# Algebra liniowa nad pierścieniami

Wykład monograficzny

Kazimierz Szymiczek

# Przedmowa

Linear algebra, like motherhood,
has become a sacred cow.
*Irving Kaplansky*

Niniejszy skrypt jest zapisem wykładu monograficznego z algebry liniowej nad pierścieniami w Uniwersytecie Śląskim w semestrze zimowym roku akademickiego 2007/2008.

W rozdziale pierwszym przedstawiamy elementarne fakty o macierzach i układach równań liniowych nad pierścieniami przemiennymi. W dalszym ciągu klasyczną algebrę liniową traktujemy jednak przede wszystkim jako teorię przestrzeni wektorowych i ich homomorfizmów. Główną ideą wykładu jest potwierdzenie tezy, że właściwym uogólnieniem klasycznej algebry liniowej jest teoria modułów projektywnych i ich homomorfizmów. Demonstrujemy to, na przykład, na teorii dualności przestrzeni wektorowych, modułów wolnych i modułów projektywnych.

Notatki z wykładu będą systematycznie rozszerzane i poprawiane. Nowa wersja rozdziału będzie zawierała datę ostatniej zmiany.

Kazimierz Szymiczek

# Rozdział 1

# Układy równań liniowych nad pierścieniami

Ostatnie zmiany 13.11.2010 r.

W tym rozdziale $R$ jest pierścieniem przemiennym. Będziemy porównywać fakty o rozwiązalności układów równań liniowych nad ciałami - znane z kursowego wykładu algebry liniowej - z odpowiednimi faktami o układach równań liniowych nad pierścieniami. Dla układów niejednorodnych bardzo szybko natrafiamy na zasadnicze różnice. Na przykład, równanie liniowe

$$a_1X_1 + a_2X_2 + \cdots + a_nX_n = b, \quad a_1, \ldots, a_n, b \in \mathbb{Z}, \tag{1.1}$$

traktowane jako równanie nad ciałem $\mathbb{Q}$ liczb wymiernych ma rozwiązania w $\mathbb{Q}$ z wyjątkiem trywialnego przypadku gdy wszystkie $a_i = 0$ natomiast $b \neq 0$. Inaczej mówiąc, równanie to ma rozwiązanie w $\mathbb{Q}$ o ile rząd macierzy współczynników przy niewiadomych jest równy rzędowi macierzy uzupełnionej. Ten warunek nie wystarcza jednak na to by takie równanie miało rozwiązanie w liczbach całkowitych. Na przykład, równanie $2X_1 = 1$ nie ma rozwiązań w liczbach całkowitych. Dla rozwiązalności równania (1.1) w liczbach całkowitych, oprócz rozwiązalności w liczbach wymiernych, potrzeba, by spełniony był warunek

$$\mathrm{nwd}(a_1, \ldots, a_n) \mid b.$$

Równanie (1.1) jest bowiem równoważne pytaniu, czy liczba całkowita $b$ należy do ideału $\mathcal{I}$ generowanego przez liczby całkowite $a_1, \ldots, a_n$. W pierścieniu $\mathbb{Z}$ każdy ideał jest główny i faktycznie $\mathcal{I} = (\mathrm{nwd}(a_1, \ldots, a_n))$ jest ideałem głównym generowanym przez największy wspólny dzielnik liczb $a_1, \ldots, a_n$. Wobec tego $b \in \mathcal{I}$ wtedy i tylko wtedy gdy $b$ jest wielokrotnością $\mathrm{nwd}(a_1, \ldots, a_n)$. Jak więc widzimy, nawet w najprostszym przypadku pierścienia liczb całkowitych, problem rozwiązalności (układów) równań liniowych ma zupełnie inne rozwiązanie niż w przypadku ciała liczb wymiernych i rolę pojęć algebry liniowej, takich jak rząd macierzy, przejmują pojęcia arytmetyczne.

W tym rozdziale dyskutujemy najpierw odwracalność macierzy nad pierścieniami i pokazujemy, że macierz kwadratowa nad pierścieniem $R$ jest odwracalna wtedy i tylko wtedy gdy jej wyznacznik jest elementem odwracalnym pierścienia $R$. Następnie wprowadzamy pojęcie rzędu macierzy o elementach z dowolnego pierścienia (dopuszczamy występowanie dzielników zera w $R$) i pokazujemy, że dla *jednorodnych* układów równań liniowych nad $R$ warunek na istnienie rozwiązań niezerowych układu jest taki sam jak w przypadku układów jednorodnych nad ciałami: rząd macierz współczynników przy niewiadomych musi być mniejszy od liczby niewiadomych.

## 1.1 Macierze nad pierścieniami

Dla pierścienia $R$ symbolem $M_n(R)$ oznacza się zbiór wszystkich macierzy kwadratowych stopnia $n$ o elementach z pierścienia $R$. *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 $M_n(R)$ jest pierścieniem. Nazywamy go *pierścieniem macierzy stopnia n nad pierścieniem R*. Jeśli $n \geqslant 2$, to $M_n(R)$ jest pierścieniem nieprzemiennym.
Macierz $A \in M_n(R)$ nazywamy macierzą *odwracalną*, jeśli istnieje macierz $B \in M_n(R)$ taka, ze $AB = BA = I$. Tutaj $I$ oznacza macierz jednostkową, która jest jedynką pierścienia $M_n(R)$.

W dalszym ciągu ważną rolę gra pojęcie wyznacznika macierzy. W kursowym wykładzie algebry wprowadza się pojęcie wyznacznika macierzy o elementach z ciała. Ta sama (indukcyjna) definicja funkcjonuje także nad pierścieniami.
A więc wyznacznikiem $\det A$ macierzy $A \in M_n(R)$ nazywamy element pierścienia $R$ określony następująco:

$$\det A = \begin{cases} a_{11} & \text{jeśli } n = 1 \\ \sum\limits_{i=1}^{n} (-1)^{i+n} a_{in} \det A_{in} & \text{jeśli } n \geqslant 2 \end{cases}$$

gdzie $A_{in}$ jest macierzą powstałą z macierzy $A$ przez skreślenie $i$-tego wiersza i $n$-tej kolumny.

Będziemy korzystać z podstawowych własności tak zdefiniowanego wyznacznika macierzy o elementach z pierścienia przemiennego $R$. Dowody tych własności, bazujące na powyższej definicji, są takie same jak w przypadku gdy $R$ jest ciałem. Wśród nich są m. in. twierdzenie Laplace'a i twierdzenie Cauchy'ego. Czytelnik, który czuje pewien dyskomfort związany z korzystaniem z nieudowodnionych twierdzeń powinien zapoznać się z fragmentem książki G. Banaszaka i W. Gajdy *Elementy algebry liniowej, część I*, WNT Warszawa 2002, §6.5 Dodatek. Macierze o współczynnikach w pierścieniu. Dyskutuje się tam uogólnianie twierdzeń a macierzach nad ciałem na przypadek macierzy nad pierścieniami przemiennymi.

Dla wprowadzenie pojęcia rzędu macierzy posługiwać się będziemy pojęciem minora stopnia $k$ macierzy $A$. Niech $A \in M_n(R)$. Wybieramy z macierzy $A$ dowolnych $k$ wierszy i dowolnych $k$ kolumn, gdzie $1 \leqslant k \leqslant n$ i tworzymy macierz $B$ stopnia $k$ z wyrazów znajdujących się na przecięciu wybranych wierszy i kolumn. Wyznacznik każdej tak skonstruowanej macierzy $B$ nazywa się minorem stopnia $k$ macierzy $A$.

Dla macierzy o elementach z ciała rząd macierzy określa się jako maksymalny stopień minora różnego od zera, lub równoważnie, jako maksymalną liczbę liniowo niezależnych wierszy macierzy. Przy tym dowodzi się, że maksymalna liczba liniowo niezależnych wierszy macierzy jest równa maksymalnej liczbie liniowo niezależnych kolumn tej macierzy.

Taka definicja rzędu macierzy byłaby nieprzydatna dla macierzy nad pierścieniami z dzielnikami zera. Okazuje się, że dla macierzy nad pierścieniem $R$ istotne jest nie tyle to czy minory stopnia $k$ są różne od zera, ale istotne jest istnienie (lub brak) różnego od zera elementu pierścienia $R$, który *anihiluje* wszystkie minory stopnia $k$ tej macierzy. W przykładzie 1.1.2 pokazujemy, że także operowanie maksymalnymi liczbami liniowo niezależnych wierszy i kolumn macierzy nie prowadzi do satysfakcjonującej definicji rzędu macierzy nad pierścieniami.

Przez anihilator elementu $a \in R$ rozumiemy każdy element $b \in R$ taki, że $ab = 0$. Podobnie anihilatorem skończonego zbioru elementów pierścienia

$$\{a_1, a_2, \ldots, a_n\}$$

nazywamy każdy element anihilujący wszystkie elementy tego zbioru, a więc każdy element $b \in R$ taki, że $a_i b = 0$ dla każdego $1 \leqslant i \leqslant n$.

Definicja rzędu macierzy nad pierścieniem jest następująca:

DEFINICJA **1.1.1.** Niech $A \in M_n(R)$. Mówimy że $\operatorname{rz} A = 0$ jeśli zbiór wszystkich elementów $a_{ij}$ macierzy $A$ ma niezerowy anihilator, to znaczy,
$\operatorname{rz} A = 0$ wtedy i tylko wtedy, gdy istnieje element $0 \neq b \in R$ taki, że $ba_{ij} = 0$ dla wszystkich $i, j$.

Jeśli $\operatorname{rz} A \neq 0$, to rzędem macierzy $A$ nazywamy maksymalny stopień $r$ minorów macierzy $A$, które nie mają wspólnego niezerowego anihilatora w $R$.

A więc $\operatorname{rz} A = r \neq 0$ jeśli wszystkie minory stopnia $r+1$ macierzy $A$ są anihilowane przez pewien niezerowy element pierścienia $R$ natomiast nie istnieje niezerowy element pierścienia $R$ anihilujący wszystkie minory stopnia $r$.

Gdy $R$ jest ciałem, to warunek *minory stopnia $r$ nie mają wspólnego niezerowego anihilatora* jest równoważny warunkowi, że *nie wszystkie minory stopnia $r$ są równe zero*. Tak więc dla macierzy $A$ nad ciałem, jej rząd jest równy maksymalnemu stopniowi minora różnego od zera. Zauważmy, że również w przypadku gdy pierścień $R$ nie ma dzielników zera, to rząd macierzy $A$ jest równy największemu stopniowi $r$ niezerowego minora macierzy $A$. W tym przypadku zbiór minorów stopnia $r$ macierzy $A$ nie ma niezerowego anihilatora tylko wtedy gdy zbiór ten zawiera jakiś niezerowy element pierścienia $R$.

