i tylko wtedy, gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn parami różnych czynników liniowych:*

$$p_\tau = (X - b_1)\cdots(X - b_k), \quad b_1, \ldots, b_k \in K, \quad b_i \neq b_j \quad \text{dla} \quad i \neq j.$$

Dowód. Konieczność warunku wynika z twierdzenia 9.2.2, przejdziemy więc do dowodu wystarczalności. Przeprowadzimy dowód indukcyjny ze względu na wymiar przestrzeni. Dla przestrzeni 1–wymiarowych twierdzenie jest oczywiście prawdziwe, zakładamy więc, że $\dim_K V > 1$.
Załóżmy, że wielomian p_τ ma wskazany rozkład nad ciałem K. Jeśli $k = 1$, to $0_V = p_\tau(\tau) = \tau - b_1 1_V$. Zatem τ jest endomorfizmem skalarnym, $\tau = b_1 1_V$, i w każdej bazie przestrzeni V ma macierz diagonalną. Możemy więc założyć, że $k > 1$. Niech

$$U := \left\{v \in V : \tau(v) = b_1 v\right\} = \ker(\tau - b_1 1_V).$$

Ponieważ b_1 jest pierwiastkiem wielomianu minimalnego endomorfizmu τ, więc jest wartością własną endomorfizmu τ (zob. twierdzenie 9.1.6) i wobec tego do U należą wszystkie wektory własne należące do wartości własnej b_1. Zatem U jest niezerową podprzestrzenią niezmienniczą endomorfizmu τ i wobec tego $\ell := \dim V/U < \dim V$. Rozpatrujemy endomorfizm $\bar{\tau}$ indukowany na przestrzeni V/U. Pokażemy, że jego wielomian minimalny $p_{\bar{\tau}}$ jest dzielnikiem wielomianu

$$f := (X - b_2)\cdots(X - b_k).$$

Wystarczy pokazać, że $f(\bar{\tau}) = 0_{V/U}$. Przede wszystkim zauważamy, że dla dowolnego $v \in V$ mamy

$$0 = p_\tau(\tau)(v) = (\tau - b_1 1_V) f(\tau)(v),$$

skąd wynika, że $f(\tau)(v) \in \ker(\tau - b_1 1_V) = U$. Zatem dla każdego $v \in V$ mamy

$$f(\bar{\tau})(v + U) = f(\tau)(v) + U = U.$$

Oznacza to, że $f(\bar{\tau}) = 0_{V/U}$ i wobec tego $p_{\bar{\tau}}$ dzieli f. Stąd wynika, że $p_{\bar{\tau}}$ jest iloczynem parami różnych czynników liniowych nad K i wobec tego na podstawie założenia indukcyjnego istnieje baza $\left\{\bar{v}_1, \ldots, \bar{v}_\ell\right\}$ przestrzeni V/U względem której endomorfizm $\bar{\tau}$ ma macierz diagonalną $\mathrm{diag}(d_1, \ldots, d_\ell)$. Przy tym zauważmy, że elementy diagonalne d_j są wartościami własnymi endomorfizmu $\bar{\tau}$, a więc pierwiastkami wielomianu

minimalnego $p_{\bar{\tau}}$. Ponieważ ten wielomian jest dzielnikiem wielomianu f, żaden ze skalarów d_j nie jest równy b_1. Ten fakt wykorzystamy w dalszej części dowodu.

W każdej warstwie bazowej $\bar{v}_j$ wybieramy wektor v_j i wtedy mamy

$$\bar{v}_j = v_j + U, \quad \bar{\tau}(\bar{v}_j) = d_j v_j + U, \quad j = 1, \ldots, \ell.$$

Jeśli $\{u_1, \ldots, u_m\}$ jest jakąkolwiek bazą podprzestrzeni U, to

$$\mathcal{A} = \{u_1, \ldots, u_m, v_1, \ldots, v_\ell\}$$

jest bazą przestrzeni V. Niech $A = \mathsf{m}(\tau, \mathcal{A})$ będzie macierzą endomorfizmu τ w bazie $\mathcal{A}$. Ponieważ

$$\tau(u_i) = b_1 u_i \quad \text{dla} \quad i = 1, \ldots, m,$$

więc początkowe m kolumn macierzy A są takie jak w macierzy skalarnej $\operatorname{diag}(b_1, \ldots, b_1)$. Pozostałe kolumny mają bardziej skomplikowaną postać. Mamy bowiem

$$\tau(v_j) + U = \bar{\tau}(\bar{v}_j) = d_j v_j + U, \quad j = 1, \ldots, \ell,$$

zatem $\tau(v_j) - d_j v_j \in U$. Istnieją więc elementy $a_{ij} \in K$ takie, że

$$\tau(v_j) = a_{1j} u_1 + \cdots + a_{mj} u_m + d_j v_j, \quad j = 1, \ldots, \ell. \tag{9.2}$$

Macierz A ma więc następującą postać:

$$A = \mathsf{m}(\tau, \mathcal{A}) = \begin{bmatrix} b_1 & 0 & \ldots & 0 & a_{11} & a_{12} & \ldots & a_{1\ell} \\ 0 & b_1 & \ldots & 0 & a_{21} & a_{22} & \ldots & a_{2\ell} \\ & & \ldots & & & & \ldots & \\ 0 & 0 & \ldots & b_1 & a_{m1} & a_{m2} & \ldots & a_{m\ell} \\ 0 & 0 & \ldots & 0 & d_1 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 & 0 & d_2 & \ldots & 0 \\ & & \ldots & & & & \ldots & \\ 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & d_\ell \end{bmatrix}$$

Pokażemy teraz, że bazę $\mathcal{A}$ można zmodyfikować tak, by w nowej bazie endomorfizm τ miał macierz diagonalną. Przede wszystkim dla każdych $x_{ji} \in K$ zbiór

$$\mathcal{B} := \{u_1, \ldots, u_m, v_1 + x_{11}u_1 + \cdots + x_{1m}u_m, \ \ldots, \ v_\ell + x_{\ell 1}u_1 + \cdots + x_{\ell m}u_m\}$$

jest bazą przestrzeni V. Udowodnimy teraz, że skalary x_{ji} można tak dobrać, że wszystkie wektory bazy $\mathcal{B}$ są wektorami własnymi endomorfizmu τ. Rzeczywiście, pokażemy, że można tak dobrać $x_{ji} \in K$, że każdy z wektorów $v_j + x_{j1}u_1 + \cdots + x_{jm}u_m$ jest wektorem własnym endomorfizmu τ należącym do wartości własnej d_j. Poszukiwane skalary x_{ji} muszą więc spełniać układ równań

$$\tau(v_j + x_{j1}u_1 + \cdots + x_{jm}u_m) = d_j(v_j + x_{j1}u_1 + \cdots + x_{jm}u_m), \quad j = 1, \ldots, \ell.$$

Wykorzystując (9.2) otrzymujemy

$$a_{1j}u_1 + \cdots + a_{mj}u_m + d_j v_j + b_1(x_{j1}u_1 + \cdots + x_{jm}u_m) = d_j(v_j + x_{j1}u_1 + \cdots + x_{jm}u_m),$$

skąd wobec zauważonego już wcześniej faktu, że $d_j \neq b_1$ dla wszystkich $j = 1, \ldots, \ell$, mamy

$$x_{j1} = \frac{a_{1j}}{d_1 - b_1}, \ldots, x_{jm} = \frac{a_{mj}}{d_j - b_1}.$$

A więc w bazie $\mathcal{B}$ endomorfizm τ ma macierz diagonalną

$$\operatorname{diag}(b_1, \ldots, b_1, d_1, \ldots, d_\ell),$$

co kończy dowód twierdzenia. □

WNIOSEK **9.4.2.** *Niech A będzie macierzą endomorfizmu τ przestrzeni V nad ciałem K w pewnej bazie przestrzeni V. Macierz A jest podobna do macierzy diagonalnej wtedy i tylko wtedy gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn parami różnych czynników liniowych.*

Dowód. Wystarczy zastosować argumentację użytą w dowodzie wniosku 9.3.8. □

9.5 Zadania

1. Niech $\tau \in \mathsf{End}_K V$ i niech $U < V$ będzie podprzestrzenią $\tau-$niezmienniczą. Udowodnić, że jeśli τ jest endomorfizmem diagonalizowalnym (triangularyzowalnym), to zacieśnienie $\tau_{|U}$ endomorfizmu τ do podprzestrzeni U jest endomorfizmem diagonalizowalnym (triangularyzowalnym).

2. Udowodnić, że endomorfizm τ przestrzeni V jest triangularyzowalny wtedy i tylko wtedy gdy każda niezerowa podprzestrzeń $\tau-$niezmiennicza przestrzeni V zawiera wektor własny endomorfizmu τ.

Wskazówka. Wykorzystać twierdzenie 10.1.7.

3. Niech $\rho, \tau \in \mathsf{End}_K V$.
(a) Udowodnić, że endomorfizmy $\rho\tau$ i $\tau\rho$ mają te same wartości własne.
(b) Udowodnić, że jeśli ρ i τ są triangularyzowalne i $\rho\tau = \tau\rho$, to ρ i τ mają wspólny wektor własny.

4. Endomorfizmy $\rho, \tau \in \mathsf{End}_K V$ nazywamy *równocześnie* diagonalizowalnymi, jeśli istnieje baza $\mathcal{B}$ przestrzeni V taka, że obydwie macierze $\mathsf{m}(\rho, \mathcal{B})$ i $\mathsf{m}(\tau, \mathcal{B})$ są diagonalne. Udowodnić, że endomorfizmy diagonalizowalne ρ i τ przestrzeni V są równocześnie diagonalizowalne wtedy i tylko wtedy, gdy są przemienne: $\rho\tau = \tau\rho$.

Wskazówka. Wykorzystać twierdzenie 10.1.7.

5. Pokazać, że macierz

$$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

jest diagonalizowalna nad ciałem liczb zespolonych, ale nie jest diagonalizowalna nad ciałem liczb rzeczywistych.

Rozdział 10

Algebra liniowa: Postacie kanoniczne

Ostatnie zmiany 27.11.2010 r.

W tym rozdziale wskażemy postacie kanoniczne macierzy endomorfizmów znane jako postać kanoniczna Jordana i postać kanoniczna Frobeniusa (nazywana także postacią kanoniczną wymierną).

W pierwszym przypadku zakładać będziemy, że wielomian minimalny p_τ endomorfizmu $\tau \in \mathsf{End}_K V$ rozkłada się nad ciałem K na iloczyn czynników liniowych. W szczególności, gdy K jest ciałem algebraicznie domkniętym, np. gdy $K = \mathbb{C}$, warunek ten spełniony jest dla *wszystkich* endomorfizmów dowolnej przestrzeni wektorowej nad ciałem K. W ten sposób otrzymujemy klasyczne twierdzenie o istnieniu postaci kanonicznej Jordana dla endomorfizmów przestrzeni zespolonych.

W przypadku postaci kanonicznej Frobeniusa nie będziemy nakładać żadnych warunków na wielomian minimalny endomorfizmu $\tau \in \mathsf{End}_K V$ i uzyskamy postać kanoniczną macierzy dowolnego endomorfizmu przestrzeni wektorowej nad dowolnym ciałem K. Ta ogólność jest jednak okupiona kształtem macierzy w postaci kanonicznej Frobeniusa. Nie są one tak wygodne w zastosowaniach jak macierze w postaci kanonicznej Jordana.

Twierdzenia o postaciach kanonicznych macierzy endomorfizmu $\tau \in \mathsf{End}_K V$ uzyskamy przez potraktowanie przestrzeni wektorowej V jako $K[X]-$modułu V_τ i wykorzystanie twierdzeń strukturalnych dla modułów nad pierścieniami ideałów głównych, udowodnionych w rozdziale 4.

Twierdzenie 10.1.7 o rozkładzie prymarnym redukuje problem znajdowania macierzy endomorfizmu do przypadku gdy wielomian minimalny endomorfizmu jest potęgą wielomianu nierozkładalnego. W związku z tym w dalszym ciągu zajmować się będziemy głównie przypadkiem, gdy endomorfizm $\tau \in \mathsf{End}_K V$ przestrzeni wektorowej V ma wielomian minimalny postaci q^m, gdzie q jest wielomianem nierozkładalnym nad ciałem K.

10.1 Struktura $K[X]-$modułu V_τ

Przypomnijmy, że dla każdego endomorfizmu τ przestrzeni wektorowej V wprowadziliśmy strukturę $K[X]-$modułu na przestrzeni V definiując działanie zewnętrzne

$$K[X] \times V \to V, \quad (f, v) \mapsto fv := f(\tau)(v).$$

Tak skonstruowany $K[X]-$moduł oznaczamy V_τ (zob. przykład 3.1.4).

Jeśli dla podprzestrzeni U przestrzeni wektorowej V mamy $\tau(U) \subseteq U$, to także $fu = f(\tau)(u) \in U$ dla każdego wielomianu $f \in K[X]$ i dla każdego $u \in U$. Zatem każda podprzestrzeń $\tau-$niezmiennicza U przestrzeni V jest podmodułem $K[X]-$modułu V_τ. Także na odwrót, jeśli U jest podmodułem $K[X]-$modułu V_τ, to dla każdego wielomianu $f \in K[X]$ mamy $f(\tau)(U) = fU \subseteq U$. Zatem w szczególności także $\tau(U) \subseteq U$.
A więc, *U jest podmodułem $K[X]-$modułu V_τ wtedy i tylko wtedy, gdy U jest podprzestrzenią niezmienniczą endomorfizmu τ.*

Znaczenie podprzestrzeni $\tau-$niezmienniczych polega na tym, że są to jedyne podprzestrzenie U przestrzeni V, dla których zacieśnienie $\tau|_U$ endomorfizmu τ do podprzestrzeni U jest endomorfizmem podprzestrzeni U. Jest to podstawa indukcyjnego podejścia do opisu działania endomorfizmu na przestrzeni wektorowej. W związku z tym rozpoczniemy od ustalenia elementarnych własności wielomianu minimalnego zacieśnienia endomorfizmu τ do podprzestrzeni niezmienniczej.

LEMAT **10.1.1.** *Niech $\tau \in \mathsf{End}_K V$ i niech $U \subseteq V$ będzie podprzestrzenią niezmienniczą endomorfizmu τ. Wtedy*
(a) *Odwzorowanie $\tau_1 : U \to U$, $\tau_1(u) = \tau(u)$ jest endomorfizmem przestrzeni U.*
(b) *Jeśli $q \in K[X]$ oraz $q(\tau) = 0_V$, to $q(\tau_1) = 0_U$.*
(c) *Wielomian minimalny endomorfizmu τ_1 dzieli wielomian minimalny endomorfizmu τ.*

Dowód. (a) wynika wprost z definicji podprzestrzeni niezmienniczej endomorfizmu.
(b) Zacieśnienie endomorfizmu $q(\tau)$ do podprzestrzeni U jest endomorfizmem $q(\tau_1)$ przestrzeni U. Stąd dla dowolnego $u \in U$ mamy $q(\tau_1)(u) = q(\tau)(u) = 0_V(u) = 0$. Stąd $q(\tau_1) = 0_U$.
(c) Jeśli p jest wielomianem minimalnym endomorfizmu τ, to na podstawie (b) mamy $p(\tau_1) = 0_U$. Zatem wielomian minimalny endomorfizmu τ_1 dzieli p na podstawie definicji wielomianu minimalnego endomorfizmu. □

DEFINICJA **10.1.2.** W oznaczeniach lematu 10.1.1, endomorfizm τ_1 przestrzeni U nazywa się endomorfizmem *indukowanym* przez endomorfizm τ przestrzeni V na podprzestrzeni $\tau-$niezmienniczej U.