**Przykład 1.1.1.** Rząd macierzy

$$A = \begin{bmatrix} 0 & 2 & 2 \\ 0 & 0 & 2 \\ 2 & 0 & 1 \end{bmatrix}$$

nad pierścieniem $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$ jest równy 1. Rzeczywiście jedyny minor stopnia 3 jest równy 2 i jest anihilowany przez $3 \neq 0$ . Minory stopnia 2 są równe 0 lub 2 lub 4 i wszystkie są anihilowane przez $3 \neq 0$. Zatem $\operatorname{rz} A \leqslant 1$ i $\operatorname{rz} A \neq 0$, gdyż elementy macierzy $A$ nie mają wspólnego niezerowego anihilatora w $\mathbb{Z}_6$.
Zauważmy jeszcze, że zarówno wiersze jak i kolumny macierzy $A$ są liniowo zależne nad $\mathbb{Z}_6$, natomiast wiersz pierwszy i trzeci, oraz kolumny pierwsza i trzecia są liniowo niezależne nad $\mathbb{Z}_6$. Tak więc maksymalna liczba liniowo niezależnych wierszy macierzy $A$ jest równa maksymalnej liczbie liniowo niezależnych kolumn macierzy $A$. Gdybyśmy więc określili rząd macierzy jako wspólną maksymalną liczbę liniowo niezależnych wierszy i kolumn macierzy, to macierz $A$ miałaby rząd 2.
Następny przykład pokazuje jednak, że nie byłaby to dobra definicja rzędu macierzy nad pierścieniem przemiennym.

**Przykład 1.1.2.** Rozpatrzmy macierz

$$B = \begin{bmatrix} 1 & 1 & -1 \\ 0 & 2 & 3 \end{bmatrix}$$

nad pierścieniem $\mathbb{Z}_{30} = \mathbb{Z}/30\mathbb{Z}$. Tutaj wiersze macierzy $B$ są liniowo niezależne nad $\mathbb{Z}_{30}$, natomiast każde dwie kolumny są liniowo zależne. A więc maksymalna liczba

liniowo niezależnych wierszy (nazywana *rzędem wierszowym* macierzy) jest równa 2, natomiast maksymalna liczba liniowo niezależnych kolumn (nazywana *rzędem kolumnowym* macierzy) jest równa 1. Zatem istotne dla wprowadzenia pojęcia rzędu macierzy twierdzenie klasycznej algebry liniowej, że dla macierzy nad dowolnym ciałem, *rząd wierszowy macierzy jest równy rzędowi kolumnowemu*, nie jest prawdziwe nad pierścieniami przemiennymi.
Z drugiej strony zauważmy, że trzy minory stopnia 2 macierzy $B$ są równe odpowiednio $2, 3, 5$, nie mają więc wspólnego niezerowego anihilatora w $\mathbb{Z}_{30}$. Zatem zgodnie z definicją 1.1.1 mamy $\operatorname{rz} B = 2$.

Definicja **1.1.2.** Macierzą dopełnień algebraicznych macierzy kwadratowej $A = [a_{ij}] \in M_n(R)$ nazywamy macierz

$$A_d = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \vdots & \vdots & & \vdots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{bmatrix}$$

gdzie $A_{ij}$ jest dopełnieniem algebraicznym elementu $a_{ik}$ macierzy $A$.
Dopełnieniem algebraicznym elementu $a_{ik}$ macierzy $A$ nazywamy element pierścienia $R$ postaci $A_{ik} = (-1)^{i+k} M_{ik}$ gdzie $M_{ik}$ jest minorem macierzy $A$ stopnia $(n-1)$, który powstaje przez skreślenie w macierzy $A$ $i$–tego wiersza oraz $k$–tej kolumny.
Macierzą *dołączoną* macierzy kwadratowej $A$ nazywamy transponowaną macierz dopełnień algebraicznych

$$\operatorname{Adj} A = [A_d]^T$$

Lemat **1.1.1.** *Jeśli $A$ jest macierzą kwadratową nad pierścieniem przemiennym, to*

$$A \cdot (\operatorname{Adj} A) = (\det A) \cdot I = (\operatorname{Adj} A) \cdot A.$$

*Dowód.* Pokażemy najpierw, że $A \cdot (\operatorname{Adj} A) = (\det A) \cdot I$.
Element znajdujący się w $i$–tym wierszu oraz $j$–tej kolumnie iloczynu $A(\operatorname{Adj} A)$ ma postać:

$$a_{i1}A_{1j} + a_{i2}A_{2j} + \dots + a_{in}A_{nj}$$

Na podstawie twierdzenia Laplace'a mamy

$$a_{i1}A_{1j} + a_{i2}A_{2j} + \dots + a_{in}A_{nj} = \begin{cases} 0 & \text{jeśli } i \neq j \\ \det A & \text{jeśli } i = j \end{cases}.$$

Wobec tego na głównej przekątnej macierzy $A(\operatorname{Adj} A)$ występuje $\det A$, a pozostałe elementy macierzy są równe zeru, a więc $A(\operatorname{Adj} A) = (\det A)I$.
Podobnie pokazujemy, że $(\operatorname{Adj} A) \cdot A = (\det A) \cdot I$.
Element znajdujący się w $i$–tym wierszu oraz $j$–tej kolumnie macierzy $(\operatorname{Adj} A) \cdot A$ ma postać:

$$A_{i1}a_{1j} + A_{i2}a_{2j} + \dots + A_{in}a_{nj} = \begin{cases} 0 & \text{jeśli } i \neq j \\ \det A & \text{jeśli } i = j \end{cases}$$

A więc w macierzy $(\operatorname{Adj} A)A$ elementy znajdujące się na głównej przekątnej są równe $\det A$, a pozostałe są równe zeru, zatem jest ona równa $(\det A)I$. □

Udowodnimy teraz odpowiednik twierdzenia algebry liniowej mówiącego, że macierz o elementach z ciała jest odwracalna wtedy i tylko wtedy gdy ma wyznacznik różny od zera.

TWIERDZENIE **1.1.1.** *Niech $R$ będzie pierścieniem przemiennym oraz $A \in M_n(R)$. Macierz $A$ jest odwracalna w pierścieniu $M_n(R)$ wtedy i tylko wtedy, gdy jej wyznacznik* $\det A$ *jest elementem odwracalnym w $R$.*

*Dowód.* Załóżmy najpierw, że macierz $A$ ma macierz odwrotną w pierścieniu $M_n(R)$, czyli istnieje taka macierz $B \in M_n(R)$, że $AB = I = BA$. Wtedy $\det(AB) = \det I = \det(BA)$ i na podstawie twierdzenia Cauchy'ego otrzymujemy

$$\det A \det B = \det(AB) = 1 = \det(BA) = \det B \det A.$$

Ponieważ $B \in M_n(R)$, więc $\det B \in R$. Stąd wynika, że $\det A$ jest odwracalny w $R$ i elementem odwrotnym do $\det A$ jest $\det B$.

Zakładamy, teraz że $\det A$ ma element odwrotny $d$ w pierścieniu $R$. Z lematu 1.1.1 wiemy, że $A(\operatorname{Adj} A) = A(\operatorname{Adj} A) = (\det A)I$. Mnożąc tę równość przez element odwrotny do $\det A$ otrzymujemy

$$dA(\operatorname{Adj} A) = d(\operatorname{Adj} A)A = d(\det A)I = I$$

czyli

$$A \cdot (d \operatorname{Adj} A) = I = (d \operatorname{Adj} A) \cdot A = I.$$

A więc macierz $A$ ma w pierścieniu $M_n(R)$ macierz odwrotną $d(\operatorname{Adj} A)$. □

## 1.2 Układy równań liniowych jednorodnych

Rozpatrzymy teraz problem istnienia rozwiązań układu równań liniowych jednorodnych o współczynnikach z pierścienia przemiennego $R$. Wiemy, że układ

$$\begin{gathered} b_{11}x_1 + b_{12}x_2 + \ldots + b_{1n}x_n = 0 \\ b_{12}x_1 + b_{22}x_2 + \ldots + b_{2n}x_n = 0 \\ \vdots \\ b_{m1}x_1 + b_{m2}x_2 + \ldots + b_{mn}x_n = 0 \end{gathered}$$

o współczynnikach należących do pewnego ciała $K$ ma nietrywialne (to znaczy niezerowe) rozwiązanie, gdy $\operatorname{rz} B < n$, gdzie

$$B = \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \vdots & & & \vdots \\ b_{n1} & b_{n2} & \ldots & b_{mn} \end{bmatrix}$$

jest macierzą współczynników przy niewiadomych. Okazuje się, że twierdzenie to ma znacznie ogólniejszą wersję dla układów równań liniowych jednorodnych nad pierścieniami przemiennymi.

TWIERDZENIE **1.2.1.** *Niech $R$ będzie pierścieniem przemiennym. Układ $m$ równań liniowych jednorodnych o $n$ niewiadomych*

$$\sum_{j=1}^{n} c_{ij}x_j = 0, \quad i = 1, \ldots, m \tag{1.2}$$

*o współczynnikach $c_{ij} \in R$ ma niezerowe rozwiązanie w pierścieniu $R$ wtedy i tylko wtedy gdy rząd macierzy $C = [c_{ij}]$ jest mniejszy niż liczba niewiadomych $n$.*

*Dowód.* Załóżmy najpierw, że układ (1.2) ma nietrywialne rozwiązanie $(a_1, \ldots, a_n)$, $a_j \in R$, gdzie $a_k \neq 0$ dla pewnego $k$. Mamy więc $m$ równości

$$\sum_{j=1}^{n} c_{ij} a_j = 0, \quad i = 1, \ldots, m \tag{1.3}$$

przy czym $a_k \neq 0$.
Jeśli $m < n$, czyli w układzie (1.2) liczba równań jest mniejsza od liczby niewiadomych, to macierz $C = [c_{ij}]$ ma $m$ wierszy i mamy oczywiście $\operatorname{rz} C \leqslant m$. Zatem $\operatorname{rz} C \leqslant m < n$.

Niech teraz $n \leqslant m$, czyli w układzie (1.2) liczba niewiadomych jest nie większa od liczby równań.
Aby pokazać, że $\operatorname{rz} C < n$ należy udowodnić, że wszystkie minory stopnia $n$ macierzy $C$ mają wspólny niezerowy anihilator. Ponieważ macierz $C$ ma $n$ kolumn, każdy minor stopnia $n$ jest wyznacznikiem macierzy, która składa się z pewnych $n$ wierszy macierzy $C$. W macierzy $C$ kolejność wierszy nie ma żadnego znaczenia dla rozpatrywanego przez nas zagadnienia rozwiązalności układu, gdyż zmiana kolejności wierszy odpowiada zmianie kolejności równań układu (1.2), a to nie wpływa na rozwiązalność układu. Zmieniając zatem ewentualnie kolejność równań w układzie (1.2) możemy założyć, że interesujący nas minor stopnia $n$ jest wyznacznikiem macierzy złożonej z pierwszych $n$ kolumn i pierwszych $n$ wierszy macierzy $C$.
Niech więc $D$ będzie macierzą stopnia $n$ składającą się z pierwszych $n$ wierszy macierzy $C$,

$$D = \begin{bmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{bmatrix}.$$

Ponieważ $D$ jest macierzą kwadratową możemy rozpatrywać dopełnienia algebraiczne $D_{ik}$ elementów $k-$tej kolumny macierzy $D$. Tutaj $k$ jest tak dobrane, że $a_k \neq 0$ w rozwiązaniu $(a_1, \ldots, a_n)$ układu (1.2). A więc

$$D_{ik} = (-1)^{i+k} \det C_{ik},$$

gdzie $C_{ik}$ powstaje z macierzy $D$ przez skreślenie $i$–tego wiersza i $k$–tej kolumny macierzy $D$.
Dla $i \leqslant n$ mnożymy $i$–tą równość układu (1.3) przez dopełnienie algebraiczne $D_{ik}$ elementu występującego w $k-$tej kolumnie:

$$\sum_{j=1}^{n} c_{ij} a_j D_{ik} = 0, \quad i = 1, \ldots, n$$

a następnie dodajemy wszystkie tak otrzymane równości i dostajemy

$$\sum_{i=1}^{n} \sum_{j=1}^{n} c_{ij} a_j D_{ik} = 0.$$

Zmieniając kolejność sumowania otrzymujemy

$$\sum_{j=1}^{n} \sum_{i=1}^{n} c_{ij} D_{ik} a_j = 0. \tag{1.4}$$

Na podstawie twierdzenia Laplace'a mamy

$$\sum_{i=1}^{n} c_{ij} D_{ik} = \begin{cases} 0 & k \neq j \\ \det D & k = j \end{cases}$$

Równość (1.4) redukuje się więc do równości $(\det D)a_k = 0$. Ponieważ $a_k \neq 0$, wynika stąd, że $a_k$ jest niezerowym anihilatorem $\det D$. Zatem stąd, że układ (1.2) ma niezerowe rozwiązanie wynika, że wszystkie minory stopnia $n$ macierzy $C$ mają wspólny niezerowy anihilator i wobec tego $\operatorname{rz} C < n$.

Pokażemy teraz, że jeśli $\operatorname{rz} C < n$, to układ (1.2) ma niezerowe rozwiązanie w pierścieniu $R$. Niech $r = \operatorname{rz} C < n$. Oczywiście $r \leqslant m$, ale możemy założyć, że także $r < m$, to znaczy liczba równań jest także większa od rzędu macierzy $C$. Gdyby bowiem $r = m$, to do układu (1.2) dołączamy równanie o współczynnikach równych zero. Dołączenie takiego równania nie zmienia rzędu macierzy współczynników przy niewiadomych i nie zmienia rozwiązalności układu.

Rozważmy najpierw przypadek gdy $r = 0$.
Wtedy zbiór wszystkich elementów $c_{ij}$ macierzy $C$ ma wspólny niezerowy anihilator. Niech $a$ będzie niezerowym anihilatorem zbioru wszystkich elementów macierzy $C$ czyli $c_{ij}a = 0$ dla każdego $i = 1, 2, \ldots, m,\ j = 1, 2, \ldots, n$.
Podstawiając w $i-$tym równaniu układu (1.2) $x_j = a$ dla $j = 1, \ldots, n$, otrzymujemy $\sum_{j=1}^{n} c_{ij}a = 0$. A więc układ (1.2) ma niezerowe rozwiązanie $(x_1, \ldots, x_n) = (a, \ldots, a)$.
Załóżmy teraz, że $r > 0$. Oznacza to, że istnieje niezerowy element $a \in R$, który anihiluje wszystkie minory stopnia $r + 1$ macierzy $C$ oraz istnieje pewien minor $M$ stopnia $r$ macierzy $C$ taki, że $aM \neq 0$. Zmieniając porządek równań w układzie (1.2) i zmieniając ewentualnie numerację niewiadomych możemy zakładać, że $M$ jest wyznacznikiem macierzy utworzonej z elementów pierwszych $r$ wierszy i pierwszych $r$ kolumn macierzy $C$.
Rozważmy teraz macierz $C'$ utworzoną z pierwszych $r+1$ kolumn i pierwszych $r+1$ wierszy macierzy $C$ (tu wykorzystujemy założenie, że $r < m$). Wtedy $\det C'$ jest minorem stopnia $r + 1$ macierzy $C$ i wobec tego mamy $a \det C' = 0$.
Niech $c'_1, c'_2, \ldots, c'_{r+1}$ będą dopełnieniami algebraicznymi elementów ostatniego wiersza macierzy $C'$. Zauważmy, że $c'_{r+1} = M$ i wobec tego $ac'_{r+1} = aM \neq 0$. Pokażemy, że

$$x_j = ac'_j, \quad j = 1, 2, \ldots, r + 1,$$

$$x_j = 0, \quad j = r + 2, \ldots, n$$

jest niezerowym rozwiązaniem układu (1.2). Zauważyliśmy już, że $x_{r+1} = ac'_{r+1} = aM \neq 0$, więc jeśli tylko elementy $x_1, \ldots, x_n$ spełniają układ (1.2), to są rzeczywiście niezerowym rozwiązaniem tego układu.
Jeśli $1 \leqslant i \leqslant r$, to $\sum_{j=1}^{n} c_{ij}x_j = \sum_{j=1}^{r+1} c_{ij}ac'_j = a\sum_{j=1}^{r+1} c_{ij}c'_j = 0$, gdyż $c'_j$ są dopełnieniami elementów ostatniego, $(r+1)-$go wiersza macierzy $C'$, natomiast $c_{ij}$ są elementami $i-$tego wiersza podczas gdy $i < r + 1$.
Jeśli $i > r$, to $\sum_{j=1}^{n} c_{ij}x_j = \sum_{j=1}^{r+1} c_{ij}ac'_j = a\sum_{j=1}^{r+1} c_{ij}c'_j = 0$, gdyż $\sum_{j=1}^{r+1} c_{ij}c'_j$ jest wyznacznikiem macierzy, która powstaje z $r$ pierwszych wierszy macierzy $C'$ przez dołączenie do nich $i-$go wiersza macierzy $C$, czyli jest pewnym minorem stopnia $r+1$ macierzy

$C$ oraz $a$ anihiluje zbiór wszystkich minorów stopnia $r+1$.
A więc jeśli $\operatorname{rz} C < n$, to układ (1.2) ma nietrywialne rozwiązanie.

□

# Rozdział 2

# Moduły

Ostatnie zmiany 13.10.2007 r.

## 2.1 Pierścienie

Pojęcie przestrzeni wektorowej nad ciałem jest szczególnym przypadkiem ogólniejszego pojęcia modułu nad pierścieniem. Rozpatrywać przy tym będziemy pierścienie niekoniecznie przemienne. A więc pierścień $R$ jest to system złożony ze zbioru $R$, dwóch działań zwanych dodawaniem (oznaczanym $+$ ) i mnożeniem (oznaczanym $\cdot$ ) oraz dwóch wyróżnionych elementów $0, 1 \in R$, spełniający następujące warunki:

- $(R,\ +\ ,\ 0\ )$ *jest grupą abelową,*
- *mnożenie w* $R$ *jest działaniem łącznym i obustronnie rozdzielnym względem dodawania, oraz*
- $1 \cdot x = x \cdot 1 = x$ *dla każdego* $x \in R$.

Jeśli w pierścieniu $R$ mnożenie jest przemienne, to $R$ nazywamy pierścieniem przemiennym. W definicji pierścienia nie zakładamy, że $0 \neq 1$. Zauważmy jednak, że jeśli $0 = 1$, to dla $x \in R$ mamy $x = 1 \cdot x = 0 \cdot x = 0$ i wobec tego $R$ jest pierścieniem zerowym, $R = \{0\}$.

Z kursowego wykładu algebry znamy wiele przykładów pierścieni przemiennych, takich jak $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $K[X]$, gdzie $K$ jest dowolnym pierścieniem przemiennym, a także przykłady pierścieni nieprzemiennych, takich jak pierścień macierzy $M_n(K)$ nad dowolnym ciałem $K$, czy pierścień $\mathsf{End}\, V$ endomorfizmów przestrzeni wektorowej $V$. Jak już zauważyliśmy w rozdziale pierwszym, dla pierścienia $R$ symbolem $M_n(R)$ oznacza się zbiór wszystkich macierzy kwadratowych stopnia $n$ o elementach z pierścienia $R$. Jeśli $n \geqslant 2$, to $M_n(R)$ jest pierścieniem nieprzemiennym.
Element $a$ pierścienia $R$ nazywa się *lewostronnie* odwracalny, jeśli istnieje $b \in R$ taki, że $ba = 1$. Element $b$ nazywa się wtedy lewostronnie odwrotnym do elementu $a$. Podobnie, $a \in R$ jest *prawostronnie* odwracalny, jeśli istnieje $c \in R$ 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. Na przykład, można pokazać, że w pierścieniu endomorfizmów pierścienia wielomianów istnieją elementy jednostronnie, ale nie obustronnie odwracalne.

Element $a \in R$ 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 $U(R)$ wszystkich elementów odwracalnych pierścienia $R$ tworzy grupę ze względu na mnożenie elementów. Nazywa się ją *grupą elementów odwracalnych* pierścienia $R$.
Pierścień $R$ nazywa się *pierścieniem z dzieleniem*, jeśli każdy różny od zera element pierścienia $R$ jest odwracalny. Przemienny pierścień z dzieleniem jest więc ciałem.
Element $a$ pierścienia $R$ nazywa się *lewostronnym dzielnikiem zera*, jeśli istnieje $b \in R,\ b \neq 0$, taki, że $ab = 0$. Podobnie, $a \in R$ jest *prawostronnym dzielnikiem zera*, jeśli istnieje $c \in R,\ c \neq 0$, taki, że $ca = 0$. Element $a \in R$ nazywa się *dzielnikiem zera* w $R$ jeśli jest równocześnie lewostronnym i prawostronnym dzielnikiem zera.
*Centrum* $Z(R)$ pierścienia $R$ nazywamy zbiór wszystkich elementów pierścienia $R$ przemiennych z każdym elementem pierścienia $R$ :

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

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

Podzbiór $\mathcal{J}$ pierścienia $R$ nazywamy *ideałem lewostronnym* pierścienia $R$, jeśli $\mathcal{J}$ jest podgrupą addytywnej grupy pierścienia $R$ oraz $\mathcal{J}$ jest zamknięty ze względu na mnożenie z *lewej* strony przez elementy pierścienia $R$, to znaczy

$$x \in R,\ a \in \mathcal{J} \quad \Rightarrow \quad xa \in \mathcal{J}.$$

Podgrupa $\mathcal{I}$ addytywnej grupy pierścienia $R$ zamknięta ze względu na mnożenie z *prawej* strony przez elementy pierścienia $R$, to znaczy

$$x \in R,\ a \in \mathcal{I} \quad \Rightarrow \quad ax \in \mathcal{I}$$

nazywa się ideałem *prawostronnym* pierścienia $R$. Ideał lewostronny, który jest równocześnie ideałem prawostronnym pierścienia $R$ nazywa się ideałem obustronnym lub krótko *ideałem* pierścienia $R$.