10.1.1 Rozkład prymarny modułu V_τ

Sformułujemy tutaj twierdzenie 4.1.6 o strukturze modułów torsyjnych nad pierścieniami ideałów głównych dla $K[X]-$modułu V_τ. Uzupełnimy je dodatkowymi informacjami i uzyskamy w ten sposób ogólne twierdzenie o rozkładzie przestrzeni wektorowej (twierdzenie 10.1.7) na sumę prostą podprzestrzeni niezmienniczych endomorfizmu $\tau \in \mathsf{End}_K V$ wyznaczonych przez czynniki wielomianu minimalnego endomorfizmu τ nierozkładalne nad ciałem K. Twierdzenie to jest podstawą analizy postaci kanonicznych macierzy endomorfizmów i redukuje badanie macierzy endomorfizmu do przypadku, gdy wielomian minimalny endomorfizmu jest potęgą wielomianu nierozkładalnego nad ciałem K.

W rozdziale 4 rozpatrywaliśmy już anihilatory modułów ograniczonych. Przypomnijmy, że moduł M nad pierścieniem ideałów głównych A nazywa się ograniczony, jeśli istnieje niezerowy element $a \in A$ taki, że $aM = 0$. Zbiór wszystkich elementów $a \in A$ takich, że $aM = 0$ nazywa się anihilatorem modułu M i oznacza $\mathsf{Ann}\, M$. Łatwo zauważyć, że $\mathsf{Ann}\, M$ jest ideałem w pierścieniu A i wobec tego, że A jest pierścieniem ideałów głównych mamy

$$\mathsf{Ann}\, M = (p) = pA$$

dla pewnego niezerowego elementu $p \in A$. Generator p anihilatora modułu M jest wyznaczony jednoznacznie z dokładnością do stowarzyszenia elementów pierścienia A i nazywa się także anihilatorem modułu M.

Ustalimy teraz potrzebne w dalszym ciągu własności anihilatora modułu ograniczonego. W poniższych lematach zakładamy, że M jest modułem ograniczonym nad pierścieniem ideałów głównych A.

LEMAT **10.1.3.** *Jeśli moduł M jest sumą swoich podmodułów,*

$$M = M_1 + \cdots + M_k, \quad (p) = \mathsf{Ann}\, M, \quad (p_i) = \mathsf{Ann}\, M_i,$$

to $p = \mathrm{nww}(p_1, \ldots, p_k)$ z dokładnością do stowarzyszenia elementów w pierścieniu A.

Dowód. Niech $w = \mathrm{nww}(p_1, \ldots, p_k)$. Ponieważ $pM_i = 0$, więc $p_i \mid p$ i wobec tego także $w \mid p$. Z drugiej strony, dla dowolnego $m \in M$ mamy przedstawienie $m = m_1 + \cdots + m_k$, gdzie $m_i \in M_i$. Zatem wobec $p_i \mid w$,

$$wm = wm_1 + \cdots + wm_k = 0$$

skąd wynika, że $p \mid w$. A więc p i w są stowarzyszone w A. □

Moduł ograniczony M jest modułem torsyjnym, zatem na podstawie twierdzenia 4.1.6 jest sumą prostą swoich prymarnych składowych $T_q(M)$, gdzie q przebiega wszystkie parami niestowarzyszone elementy pierwsze pierścienia A. Dwa następujące lematy udowodniliśmy już w rozdziale 4 (lemat 4.1.4 i lemat 4.1.5).

LEMAT **10.1.4.** *Niech p będzie anihilatorem modułu ograniczonego M i niech q będzie elementem pierwszym pierścienia A. Wtedy*

$$T_q(M) \neq 0 \iff q \mid p.$$

LEMAT **10.1.5.** *Jeśli q^ℓ jest najwyższą potęgą elementu pierwszego q dzielącą anihilator p modułu ograniczonego M, to*

$$T_q(M) = \Big\{m \in M : q^\ell m = 0\Big\}.$$

Rozpatrzmy teraz $K[X]-$moduł V_τ. Jest to moduł ograniczony, gdyż $p_\tau v = p_\tau(\tau)(v) = 0_V(v) = 0$, a więc $p_\tau V = 0$. Ponadto

$$\mathsf{Ann}\, V_\tau = \Big\{f \in K[X] : fv = 0 \quad \forall\, v \in V\Big\} = \Big\{f \in K[X] : f(\tau) = 0_V\Big\} = (p_\tau),$$

to znaczy, anihilator $K[X]-$modułu V_τ jest ideałem głównym generowanym przez wielomian minimalny endomorfizmu τ. Moduł V_τ jako moduł *ograniczony* nad pierścieniem $K[X]$, jest na podstawie twierdzenia 4.1.6 sumą prostą swoich prymarnych składowych:

$$V_\tau = \bigoplus T_q(V_\tau),$$

gdzie q przebiega parami niestowarzyszone wielomiany nierozkładalne pierścienia $K[X]$. Składowe prymarne $T_q(V_\tau)$ są podprzestrzeniami $\tau-$niezmienniczymi przestrzeni wektorowej τ.

Sformułujemy teraz rezultaty lematów 10.1.3, 10.1.4 i 10.1.5 dla modułu V_τ.

LEMAT **10.1.6.** (a) *Niech $V = V_1 + \cdots + V_k$, gdzie $V_1, \ldots, V_k$ są podprzestrzeniami niezmienniczymi endomorfizmu τ przestrzeni V. Niech τ_i będzie zacieśnieniem endomorfizmu τ do podprzestrzeni V_i i niech p_i będzie wielomianem minimalnym endomorfizmu τ_i dla $i = 1, \ldots, k$.*
Wtedy wielomian minimalny $p = p_\tau$ endomorfizmu τ jest najmniejszą wspólną wielokrotnością wielomianów $p_1, \ldots, p_k$:

$$p = \mathrm{nww}(p_1, \ldots, p_k).$$

(b) *Jeśli wielomian nierozkładalny $q \in K[X]$ nie dzieli wielomianu minimalnego p_τ, to $T_q(V_\tau) = 0$.*
(c) *Niech q^ℓ będzie najwyższą potęgą wielomianu nierozkładalnego q dzielącą wielomian minimalny p_τ endomorfizmu τ. Wtedy*

$$T_q(V) = \{v \in V : \quad q^\ell(\tau)(v) = 0\} \neq 0.$$

Możemy teraz sformułować twierdzenie strukturalne (twierdzenie 4.1.6) dla modułów nad pierścieniami ideałów głównych w przypadku $K[X]-$modułu V_τ. Milcząco zakładamy oczywiście, że przestrzeń V jest niezerowa.

TWIERDZENIE **10.1.7** (Twierdzenie o rozkładzie prymarnym)**.** *Niech $\tau \in \mathsf{End}_K V$ i niech $p := p_\tau \in K[X]$ będzie wielomianem minimalnym endomorfizmu τ. Niech*

$$p = q_1^{m_1} \cdots q_k^{m_k}, \quad m_1 \geqslant 1, \ldots, m_k \geqslant 1$$

będzie rozkładem wielomianu p na iloczyn potęg parami niestowarzyszonych wielomianów nierozkładalnych nad ciałem K. Dla każdego $i = 1, \ldots, k$ niech

$$V_i := \ker q_i^{m_i}(\tau) \ = \ \{v \in V : \quad q_i^{m_i}(\tau)(v) = 0\}.$$

Wtedy

(a) *V_i jest niezerową podprzestrzenią niezmienniczą endomorfizmu τ.*

(b) *$V = V_1 \oplus \cdots \oplus V_k$.*

(c) *Endomorfizm indukowany τ_i na przestrzeni V_i ma wielomian minimalny $q_i^{m_i}$.*

Dowód. (a) Na podstawie lematu 10.1.6 podprzestrzeń $V_i = T_{q_i}(V)$ jest q_i-prymarną składową modułu V_τ, zatem jest niezerową podprzestrzenią niezmienniczą przestrzeni V.

(b) wynika z (a) i z twierdzenia 4.1.6.
(c) Z określenia podprzestrzeni V_i wynika, że dla każdego $v \in V_i$ mamy

$$q_i^{m_i}(\tau_i)(v) = q_i^{m_i}(\tau)(v) = 0.$$

Innymi słowy $q_i^{m_i}(\tau_i) = 0_{V_i}$, co oznacza, że wielomian minimalny p_i endomorfizmu indukowanego τ_i jest dzielnikiem wielomianu $q_i^{m_i}$. Ponieważ wielomian q_i jest nierozkładalny nad ciałem K, wynika stąd, że $p_i = q_i^{n_i}$, gdzie $n_i \leqslant m_i$. Na podstawie lematu 10.1.6 i punktu (b), wielomian minimalny endomorfizmu τ jest najmniejszą wspólną wielokrotnością wielomianów p_i, a więc ich iloczynem. Stąd

$$\prod_{i=1}^{k} q_i^{m_i} = p = \prod_{i=1}^{k} q_i^{n_i}.$$

Wobec jednoznaczności rozkładu na czynniki nierozkładalne w pierścieniu $K[X]$ otrzymujemy $m_i = n_i$ dla $i = 1, \ldots, k$. A więc wielomian minimalny p_i endomorfizmu indukowanego τ_i jest równy $q_i^{m_i}$. □

Twierdzenie 10.1.7 o rozkładzie ma następującą interpretację macierzową. W oznaczeniach tego twierdzenia, niech $\mathcal{B}_i$ będzie bazą uporządkowaną podprzestrzeni V_i i niech $B_i = \mathsf{m}(\tau_i, \mathcal{B}_i)$ będzie macierzą endomorfizmu indukowanego τ_i podprzestrzeni V_i. Wtedy wobec części (b) twierdzenia zbiór

$$\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$$

jest bazą przestrzeni V i endomorfizm τ przestrzeni V ma w tej bazie macierz klatkową

$$\mathsf{m}(\tau, \mathcal{B}) = \begin{bmatrix} B_1 & & & \\ & B_2 & & \\ & & \ddots & \\ & & & B_k \end{bmatrix}. \tag{10.1}$$

Jeśli $\dim V_i = n_i$, to $B_i \in M_{n_i}(K)$ oraz $n = \dim V = n_1 + \cdots + n_k$. W ten sposób twierdzenie o rozkładzie pozwala uczynić pierwszy krok w kierunku *diagonalizacji* macierzy endomorfizmu τ. Dalsze upraszczanie macierzy endomorfizmu τ sprowadza się do poszukiwania baz w przestrzeniach V_i, względem których endomorfizmy τ_i mają jak najprostszą macierz. Jednakże endomorfizm τ_i ma wielomian minimalny $q_i^{m_i}$ i w ten sposób problem znalezienia bazy przestrzeni, w której endomorfizm ma satysfakcjonującą nas macierz, został sprowadzony do przypadku, gdy wielomian minimalny endomorfizmu jest potęgą wielomianu nierozkładalnego.

Jako przykład zastosowania twierdzenia o rozkładzie prymarnym podamy jeszcze jeden dowód twierdzenia o diagonalizowalności endomorfizmu. Dowód warunku koniecznego diagonalizowalności wskazany w twierdzeniu 9.2.2 jest prosty i bezpośredni, natomiast dowód warunku wystarczającego podany w twierdzeniu 9.4.1 jest dość skomplikowany. Poniższy dowód jest bardzo przejrzysty.

Twierdzenie **10.1.8.** *Endomorfizm $\tau \in \mathsf{End}_K V$ jest diagonalizowalny wtedy i tylko wtedy, gdy wielomian minimalny p_τ endomorfizmu τ rozkłada się nad ciałem K na iloczyn parami różnych czynników liniowych:*

$$p_\tau = (X - b_1) \cdots (X - b_k), \quad b_1, \ldots, b_k \in K, \quad b_i \neq b_j \quad \text{dla} \quad i \neq j.$$

Dowód. Udowodnimy tylko wystarczalność warunku. Załóżmy, że wielomian p_τ ma wskazany rozkład nad ciałem K. Niech $V_i = \ker(\tau - b_i 1_V)$. Na podstawie twierdzenia o rozkładzie prymarnym V_i jest niezerową podprzestrzenią $\tau-$niezmienniczą przestrzeni V oraz $V = V_1 \oplus \cdots \oplus V_k$. Zauważmy, że każdy niezerowy wektor podprzestrzeni V_i jest wektorem własnym endomorfizmu τ należącym do wartości własnej b_i. Jeśli $\mathcal{B}_i$ jest dowolną bazą podprzestrzeni V_i, to endomorfizm indukowany τ_i podprzestrzeni V_i ma względem tej bazy macierz diagonalną (faktycznie skalarną) $B_i = b_i I_i$, gdzie I_i oznacza macierz jednostkową stopnia $\dim V_i$. Zatem macierz klatkowa (10.1) jest diagonalna. □

10.1.2 Rozkład modułu V_τ na sumę prostą podmodułów cyklicznych

Niech τ będzie endomorfizmem przestrzeni wektorowej V. W $K[X]-$module V_τ podmoduł cykliczny generowany przez wektor $v \in V$ oznaczamy $K[X]v$ lub $K[\tau]v$. Jest to zbiór wszystkich wektorów przestrzeni V postaci $fv = f(\tau)(v)$, gdzie f jest dowolnym wielomianem o współczynnikach z ciała K. Jak każdy podmoduł modułu V_τ, podmoduł cykliczny $K[X]v$ jest podprzestrzenią $\tau-$niezmienniczą przestrzeni wektorowej V. Podprzestrzenie $K[X]v$ nazywamy także podprzestrzeniami $\tau-$cyklicznymi przestrzeni wektorowej V.

Ponieważ moduł V_τ jest skończenie generowanym modułem nad pierścieniem euklidesowym $K[X]$, więc jego strukturę opisuje twierdzenie 4.2.1 z rozdziału 4. Zanotujmy ten rezultat.

Twierdzenie **10.1.9.** *Dla każdego endomorfizmu τ przestrzeni wektorowej V istnieje rozkład przestrzeni V na sumę prostą podprzestrzeni $\tau-$cyklicznych.*

Główne własności podprzestrzeni $\tau-$cyklicznych opisane są w następującym lemacie.

Lemat **10.1.10.** *Niech $U = K[X]v$ będzie podprzestrzenią $\tau-$cykliczną przestrzeni V i niech*

$$q = c_0 + c_1 X + \cdots + c_{m-1} X^{m-1} + X^m \in K[X]$$

będzie wielomianem minimalnym endomorfizmu $\tau|_U$ indukowanego przez τ na podprzestrzeni U. Wtedy

(a) $K[X]v = \mathsf{lin}\{v, \tau(v), \ldots, \tau^{m-1}(v)\}$.
(b) *Zbiór* $\left\{v, \tau(v), \ldots, \tau^{m-1}(v)\right\}$ *jest bazą* $K[X]v$.
(c) $\dim K[X]v = m = \deg q$.