Każdy podzbiór $S$ pierścienia $R$ generuje pewien ideał. Łatwo sprawdzamy, że zbiory

$$SR := \{s_1x_1 + \cdots + s_nx_n \in R : s_i \in S,\ x_i \in R,\ n \in \mathbb{N}\}$$
$$RS := \{x_1s_1 + \cdots + x_ns_n \in R : s_i \in S,\ x_i \in R,\ n \in \mathbb{N}\}$$

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

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

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

dla każdych $a, b \in P$, nazywamy *homomorfizmem* pierścienia $P$ w pierścień $R$.

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 ideałem pierścienia $P$.

Niech teraz $\mathcal{I}$ będzie ideałem lewostronnym pierścienia $R$. Zatem $\mathcal{I}$ można traktować jako podgrupę addytywnej grupy pierścienia $R$ i utworzyć grupę ilorazową $R/\mathcal{I}$. 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 na zbiorze warstw $R/\mathcal{I}$ nie można na ogół określić działania mnożenia za pomocą warunku

$$(a + \mathcal{I})(b + \mathcal{I}) = ab + \mathcal{I}. \tag{2.1}$$

Aby taka definicja była poprawna, musimy wymagać by była niezależna od wyboru elementów reprezentujących warstwy, to znaczy by spełniony był warunek

$$a + \mathcal{I} = a' + \mathcal{I}, \quad b + \mathcal{I} = b' + \mathcal{I} \quad \Rightarrow \quad ab + \mathcal{I} = a'b' + \mathcal{I}.$$

Zakładamy więc, że $a - a' \in \mathcal{I}$ oraz $b - b' \in \mathcal{I}$ i oczekujemy, że wtedy $ab - a'b' \in \mathcal{I}$. Tymczasem jednak

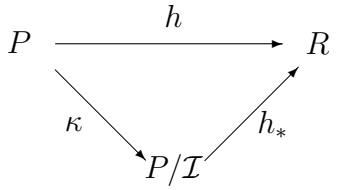
$$ab - a'b' = (a - a')b + a'(b - b')$$

i wobec tego, że $\mathcal{I}$ jest ideałem lewostronnym oraz $b - b' \in \mathcal{I}$ otrzymujemy tylko $a'(b - b') \in \mathcal{I}$. Jeśli $\mathcal{I}$ nie jest ideałem obustronnym, to zawsze można dobrać elementy $a, a', b \in R$ tak, że $(a - a')b \notin \mathcal{I}$ i wtedy $ab - a'b' \notin \mathcal{I}$. Tak więc dla ideału jednostronnego $\mathcal{I}$ nie można na addytywnej grupie ilorazowej $R/\mathcal{I}$ określić mnożenia przy pomocy (2.1). Natomiast jest to możliwe gdy $\mathcal{I}$ jest ideałem obustronnym i wtedy na zbiorze warstw $R/\mathcal{I}$ mamy określone dwa działania: dodawania i mnożenia warstw. Wykorzystując łączność mnożenia i rozdzielność mnożenia względem dodawania w $R$ dowodzimy łączności mnożenia i rozdzielności mnożenia względem dodawania w $R/\mathcal{I}$. Ponadto, $(1 + \mathcal{I})(a + \mathcal{I}) = a + \mathcal{I} = (a + \mathcal{I})(1 + \mathcal{I})$. Zatem $R/\mathcal{I}$ jest pierścieniem z jedynką $1 + \mathcal{I}$. Pierścień ten nazywamy *pierścieniem ilorazowym* pierścienia $R$ względem ideału $\mathcal{I}$ (lub modulo $\mathcal{I}$). Zauważmy jeszcze, że dla $\mathcal{I} = R$ jako pierścień ilorazowy $R/R$ otrzymujemy pierścień zerowy. Jest to główny powód, dla którego w definicji pierścienia nie wymagaliśmy by $0 \neq 1$.
Odwzorowanie

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

jest homomorfizmem pierścieni oraz $\ker \kappa = \mathcal{I}$. Homomorfizm $\kappa$ nazywamy *homomorfizmem kanonicznym* pierścienia $R$ na pierścień ilorazowy $R/\mathcal{I}$. Zauważamy też od razu, że każdy ideał $\mathcal{I}$ pierścienia $R$ jest jądrem pewnego homomorfizmu pierścienia $R$. A więc ideały odgrywają w twierdzeniach o homomorfizmach pierścieni podobną rolę jak podgrupy normalne w twierdzeniach o homomorfizmach grup. Sformułujemy tutaj podstawowe twierdzenie o homomorfizmach pierścieni.

TWIERDZENIE **2.1.1.** (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 o faktoryzacji homomorfizmów grup dla homomorfizmu $h$ traktowanego jako homomorfizm addytywnych grup pierścieni $P$ i $R$ i stwierdzamy, że $h_*$ jest homomorfizmem pierścieni. □

## 2.2 Moduły

Kluczowe we współczesnej algebrze pojęcie modułu nad pierścieniem definiuje się następująco.

Definicja **2.2.1.** Niech $R$ będzie dowolnym pierścieniem i niech $M$ będzie addytywną grupą abelową.
Grupę $M$ nazywamy lewostronnym *modułem* nad pierścieniem $R$, lub krócej lewostronnym $R-$modułem, jeśli na grupie $M$ określone jest *działanie zewnętrzne* z pierścieniem skalarów $R$ :

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

i ma ono następujące własności:

$$\begin{aligned} a(m_1 + m_2) &= am_1 + am_2 && (2.2)\\ (a_1 + a_2)m &= a_1m + a_2m && (2.3)\\ (a_1a_2)m &= a_1(a_2m) && (2.4)\\ 1m &= m && (2.5) \end{aligned}$$

dla wszystkich $a, a_1, a_2 \in R,\ m_1, m_2, m \in M$.

Jak widzimy, w przypadku gdy pierścień $R$ jest ciałem, definicja ta redukuje się do definicji przestrzeni wektorowej.
Jeśli w tej definicji warunek (2.3) zastąpimy przez

$$(a_1a_2)m = a_2(a_1m) \quad \text{dla wszystkich} \quad a_1, a_2 \in R,\ m \in M,$$

to otrzymamy definicję *prawostronnego* $R-$modułu $M$. Oczywiście, jeśli $R$ jest pierścieniem przemiennym i $M$ jest lewostronnym $R-$modułem, to z równości

$$(a_1a_2)m = (a_2a_1)m = a_2(a_1m)$$

wynika, że $M$ jest także prawostronnym $R-$modułem i na odwrót. Zatem nad pierścieniami przemiennymi nie ma potrzeby rozróżniania lewo- i prawostronnych modułów. Natomiast nad pierścieniami nieprzemiennymi dla modułów prawostronnych stosuje się na ogół inną symbolikę dla działania zewnętrznego. Zamiast pisać $am$ piszemy $ma$ dla rezultatu tego działania na elementach $a \in R$ oraz $m \in M$. Wtedy warunki określające moduł prawostronny wyglądają bardziej naturalnie:

$$\begin{aligned} (m_1 + m_2)a &= m_1a + m_2a, && (2.6)\\ m(a_1 + a_2) &= ma_1 + ma_2, && (2.7)\\ m(a_1a_2) &= (ma_1)a_2, && (2.8)\\ m1 &= m. && (2.9) \end{aligned}$$

W każdym razie nie ma potrzeby budowania dwóch odrębnych teorii dla modułów lewo- i prawostronnych. Jeśli bowiem mamy lewostronny (prawostronny) $R-$moduł $M$, to jest on identyczny z prawostronnym (lewostronnym) $R^0-$modułem $M$, gdzie $R^0$ jest pierścieniem *przeciwnym* do $R$ w tym sensie, że zbiory $R^0$ i $R$ są równe, działania dodawania w obydwu zbiorach są identyczne, elementy wyróżnione w obydwu zbiorach są identyczne, natomiast iloczyn dwóch elementów $a, b \in R^0$ jest określony jako iloczyn $ba$ w pierścieniu $R$.

W związku z tym będziemy w dalszym ciągu rozpatrywać najczęściej moduły lewostronne i będziemy je nazywać krótko modułami.

### 2.2.1 Przykłady modułów

Rozpoczniemy od wskazania niektórych podstawowych przykładów modułów.

**Przykład 2.2.1.** Przestrzeń wektorowa $V$ nad ciałem $K$ jest $K-$modułem.

**Przykład 2.2.2.** Grupa abelowa $M$ jest $\mathbb{Z}-$modułem.

**Przykład 2.2.3.** Ideał lewostronny $\mathcal{J}$ pierścienia $R$ jest lewostronnym $R-$modułem. Podobnie, każdy ideał prawostronny $\mathcal{I}$ pierścienia $R$ jest prawostronnym $R-$modułem. Jeśli ideał prawostronny $\mathcal{I}$ nie jest równocześnie ideałem lewostronnym, to $\mathcal{I}$ jest prawostronnym $R-$modułem (z mnożeniem przez skalary z $R$ określonym jako mnożenie w $R$) ale nie jest lewostronnym $R-$modułem (z mnożeniem przez skalary z $R$ określonym jako mnożenie w $R$).

**Przykład 2.2.4.** Pierścień $R$ jest $R-$modułem. Ogólniej, dla każdej liczby naturalnej $n$, zbiór $R^n$ wszystkich $n-$elementowych ciągów elementów z $R$ z działaniami

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n), \quad a \cdot (a_1, \ldots, a_n) = (aa_1, \ldots, aa_n)$$

jest $R-$modułem.

**Przykład 2.2.5.** Niech $R = K[X]$ będzie pierścieniem wielomianów jednej zmiennej nad ciałem $K$. Niech $M = V$ będzie przestrzenią wektorową nad ciałem $K$ i niech $\tau$ będzie endomorfizmem przestrzeni $V$. Na przestrzeni $V$ określamy działanie zewnętrzne następująco:

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

A więc $fv := f(\tau)(v)$. Zgodnie z definicją 2.2.1, przestrzeń wektorowa $V$ jest $K[X]-$modułem. Tak skonstruowany $K[X]-$moduł oznaczamy $V_\tau$.
Ten przykład stanowi podstawę zastosowań teorii modułów w badaniu postaci kanonicznych endomorfizmów przestrzeni wektorowych.

**Przykład 2.2.6.** Niech $M$ będzie $R-$modułem i niech $f : A \to R$ będzie homomorfizmem pierścieni. Wtedy określamy działanie zewnętrzne na $M$ z pierścieniem skalarów $A$ kładąc

$$am := f(a)m$$

dla każdego $a \in A$. Z łatwością stwierdza się, że z tak zdefiniowanym działaniem zewnętrznym $M$ staje się $A-$modułem. Mówimy, że ten $A-$moduł powstaje z $R-$modułu $M$ przez *zwężenie* lub *ograniczenie* pierścienia skalarów (z $R$ do $A$).

### 2.2.2 Podmoduły

DEFINICJA **2.2.2.** 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 2.2.7.** Każda podprzestrzeń wektorowa przestrzeni wektorowej $V$ nad ciałem $K$ jest podmodułem $K-$modułu $V$.
Każda podgrupa $N$ grupy abelowej $M$ jest podmodułem $\mathbb{Z}-$modułu $M$.
Każdy ideał lewostronny $\mathcal{J}$ pierścienia $R$ jest podmodułem $R-$modułu $R$.
Jeśli $\mathcal{J}$ jest ideałem lewostronnym pierścienia $R$ oraz $M$ jest $A-$modułem, to

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

jest podmodułem modułu $M$.
Dla endomorfizmu $\tau$ przestrzeni wektorowej $V$, każda podprzestrzeń $\tau-$niezmiennicza $U$ przestrzeni $V$ (to znaczy, podprzestrzeń spełniająca $\tau(U) \subseteq U$) jest podmodułem $K[X]-$modułu $V_\tau$. 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 $V_\tau$, 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 $V_\tau$ wtedy i tylko wtedy, gdy $U$ jest podprzestrzenią niezmienniczą endomorfizmu $\tau$.

DEFINICJA **2.2.3.** 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

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

**Przykład 2.2.8.** 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.
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 $R$.
Jeśli $V$ jest skończenie wymiarową przestrzenią wektorową nad ciałem $K$, to rozpatrywany w przykładzie 2.2.5 $K[X]-$moduł $V_\tau$ jest skończenie generowany.

### 2.2.3 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

$$N_1 + N_2 = \{n_1 + n_2 \in M : n_1 \in N_1,\ n_1 \in N_2\}$$

podgrup grupy abelowej $M$ jest podmodułem $R-$modułu $M$. Nazywamy ją *sumą podmodułów* $N_1$ i $N_2$.
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 $M = N_1 \oplus N_2$. Łatwo sprawdzamy, że $M$ 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 $n_1 \in N_1$, $n_2 \in N_2$. Rzeczywiście, $M = N_1 + N_2$ oznacza, że każdy element $m \in M$ ma przedstawienie w postaci $m = n_1 + n_2$, gdzie $n_1 \in N_1$, $n_2 \in N_2$, natomiast jednoznaczność przedstawienia jest równoważna warunkowi $N_1 \cap N_2 = 0$.

Będziemy także rozpatrywać sumy i sumy proste dowolnych rodzin podmodułów modułu $M$. Jeśli $\{N_i,\ i \in I\}$ jest dowolną rodziną podmodułów modułu $M$, to zbiór

$$\sum_{i \in I} N_i$$

wszystkich skończonych sum postaci

$$n_{i_1} + \cdots + n_{i_k} \quad \text{gdzie} \quad n_{i_j} \in N_{i_j}$$

jest podmodułem modułu $M$. Nazywamy go *sumą* rodziny podmodułów $\{N_i,\ i \in I\}$. Mówimy, że moduł $M$ jest *sumą prostą* rodziny swoich podmodułów $N_i$, $i \in I$, jeśli moduł $M$ jest sumą rodziny podmodułów $\{N_i,\ i \in I\}$ oraz każdy podmoduł $N_j$ jest rozłączny z sumą wszystkich pozostałych modułów tej rodziny:

$$N_j \cap \sum_{i \in I \setminus \{j\}} N_i = \{0\} \quad \text{dla każdego} \quad j \in I.$$

Piszemy wtedy

$$M = \bigoplus_{i \in I} N_i.$$

Podobnie jak w przypadku rodziny dwuelementowej sprawdzamy, że moduł $M$ jest sumą prostą rodziny podmodułów $\{N_i,\ i \in I\}$ wtedy i tylko wtedy gdy każdy element $m \in M$ ma *jednoznaczne* przedstawienie w postaci

$$m = n_{i_1} + \cdots + n_{i_k} \quad \text{gdzie} \quad n_{i_j} \in N_{i_j}.$$

Definicja **2.2.4.** Mówimy, że podmoduł $N_1$ modułu $M$ jest *składnikiem prostym* modułu $M$ jeśli istnieje podmoduł $N_2$ taki, że

$$M = N_1 \oplus N_2.$$

Podmoduł $N_2$ nazywa się podmodułem *dopełniającym* dla składnika prostego $N_1$.

W przestrzeni wektorowej $V$ każda podprzestrzeń jest składnikiem prostym przestrzeni $V$. Jest to sytuacja raczej wyjątkowa. Na przykład, w pierścieniu całkowitym $R$ traktowanym jako $R-$moduł jedynymi składnikami prostymi są podmoduły 0 i $R$.

Podmodułami w $R-$module $R$ są ideały pierścienia $R$ i każde dwa niezerowe ideały mają niezerową część wspólną. Rzeczywiście, jeśli $\mathcal{I}$ oraz $\mathcal{J}$ są ideałami (podmodułami) w $R$ oraz $a \in \mathcal{I}$, $b \in \mathcal{J}$, $a \neq 0$, $b \neq 0$, to $ab \neq 0$ (bo pierścień jest całkowity) oraz $ab \in \mathcal{I} \cap \mathcal{J}$.

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 $M'$. Zauważmy, że

$$N_1 = M \times \{0\}, \quad N_2 = \{0\} \times M'$$

są podmodułami modułu $M \times M'$ oraz

$$M \times M' = N_1 \oplus N_2.$$

A więc iloczyn prosty dwóch $R-$modułów można w naturalny sposób traktować jako sumę prostą podmodułów $N_1$ i $N_2$.
Podobnie określa się iloczyn prosty dowolnej rodziny $R-$modułów $M_i, i \in I$.

## 2.3 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).
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 $a \in R$ zawiera się w dokładnie jednej warstwie modułu $M$ względem podmodułu $N$:

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

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 $N$.

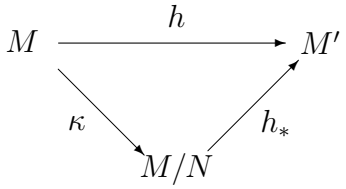
Niech $N$ będzie podmodułem $R-$modułu $M$ i niech

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

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

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

TWIERDZENIE **2.3.1.** (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 **2.3.2.** (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. □

### 2.3.1 Rozszczepialne ciągi dokładne

DEFINICJA **2.3.1.** Ciąg $R-$modułów i homomorfizmów

$$0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{2.10}$$

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

A więc dokładność ciągu (2.10) oznacza, że $\ker f = 0,\ \operatorname{im} f = \ker g,\ \operatorname{im} g = M''$. Zauważmy, że dla podmodułu $N$ modułu $M$ i homomorfizmu kanonicznego $\kappa : M \to M/N$ mamy zawsze ciąg dokładny

$$0 \to N \xrightarrow{f} M \xrightarrow{\kappa} M/N \to 0 \tag{2.11}$$

gdzie $f : N \to M$ jest identycznościowym włożeniem podmodułu $N$ w moduł $M$. Z drugiej strony, w ciągu dokładnym (2.10) mamy $M'' \cong M/\ker g = M/f(M')$, gdzie $f(M')$ jest podmodułem modułu $M$. A więc, z dokładnością do izomorfizmu modułów, każdy ciąg dokładny ma postać (2.11).

Zamiast pięcioczłonowych ciągów dokładnych można rozpatrywać ciągi dowolnej długości (nawet nieskończone). Mówimy, że ciąg modułów i homomorfizmów

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

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 2.3.1.** Jeśli $M = M' \oplus M''$ oraz $f : M' \to M$ jest włożeniem modułu $M'$ w moduł $M$ zaś $g : M \to M''$ jest rzutowaniem $M$ na składnik prosty $M''$, to mamy ciąg dokładny

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

Rzeczywiście, $\operatorname{im} f = M' = \ker g$. Ten ciąg dokładny ma jednak pewną ważną dodatkową własność, której ciągi dokładne na ogół nie mają. Jeśli $\varphi : M'' \to M$ oznacza włożenie składnika prostego $M''$ w moduł $M$ oraz $\psi : M \to M'$ oznacza rzutowanie $M$ na składnik prosty $M'$, to homomorfizmy $\varphi, \psi$ mają własność następującą:

$$g \circ \varphi = \mathbf{1}_{M''}, \quad \psi \circ f = \mathbf{1}_{M'}. \tag{2.12}$$

Rzeczywiście, $g \circ \varphi(m'') = g(\varphi(m'')) = g(m'') = m''$ dla każdego $m'' \in M''$, i podobnie, $\psi \circ f(m') = \psi(f(m')) = \psi(m') = m'$ dla każdego $m' \in M'$. Przystępujemy teraz do dowodu twierdzenia odwrotnego: jeśli istnieje ciąg dokładny (2.10) oraz dwa homomorfizmy $\varphi, \psi$ mające własności (2.12), to $M$ rozkłada się na sumę prostą podmodułów izomorficznych odpowiednio z $M'$ i $M''$.

Twierdzenie **2.3.3.** *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 $\varphi$ 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 **2.3.4.** *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 $\psi$ jest homomorfizmem $R-$modułów oraz

$$(\psi \circ f)(m') = \psi(f(m')) = m' = \mathbf{1}_{M'}(m')$$

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 2.3.3 i 2.3.4 otrzymujemy następujący rezultat.

TWIERDZENIE **2.3.5.** *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 **2.3.2.** (a) Mówimy, że ciąg dokładny

$$0 \ \to \ M' \ \xrightarrow{f} \ M \ \xrightarrow{g} \ M'' \ \to \ 0 \tag{2.13}$$

*rozszczepia się*, jeśli spełniony jest warunek (a) twierdzenia 2.3.5.
(b) Mówimy, że ciąg dokładny

$$M \ \xrightarrow{g} \ M'' \ \to \ 0 \tag{2.14}$$

*rozszczepia się*, gdy spełniony jest warunek (b) twierdzenia 2.3.5.
Homomorfizm $\varphi$ nazywamy wtedy homomorfizmem *rozszczepiającym* ciąg dokładny

(2.14).
(c) Mówimy, że ciąg dokładny

$$0 \to M' \xrightarrow{f} M \tag{2.15}$$

*rozszczepia się*, jeśli spełniony jest warunek (c) twierdzenia 2.3.5.
Homomorfizm $\psi$ nazywamy wtedy homomorfizmem *rozszczepiającym* ciąg dokładny (2.15).