Dowód. (a) Oczywiście $K[X]v \supseteq \mathsf{lin}\{v, \tau(v), \ldots, \tau^{m-1}(v)\}$.
Jeśli natomiast $w = f(\tau)(v) \in K[X]v$, gdzie $f \in K[X]$, to na podstawie twierdzenia o dzieleniu z resztą istnieją wielomiany $g, h \in K[X]$ takie, że

$$f = gq + h, \quad \deg h < m = \deg q.$$

Wtedy wobec $q(\tau)(v) = q(\tau|_U)(v) = 0$ mamy

$$w = f(\tau)(v) = g(\tau)(q(\tau)(v)) + h(\tau)(v) = h(\tau)(v).$$

Zatem wektor w jest kombinacją liniową wektorów $v, \tau(v), \ldots, \tau^{m-1}(v)$.

(b) Sprawdzimy najpierw, że jeśli $f \in K[X]$ oraz $f(\tau)(v) = 0$, to $q|f$.
Rzeczywiście, dla dowolnego wektora

$$u = a_0 v + a_1\tau(v) + \cdots + a_{m-1}\tau^{m-1}(v) = g(\tau)(v) \in U,$$

gdzie $g = a_0 + a_1 X + \cdots + a_{m-1}X^{m-1} \in K[X]$, mamy

$$\begin{aligned} f(\tau)(u) &= f(\tau)(g(\tau)(v)) \\ &= (f(\tau)g(\tau))(v) \;=\; (g(\tau)f(\tau))(v)) = g(\tau)(f(\tau)(v)) = g(\tau)(0) = 0. \end{aligned}$$

Zatem $f(\tau|_U) = 0_U$ i wielomian minimalny q endomorfizmu $\tau|_U$ dzieli f.
Stąd wynika już, że wektory $v, \tau(v), \ldots, \tau^{m-1}(v)$ są liniowo niezależne. Jeśli bowiem

$$b_0 v + b_1\tau(v) + \cdots + b_{m-1}\tau^{m-1}(v) = 0$$

dla pewnych $b_0, b_1, \ldots, b_{m-1} \in K$, to dla wielomianu

$$f = b_0 + b_1 X + \cdots + b_{m-1}X^{m-1} \in K[X]$$

mamy $f(\tau)(v) = 0$. Stąd zaś jak już wiemy wynika, że $q|f$, co dla niezerowego wielomianu f jest niemożliwe, gdyż wtedy stopień wielomianu f jest co najwyżej $m-1$. Zatem f jest wielomianem zerowym i wobec tego wektory $v, \tau(v), \ldots, \tau^{m-1}(v)$ są liniowo niezależne.
Na podstawie (a) zbiór $\{v, \tau(v), \ldots, \tau^{m-1}(v)\}$ jest więc bazą przestrzeni U.

(c) wynika z (b). □

Możemy teraz rozstrzygnąć problem znalezienia optymalnego oszacowania dla stopnia wielomianu minimalnego endomorfizmu skończenie wymiarowej przestrzeni wektorowej. Przypomnijmy, że jak dotąd, jedynej informacji na ten temat dostarcza wniosek 8.4.3, z którego otrzymujemy, że jeśli $\tau \in \mathsf{End}_K V$ oraz $\dim_K V = n$, to $\deg p_\tau \leqslant n^2$.

Twierdzenie **10.1.11.** *Stopień wielomianu minimalnego dowolnego endomorfizmu przestrzeni $n-$wymiarowej nie przekracza n.*

Dowód. Niech $\tau \in \mathsf{End}_K V$ oraz $\dim_K V = n$. Zgodnie z twierdzeniem 10.1.9 mamy rozkład

$$V = U_1 \oplus \cdots \oplus U_k,$$

gdzie U_i są podprzestrzeniami $\tau-$cyklicznymi przestrzeni V. Niech τ_i będzie endomorfizmem indukowanym przez τ na U_i i niech $p_i = p_{\tau_i}$ będzie wielomianem minimalnym endomorfizmu τ_i. Na podstawie lematu 10.1.6 mamy $p_\tau = \mathrm{nww}(p_1, \ldots, p_k)$. Stąd wynika, że p_τ dzieli iloczyn $p_1 \cdots p_k$ i wobec tego

$$\deg p_\tau \leqslant \sum_{i=1}^{k} \deg p_i.$$

Z drugiej strony, na podstawie lematu 10.1.10 mamy $\deg p_i = \dim U_i$ i wobec tego

$$\sum_{i=1}^{k} \deg p_i = \sum_{i=1}^{k} \dim U_i = \dim V = n.$$

Zatem $\deg p_\tau \leqslant n$. □

Drugą ważną obserwacją wynikającą z lematów 10.1.6 i 10.1.10 jest możliwość efektywnego wyznaczenia wielomianu minimalnego dowolnego endomorfizmu skończenie wymiarowej przestrzeni wektorowej. Jeśli $\tau \in \mathsf{End}_K V$ oraz $\mathcal{B} = \{v_1, \ldots, v_n\}$ jest bazą przestrzeni V, to dla podprzestrzeni $\tau-$cyklicznych $U_i = K[X]v_i$ mamy oczywiście rozkład

$$V = U_1 + \cdots + U_n$$

przestrzeni V na sumę podprzestrzeni $\tau-$niezmienniczych. Na podstawie lematu 10.1.6, jeśli τ_i jest zacieśnieniem endomorfizmu τ do podprzestrzeni U_i i p_i jest wielomianem minimalnym endomorfizmu τ_i dla $i = 1, \ldots, n$, to wielomian minimalny p_τ endomorfizmu τ jest najmniejszą wspólną wielokrotnością wielomianów $p_1, \ldots, p_n$:

$$p_\tau = \mathrm{nww}(p_1, \ldots, p_n).$$

Dla wyznaczenia wielomianu p_τ należy więc wyznaczyć wszystkie wielomiany $p_1, \ldots, p_n$. Postępujemy tu następująco. Badając kolejno układy wektorów

$$\{v_i, \tau(v_i)\}, \quad \{v_i, \tau(v_i), \tau^2(v_i)\}, \quad \{v_i, \tau(v_i), \tau^2(v_i), \tau^3(v_i)\}, \ldots$$

znajdujemy największą liczbę naturalną m_i taką, że zbiór

$$\{v_i, \tau(v_i), \tau^2(v_i), \ldots, \tau^{m_i-1}(v_i)\}$$

jest liniowo niezależny. Wtedy zbiór ten jest bazą podprzestrzeni U_i. Ponadto istnieją $c_0, c_1, \ldots, c_{m_i-1} \in K$ takie, że

$$c_0 v_i + c_1 \tau(v_i) + \cdots + c_{m_i-1}\tau^{m_i-1}(v) + \tau^{m_i}(v) = 0$$

i wtedy wielomian

$$f_i = c_0 + c_1 X + \cdots + c_{m_i-1}X^{m_i-1} + X^{m_i}$$

jest wielomianem minimalnym endomorfizmu $\tau_i = \tau|_{U_i}$. Rzeczywiście, f_i jest wielomianem najniższego stopnia wśród niezerowych wielomianów $g \in K[X]$ takich, że $g(\tau)(v_i) = 0$. Wobec tego $\deg p_{\tau_i} \geqslant m_i = \deg f_i$. Z drugiej strony, jak pokazaliśmy w dowodzie części (b) lematu 10.1.10, jeśli dla $f_i \in K[X]$ mamy $f_i(\tau)(v_i) = 0$, to $p_{\tau_i} \mid f_i$. Wobec tego $p_{\tau_i} = f_i$.

10.2 Endomorfizmy nilpotentne

Udowodnimy tutaj twierdzenie o postaci kanonicznej Jordana macierzy endomorfizmów nilpotentnych. Głównym narzędziem będzie twierdzenie o rozkładzie skończenie generowanych modułów nad pierścieniami euklidesowymi na sumy proste podmodułów cyklicznych przystosowane do $K[X]-$modułu V_σ dla endomorfizmu nilpotentnego σ (twierdzenie 10.1.9).

Jeśli endomorfizm $\tau \in \mathsf{End}_K V$ ma wielomian minimalny $p = (X - a)^m$, to dla endomorfizmu $\sigma = \tau - a1_V$ mamy

$$0_V = p(\tau) = (\tau - a1_V)^m = \sigma^m.$$

A więc endomorfizm σ jest *nilpotentny*.
Na odwrót, jeśli σ jest endomorfizmem nilpotentnym przestrzeni V oraz $\sigma^m = 0_V$, to dla dowolnego $a \in K$ endomorfizm $\tau = \sigma + a1_V$ ma wielomian minimalny będący potęgą wielomianu liniowego $X - a$. Mamy bowiem

$$0_V = \sigma^m = (\tau - a1_V)^m,$$

czyli τ jest zerem wielomianu $(X - a)^m$. Ponieważ dla dowolnej bazy $\mathcal{B}$ przestrzeni V mamy

$$\mathsf{m}(\tau, \mathcal{B}) = \mathsf{m}(\sigma + a1_V, \mathcal{B}) = \mathsf{m}(\sigma, \mathcal{B}) + \mathsf{m}(a1_V, \mathcal{B}) = \mathsf{m}(\sigma, \mathcal{B}) + aI$$

więc dla znalezienia stosownej postaci kanonicznej macierzy endomorfizmu τ, którego wielomian minimalny jest potęgą wielomianu liniowego, musimy najpierw zbadać postać kanoniczną macierzy endomorfizmów nilpotentnych.

10.2.1 Postać kanoniczna Jordana

Endomorfizm nilpotentny $\sigma \in \mathsf{End}_K V$ spełnia $\sigma^m = 0_V$ dla pewnej liczby naturalnej m. Najmniejszą liczbę naturalną m o tej własności nazywamy *stopniem* endomorfizmu nilpotentnego σ (lub stopniem nilpotentności endomorfizmu σ). A więc m jest stopniem endomorfizmu nilpotentnego σ jeśli

$$\sigma^m = 0_V \quad \text{i} \quad \sigma^{m-1} \neq 0_V,$$

lub równoważnie, gdy $X^m \in K[X]$ jest wielomianem minimalnym endomorfizmu σ. Na podstawie twierdzenia 10.1.11 mamy $m \leqslant n = \dim V$.

Niech σ będzie endomorfizmem nilpotentnym przestrzeni V stopnia m oraz $U = K[X]v$ niech będzie podprzestrzenią $\sigma-$cykliczną przestrzeni V generowaną przez dowolny wektor $v \in V$. Niech $\sigma_1 = \sigma|_U$ będzie endomorfizmem indukowanym przez σ na podprzestrzeni U. Wtedy wielomian minimalny p_{σ_1} dzieli wielomian $p_\sigma = X^m$ (na podstawie lematu 10.1.1), zatem $p_{\sigma_1} = X^{m_1}$, gdzie $m_1 \leqslant m$. Inaczej mówiąc, σ_1 jest endomorfizmem nilpotentnym przestrzeni U stopnia nilpotentności m_1. Na podstawie lematu 10.1.10 wektory $v, \sigma(v), \ldots, \sigma^{m_1-1}(v)$ tworzą bazę podprzestrzeni U.

LEMAT **10.2.1.** *Niech σ będzie endomorfizmem nilpotentnym przestrzeni V i niech σ_1 będzie endomorfizmem indukowanym przez σ na podprzestrzeni $\sigma-$cyklicznej $U = K[X]v$. Jeśli m_1 jest stopniem nilpotentności endomorfizmu σ_1, to*

$$\mathcal{B} = \{v, \sigma(v), \ldots, \sigma^{m_1-1}(v)\}$$

jest bazą przestrzeni U oraz

$$\mathsf{m}(\sigma_1, \mathcal{B}) = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & 0 \\ 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & 1 & 0 & \ldots & 0 & 0 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & 0 \end{bmatrix} =: J_{m_1}.$$

Dowód. $\sigma(\sigma^{i-1}(v)) = \sigma^i(v)$ dla $i = 1, \ldots, m$. □

DEFINICJA **10.2.2.** Macierz J_{m_1} nazywamy *osobliwą klatką Jordana* stopnia m_1.

Macierz J_{m_1} jest macierzą dolną trójkątną. Zmieniając porządek wektorów w bazie $\mathcal{B}$ otrzymamy dla endomorfizmu σ_1 w bazie $\{\sigma^{m_1-1}(v), \ldots, \sigma(v), v\}$ macierz górną trójkątną

$$\begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ & & & \ldots & \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & 0 & 0 & \ldots & 0 \end{bmatrix}.$$

W dalszym ciągu pozostaniemy przy macierzach dolnych trójkątnych.

TWIERDZENIE **10.2.3** (Postać kanoniczna Jordana.)**.** *Niech σ będzie endomorfizmem nilpotentnym stopnia m skończenie wymiarowej przestrzeni wektorowej V. Wtedy istnieją podprzestrzenie $\sigma-$cykliczne $U_1, \ldots, U_r$ przestrzeni V takie, że*

$$V = U_1 \oplus \cdots \oplus U_r \quad \text{oraz} \quad m = \dim U_1 \geqslant \cdots \geqslant \dim U_r.$$

Ponadto, endomorfizm σ_i indukowany na podprzestrzeni U_i przez endomorfizm σ jest endomorfizmem nilpotentnym stopnia $m_i = \dim U_i$.

Dowód. Rozpatrzmy $K[X]-$moduł V_σ. Jest to skończenie generowany moduł nad pierścieniem euklidesowym. Zatem na podstawie twierdzenia 10.1.9 moduł V_σ jest sumą prostą skończonego zbioru podprzestrzeni $\sigma-$cyklicznych $V = U_1 \oplus \cdots \oplus U_r$. Niech σ_i oznacza endomorfizm indukowany na U_i przez σ. Wtedy na podstawie lematu 10.1.1 wielomian minimalny q_i endomorfizmu σ_i jest dzielnikiem wielomianu minimalnego X^m endomorfizmu σ. Zatem $q_i = X^{m_i}$, gdzie $m_i \leqslant m$, skąd wynika, że każdy endomorfizm σ_i jest nilpotentny stopnia m_i. Zmieniając ewentualnie porządek podprzestrzeni $U_1, \ldots, U_r$ możemy zakładać, że $m \geqslant m_1 \geqslant \cdots \geqslant m_r \geqslant 1$. Gdyby $m > m_1$, to dla każdego wektora $v \in U_1 \oplus \cdots \oplus U_r$ mielibyśmy $\sigma^{m-1}(v) = 0$, wbrew temu, że $\sigma^{m-1} \neq 0_V$. Zatem $m = m_1$. Dla dowodu, że $m_i = \dim U_i$ dla $i = 1, \ldots, r$ wystarczy powołać się na lemat 10.1.10. □

Zanotujmy jeszcze wersję macierzową twierdzenia 10.2.3.

TWIERDZENIE **10.2.4.** *Jeśli $\dim V = n$ oraz σ jest endomorfizmem nilpotentnym przestrzeni V stopnia m, to istnieje baza $\mathcal{B}$ przestrzeni V taka, że*

$$\mathsf{m}(\sigma, \mathcal{B}) = \begin{bmatrix} J_{m_1} & 0 & \ldots & 0 \\ 0 & J_{m_2} & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & J_{m_r} \end{bmatrix},$$

gdzie $J_{m_1}, \ldots, J_{m_r}$ są osobliwymi klatkami Jordana stopni $m_1, \ldots, m_r$ oraz

$$m = m_1 \geqslant m_2 \geqslant \cdots \geqslant m_r, \quad m_1 + m_2 + \cdots + m_r = n.$$

Dowód. Wystarczy zastosować lemat 10.2.1 do każdej z podprzestrzeni cyklicznych U_i w twierdzeniu 10.2.3. □

Dla zwięzłego formułowania twierdzeń o postaciach kanonicznych macierzy endomorfizmów wprowadzimy jeszcze jedną definicję.

DEFINICJA **10.2.5.** Niech $M_1, M_2, \ldots, M_k$ będą macierzami kwadratowymi dowolnych stopni o elementach z ciała K. Macierz klatkową

$$M = \begin{bmatrix} M_1 & 0 & \ldots & 0 & 0 \\ 0 & M_2 & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 \\ & & \ldots & & \\ 0 & 0 & \ldots & 0 & M_k \end{bmatrix}$$

nazywamy *sumą prostą* macierzy $M_1, M_2, \ldots, M_k$ i oznaczamy

$$M := M_1 \oplus M_2 \oplus \cdots \oplus M_k.$$

A więc twierdzenie 10.2.4 mówi, że dla endomorfizmu nilpotentnego σ stopnia m istnieje baza przestrzeni V, w której macierz endomorfizmu σ jest sumą prostą osobliwych klatek Jordana stopni $\leqslant m$.

10.2.2 Jednoznaczność postaci kanonicznej Jordana

LEMAT **10.2.6.** *Niech U będzie podprzestrzenią $\sigma-$cykliczną przestrzeni V. Jeśli $\dim U = m$, to dla każdej liczby naturalnej $k \leqslant m$ mamy*

$$\dim \sigma^k(U) = m - k.$$

Dowód. Zbiór $\{v, \sigma(v), \ldots, \sigma^{m-1}(v)\}$ jest bazą podprzestrzeni $\sigma-$cyklicznej U i wobec tego zbiór

$$\{\sigma^k(v), \sigma^{k+1}(v), \ldots, \sigma^{m-1}(v)\}$$

rozpina podprzestrzeń $\sigma^k(U)$. Ponieważ zbiór ten jest liniowo niezależny (jako podzbiór bazy przestrzeni U), jest on bazą podprzestrzeni $\sigma^k(U)$.
Zatem $\dim \sigma^k(U) = m - k$. □

TWIERDZENIE **10.2.7.** *Niech σ będzie endomorfizmem nilpotentnym przestrzeni V i niech*

$$V = U_1 \oplus \cdots \oplus U_r = U_1' \oplus \cdots \oplus U_s'$$

będą dwoma rozkładami przestrzeni V na sumę prostą podprzestrzeni $\sigma-$cyklicznych. Załóżmy, że $\dim U_i = m_i$, $\dim U_j' = n_j$, dla $i = 1, \ldots, r$, $j = 1, \ldots, s$ i załóżmy, że

$$m_1 \geqslant \cdots \geqslant m_r, \quad n_1 \geqslant \cdots \geqslant n_s.$$

Wtedy

$$r = s \quad \text{oraz} \quad m_i = n_i, \quad i = 1, \ldots, r.$$

Dowód. Niech i będzie najmniejszym wskaźnikiem takim, że $m_i \neq n_i$. Możemy oczywiście założyć, że $m_i > n_i$. Zatem

$$m_1 = n_1, \quad \ldots, \quad m_{i-1} = n_{i-1}, \quad m_i > n_i. \tag{10.2}$$

Rozpatrzymy teraz podprzestrzeń $\sigma^{n_i}(V)$ przestrzeni V. Z jednej strony mamy

$$\sigma^{n_i}(V) = \sigma^{n_i}(U_1) \oplus \cdots \oplus \sigma^{n_i}(U_i) \oplus \cdots \oplus \sigma^{n_i}(U_r).$$

Na podstawie lematu 10.2.6 mamy

$$\dim \sigma^{n_i}(U_j) = m_j - n_i, \quad j = 1, \ldots, i.$$

Stąd otrzymujemy

$$\dim \sigma^{n_i}(V) \geqslant (m_1 - n_i) + (m_2 - n_i) + \cdots + (m_i - n_i). \tag{10.3}$$

Z drugiej zaś strony mamy

$$\sigma^{n_i}(V) = \sigma^{n_i}(U_1') \oplus \cdots \oplus \sigma^{n_i}(U_i') \oplus \cdots \oplus \sigma^{n_i}(U_s').$$

Tutaj $\sigma^{n_i}(U_i') = \cdots = \sigma^{n_i}(U_s') = 0$, oraz na podstawie lematu 10.2.6 mamy

$$\dim \sigma^{n_i}(U_j') = n_j - n_i, \quad j = 1, \ldots, i.$$

Stąd otrzymujemy

$$\dim \sigma^{n_i}(V) = (n_1 - n_i) + (n_2 - n_i) + \cdots + (n_{i-1} - n_i)$$

i wobec (10.2) mamy także

$$\dim \sigma^{n_i}(V) = (m_1 - n_i) + (m_2 - n_i) + \cdots + (m_{i-1} - n_i). \tag{10.4}$$

Porównując teraz (10.3) i (10.4) otrzymujemy $m_i - n_i \leqslant 0$, czyli $m_i \leqslant n_i$, wbrew założeniu, że $m_i > n_i$. A więc mamy równości $m_i = n_i$ dla każdego $i \leqslant \min(r, s)$. Ponieważ jednak $\sum_{i=1}^{r} m_i = n = \sum_{j=1}^{s} n_j$, wynika stąd, że także $r = s$. □

Definicja **10.2.8.** Niech σ będzie endomorfizmem nilpotentnym przestrzeni V i niech

$$V = U_1 \oplus \cdots \oplus U_r,$$

będzie rozkładem przestrzeni V na sumę prostą podprzestrzeni $\sigma-$cyklicznych.
Niech $\dim U_i =: m_i$, $i = 1, \ldots, r$ oraz $m_1 \geqslant \cdots \geqslant m_r$.
Ciąg liczb $(m_1, \ldots, m_r)$ nazywa się *ciągiem niezmienników* endomorfizmu σ.

Zauważmy, że endomorfizm nilpotentny σ przestrzeni V ma ciąg niezmienników $(m_1, \ldots, m_r)$ wtedy i tylko wtedy, gdy istnieje baza uporządkowana $\mathcal{B}$ przestrzeni V taka, że

$$\mathsf{m}(\sigma, \mathcal{B}) = J_{m_1} \oplus \cdots \oplus J_{m_r}.$$

Wniosek **10.2.9.** *Ciąg niezmienników endomorfizmu nilpotentnego σ jest wyznaczony jednoznacznie przez endomorfizm σ.*

Twierdzenie **10.2.10.** *Endomorfizmy nilpotentne ρ i τ przestrzeni V są podobne wtedy i tylko wtedy, gdy mają równe ciągi niezmienników.*

Dowód. Endomorfizmy ρ i τ mają równe ciągi niezmienników $(m_1, \ldots, m_r)$ wtedy i tylko wtedy gdy w odpowiednich bazach przestrzeni V mają tę samą macierz klatkową $J_{m_1} \oplus \cdots \oplus J_{m_r}$. Na podstawie twierdzenia 8.7.6 ma to miejsce wtedy i tylko wtedy gdy endomorfizmy ρ i τ są podobne. □

Przypomnijmy, że relacja podobieństwa endomorfizmów przestrzeni wektorowej V jest relacją równoważnościową. Pokażemy, że liczba klas abstrakcji tej relacji jest skończona i wyznaczymy liczbę tych klas w zależności od wymiaru przestrzeni.

Wniosek **10.2.11.** *Liczba klas podobieństwa endomorfizmów nilpotentnych $n-$wymiarowej przestrzeni wektorowej jest równa liczbie partycji liczby naturalnej n.*

Dowód. Tutaj przez *partycję* liczby naturalnej n rozumiemy każde przedstawienie liczby n w postaci

$$n = m_1 + \cdots + m_r, \quad m_1 \geqslant \cdots \geqslant m_r, \quad r \geqslant 1,$$

gdzie m_i są liczbami naturalnymi. Liczbę wszystkich partycji liczby n oznacza się $p(n)$. A więc $p(1) = 1$, $p(2) = 2$, $p(5) = 7$. Słynny rezultat Hardy'ego i Ramanujana z 1917 roku pozwala obliczyć $p(200) = 3972999029388$. [1]
Co do dowodu wniosku zauważmy, że na podstawie twierdzenia 10.2.10 każda klasa podobnych endomorfizmów nilpotentnych wyznacza dokładnie jeden ciąg niezmienników $(m_1, \ldots, m_r)$ i każdy taki ciąg wyznacza partycję liczby $n = \dim V$. A więc liczba klas podobieństwa endomorfizmów nilpotentnych przestrzeni V jest nie większa niż liczba partycji $p(n)$. Na odwrót każda partycja $n = m_1 + \cdots + m_r$ pozwala skonstruować macierz klatkową $J_{m_1} \oplus \cdots \oplus J_{m_r}$, która w sposób naturalny jest macierzą pewnego endomorfizmu nilpotentnego σ na przestrzeni V (i jest także macierzą każdego endomorfizmu podobnego do σ). Przy tym na podstawie twierdzenia 10.2.10 różnym partycjom odpowiadają różne klasy podobieństwa. Zatem liczba partycji liczby n jest nie większa od liczby klas podobieństwa. □

10.3 Postać kanoniczna Jordana

W tym rozdziale wskażemy postać kanoniczną endomorfizmu $\tau \in \mathsf{End}_K V$ w przypadku, gdy wielomian minimalny endomorfizmu τ rozkłada się na czynniki liniowe nad ciałem K. Zauważmy, że na podstawie twierdzenia 9.3.3 przestrzeń V ma bazę, w której macierz endomorfizmu τ jest trójkątna. Zastosowanie twierdzenia 10.1.7 o rozkładzie i rezultatów o postaci kanonicznej endomorfizmów nilpotentnych prowadzi jednak do znacznie dokładniejszego twierdzenia o postaci kanonicznej Jordana macierzy takiego endomorfizmu.

10.3.1 Postać kanoniczna

Załóżmy więc, że endomorfizm $\tau \in \mathsf{End}_K V$ ma wielomian minimalny

$$p = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k},$$

[1] Zob. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford 1960, str. 286.

gdzie $a_1, \ldots, a_k \in K$, przy czym $a_i \neq a_j$ dla $i \neq j$ oraz $m_i \geqslant 1$ dla $i = 1, \ldots, k$. Wtedy

$$p = q_1^{m_1} \cdots q_k^{m_k},$$

gdzie $q_i = X - a_i$ są wielomianami nierozkładalnymi nad ciałem K.
Na podstawie twierdzenia 10.1.7 o rozkładzie, przestrzeń V ma rozkład

$$V = V_1 \oplus \cdots \oplus V_k, \tag{10.5}$$

gdzie V_i jest podprzestrzenią niezmienniczą endomorfizmu τ oraz endomorfizm indukowany τ_i na przestrzeni V_i ma wielomian minimalny $q_i^{m_i} = (X - a_i)^{m_i}$. W szczególności więc $(\tau_i - a_i 1_{V_i})^{m_i} = 0_{V_i}$. Wynika stąd, że endomorfizm $\sigma_i := \tau_i - a_i 1_{V_i}$ przestrzeni V_i jest nilpotentny

$$\sigma_i^{m_i} = 0_{V_i},$$

oraz m_i jest stopniem nilpotentności endomorfizmu σ_i. Zauważmy, że jeśli $\mathcal{B}_i$ jest bazą podprzestrzeni V_i, to

$$\mathsf{m}(\tau_i, \mathcal{B}_i) = \mathsf{m}(a_i 1_{V_i} + \sigma_i, \mathcal{B}_i) = a_i I_{m_i} + \mathsf{m}(\sigma_i, \mathcal{B}_i),$$

gdzie I_{m_i} jest macierzą jednostkową stopnia m_i.
Wobec tego, na podstawie twierdzenia 10.2.4, podprzestrzeń V_i ma bazę $\mathcal{B}_i$ taką, że

$$\mathsf{m}(\tau_i, \mathcal{B}_i) = a_i I_{m_i} + \begin{bmatrix} J_{m_{i1}} & 0 & \ldots & 0 \\ 0 & J_{m_{i2}} & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & J_{m_{ir_i}} \end{bmatrix}$$

$$= \begin{bmatrix} J_{m_{i1}}(a_i) & 0 & \ldots & 0 \\ 0 & J_{m_{i2}}(a_i) & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & J_{m_{ir_i}}(a_i) \end{bmatrix}$$

gdzie $m_i =: m_{i1} \geqslant m_{i2} \geqslant \cdots \geqslant m_{ir_i}$, oraz dla dowolnej liczby naturalnej m i dowolnego $a \in K$ symbol $J_m(a)$ oznacza macierz stopnia m postaci

$$J_m(a) := aI_m + J_m = \begin{bmatrix} a & 0 & 0 & \ldots & 0 & 0 \\ 1 & a & 0 & \ldots & 0 & 0 \\ 0 & 1 & a & \ldots & 0 & 0 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & a \end{bmatrix}.$$

Macierz $J_m(a)$ nazywa się *klatką Jordana* stopnia m wyznaczoną przez element $a \in K$ albo należącą do $a \in K$.

Możemy więc powiedzieć, że macierz $\mathsf{m}(\tau_i, \mathcal{B}_i)$ jest sumą prostą klatek Jordana należących do wartości własnej a_i endomorfizmu τ :

$$\mathsf{m}(\tau_i, \mathcal{B}_i) = J_{m_{i1}}(a_i) \oplus \cdots \oplus J_{m_{ir_i}}(a_i).$$

W macierzy tej na głównej przekątnej występuje wszędzie wartość własna a_i endomorfizmu τ. Liczba elementów diagonalnych (czyli stopień macierzy $\mathsf{m}(\tau_i, \mathcal{B}_i)$) jest

równa wymiarowi podprzestrzeni niezmienniczej V_i przestrzeni V.
Przechodząc teraz do przestrzeni V rozpatrujemy rozkład (10.5) i związaną z nim bazę

$$\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_k$$

przestrzeni V, którą nazywamy *bazą kanoniczną Jordana* przestrzeni V. Dla macierzy endomorfizmu τ w tej bazie mamy

$$\mathsf{m}(\tau, \mathcal{B}) = \mathsf{m}(\tau_1, \mathcal{B}_1) \oplus \cdots \oplus \mathsf{m}(\tau_k, \mathcal{B}_k),$$

czyli macierz o bardzo specjalnej budowie. Jest to właśnie *postać kanoniczna Jordana* macierzy endomorfizmu τ.