Twierdzenie 2.3.5 mówi więc, że jeśli ciąg (2.13) jest dokładny, to jego rozszczepialność jest równoważna rozszczepialności każdego z ciągów (2.14), (2.15).
Homomorfizmy $\varphi$ i $\psi$ nazywają się homomorfizmami *rozszczepiającymi* ciąg dokładny (2.13).

WNIOSEK **2.3.1.** *Jeśli ciąg dokładny* (2.13) *rozszczepia się i* $\varphi, \psi$ *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 (2.13) wynika równość $\ker g = \operatorname{im} f$. Ponieważ $f$ jest monomorfizmem, mamy $\operatorname{im} f \cong M'$. Z warunku (b) wynika, że $\varphi$ 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 **2.3.2.** *Niech* $N$ *będzie podmodułem modułu* $M$ *i niech*

$$f : N \to M, \quad g : M \to M/N$$

*będą odpowiednio identycznościowym włożeniem 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 **2.3.3.** *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 2.3.1. $\square$

**Uwaga 2.3.1.** Dla przestrzeni wektorowych problem rozszczepialności ciągów dokładnych nie jest istotny, gdyż *każdy* ciąg dokładny przestrzeni wektorowych rozszczepia się. Jest to konsekwencja wniosku 2.3.3 oraz faktu, że każda podprzestrzeń przestrzeni wektorowej jest jej składnikiem prostym.

## 2.4 Moduły homomorfizmów

Niech $M$ i $N$ będą $R-$modułami. Zbiór wszystkich homomorfizmów $h : M \to N$ oznaczamy $\mathsf{Hom}(M,N)$ lub $\mathsf{Hom}_R(M,N)$. W zbiorze $\mathsf{Hom}(M,N)$ wprowadzamy działanie *dodawania* homomorfizmów określając dla homomorfizmów $g,h \in \mathsf{Hom}(M,N)$ ich sumę $g+h$ jako odwzorowanie

$$g+h : M \to N, \quad (g+h)(m) = g(m)+h(m)$$

dla wszystkich $m \in M$. Z łatwością sprawdzamy, że wtedy także $g+h \in \mathsf{Hom}(M,N)$. Ponieważ dla homomorfizmu zerowego $\theta : M \to N$, gdzie $\theta(m) = 0$ dla wszystkich $m \in M$, mamy $h+\theta = \theta+h = h$ dla wszystkich $h \in \mathsf{Hom}(M,N)$, łatwo sprawdzamy, że $(\mathsf{Hom}(M,N),+,\theta)$ jest grupą abelową (czyli $\mathbb{Z}-$modułem). Wydaje się także rzeczą naturalną określić iloczyn homomorfizmu $h \in \mathsf{Hom}(M,N)$ przez skalar $a \in R$ przy pomocy formuły

$$ah : M \to N, \quad (ah)(m) = ah(m)$$

dla wszystkich $m \in M$. Wprawdzie w ten sposób otrzymujemy zawsze funkcję $ah$ określoną na $M$ o wartościach w $N$, ale funkcja ta *nie jest* na ogół homomorfizmem $R-$modułów! Rzeczywiście, dla $x \in R$ oraz $m \in M$ mamy

$$(ah)(xm) = ah(xm) = axh(m), \quad x(ah)(m) = x(ah(m)) = xah(m).$$

A więc funkcja $ah$ spełnia warunek jednorodności tylko wtedy gdy $(ax-xa)h(m) = 0$ dla wszystkich $x \in R$. Ten warunek jest zawsze spełniony, gdy pierścień $R$ jest przemienny, ale na ogół nie jest spełniony, gdy pierścień $R$ jest nieprzemienny.

Jeśli $R$ jest pierścieniem przemiennym, to $\mathsf{Hom}_R(M,N)$ z operacjami dodawania homomorfizmów i mnożenia homomorfizmów przez skalary z $R$ jest $R-$modułem (łatwe sprawdzenie aksjomatów modułu pozostawiamy jako ćwiczenie). Natomiast jeśli $R$ jest dowolnym pierścieniem, będziemy $\mathsf{Hom}_R(M,N)$ traktować jako $\mathbb{Z}-$moduł, czyli jako addytywną grupę abelową. Jeśli moduł $M$ rozkłada się na sumę prostą podmodułów (iloczyn prosty modułów), to opis struktury $\mathsf{Hom}_R(M,N)$ sprowadza się do opisu odpowiednich grup homomorfizmów pomiędzy składnikami tego rozkładu i modułem $N$.

TWIERDZENIE **2.4.1.** *Niech $M, N_1, N_2$ będą $R-$modułami. Wtedy mamy następujące izomorfizmy grup abelowych:*

$$\mathsf{Hom}_R(N_1 \times N_2, M) \cong \mathsf{Hom}_R(N_1, M) \times \mathsf{Hom}_R(N_2, M).$$

$$\mathsf{Hom}_R(M, N_1 \times N_2) \cong \mathsf{Hom}_R(M, N_1) \times \mathsf{Hom}_R(M, N_2).$$

*Jeśli $R$ jest pierścieniem przemiennym, to są to izomorfizmy $R-$modułów.*

*Dowód.* Niech $\mathrm{inj}_i : N_i \to N_1 \times N_2$ będzie kanonicznym włożeniem modułu $N_i$ w moduł $N_1 \times N_2$. A więc $\mathrm{inj}_1(n_1) = (n_1, 0)$, $\mathrm{inj}_2(n_2) = (0, n_2)$ dla $n_1 \in N_1, n_2 \in N_2$. Określamy odwzorowanie

$$\varphi : \mathsf{Hom}_R(N_1 \times N_2, M) \to \mathsf{Hom}_R(N_1, M) \times \mathsf{Hom}_R(N_2, M), \quad f \mapsto (f \circ \mathrm{inj}_1, f \circ \mathrm{inj}_2).$$

Łatwo sprawdzamy, że $\varphi$ jest homomorfizmem grup abelowych. Dla dowodu, że $\varphi$ jest monomorfizmem załóżmy, że $f \in \ker \varphi$. Wtedy dla każdego elementu $(n_1, n_2) \in N_1 \times N_2$ mamy $0 = \varphi(f) = (f \circ \mathrm{inj}_1, f \circ \mathrm{inj}_2)$, to znaczy

$$f \circ \mathrm{inj}_1(n_1) = 0, \quad f \circ \mathrm{inj}_2(n_2) = 0$$

dla wszystkich $n_1 \in N_1, n_2 \in N_2$. Wtedy

$$f(n_1, n_2) = f(n_1, 0) + f(0, n_2) = f \circ \mathrm{inj}_1(n_1) + f \circ \mathrm{inj}_2(n_2) = 0$$

dla wszystkich $n_1 \in N_1, n_2 \in N_2$. Zatem $f = 0$ i wobec tego $\varphi$ jest monomorfizmem. Dla dowodu, że $\varphi$ jest epimorfizmem weźmy $(g_1, g_2) \in \mathsf{Hom}_R(N_1, M) \times \mathsf{Hom}_R(N_2, M)$. Definiujemy $R-$homomorfizm $f \in \mathsf{Hom}_R(N_1 \times N_2, M)$ kładąc

$$f(n_1, n_2) = g_1(n_1) + g_2(n_2)$$

dla wszystkich $n_1 \in N_1, n_2 \in N_2$. Wtedy $f(n_1, 0) = g_1(n_1)$ oraz $f(0, n_2) = g_2(n_2)$, zatem $f \circ \mathrm{inj}_1 = g_1$ oraz $f \circ \mathrm{inj}_2 = g_2$. Wobec tego

$$(g_1, g_2) = (f \circ \mathrm{inj}_1, f \circ \mathrm{inj}_2) = \varphi(f)$$

co oznacza surjektywność homomorfizmu $\varphi$.

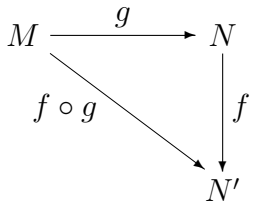
Dowód drugiej części twierdzenia jest podobny. Niech $\mathrm{pr}_i : N_1 \times N_2 \to N_i$ będzie kanonicznym rzutowaniem modułu $N_1 \times N_2$ na moduł $N_i$. Wtedy określamy odwzorowanie

$$\varphi : \mathsf{Hom}_R(M, N_1 \times N_2) \to \mathsf{Hom}_R(M, N_1) \times \mathsf{Hom}_R(M, N_2), \quad f \mapsto (\mathrm{pr}_1 \circ f, \mathrm{pr}_2 \circ f).$$

Łatwo sprawdzamy, że $\varphi$ jest homomorfizmem grup abelowych i używając podobnych argumentów jak w pierwszej części dowodu pokazujemy, że $\varphi$ jest izomorfizmem. Łatwo też sprawdzić, że w obydwu przypadkach $\varphi$ jest izomorfizmem $R-$modułów, jeśli tylko $R$ jest pierścieniem przemiennym. □

## 2.5 Projektywność przestrzeni wektorowych

Jeśli $f : N \to N'$ jest homomorfizmem $R-$modułów, to dla każdego homomorfizmu $g : M \to N$ otrzymujemy homomorfizm $R-$modułów $f \circ g : M \to N'$.




W ten sposób definiuje się *homomorfizm indukowany* grup abelowych

$$f_* : \mathsf{Hom}(M, N) \to \mathsf{Hom}(M, N'), \quad f_*(g) = f \circ g.$$

Jeśli $R$ jest pierścieniem przemiennym, to homomorfizm indukowany $f_*$ jest homomorfizmem $R-$modułów.

Jest rzeczą naturalną oczekiwać, że własności homomorfizmów $f_*$ i $f$ ściśle od siebie zależą. Na przykład, jeśli $f_*$ jest surjektywny, to $f$ też, na ogół, jest surjektywny. Jest tak w przypadku, gdy $M, N, N'$ są przestrzeniami wektorowymi. Jeśli bowiem $n' \in N'$ nie należy do obrazu homomorfizmu $f$, to $n'$ nie należy do obrazu żadnego homomorfizmu $f_*(g) : M \to N'$ dla $g \in \mathsf{Hom}(M, N)$. Wobec tego $f_*$ nie może być surjektywny, gdyż zawsze znajdziemy homomorfizm $h : M \to N'$, który w obrazie ma wektor $n'$ i wobec tego nie należy do obrazu $f_*$.

Dla ustalonego modułu $M$ będziemy badać czy surjektywność homomorfizmu $f$ pociąga surjektywność homomorfizmu indukowanego $f_*$. Okazuje się, że na ogół tak nie jest ale jeśli moduł $M$ jest dostatecznie regularny (na przykład, jeśli jest przestrzenią wektorową), to surjektywność $f$ pociąga surjektywność $f_*$. Ta własność prowadzi do kluczowego pojęcia modułu *projektywnego*.

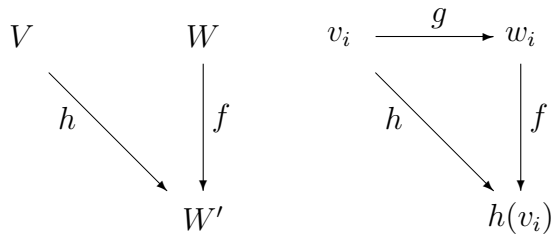
DEFINICJA **2.5.1.** $R-$moduł $M$ nazywa się *projektywny*, jeśli dla każdego surjektywnego homomorfizmu $R-$modułów $f : N \to N'$ indukowany homomorfizm $f_* : \mathsf{Hom}(M, N) \to \mathsf{Hom}(M, N')$ grup abelowych jest także surjektywny.

STWIERDZENIE **2.5.1.** *Niech $V, W, W'$ będą przestrzeniami wektorowymi nad ciałem $K$. Dla każdego epimorfizmu $f : W \to W'$ przestrzeni wektorowych homomorfizm indukowany*

$$f_* : \mathsf{Hom}_K(V, W) \to \mathsf{Hom}_K(V, W')$$

*jest także epimorfizmem przestrzeni wektorowych. Inaczej mówiąc, każda przestrzeń wektorowa jest modułem projektywnym.*

*Dowód.* Niech $h \in \mathsf{Hom}(V, W')$ i niech $\{v_i\}$ będzie bazą przestrzeni $V$. Ponieważ $f$ jest epimorfizmem, więc istnieją $w_i \in W$ takie, że $f(w_i) = h(v_i)$ dla każdego $i$.




Obieramy teraz homomorfizm $g \in \mathsf{Hom}(V, W)$ taki, że $g(v_i) = w_i$ dla każdego $i$. Wtedy $h = f \circ g = f_*(g)$. A więc $f_*$ jest epimorfizmem. □

# Rozdział 3

# Moduły wolne

Ostatnie zmiany 8.11.2007 r.

## 3.1 Moduły wolne

Moduły wolne stanowią uogólnienie przestrzeni wektorowych i grup abelowych wolnych. Charakterystyczną cechą modułów wolnych jest istnienie bazy, to znaczy podzbioru liniowo niezależnego generującego moduł. W definicji $R-$modułu wolnego pierścień $R$ jest dowolnym pierścieniem, niekoniecznie przemiennym.

Definicja **3.1.1.** $R-$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

$$x_1 b_1 + \cdots + x_n b_n = 0 \quad \Rightarrow \quad x_1 = \cdots = x_n = 0.$$

(b) Każdy element $m \in F$ ma przedstawienie w postaci

$$m = x_1 b_1 + \cdots + x_n b_n, \quad b_1, \ldots, b_n \in \mathcal{B}, \; x_1, \ldots, x_n \in R. \tag{3.1}$$

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 przypadku przestrzeni wektorowych 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 (3.1).

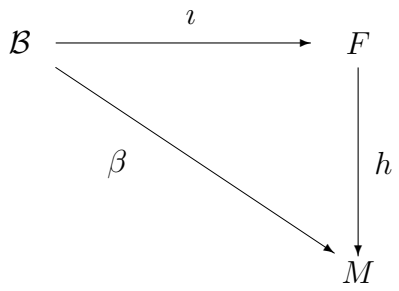
**Przykład 3.1.1.** $R-$moduł $R$ jest przykładem $R-$modułu wolnego. Rzeczywiście, zbiór jednoelementowy $\mathcal{B} = \{1\}$ jest bazą $R-$modułu $R$. Również $R-$moduł $R^n$, dla dowolnej liczby naturalnej $n$, jest $R-$modułem wolnym. Bazę tego modułu tworzą, na przykład, elementy $e_1, \ldots, e_n$, gdzie $e_i$ ma wszystkie współrzędne równe 0 z wyjątkiem $i-$tej, która jest równa 1. Tę bazę modułu $R^n$ nazywa się bazą *standardową*.
Ogólniej, suma prosta (koprodukt) 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 $j \neq i$. Przypomnijmy, że koprodukt $F$ jest podmodułem produktu kartezjańskiego $R^I = \prod_{i \in I} R$ i składa się z tych elementów produktu, które mają skończone nośniki. Produkt $R^I$ składa się z wszystkich funkcji $f : I \to R$. Nośnikiem funkcji $f$ nazywa się zbiór tych elementów w $I$, na których $f$ przyjmuje wartości $\neq 0$.
Wynika stąd, że dla każdej liczby kardynalnej $\alpha$ istnieje $R-$moduł wolny $F$ z bazą mocy $\alpha$.

**Przykład 3.1.2.** $\mathbb{Z}-$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 **3.1.1.** *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 $\imath : \mathcal{B} \to F$ oznaczymy włożenie $\imath(b) = b$, to występujące w twierdzeniu odwzorowania tworzą diagram przemienny




Twierdzenie mówi w szczególności, że jeśli na bazie $\mathcal{B}$ modułu wolnego $F$ określone jest jakiekolwiek odwzorowanie w dowolny moduł $M$, to odwzorowanie to można jednoznacznie przedłużyć do homomorfizmu modułu $F$ w moduł $M$.

*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 $\beta$ 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 $\beta$ 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 $\beta$ 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 $\beta$ 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 $\beta$ 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

$$\beta_1 : \mathcal{B} \to F/F_1, \quad \beta_1(b) = b + F_1 = 0 \in F/F_1$$

dla wszystkich $b \in \mathcal{B}$. 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 $\beta_1$ 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 **3.1.2.** *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 $|I|$. Niech $\mathcal{B} = \{b_i : i \in I\}$ będzie bazą modułu $F$. Na podstawie twierdzenia 3.1.1 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 **3.1.3.** *Niech $R$ będzie pierścieniem przemiennym. Moc bazy wolnego $R-$modułu $F$ jest jednoznacznie wyznaczona przez moduł $F$. Każde dwie bazy modułu wolnego $F$ są równoliczne.*

*Dowód.* Na podstawie kursowego twierdzenia pierścień przemienny $R$ ma co najmniej jeden ideał maksymalny $\mathfrak{m}$. Zatem pierścień ilorazowy $R/\mathfrak{m}$ 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 2.2.7). Rozpatrujemy teraz $R-$moduł ilorazowy $F/\mathfrak{m}F$ i zauważamy, że ma on także strukturę modułu nad ciałem $R/\mathfrak{m}$. Rzeczywiście, mnożenie warstw $f + \mathfrak{m}F$ przez skalary $a + \mathfrak{m}$ ciała $R/\mathfrak{m}$ 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 $R-$modułu wolnego $F$ skonstruowaliśmy przestrzeń wektorową $F/\mathfrak{m}F$ nad ciałem $R/\mathfrak{m}$. Jeśli teraz $\mathcal{B}$ jest bazą modułu wolnego $F$ to zbiór

$$\mathcal{B} + \mathfrak{m}F := \{b + \mathfrak{m}F : b \in \mathcal{B}\}$$

jest bazą przestrzeni wektorowej $F/\mathfrak{m}F$ nad ciałem $R/\mathfrak{m}$. Rzeczywiście, jeśli

$$\sum(x_i + \mathfrak{m})(b_i + \mathfrak{m}F) = \mathfrak{m}F \tag{3.2}$$

dla pewnych $x_i \in R$, $b_i \in B$, to $\sum x_i b_i \in \mathfrak{m}F$. Stąd wynika, że istnieją $y_i \in \mathfrak{m}$ takie, że

$$\sum x_i b_i = \sum y_i b_i.$$

Zatem $x_i = y_i \in \mathfrak{m}$ i wobec tego wszystkie współczynniki kombinacji liniowej (3.2) są równe zero w ciele $R/\mathfrak{m}$. 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 $x_i \in R$, $b_i \in \mathcal{B}$ 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 $R/\mathfrak{m}$. Każda baza modułu wolnego $F$ jest więc 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 3.1.3 (znane jako *invariant basis property*, w skrócie IBP) brzmi następująco.

Wniosek **3.1.1.** *Dla każdego pierścienia przemiennego $R$ i dla każdych liczb naturalnych $n, m$, jeśli $R-$moduły $R^n$ i $R^m$ są izomorficzne, to $n = m$.*

**Uwaga 3.1.1.** Własności IBP nie mają już na ogół $R-$moduły wolne nad pierścieniami nieprzemiennymi. Można pokazać, że pierścienie endomorfizmów skończenie wymiarowych przestrzeni wektorowych (a więc także pierścienie macierzy $M_n(K)$ nad dowolnym ciałem $K$) mają własność IBP, natomiast pierścienie endomorfizmów przestrzeni nieskończenie wymiarowych nie mają własności IBP.

Twierdzenie 3.1.3 pozwala wprowadzić dla modułów wolnych nad pierścieniami przemiennymi odpowiednik pojęcia wymiaru przestrzeni wektorowej.

Definicja **3.1.2.** Niech $F$ będzie modułem wolnym nad pierścieniem przemiennym. Moc dowolnej bazy modułu $F$ nazywamy *rangą* modułu $F$ i oznaczamy $\mathsf{rank}\, F$.

Stwierdzenie **3.1.1.** *Niech $F$ będzie modułem nad pierścieniem przemiennym $R$. $F$ jest $R-$modułem wolnym rangi $n$ wtedy i tylko wtedy gdy $F \cong R^n$.*

*Dowód.* Niech $F$ będzie $R-$modułem wolnym z bazą $\mathcal{B} = \{b_1, \ldots, b_n\}$ i niech $\mathcal{E} = \{e_1, \ldots, e_n\}$ będzie bazą standardową modułu $R^n$. Odwzorowanie $\beta : \mathcal{B} \to \mathcal{E}$, $\beta(b_i) = e_i$ ma na podstawie twierdzenia 3.1.1 dokładnie jedno przedłużenie do homomorfizmu $h : F \to R^n$. Jest jasne, że homomorfizm $h$ jest surjektywny. Jeśli $\sum x_i b_i \in \ker h$, to $\sum x_i e_i = 0$, skąd wynika, że $x_1 = \cdots = x_n = 0$. A więc $\ker h = 0$, skąd wynika, że $h$ jest izomorfizmem $R-$modułów.
Z drugiej strony, jeśli $g : R^n \to F$ jest izomorfizmem $R-$modułów, to łatwo sprawdzić, że $g(\mathcal{E})$ jest bazą modułu $F$ i wobec tego $F$ jest wolnym $R-$modułem. □

## 3.2 Projektywność modułów wolnych

W rozdziale 1 wprowadziliśmy pojęcie modułu projektywnego (definicja 2.5.1) i pokazaliśmy, że każda przestrzeń wektorowa jest modułem projektywnym (twierdzenie 2.5.1). Teraz sformułujemy ogólniejsze twierdzenie mówiące, że także moduły wolne są projektywne.