TWIERDZENIE **10.3.1.** (Postać kanoniczna Jordana macierzy endomorfizmu.)
Niech $\tau \in \mathsf{End}_K V$ i niech wielomian minimalny p_τ endomorfizmu τ rozkłada się na czynniki liniowe nad ciałem K :

$$p_\tau = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k},$$

gdzie $a_1, \ldots, a_k \in K$, $a_i \neq a_j$ dla $i \neq j$ oraz $m_i \geqslant 1$ dla $i = 1, \ldots, k$.
Wtedy istnieje baza $\mathcal{B}$ przestrzeni V taka, że

$$\mathsf{m}(\tau, \mathcal{B}) = M_1 \oplus \cdots \oplus M_k,$$

gdzie dla $i = 1, \ldots, k$, macierz M_i jest sumą prostą klatek Jordana należących do wartości własnej a_i endomorfizmu τ :

$$M_i = J_{m_{i1}}(a_i) \oplus \cdots \oplus J_{m_{ir_i}}(a_i).$$

Ponadto, jeśli $m_{i1} \geqslant \cdots \geqslant m_{ir_i}$, to $m_{i1} = m_i$ jest krotnością pierwiastka a_i wielomianu minimalnego p_τ endomorfizmu τ.

Postacią kanoniczną Jordana macierzy endomorfizmu τ nazywamy macierz

$$J = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} J_{m_{ij}}(a_i).$$

To przedstawienie macierzy J nie jest jednoznaczne, zależy bowiem od porządku w jakim występują klatki $J_{m_{ij}}(a_i)$. Każdą macierz J tej postaci, niezależnie od porządku występujących w niej klatek Jordana, nazywać będziemy postacią kanoniczną Jordana macierzy endomorfizmu τ. Zmiana porządku klatek Jordana w przedstawieniu macierzy J odpowiada zmianie porządku wektorów w bazie kanonicznej Jordana przestrzeni V. W każdym razie J pozostaje macierzą endomorfizmu τ.

Podkreślmy, że postać kanoniczna Jordana macierzy endomorfizmu $\tau \in \mathsf{End}_K V$ istnieje tylko wtedy, gdy wielomian minimalny endomorfizmu τ rozkłada się na czynniki liniowe nad ciałem K. Istnieją więc ciała K, dla których twierdzenie o istnieniu postaci kanonicznej Jordana jest prawdziwe dla *wszystkich* endomorfizmów *dowolnej* (skończenie wymiarowej) przestrzeni wektorowej nad ciałem K. Są to oczywiście ciała *algebraicznie domknięte*, nad którymi *każdy* wielomian rozkłada się na czynniki liniowe. W szczególności otrzymujemy następujący wniosek.

WNIOSEK **10.3.2.** *Każdy endomorfizm dowolnej przestrzeni wektorowej nad ciałem liczb zespolonych ma macierz w postaci kanonicznej Jordana (w odpowiedniej bazie przestrzeni).*

TWIERDZENIE **10.3.3.** *Niech ρ i τ będą endomorfizmami przestrzeni wektorowej V nad ciałem K i niech wielomiany minimalne endomorfizmów ρ i τ rozkładają się nad ciałem K na iloczyny czynników liniowych. Endomorfizmy ρ i τ są podobne wtedy i tylko wtedy gdy ich postacie kanoniczne Jordana są identyczne.*

Dowód. Jeśli ρ i τ mają w odpowiednich bazach przestrzeni V tę samą macierz, to są podobne na podstawie twierdzenia 8.7.6.
Na odwrót, jeśli $\rho = \sigma^{-1}\tau\sigma$, gdzie $\sigma \in \mathsf{Aut}\, V$ i $\mathcal{A}$ jest dla endomorfizmu ρ bazą kanoniczną Jordana przestrzeni V oraz $\mathsf{m}(\rho, \mathcal{A}) = J$ jest postacią kanoniczną Jordana macierzy endomorfizmu ρ, to na podstawie twierdzenia 8.7.6 endomorfizm τ ma w bazie $\mathcal{B} = \sigma(\mathcal{A})$ także macierz J. Zatem macierze endomorfizmów ρ i τ mają tę samą postać kanoniczną Jordana. □

10.3.2 Jednoznaczność postaci kanonicznej

Przechodzimy teraz do zagadnienia jednoznaczności postaci kanonicznej Jordana macierzy endomorfizmu. Zamierzamy udowodnić, że dwie postacie kanoniczne macierzy endomorfizmu τ mogą się różnić tylko porządkiem klatek. Natomiast liczba klatek należących do danej wartości własnej oraz rozmiary tych klatek są wyznaczone jednoznacznie przez endomorfizm τ i nie zależą od sposobu rozkładu przestrzeni V na sumę prostą podprzestrzeni cyklicznych.

Niech więc $\mathcal{B}$ będzie jakąkolwiek bazą kanoniczną Jordana przestrzeni V i niech

$$\mathsf{m}(\tau, \mathcal{B}) = M_1 \oplus \cdots \oplus M_k, \tag{10.6}$$

gdzie dla $i = 1, \ldots, k$, macierz M_i jest sumą prostą klatek Jordana należących do wartości własnej a_i endomorfizmu τ :

$$M_i = J_{d_{i1}}(a_i) \oplus \cdots \oplus J_{d_{is_i}}(a_i). \tag{10.7}$$

Przedstawieniu macierzy endomorfizmu τ w postaci (10.6) odpowiada rozkład przestrzeni V na sumę prostą podprzestrzeni niezmienniczych:

$$V = U_1 \oplus \cdots \oplus U_k.$$

Ponadto, w każdej podprzestrzeni U_i istnieje baza $\mathcal{B}_i$ taka, że

$$\mathsf{m}(\tau_i, \mathcal{B}_i) = M_i,$$

gdzie $\tau_i = \tau|_{U_i}$ jest endomorfizmem indukowanym przez τ na podprzestrzeni niezmienniczej U_i. Zauważmy, że endomorfizm $\tau_i - a_i 1_{U_i}$ ma w bazie $\mathcal{B}_i$ macierz $M_i - a_i I_{d_i}$, gdzie $d_i = \dim U_i$ oraz I_{d_i} jest macierzą jednostkową stopnia d_i. Ponieważ

$$M_i - a_i I_{d_i} = J_{d_{i1}}(0) \oplus \cdots \oplus J_{d_{is_i}}(0)$$

jest sumą prostą osobliwych klatek Jordana, więc endomorfizm $\tau_i - a_i 1_{U_i}$ jest nilpotentny i ma stopień nilpotentności d_i. Inaczej mówiąc, dla wielomianu $q_i = X - a_i$ mamy

$$q_i^{d_i}(\tau)(U_i) = 0.$$

Przypomnijmy, że w dowodzie twierdzenia 10.3.1 użyliśmy rozkładu

$$V = V_1 \oplus \cdots \oplus V_k, \quad V_i = \ker q_i^{m_i}(\tau), \quad i = 1, \ldots, k. \tag{10.8}$$

z twierdzenia 10.1.7 o rozkładzie, w którym podprzestrzenie niezmiennicze V_i spełniają

$$q_i^{m_i}(\tau)(V_i) = 0,$$

gdzie m_i jest krotnością a_i jako pierwiastka wielomianu minimalnego endomorfizmu τ. Dla dowodu jednoznaczności postaci kanonicznej Jordana musimy więc przede wszystkim pokazać, że

$$\dim U_i = \dim V_i, \quad i = 1, \ldots, k.$$

Udowodnimy znacznie mocniejszy fakt, mianowicie pokażemy, że $U_i = V_i$ dla każdego $i = 1, \ldots, k$. Wynika to z następującego uzupełnienia twierdzenia 10.1.7 o rozkładzie.

TWIERDZENIE **10.3.4.** *Niech $\tau \in \mathsf{End}_K V$ i niech $p_\tau = q_1^{m_1} \cdots q_k^{m_k}$ będzie rozkładem wielomianu minimalnego endomorfizmu τ na iloczyn potęg wielomianów nierozkładalnych nad ciałem K. Niech*

$$V = U_1 \oplus \cdots \oplus U_k \tag{10.9}$$

gdzie U_i są podprzestrzeniami niezmienniczymi takimi, że

$$q_i^{d_i}(\tau)(U_i) = 0, \quad i = 1, \ldots, k$$

dla pewnych liczb naturalnych d_i. Wtedy

$$U_i = \ker q_i^{m_i}(\tau), \quad i = 1, \ldots, k.$$

Dowód. Połóżmy $V_i := \ker q_i^{m_i}(\tau)$. Przypomnijmy, że na podstawie twierdzenia 10.1.7, V_i jest niezerową podprzestrzenią niezmienniczą endomorfizmu τ oraz V jest sumą prostą podprzestrzeni V_i. Faktycznie V_i jest q_i-prymarną składową $T_{q_i}(V)$ modułu V_τ. Zauważmy najpierw, że dla każdego i mamy inkluzję

$$U_i \subseteq V_i. \tag{10.10}$$

Rzeczywiście, dla $v \in U_i$ mamy $q_i^{d_i}(\tau)(v) = 0$, czyli w oznaczeniach $K[X]-$modułu V_τ mamy $q_i^{d_i} v = 0$. Zatem $v \in T_{q_i}(V) = V_i$. Teraz z (10.8), (10.9) i (10.10) wynika, że $U_i = V_i$ dla każdego $i = 1, \ldots, k$. □

WNIOSEK **10.3.5.** *Suma wymiarów klatek Jordana należących do tej samej wartości własnej endomorfizmu τ nie zależy od wyboru bazy kanonicznej Jordana w przestrzeni V.*

Dowód. Suma wymiarów klatek Jordana należących do wartości własnej a_i jest równa stopniowi macierzy M_i w rozkładzie (10.6) a ten jest równy $\dim U_i$, gdzie U_i jest składnikiem prostym występującym w rozkładzie (10.9). Na podstawie twierdzenia 10.3.4,

$$\dim U_i = \dim V_i,$$

przy czym $V_i = \ker q_i^{m_i}(\tau)$ nie zależy od wyboru bazy kanonicznej Jordana w przestrzeni V. □

W oznaczeniach (10.7) wniosek 10.3.5 mówi, że

$$n_i := \dim U_i = d_{i1} + \cdots + d_{is_i}$$

nie zależy od wyboru bazy kanonicznej Jordana. Pokażemy teraz, że nie tylko suma $d_{i1} + \cdots + d_{is_i}$ ale także jej składniki d_{ij} nie zależą od wyboru bazy kanonicznej Jordana w przestrzeni V. Podamy dwa różne dowody tego faktu.

Niech J będzie postacią kanoniczną Jordana macierzy endomorfizmu τ. Zatem macierz J jest sumą prostą klatek Jordana należących do wartości własnych endomorfizmu τ. Dla każdego $j \leqslant n$ niech ℓ_{ij} będzie *liczbą klatek Jordana stopnia j należących do wartości własnej a_i.*

Aby stwierdzić, że liczby ℓ_{ij} klatek $j-$wymiarowych są niezależne od wyboru bazy w przestrzeni V pokażemy, że ℓ_{ij} są jednoznacznie wyznaczone przez rzędy pewnych macierzy, których niezależność od wyboru bazy przestrzeni V jest oczywista.

Niech $A = \mathsf{m}(\tau, \mathcal{A})$ będzie macierzą endomorfizmu τ w jakiejkolwiek bazie $\mathcal{A}$ przestrzeni $n-$wymiarowej V i niech P będzie macierzą nieosobliwą taką, że

$$P^{-1}AP = J.$$

Dla dowolnej wartości własnej a_i endomorfizmu τ mamy

$$A - a_iI = PJP^{-1} - a_iI = P(J - a_iI)P^{-1}.$$

Zauważmy, że macierze $A - a_iI$ oraz $J - a_iI$, jako macierze podobne mają równe rzędy. Z tego samego powodu

$$\mathsf{rank}(A - a_iI)^t = \mathsf{rank}(J - a_iI)^t$$

dla każdego $t \geqslant 1$. Ponieważ dla $k-$wymiarowych klatek Jordana $J_k(a_i)$ i $J_k(a_j)$ gdzie $a_i \neq a_j$ mamy oczywiście

$$\mathsf{rank}(J_k(a_i) - a_iI_k) = k - 1, \quad \mathsf{rank}(J_k(a_j) - a_iI_k) = k,$$

więc

$$\mathsf{rank}(A - a_iI) = \ell_{i2} + 2\ell_{i3} + \cdots + (n-1)\ell_{in} + n - n_i.$$

Podobnie

$$\mathsf{rank}(A - a_iI)^2 = \ell_{i3} + 2\ell_{i4} + \cdots + (n-2)\ell_{in} + n - n_i,$$

i ogólnie

$$\mathsf{rank}(A - a_iI)^t = \sum_{j=t+1}^{n} (j-t)\ell_{ij} + n - n_i.$$

Ponieważ także

$$\ell_{i1} + \ell_{i2} + \cdots + \ell_{in} = n_i,$$

więc z równości tych wyznaczymy jednoznacznie $\ell_{i1}, \ell_{i2}, \ldots, \ell_{in}$ w zależności od liczb n, n_i oraz rzędów macierzy $(A - a_i I)^t$. Ponieważ $n, n_i, \mathsf{rank}(A - a_i I)^t$ nie zależą od wyboru bazy kanonicznej Jordana przestrzeni V (niezależność n_i od wyboru bazy wynika z wniosku 10.3.5) także liczby ℓ_{ij} nie zależą od wyboru bazy. Jest to zapowiedziany wcześniej pierwszy dowód następującego twierdzenia.

TWIERDZENIE **10.3.6.** (Jednoznaczność postaci kanonicznej Jordana.)
Postać kanoniczna Jordana macierzy endomorfizmu τ jest wyznaczona jednoznacznie przez endomorfizm τ z dokładnością do kolejności występujących w niej klatek Jordana.

Dowód. A oto drugi dowód, wykorzystujący jednoznaczność postaci kanonicznej Jordana macierzy endomorfizmu nilpotentnego (zobacz rozdział 10.2.2).

Niech $J = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} J_{m_{ij}}(a_i)$ będzie postacią kanoniczną macierzy endomorfizmu τ. Macierz J zapiszemy w postaci $J = M_1 \oplus \cdots \oplus M_k$ gdzie $M_i = \bigoplus_{j=1}^{r_i} J_{m_{ij}}(a_i)$. Z tym drugim rozkładem macierzy J związany jest rozkład (10.8) przestrzeni V na sumę prostą podprzestrzeni niezmienniczych V_i, przy czym na podstawie twierdzenia 10.3.4, podprzestrzeń V_i ma bazę $\mathcal{B}_i$ taką, że

$$\mathsf{m}(\tau_i, \mathcal{B}_i) = M_i,$$

gdzie $\tau_i = \tau|_{V_i}$ jest endomorfizmem indukowanym przez τ na V_i. A więc stopień macierzy M_i jest wyznaczony jednoznacznie i jest równy $n_i := \dim V_i$.

Rozpatrzmy teraz endomorfizm $\sigma_i := \tau_i - a_i 1_{V_i}$ przestrzeni V_i. Znając macierz endomorfizmu τ_i w bazie $\mathcal{B}_i$ znajdujemy z łatwością macierz σ_i w tej samej bazie:

$$\mathsf{m}(\sigma_i, \mathcal{B}_i) = M_i - a_i I_{n_i} = \bigoplus_{j=1}^{r_i} J_{m_{ij}}(0).$$

Jest to suma prosta osobliwych klatek Jordana, zatem σ_i jest endomorfizmem nilpotentnym a przestrzeń V_i ma rozkład na sumę prostą podprzestrzeni σ_i-cyklicznych o wymiarach

$$m_{i1} \geqslant \cdots \geqslant m_{ir_i}.$$

Jest to ciąg niezmienników endomorfizmu nilpotentnego σ_i i jest on wyznaczony jednoznacznie przez σ_i na podstawie twierdzenia 10.2.7. Stąd wynika, że rozmiary klatek Jordana należących do wartości własnej a_i w postaci kanonicznej endomorfizmu τ nie zależą od wyboru bazy kanonicznej Jordana w przestrzeni V. □

10.4 Wielomian charakterystyczny, wyznacznik, ślad

Dla uproszczenia zakładamy, że ciało K jest algebraicznie domknięte. Wtedy wielomian minimalny *każdego* endomorfizmu dowolnej przestrzeni wektorowej nad K rozkłada się nad K na iloczyn czynników liniowych i mamy pełną swobodę wykorzystywania naszych rezultatów.

10.4.1 Wielomian charakterystyczny

Niech τ będzie endomorfizmem przestrzeni wektorowej V i niech

$$p_\tau = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k}$$

będzie wielomianem minimalnym endomorfizmu τ, gdzie $a_1, \ldots, a_k$ są elementami ciała K, przy czym $a_i \neq a_j$ dla $i \neq j$ oraz $m_i \geqslant 1$ dla $i = 1, \ldots, k$. Wtedy na podstawie twierdzenia 10.1.7 o rozkładzie prymarnym, przestrzeń V ma rozkład

$$V = V_1 \oplus \cdots \oplus V_k,$$

gdzie V_i jest podprzestrzenią niezmienniczą endomorfizmu τ oraz endomorfizm indukowany $\tau_i = \tau|_{V_i}$ na przestrzeni V_i ma wielomian minimalny $(X - a_i)^{m_i}$. Jak wiemy z twierdzenia o rozkładzie,

$$V_i = \ker(\tau - a_i 1_V)^{m_i}.$$

Ponadto, V_i ma bazę $\mathcal{B}_i$ taką, że dla endomorfizmu τ_i indukowanego przez τ na V_i mamy

$$\mathsf{m}(\tau_i, \mathcal{B}_i) = J_{m_{i1}}(a_i) \oplus \cdots \oplus J_{m_{ir_i}}(a_i).$$

Z wniosku 10.3.5 wiemy, że rozmiary $m_{i1} \geqslant \cdots \geqslant m_{ir_i}$ występujących tu klatek Jordana są wyznaczone jednoznacznie przez endomorfizm τ.

Definicja **10.4.1.** *Krotnością algebraiczną* $k_{alg}(a_i)$ wartości własnej a_i endomorfizmu τ nazywamy wymiar podprzestrzeni $V_i = \ker(\tau - a_i 1_V)^{m_i}$:

$$k_{alg}(a_i) := \dim V_i = m_{i1} + \cdots + m_{ir_i}.$$

Krotnością geometryczną $k_g(a_i)$ wartości własnej a_i endomorfizmu τ nazywamy wymiar przestrzeni wektorów własnych endomorfizmu τ należących do wartości własnej a_i:

$$k_g(a_i) = \dim \ker(\tau - a_i \mathbf{1}_V).$$

A więc krotność algebraiczna wartości własnej a_i wskazuje ile razy wartość własna a_i pojawia się na głównej przekątnej postaci kanonicznej Jordana macierzy endomorfizmu τ.

Krotność geometryczną wartości własnej a_i można także zinterpretować poprzez postać kanoniczną Jordana endomorfizmu τ. Mianowicie, $k_g(a_i)$ jest *liczbą klatek Jordana należących do wartości własnej* a_i.

Rzeczywiście, zapiszmy postać kanoniczną Jordana macierzy endomorfizmu τ w bazie kanonicznej $\mathcal{B}$ jako

$$J = M_1 \oplus \cdots \oplus M_k$$

gdzie $M_\ell = \bigoplus_{j=1}^{r_\ell} J_{m_{\ell j}}(a_\ell)$. Endomorfizm $\tau - a_i 1_V$ przestrzeni V ma w bazie $\mathcal{B}$ macierz

$$\mathsf{m}(\tau - a_i 1_V, \mathcal{B}) = \bigoplus_{\ell=1}^{k} (M_\ell - a_i I_{n_\ell}).$$

Wszystkie klatki $M_\ell - a_i I_{n_\ell}$ dla $\ell \neq i$ są macierzami nieosobliwymi, natomiast

$$M_i - a_i I_{n_i} = \bigoplus_{j=1}^{r_i} J_{m_{ij}}(0)$$

jest macierzą rzędu $n_i - r_i$. Wobec tego macierz $\mathsf{m}(\tau - a_i 1_V, \mathcal{B})$ ma rząd $n - r_i$ oraz

$$n = \dim \ker(\tau - a_i 1_V) + \dim \operatorname{im}(\tau - a_i 1_V) = \dim \ker(\tau - a_i 1_V) + n - r_i$$

skąd

$$k_g(a_i) = \dim \ker(\tau - a_i \mathbf{1}_V) = r_i$$

jest liczbą klatek Jordana należących do wartości własnej a_i.

Zauważmy, że wartość własna a_i ma też swoją krotność m_i jako pierwiastek wielomianu minimalnego endomorfizmu τ. Związek pomiędzy m_i oraz n_i jest następujący:

$$n_i = \dim V_i = m_{i1} + \cdots + m_{ir_i} \geqslant m_{i1} = m_i.$$

A więc krotność n_i wartości własnej a_i endomorfizmu τ jest niemniejsza niż krotność m_i pierwiastka a_i wielomianu minimalnego p endomorfizmu τ. Ciąg liczb $m_{i1}, \ldots, m_{ir_i}$ jest ciągiem niezmienników endomorfizmu nilpotentnego $\sigma_i = \tau_i - a_i 1_{V_i}$ i wraz z wartością własną a_i dostarcza kompletnego opisu działania endomorfizmu τ na podprzestrzeni V_i. Zauważmy jeszcze, że zgodnie z twierdzeniem 10.2.3 liczby m_{ij}, $j = 1, \ldots, r_i$, są stopniami nilpotentności endomorfizmów indukowanych przez σ_i na cyklicznych składnikach prostych przestrzeni V_i. Zatem endomorfizmy indukowane przez τ na tych składnikach prostych mają wielomiany minimalne

$$q_{ij} := (X - a_i)^{m_{ij}}, \quad j = 1, \ldots, r_i.$$

Definicja **10.4.2.** Wielomiany $q_{ij},\ j = 1, \ldots, r_i$ nazywamy *dzielnikami elementarnymi* endomorfizmu τ należącymi do wartości własnej a_i endomorfizmu τ.

Wobec definicji krotności wartości własnej endomorfizmu mamy następującą równość:

$$(X - a_i)^{n_i} = \prod_{1 \leqslant j \leqslant r_i} q_{ij}.$$

Definicja **10.4.3.** Niech $a_1, \ldots, a_k$ będą wartościami własnymi endomorfizmu τ i niech $n_1, \ldots, n_k$ będą ich krotnościami algebraicznymi. Wielomian

$$f_\tau = (X - a_1)^{n_1} \cdots (X - a_k)^{n_k} \in K[X]$$

nazywamy *wielomianem charakterystycznym* endomorfizmu τ.

Przywołując definicję 10.4.2 możemy więc powiedzieć, że wielomian charakterystyczny endomorfizmu τ jest iloczynem wszystkich dzielników elementarnych endomorfizmu τ :

$$f_\tau = \prod_{1 \leqslant i \leqslant k} \prod_{1 \leqslant j \leqslant r_i} q_{ij}.$$

TWIERDZENIE **10.4.4.** *Wielomian minimalny endomorfizmu τ jest dzielnikiem wielomianu charakterystycznego endomorfizmu τ. Ponadto, stopień wielomianu charakterystycznego endomorfizmu przestrzeni $n-$wymiarowej V jest równy n.*

Dowód. Wobec $m_i \leqslant n_i$ mamy oczywiście $p_\tau | f_\tau$. Z drugiej strony, na podstawie twierdzenia o rozkładzie mamy

$$n = \dim V = \dim V_1 + \cdots + \dim V_k = n_1 + \cdots + n_k = \deg f_\tau.$$

□

Zauważmy, że podzielność $p_\tau | f_\tau$ pociąga natychmiast następujące twierdzenie.

TWIERDZENIE **10.4.5.** (Twierdzenie Cayleya-Hamiltona). $f_\tau(\tau) = 0_V$.

10.4.2 Wyznacznik endomorfizmu

Wprowadzimy teraz pojęcie wyznacznika endomorfizmu $\tau \in \mathsf{End}_K V$, przy założeniu, że K jest ciałem algebraicznie domkniętym.

DEFINICJA **10.4.6.** Niech $a_1, \ldots, a_k$ będą wartościami własnymi endomorfizmu τ i niech $n_1, \ldots, n_k$ będą ich krotnościami algebraicznymi.
Wyznacznikiem $\det \tau$ endomorfizmu τ nazywamy następujący iloczyn potęg wartości własnych endomorfizmu τ

$$\det \tau := a_1^{n_1} \cdots a_k^{n_k}.$$

Ponieważ a_i jest n_i-krotną wartością własną endomorfizmu τ, można także powiedzieć, że wyznacznik endomorfizmu τ jest iloczynem wartości własnych tego endomorfizmu z uwzględnieniem ich krotności. Zauważmy także, że $\det \tau = (-1)^n f_\tau(0)$.

TWIERDZENIE **10.4.7.** *Endomorfizm τ jest osobliwy wtedy i tylko wtedy, gdy*

$$\det \tau = 0.$$

Dowód. Endomorfizm τ jest osobliwy wtedy i tylko wtedy, gdy $\tau - 0 \cdot 1_V$ jest endomorfizmem osobliwym, a więc wtedy i tylko wtedy gdy $0 \in K$ jest wartością własną endomorfizmu τ. Osobliwość τ jest więc równoważna temu, że $\det \tau = 0$. □

TWIERDZENIE **10.4.8.** *Wielomian charakterystyczny i wyznacznik endomorfizmu są niezmiennikami podobieństwa endomorfizmów.*

Dowód. Endomorfizmy podobne mają identyczne postaci kanoniczne Jordana (na podstawie twierdzenia 10.3.3), zatem mają te same wartości własne a także krotności algebraiczne wartości własnych. Zatem mają równe wielomiany charakterystyczne i wyznaczniki. □

10.4.3 Wyznacznik macierzy

DEFINICJA **10.4.9.** Niech $A \in M_n(K)$, gdzie K jest ciałem algebraicznie domkniętym i niech $V = K^n$ będzie $n-$wymiarową przestrzenią wektorową współrzędnych nad ciałem K. Niech $\mathcal{A}$ będzie dowolną bazą przestrzeni V i niech τ będzie endomorfizmem przestrzeni V takim, że

$$\mathsf{m}(\tau, \mathcal{A}) = A.$$

(a) *Wyznacznikiem* $\det A$ macierzy A nazywamy wyznacznik endomorfizmu τ.
(b) *Wartościami własnymi* macierzy A nazywamy wartości własne endomorfizmu τ.
(c) *Krotnością algebraiczną* wartości własnej a_i macierzy A nazywamy krotność algebraiczną wartości własnej a_i endomorfizmu τ.
(d) *Wielomianem charakterystycznym* f_A macierzy A nazywamy wielomian charakterystyczny f_τ endomorfizmu τ.
(e) *Postacią kanoniczną Jordana* J_A macierzy A nazywamy postać kanoniczną J_τ macierzy endomorfizmu τ.

Zauważmy, że jeśli także ρ jest endomorfizmem przestrzeni V i ρ ma w jakiejś bazie przestrzeni V macierz A, to endomorfizmy ρ i τ są podobne, więc mają równe wartości własne, krotności wartości własnych, wielomiany charakterystyczne, wyznaczniki i postacie kanoniczne. Stąd wynika, że nasza definicja wyznacznika macierzy A, jej wartości własnych, wielomianu charakterystycznego i postaci kanonicznej Jordana nie zależy od wyboru endomorfizmu τ.

LEMAT **10.4.10.** *Niech $\tau \in \mathsf{End}_K V$ oraz $A \in M_n(K)$, gdzie K jest ciałem algebraicznie domkniętym i $\dim V = n$. Wtedy dla dowolnego $a \in K$ mamy*

$$\det a\tau = a^n \det \tau \quad \text{oraz} \quad \det aA = a^n \det A.$$

Dowód. Zauważmy najpierw, że lemat jest prawdziwy dla $a = 0$, gdyż endomorfizm zerowy ma $n-$krotną wartość własną 0. Załóżmy więc, że $a \neq 0$ i niech $a_1, \ldots, a_k$ będą wartościami własnymi endomorfizmu τ o krotnościach algebraicznych $n_1, \ldots, n_k$. Wtedy mamy następujące łatwe do stwierdzenia fakty:

• $aa_1, \ldots, aa_k$ są wszystkimi wartościami własnymi endomorfizmu $a\tau$.
Rzeczywiście, jeśli dla niezerowego wektora v oraz $b \in K$ mamy $a\tau(v) = bv$, to ba^{-1} jest wartością własną endomorfizmu τ, zatem $b = aa_i$ dla pewnego i. Z drugiej strony, wszystkie aa_i są wartościami własnymi $a\tau$, gdyż $\tau(v) = a_i v$ pociąga $a\tau(v) = aa_i v$.

• Jeśli $p_\tau = (X - a_1)^{m_1} \cdots (X - a_k)^{m_k}$, to $p_{a\tau} = (X - aa_1)^{m_1} \cdots (X - aa_k)^{m_k}$.
Niech $f := (X - aa_1)^{m_1} \cdots (X - aa_k)^{m_k}$. Z równości $p_\tau(\tau) = 0_V$ wynika $f(a\tau) = 0_v$, zatem $p_{a\tau} \mid f$. Gdyby $\deg p_{a\tau} < \deg f$, to z równości $p_{a\tau}(a\tau) = 0_V$ wynikałoby, że endomorfizm τ zeruje pewien wielomian stopnia mniejszego niż $\deg p_\tau = \deg f$, sprzeczność. Zatem $p_{a\tau} = f$.

• $n_i = \dim \ker(\tau - a_i 1_V)^{m_i} = \dim \ker(a\tau - aa_i 1_V)^{m_i}$.
Faktycznie $\ker(\tau - a_i 1_V)^{m_i} = \ker(a\tau - aa_i 1_V)^{m_i}$ gdyż $(a\tau - aa_i 1_V)^{m_i} = a^{m_i}(\tau - a_i 1_V)^{m_i}$ i wobec tego

$$(a\tau - aa_i 1_V)^{m_i}(v) = 0 \iff (\tau - a_i 1_V)^{m_i}(v) = 0.$$

A więc wartość własna aa_i endomorfizmu $a\tau$ ma taką samą krotność algebraiczną jak wartość własna a_i endomorfizmu τ. Stąd otrzymujemy

$$\det a\tau = (aa_1)^{n_1} \cdots (aa_k)^{n_k} = a^n a_1^{n_1} \cdots a_k^{n_k} = a^n \det \tau,$$

oraz $\det aA = \det a\tau = a^n \det \tau = a^n \det A$. □

TWIERDZENIE **10.4.11.** *Niech $A \in M_n(K)$, gdzie K jest ciałem algebraicznie domkniętym. Dla każdego $x \in K$ mamy*

$$\det(xI - A) = f_A(x).$$

Dowód. Niech V będzie $n-$wymiarową przestrzenią wektorową nad ciałem K z bazą $\mathcal{A}$ i niech τ będzie endomorfizmem przestrzeni V takim, że

$$\mathsf{m}(\tau, \mathcal{A}) = A.$$

Niech $J = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} J_{m_{ij}}(a_i)$ będzie postacią kanoniczną Jordana endomorfizmu τ w bazie $\mathcal{B}$ przestrzeni V. Wtedy

$$\mathsf{m}(\tau - x1_V, \mathcal{B}) = J - xI = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} J_{m_{ij}}(a_i - x).$$

A więc baza $\mathcal{B}$ jest także bazą kanoniczną Jordana endomorfizmu $\tau - x1_V$ i endomorfizm ten ma wartości własne $a_i - x$, przy czym krotność algebraiczna wartości własnej $a_i - x$ endomorfizmu $\tau - x1_V$ jest równa krotności algebraicznej n_i wartości własnej a_i endomorfizmu τ. Stąd otrzymujemy

$$\det(\tau - x1_V) = \prod_{i=1}^{k} (a_i - x)^{n_i} = (-1)^n \prod_{i=1}^{k} (x - a_i)^{n_i} = (-1)^n f_\tau(x) = (-1)^n f_A(x).$$

Zatem na podstawie lematu 10.4.10 mamy

$$f_A(x) = (-1)^n \det(\tau - x1_V) = \det(x1_V - \tau) = \det(xI - A),$$

gdzie ostatnia równość wynika stąd, że $\mathsf{m}(x1_V - \tau, \mathcal{A}) = xI - A$. □

10.4.4 Ślad endomorfizmu

Śladem macierzy $A = [a_{ij}] \in M_n(K)$ nazywamy $\mathsf{Tr}\, A = \sum_{i=1}^{n} a_{ii}$. Sprawdzamy bez trudu, że $\mathsf{Tr} : M_n(K) \to K$ jest funkcjonałem liniowym na przestrzeni wektorowej macierzy $M_n(K)$.

TWIERDZENIE **10.4.12.** $\mathsf{Tr}\, AB = \mathsf{Tr}\, BA$.

Dowód. $\mathsf{Tr}\, AB = \sum_{i=1}^{n} \sum_{j=1}^{n} a_{ij} b_{ji} = \sum_{j=1}^{n} \sum_{i=1}^{n} b_{ji} a_{ij} = \mathsf{Tr}\, BA$. □

WNIOSEK **10.4.13.** *Macierze podobne mają równe ślady.*

Dowód. Niech $B = S^{-1}AS$. Wtedy

$\mathsf{Tr}\, B = \mathsf{Tr}(S^{-1}A) \cdot S = \mathsf{Tr}\, S \cdot (S^{-1}A) = \mathsf{Tr}(SS^{-1}) \cdot A = \mathsf{Tr}\, A$. □

DEFINICJA **10.4.14.** Śladem endomorfizmu $\tau \in \mathsf{End}_K V$ nazywamy ślad macierzy endomorfizmu τ w dowolnej bazie przestrzeni V.

W szczególności więc możemy wziąć postać kanoniczną J macierzy A endomorfizmu τ i wtedy $\mathsf{Tr}\,\tau = \mathsf{Tr}\,A = \mathsf{Tr}\,J$ jest sumą wartości własnych endomorfizmu τ z uwzględnieniem ich krotności.

Definicje 10.4.3, 10.4.9 i 10.4.14 akcentują geometryczny aspekt wielomianu charakterystycznego endomorfizmu, wyznacznika i śladu macierzy. Wyznacznik macierzy A jest więc iloczynem wartości własnych endomorfizmu o macierzy A, z uwzględnieniem ich krotności, a ślad jest ich sumą. Dla znalezienia wartości wyznacznika $\det A$, śladu $\mathsf{Tr}\,A$ a także wielomianu charakterystycznego f_τ należałoby zatem najpierw znaleźć wszystkie wartości własne endomorfizmu τ a także ich krotności. Zauważmy jeszcze, że wyznacznik macierzy A, z dokładnością do znaku, jest równy wyrazowi wolnemu wielomianu charakterystycznego macierzy A :

$$\det A = (-1)^n f_A(0).$$

Klasyczne definicje wyznacznika, śladu i wielomianu charakterystycznego nie oferują żadnej geometrycznej interpretacji, ale pozwalają znaleźć wartość wyznacznika macierzy i jej wielomian charakterystyczny poprzez arytmetyczne manipulacje na elementach macierzy A.

10.5 Postać kanoniczna Frobeniusa

W tym rozdziale wskażemy postać kanoniczną endomorfizmu $\tau \in \mathsf{End}_K V$, gdzie K jest dowolnym ciałem i wielomian minimalny endomorfizmu τ jest dowolnym wielomianem nad K.

10.5.1 Podprzestrzenie cykliczne

Podprzestrzenie $\tau-$cykliczne rozpatrywaliśmy już w rozdziale 10.1.2 (zob. lemat 10.1.10). W tym rozdziale zbadamy własności podprzestrzeni $\tau-$cyklicznych dla wszystkich endomorfizmów τ, których wielomiany minimalne są potęgami wielomianów nierozkładalnych.
Niech więc $\tau \in \mathsf{End}_K V$ i niech wielomian minimalny p_τ endomorfizmu τ będzie potęgą wielomianu $q \in K[X]$ nierozkładalnego nad ciałem K :

$$p_\tau = q^m.$$

Niech $U = K[X]v$ będzie podprzestrzenią $\tau-$cykliczną przestrzeni V generowaną przez wektor v. Niech $\tau_1 = \tau|_U$ będzie endomorfizmem przestrzeni U indukowanym przez τ na U. Wtedy (na podstawie lematu 10.1.1) wielomian minimalny p_{τ_1} endomorfizmu τ_1 jest dzielnikiem wielomianu minimalnego endomorfizmu τ, zatem dla pewnych liczb naturalnych $m_1 \leqslant m$ oraz r mamy

$$p_{\tau_1} = q^{m_1} = c_0 + c_1 X + \cdots + c_{r-1}X^{r-1} + X^r \in K[X]. \tag{10.11}$$

LEMAT **10.5.1.** *Niech $\tau \in \mathsf{End}_K V$ i niech wielomian minimalny p_τ endomorfizmu τ będzie potęgą wielomianu nierozkładalnego nad K. Niech U będzie podprzestrzenią $\tau-$cykliczną przestrzeni V generowaną przez wektor $v \in V$ i niech endomorfizm τ_1 podprzestrzeni U indukowany przez τ na U ma wielomian minimalny postaci* (10.11). *Wtedy*

$$\mathcal{B} = \{v, \tau(v), \tau^2(v), \ldots, \tau^{r-1}(v)\}$$

jest bazą podprzestrzeni U oraz

$$\mathsf{m}(\tau_1, \mathcal{B}) = \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & -c_{r-1} \end{bmatrix}.$$

Dowód. $\mathcal{B}$ jest bazą U na podstawie lematu 10.1.10, $\tau(\tau^{i-1}(v)) = \tau^i(v)$ dla $i = 1, \ldots, r-2$ oraz $\tau(\tau^{r-1}(v)) = \tau^r(v) = -c_0 v - c_1\tau(v) - \cdots - c_{r-1}\tau^{r-1}(v)$. □

DEFINICJA **10.5.2.** Macierz

$$S(f) := \begin{bmatrix} 0 & 0 & 0 & \ldots & 0 & -c_0 \\ 1 & 0 & 0 & \ldots & 0 & -c_1 \\ 0 & 1 & 0 & \ldots & 0 & -c_2 \\ & & & \ldots & & \\ 0 & 0 & 0 & \ldots & 1 & -c_{r-1} \end{bmatrix}$$

nazywa się macierzą *stowarzyszoną* (ang. *companion matrix*) z wielomianem

$$f = c_0 + c_1 X + \cdots + c_{r-1}X^{r-1} + X^r.$$

A więc lemat 10.5.1 mówi, że (przy odpowiednich założeniach o endomorfizmie τ) endomorfizm τ_1 podprzestrzeni $\tau-$cyklicznej U ma w odpowiedniej bazie podprzestrzeni U macierz stowarzyszoną z wielomianem minimalnym endomorfizmu τ_1.

Zauważmy, że dla wielomianu $f = X^d$ macierz stowarzyszona $S(f)$ jest osobliwą klatką Jordana J_d stopnia d. Dla endomorfizmów nilpotentnych otrzymujemy zatem rezultat znany nam już z lematu 10.2.1.

10.5.2 Postać kanoniczna wymierna

Przystępujemy teraz do opisu postaci kanonicznej *Frobeniusa* (zwanej także postacią kanoniczną wymierną) macierzy dowolnego endomorfizmu $\tau \in \mathsf{End}_K V$, gdzie K jest dowolnym ciałem. Zgodnie z ogólną strategią podyktowaną przez twierdzenie 10.1.7 o rozkładzie prymarnym, rozpatrzymy najpierw przypadek, gdy wielomian minimalny p_τ jest potęgą wielomianu nierozkładalnego. Dysponujemy tutaj twierdzeniem 10.1.9, które umożliwia rozkład przestrzeni na sumę prostą podprzestrzeni $\tau-$cyklicznych. Następujące twierdzenie jest uogólnieniem twierdzenia 10.2.3.

TWIERDZENIE **10.5.3.** *Niech endomorfizm $\tau \in \mathsf{End}_K V$ ma wielomian minimalny postaci $p_\tau = q^m$, gdzie q jest wielomianem nierozkładalnym nad ciałem K. Wtedy istnieją podprzestrzenie $\tau-$cykliczne $U_1, \ldots, U_t$ przestrzeni V takie, że*

$$V = U_1 \oplus \cdots \oplus U_t \quad \textit{oraz} \quad \deg p_\tau = \dim U_1 \geqslant \cdots \geqslant \dim U_t.$$

Ponadto, endomorfizm τ_i indukowany na podprzestrzeni U_i przez endomorfizm τ ma wielomian minimalny postaci q^{s_i}, przy czym

$$\deg q^{s_i} = \dim U_i, \quad i = 1, \ldots, t.$$

Dowód. Przedstawienie przestrzeni V w postaci sumy prostej podprzestrzeni $\tau-$cyklicznych wynika z twierdzenia 10.1.9. Niech f_i będzie wielomianem minimalnym endomorfizmu $\tau_i = \tau|_{U_i}$. Ponieważ $q^m(\tau)(u) = 0$ dla każdego $u \in U_i$, więc f_i dzieli q^m (zob. lemat 10.1.1) i wobec nierozkładalności wielomianu q, dla pewnej liczby naturalnej $s_i \leqslant m$ mamy

$$f_i = q^{s_i}.$$

Niech $s = \max s_i$. W szczególności więc mamy $s \leqslant m$. Wtedy $q^s(\tau)(U_i) = 0$ dla każdego $i = 1, \ldots, t$ i wobec tego także $q^s(\tau)(V) = 0$. Stąd wynika, że wielomian minimalny q^m endomorfizmu τ dzieli q^s, a więc $m \leqslant s$. Zatem $m = s$, czyli jeden z endomorfizmów τ_i ma wielomian minimalny q^m. Zmieniając ewentualnie numerację podprzestrzeni U_i możemy zakładać, że $i = 1$, to znaczy, że endomorfizm indukowany przez τ na podprzestrzeni U_1 ma wielomian minimalny q^m.
Z lematu 10.1.10 wynika, że dla każdego i mamy $\deg q^{s_i} = \dim U_i$. □

Sformułujemy teraz wersję macierzową twierdzenia 10.5.3.

TWIERDZENIE **10.5.4.** *Niech endomorfizm $\tau \in \mathsf{End}_K V$ ma wielomian minimalny postaci $p_\tau = q^m$, gdzie q jest wielomianem nierozkładalnym nad ciałem K. Wtedy istnieje baza $\mathcal{B}$ przestrzeni V taka, że*

$$\begin{aligned} \mathsf{m}(\tau, \mathcal{B}) &= S(q^{s_1}) \oplus \cdots \oplus S(q^{s_t}) \\ &= \begin{bmatrix} S(q^{s_1}) & 0 & \ldots & 0 & 0 \\ 0 & S(q^{s_2}) & \ldots & 0 & 0 \\ 0 & 0 & \ldots & 0 & 0 \\ & & \ldots & & \\ 0 & 0 & \ldots & 0 & S(q^{s_t}) \end{bmatrix}, \end{aligned}$$

gdzie $m = s_1 \geqslant s_2 \geqslant \cdots \geqslant s_t \geqslant 1$ jest pewnym ciągiem liczb naturalnych.

Dowód. Rozważmy rozkład przestrzeni V z twierdzenia 10.5.3. Ponieważ endomorfizm indukowany τ_i na podprzestrzeni U_i ma wielomian minimalny q^{s_i}, więc na podstawie lematu 10.5.1 istnieje baza $\mathcal{B}_i$ przestrzeni U_i taka, że $\mathsf{m}(\tau_i, \mathcal{B}_i) = S(q^{s_i})$. Zatem w bazie $\mathcal{B} = \mathcal{B}_1 \cup \cdots \cup \mathcal{B}_t$ endomorfizm τ ma macierz $S(q^{s_1}) \oplus \cdots \oplus S(q^{s_t})$. □

Uwaga 10.5.5. W szczególnym przypadku gdy $q = X$ endomorfizm τ jest nilpotentny i dla dowolnego $s \in \mathbb{N}$ macierz $S(q^s) = S(X^s) = J_s(0)$ jest osobliwą klatką Jordana stopnia s. Twierdzenie 10.5.4 powtarza zatem rezultat twierdzenia 10.2.4 dla endomorfizmów nilpotentnych: $\mathsf{m}(\tau, \mathcal{B}) = J_{s_1} \oplus \cdots \oplus J_{s_t}$.

Jesteśmy teraz przygotowani do rozpatrzenia sytuacji, gdy na endomorfizm $\tau \in \mathsf{End}_K V$ nie nakładamy żadnych specjalnych warunków. A więc wielomian minimalny endomorfizmu τ jest iloczynem potęg $q_i^{m_i}$ wielomianów nierozkładalnych nad

ciałem K. Na podstawie twierdzenia 10.1.7 o rozkładzie prymarnym przestrzeń V ma rozkład

$$V = V_1 \oplus \cdots \oplus V_k,$$

gdzie V_i jest podprzestrzenią niezmienniczą endomorfizmu τ oraz endomorfizm indukowany τ_i na przestrzeni V_i ma wielomian minimalny $q_i^{m_i}$. Wykorzystując teraz twierdzenie 10.5.3 otrzymujemy natychmiast następujące ogólne twierdzenie.

TWIERDZENIE **10.5.6.** (Postać kanoniczna Frobeniusa macierzy endomorfizmu.)
Niech endomorfizm $\tau \in \mathsf{End}_K V$ ma wielomian minimalny

$$p_\tau = q_1^{m_1} \cdots q_k^{m_k},$$

gdzie q_i są unormowanymi wielomianami nierozkładalnymi nad ciałem K, $q_i \neq q_j$ dla $i \neq j$ oraz $m_i \geqslant 1$ są liczbami naturalnymi.
Wtedy istnieje baza $\mathcal{A}$ przestrzeni V taka, że

$$\mathsf{m}(\tau, \mathcal{A}) = M_1 \oplus \cdots \oplus M_k,$$

gdzie M_i jest sumą prostą macierzy stowarzyszonych z odpowiednimi potęgami wielomianu q_i:

$$\begin{aligned} M_i &= S(q_i^{s_{i1}}) \oplus \cdots \oplus S(q_i^{s_{ir_i}}) \\ &= \begin{bmatrix} S(q_i^{s_{i1}}) & 0 & \dots & 0 & 0 \\ 0 & S(q_i^{s_{i2}}) & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ & & \dots & & \\ 0 & 0 & \dots & 0 & S(q_i^{s_{ir_i}}) \end{bmatrix} \end{aligned}$$

oraz $m_i = s_{i1} \geqslant s_{i2} \geqslant \cdots \geqslant s_{ir_i}$ jest pewnym ciągiem liczb naturalnych.

DEFINICJA **10.5.7.** W oznaczeniach twierdzenia 10.5.6 wielomiany

$$q_1^{s_{11}}, \dots, q_1^{s_{1r_1}}, \ \dots, \ q_k^{s_{k1}}, \dots, q_k^{s_{kr_k}}$$

nazywają się *dzielnikami elementarnymi* endomorfizmu τ.

Można udowodnić, że dwa endomorfizmy σ i τ przestrzeni V są podobne wtedy i tylko wtedy, gdy mają te same dzielniki elementarne. Zauważmy także, że w przypadku gdy wielomiany q_i są liniowe, $q_i = X - a_i$, powyższa definicja dzielników elementarnych pokrywa się z definicją 10.4.2 dzielników elementarnych endomorfizmu τ należących do wartości własnej a_i. W obydwu przypadkach dzielnikami elementarnymi nazwaliśmy wielomiany postaci $q_i^{m_{ij}}$, gdzie m_{ij} są wymiarami podprzestrzeni $\tau-$cyklicznych w rozkładzie q_i-prymarnej składowej V_i przestrzeni V na sumę prostą podprzestrzeni cyklicznych. W związku z tym następująca definicja zawiera w sobie definicję 10.4.3.

DEFINICJA **10.5.8.** *Wielomianem charakterystycznym* f_τ endomorfizmu τ nazywamy iloczyn wszystkich dzielników elementarnych endomorfizmu τ. A więc

$$f_\tau = q_1^{n_1} \cdots q_k^{n_k},$$

gdzie $n_i = s_{i1} + \cdots + s_{ir_i}$.

W szczególności więc wielomian minimalny p_τ endomorfizmu τ jest dzielnikiem wielomianu charakterystycznego f_τ endomorfizmu τ, skąd wynika, że $f_\tau(\tau) = 0_V$. Nasza definicja wielomianu charakterystycznego endomorfizmu gwarantuje więc własność znaną jako twierdzenie Cayleya-Hamiltona.

Uwaga 10.5.9. Jeśli wszystkie czynniki nierozkładalne q_i wielomianu p_τ są wielomianami liniowymi $q_i = X - a_i$, to dla macierzy endomorfizmu τ mamy zarówno postać kanoniczną Jordana jak i postać kanoniczną Frobeniusa. Łatwo zauważyć, że te dwie macierze są równe jedynie wtedy gdy endomorfizm τ jest diagonalizowalny.

10.5.3 Jednoznaczność postaci kanonicznej

Ze względu na jednoznaczność rozkładu modułu (nad pierścieniem ideałów głównych) na sumę prostą podmodułów prymarnych pozostaje ustalić w jakim stopniu jest jednoznaczny rozkład prymarnych podmodułów V_τ na sumy proste podmodułów cyklicznych. Sformułujemy odpowiednie twierdzenia, ale pozostawimy je bez dowodu.

TWIERDZENIE **10.5.10.** *Niech endomorfizm $\tau \in \mathsf{End}_K V$ ma wielomian minimalny postaci $p_\tau = q^m$, gdzie q jest wielomianem nierozkładalnym nad ciałem K. Niech*

$$V = U_1 \oplus \cdots \oplus U_t = V_1 \oplus \cdots \oplus V_\ell$$

będą dwoma rozkładami przestrzeni V na sumy proste podprzestrzeni $\tau-$cyklicznych. Niech endomorfizmy indukowane przez τ na podprzestrzeniach U_i oraz V_j mają odpowiednio wielomiany minimalne q^{s_i} oraz q^{r_j} przy czym

$$s_1 \geqslant \cdots \geqslant s_t \geqslant 1 \quad \text{oraz} \quad r_1 \geqslant \cdots \geqslant r_\ell \geqslant 1.$$

Wtedy

$$t = \ell \quad \text{oraz} \quad s_i = r_i \quad \text{dla} \quad i = 1, \ldots, t.$$

Dowód. □

WNIOSEK **10.5.11.** *Niech endomorfizm $\tau \in \mathsf{End}_K V$ ma wielomian minimalny*

$$p_\tau = q_1^{m_1} \cdots q_k^{m_k},$$

gdzie q_i są unormowanymi parami niestowarzyszonymi wielomianami nierozkładalnymi nad ciałem K. Dzielniki elementarne $q_i^{s_{ij}}$ endomorfizmu τ są wyznaczone jednoznacznie przez endomorfizm τ i nie zależą od rozkładu przestrzeni V na sumę prostą podprzestrzeni $\tau-$cyklicznych.

WNIOSEK **10.5.12.** *Niech $\rho, \tau \in \mathsf{End}_K V$. Endomorfizmy ρ i τ są podobne wtedy i tylko wtedy, gdy mają te same dzielniki elementarne.*

Dowód. □

10.6 Rozmaitości o endomorfizmach

Podamy tu przeważnie bez dowodów kilka interesujących faktów o endomorfizmach przestrzeni wektorowych. Dowody wymagają na ogół użycia twierdzeń o postaciach kanonicznych dla redukcji dowodów do przypadków, gdy wielomian minimalny endomorfizmu ma szczególnie prostą postać.

10.6.1 Podobieństwo przy zwężaniu ciała

TWIERDZENIE **10.6.1.** *Niech ciało E będzie rozszerzeniem ciała nieskończonego K i niech $A, B \in M_n(K)$. Macierze A i B są podobne nad ciałem E wtedy i tylko wtedy gdy są podobne nad ciałem K.*

Dowód. Jeśli S jest macierzą nieosobliwą nad E oraz $AS = SB$, to odpowiedni układ n^2 równań liniowych jednorodnych o n^2 niewiadomych i współczynnikach z ciała K ma rozwiązanie s_{ij} w ciele E tworzące macierz nieosobliwą. Z algebry liniowej wiadomo, że istnienie rozwiązania układu równań liniowych nad E pociąga rozwiązalność tego układu nad K. Aby pokazać istnienie nieosobliwej macierzy S nad K posłużymy się pojęciem i własnościami wyznacznika. Podprzestrzeń rozwiązań układu równań $AS - SB = 0$ ma wymiar $k > 0$ i nieosobliwość macierzy S zależy od niezerowania się wyznacznika tej macierzy, który można traktować jako wielomian k zmiennych o współczynnikach z ciała K. Jeśli jest to wielomian niezerowy nad E, to nie może przyjmować tylko wartości zero nad K jeśli K jest ciałem *nieskończonym*. Zatem dla pewnego układu parametrów w ciele K dostaniemy nieosobliwą macierz S nad K taką, że $AS = SB$. □

TWIERDZENIE **10.6.2.** *Niech $A \in M_n(K)$ i niech $\tau \in \mathsf{End}_K K^n$ ma macierz A w pewnej bazie przestrzeni K^n. Niech f_τ będzie wielomianem charakterystycznym endomorfizmu τ (i macierzy A). Niech E będzie ciałem rozkładu wielomianu f_τ i niech*

$$f_\tau = \prod_{i=1}^{k} (X - \lambda_i)^{n_i}, \quad \lambda_i \in E,$$

gdzie $\lambda_i \neq \lambda_j$ dla $i \neq j$. Wtedy

$$\mathsf{Tr}\, A = \mathsf{Tr}\, \tau = \sum_{i=1}^{k} n_i \lambda_i \quad \text{oraz} \quad \det A = \det \tau = \prod_{i=1}^{k} \lambda_i^{n_i}.$$

Dowód. Macierz A ma postać kanoniczną Jordana nad ciałem E. □

10.6.2 Charakteryzacja endomorfizmów nilpotentnych

Endomorfizm nilpotentny ma tylko jedną wartość własną $a = 0$ i wobec tego ma ślad równy zero. Zatem także każda potęga endomorfizmu nilpotentnego ma ślad zero. Okazuje się, że ta własność charakteryzuje endomorfizmy nilpotentne.

TWIERDZENIE **10.6.3.** *Jeśli K jest ciałem o charakterystyce zero, $\tau \in \mathsf{End}_K V$ oraz*

$$\mathsf{Tr}\, \tau^i = 0_V \quad \text{dla} \quad \mathrm{i} = 1, 2, \ldots,$$

to τ jest endomorfizmem nilpotentnym.

Dowód. Indukcja ze względu na wymiar przestrzeni. Szczegóły dowodu można znaleźć w książce I. N. Herstein, *Topics in Algebra*, Wiley 1975, str. 315. □

10.6.3 Transponowanie macierzy

TWIERDZENIE **10.6.4.** *Macierze A i A^T są podobne.*

Dowód. A ma postać kanoniczną wymierną, wystarczy więc udowodnić twierdzenie w przypadku, gdy A jest macierzą stowarzyszoną z pewnym wielomianem. W tym przypadku jest możliwa wyraźna konstrukcja macierzy (symetrycznej) nieosobliwej S takiej, że $SA = A^T S$ (zob. I. Kaplansky, *Linear Algebra and Geometry. A second course*. Allyn and Bacon 1969, str. 76).

Jeśli założymy dodatkowo, że A jest macierzą nad nieskończonym ciałem K, to kompletny dowód otrzymujemy wykorzystując twierdzenie 10.6.1 oraz twierdzenie o istnieniu postaci kanonicznej Jordana macierzy A nad algebraicznym domknięciem E ciała K (zob. zadanie **5** poniżej). □

10.7 Zadania

1. Niech $\rho, \tau \in \mathsf{End}_K V$. Udowodnić, że następujące warunki są równoważne:

(a) $V_\rho \cong V_\tau$ (izomorfizm $K[X]-$modułów).
(b) ρ i τ są podobne.

2. Niech $f \in K[X]$ będzie wielomianem stopnia $n \geqslant 1$ i niech $S(f)$ będzie macierzą *stowarzyszoną* z wielomianem f.

(a) Udowodnić, że $f(S(f)) = 0 \in M_n(K)$.
(b) Udowodnić, że f jest wielomianem minimalnym macierzy $S(f) \in M_n(K)$.

3. Niech V będzie przestrzenią $\tau-$cykliczną. Udowodnić, że każdy endomorfizm σ przestrzeni V przemienny z τ ma postać $\sigma = f(\tau)$, gdzie $f \in K[X]$.

4. Udowodnić, że nad ciałem algebraicznie domkniętym E każda macierz $A \in M_n(E)$ jest podobna do macierzy transponowanej A^T.

5. Niech ρ i τ będą endomorfizmami przestrzeni wektorowej V nad ciałem $\mathbb{C}$ liczb zespolonych. Udowodnić, że jeśli $\rho^2 = \tau^2 = 1_V$, to przestrzeń V zawiera podprzestrzeń U o wymiarze 1 lub 2, która jest podprzestrzenią niezmienniczą obydwu endomorfizmów ρ i τ.

6. Niech K będzie ciałem o charakterystyce $\neq 2$.
(a) Jeśli $\sigma \in \mathsf{End}_K V$ jest endomorfizmem nilpotentnym, to istnieje taki endomorfizm $\rho \in \mathsf{End}_K V$, że $1_V + \sigma = \rho^2$.
(b) Jeśli w ciele K każdy element jest kwadratem ($K = K^2$), to dla każdego endomorfizmu odwracalnego $\tau \in \mathsf{End}_K V$ istnieje taki endomorfizm $\rho \in \mathsf{End}_K V$, że $\tau = \rho^2$.

Wskazówka. (a) Jeśli $\sigma^m = 0_V$, to $\rho = 1_V + x_1\sigma + \cdots + x_{m-1}\sigma^{m-1}$ dla odpowiednio dobranych $x_1, \ldots, x_{m-1} \in K$.

(b) Wykorzystać (a) i twierdzenie o rozkładzie.

7. Niech wielomian minimalny p_τ endomorfizmu τ przestrzeni V ma stopień równy wymiarowi przestrzeni: $\deg p_\tau = \dim V$. Udowodnić, że
(a) Moduł V_τ jest cykliczny.
(b) Każdy endomorfizm ρ przestrzeni V przemienny z τ ma postać $\rho = f(\tau)$, gdzie $f \in K[X]$.

8. Niech $n \geqslant 2$, $a, b \in K, b \neq 0$ i niech $A \in M_n(K)$ będzie macierzą, której wszystkie elementy diagonalne są równe a, zaś wszystkie pozostałe elementy są równe b.
(a) Pokazać, że $a - b$ jest wartością własną macierzy A o krotności geometrycznej $n - 1$.
(b) Pokazać, że $a + (n - 1)b$ jest wartością własną macierzy A o krotności geometrycznej 1.
(c) Znaleźć wielomian charakterystyczny i wielomian minimalny macierzy A.
(d) Znaleźć postać kanoniczną Jordana J macierzy A oraz macierz nieosobliwą S taką, że $A = S^{-1}JS$.

9. Niech $\sigma, \tau \in \mathsf{End}_K V$, gdzie K jest ciałem algebraicznie domkniętym.
(a) Udowodnić, że jeśli $\dim V \leqslant 3$, to endomorfizmy σ i τ są podobne wtedy i tylko wtedy gdy mają równe wielomiany minimalne i równe wielomiany charakterystyczne.
(b) Udowodnić, że jeśli $\dim V \geqslant 4$, to równość wielomianów minimalnych i równość wielomianów charakterystycznych nie pociąga podobieństwa endomorfizmów.

10. Niech $\sigma, \tau \in \mathsf{End}_K V$, gdzie K jest ciałem algebraicznie domkniętym.
(a) Udowodnić, że jeśli $\dim V \leqslant 6$, to endomorfizmy σ i τ są podobne wtedy i tylko wtedy gdy mają równe wielomiany minimalne, równe wielomiany charakterystyczne i równe krotności geometryczne każdej wartości własnej.
(b) Udowodnić, że jeśli $\dim V \geqslant 7$, to równość wielomianów minimalnych, równość wielomianów charakterystycznych i równość krotności geometrycznych wartości własnych nie pociąga podobieństwa endomorfizmów.

Wskazówka. (b) $3 + 3 + 1 = 3 + 2 + 2$.

Skorowidz