TWIERDZENIE **3.2.1.** *Niech $F$ będzie wolnym $R-$modułem i niech $W$, $W'$ będą $R-$modułami. Dla każdego surjektywnego homomorfizmu modułów $f : W \to W'$ homomorfizm indukowany*

$$f_* : \mathsf{Hom}_R(F, W) \to \mathsf{Hom}_R(F, W')$$

*jest także surjektywnym homomorfizmem grup abelowych. Inaczej mówiąc, każdy moduł wolny jest modułem projektywnym.*

*Dowód.* Argumentacja użyta w dowodzie twierdzenia 2.5.1 stosuje się bez żadnych zmian także tutaj. Wykorzystujemy bowiem tylko istnienie bazy modułu $F$ oraz możliwość określania homomorfizmów na $F$ poprzez zadanie wartości homomorfizmu na elementach bazy modułu $F$ (twierdzenie 3.1.1). □

Sformułujemy jeszcze dwa twierdzenie o modułach wolnych i ich homomorfizmach. Na podstawie twierdzenia 3.1.2 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 **3.2.2.** *Jeśli $F$ jest $R-$modułem wolnym, to każdy ciąg dokładny $R-$modułów i homomorfizmów*

$$0 \;\to\; M' \;\xrightarrow{f}\; M \;\xrightarrow{g}\; F \;\to\; 0$$

*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 $g \circ \varphi = \mathbf{1}_F$. □

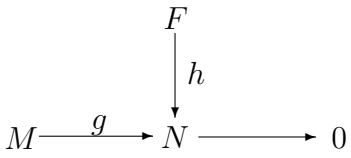
WNIOSEK **3.2.1.** *Jeśli moduł wolny $F$ jest homomorficznym obrazem modułu $M$, to $F$ jest składnikiem prostym modułu $M$.*

*Dowód.* Na podstawie założenia istnieje rozszczepialny ciąg dokładny $M \to F \to 0$ i wobec tego z wniosku 2.3.3 wynika, że $F$ jest składnikiem prostym modułu $M$. □

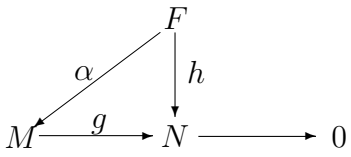
Udowodnimy w końcu jeszcze jedną własność modułów wolnych, która będzie grała ważną rolę w opisie modułów projektywnych.

TWIERDZENIE **3.2.3.** *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




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 $\alpha$ wpisuje się w diagram




który wobec $g \circ \alpha = h$ jest diagramem przemiennym. □

Twierdzenia 3.2.1, 3.2.2 i 3.2.3 przedstawiają trzy fundamentalne własności modułów wolnych wyrażone poprzez własności homomorfizmów modułów. Ale w odróżnieniu od twierdzenia 3.1.1, nie są to własności charakteryzujące moduły wolne. W następnym rozdziale pokażemy, że są to własności charakteryzujące moduły *projektywne*.

# Rozdział 4

# Moduły projektywne

Ostatnie zmiany 07.12.2004 r.

## 4.1 Charakteryzacja modułów projektywnych

Moduły projektywne zdefiniowaliśmy w rozdziale 1 jako moduły o własności (HI) sformułowanej poniżej (zobacz także definicję 2.5.1). Pokażemy teraz, że własność (HI) homomorfizmów indukowanych jest równoważna trzem innym własnościom, które będziemy nazywać odpowiednio własnościami podnoszenia homomorfizmów (PH), rozszczepialności ciągów dokładnych (CD) oraz bycia składnikiem prostym modułu wolnego (SP). Każda z tych czterech własności charakteryzuje więc w pełni moduły projektywne i może być przyjęta jako własność definiująca moduły projektywne. W dalszym ciągu przedstawimy jeszcze inne charakteryzacje modułów projektywnych.

Twierdzenie **4.1.1.** *Dla $R-$modułu $P$ następujące własności są równoważne.*

**(HI)** *Dla każdego epimorfizmu $f : M \to N$ homomorfizm indukowany*

$$f_* : \mathsf{Hom}(P, M) \to \mathsf{Hom}(P, N), \quad f_*(g) = f \circ g$$

*jest także epimorfizmem.*

**(PH)** *Dla każdego homomorfizmu modułów $h : P \to N$ i dla każdego epimorfizmu $f : M \to N$ istnieje homomorfizm $g : P \to M$ taki, że $h = f \circ g$.*

**(CD)** *Każdy ciąg dokładny $R-$modułów i homomorfizmów*

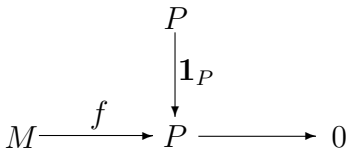
$$0 \to M' \xrightarrow{g} M \xrightarrow{f} P \to 0$$

*rozszczepia się.*

**(SP)** *Moduł $P$ jest składnikiem prostym pewnego modułu wolnego.*

*Dowód.* (HI) $\iff$ (PH). Jeśli zachodzi (HI), to każdy homomorfizm $h : P \to N$ leży w obrazie homomorfizmu indukowanego $f_*$, to znaczy, istnieje homomorfizm $g : P \to M$ taki, że $h = f_*(g) = f \circ g$. Zatem spełniony jest warunek (PH). Z drugiej strony, jeśli spełniony jest warunek (PH), to każdy homomorfizm $h : P \to N$ jest postaci $h = f \circ g = f_*(g)$. Zatem homomorfizm indukowany $f_*$ jest epimorfizmem i spełniony jest warunek (HI).

(PH) $\Rightarrow$ (CD). Jeśli $M \xrightarrow{f} P \to 0$ jest ciągiem dokładnym, to na podstawie warunku (PH) diagram



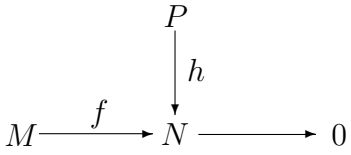

można uzupełnić do diagramu przemiennego homomorfizmem $g : P \to M$ takim, że $f \circ g = \mathbf{1}_P$. Zatem ciąg dokładny występujący w warunku (CD) rozszczepia się.

(CD) $\Rightarrow$ (SP). Wiemy, że moduł $P$ jest homomorficznym obrazem pewnego modułu wolnego $F$, a więc istnieje ciąg dokładny

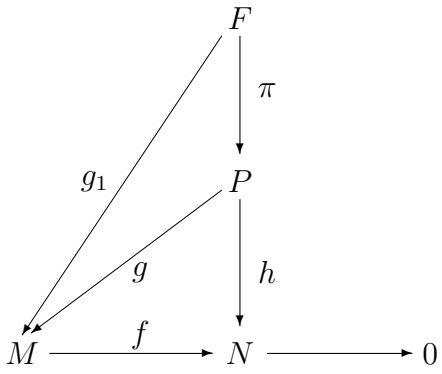
$$0 \ \to \ M' \ \to \ F \ \to \ P \ \to \ 0.$$

Ponieważ na podstawie (CD) ciąg ten rozszczepia się, moduł $P$ jest składnikiem prostym modułu $F$ (na podstawie wniosku 2.3.3).

(SP) $\Rightarrow$ (PH). Przypuśćmy, że $F = P \oplus Q$, gdzie $F$ jest modułem wolnym i rozpatrzmy diagram




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 3.2.3 moduł wolny $F$ ma własność (PH), zatem istnieje homomorfizm $g_1 : F \to M$ taki, że $f \circ g_1 = h \circ \pi$.




Wtedy zacieśnienie $g$ homomorfizmu $g_1$ do modułu $P$ spełnia $f \circ g = h$, bowiem dla $p \in P$ mamy

$$(f \circ g)(p) = f(g(p)) = f(g_1(p)) = h(\pi(p)) = h(p).$$

A więc spełniony jest warunek (PH). □

**Uwaga 4.1.1.** Własność homomorfizmu indukowanego (HI) można także sformułować w równoważnej postaci, która na pierwszy rzut oka wydaje się silniejsza niż (HI). Jest to następująca własność modułu $P$:

**(HI′)** Jeśli $0 \to M' \xrightarrow{g} M \xrightarrow{f} N \to 0$ jest dowolnym ciągiem dokładnym modułów i ich homomorfizmów, to także

$$0 \to \mathsf{Hom}(P, M') \xrightarrow{g_*} \mathsf{Hom}(P, M) \xrightarrow{f_*} \mathsf{Hom}(P, N) \to 0$$

jest ciągiem dokładnym.

Dowód równoważności (HI) $\iff$ (HI′) opiera się na obserwacji, że dla *każdego* modułu $P$, jeśli ciąg $0 \to M' \xrightarrow{g} M \xrightarrow{f} N$ jest dokładny, to także ciąg $0 \to \mathsf{Hom}(P, M') \xrightarrow{g_*} \mathsf{Hom}(P, M) \xrightarrow{f_*} \mathsf{Hom}(P, N)$ jest dokładny (zob. zadanie 32). Wobec tego (HI′) stawia modułowi $P$ jedynie wymaganie by surjektywność homomorfizmu $f$ pociągała surjektywność homomorfizmu indukowanego $f_*$, a to jest warunek (HI).

Wniosek **4.1.1.** *Każdy moduł jest homomorficznym obrazem pewnego modułu projektywnego.*

*Dowód.* Na podstawie twierdzenia 3.1.2 każdy moduł jest homomorficznym obrazem pewnego modułu wolnego, natomiast każdy moduł wolny jest projektywny na podstawie twierdzenia 3.2.1. □

Wniosek **4.1.2.** *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 **4.1.3.** *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 $F$. □

Jak dotąd, wiemy tylko, że każda przestrzeń wektorowa i ogólniej, każdy moduł wolny jest modułem projektywnym (zob. twierdzenia 2.5.1, 3.2.1). Okazuje się jednak, że klasa modułów projektywnych jest istotnie szersza niż klasa modułów wolnych. Pokażemy dwa przykłady modułów projektywnych, które nie są modułami wolnymi.

**Przykład 4.1.1.** 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.

**Przykład 4.1.2.** Niech $m > 1, n > 1$ będą liczbami naturalnymi i niech $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ oraz $\mathbb{Z}_{mn} = \mathbb{Z}/mn\mathbb{Z}$ będą pierścieniami reszt modulo $m$ i $mn$. Zauważmy, że odwzorowanie

$$f : \mathbb{Z}_{mn} \to \mathbb{Z}_m, \quad f(a + mn\mathbb{Z}) = a + m\mathbb{Z}$$

jest homomorfizmem pierścieni. Przede wszystkim odwzorowanie $h$ jest dobrze określone na warstwach gdyż

$$a + mn\mathbb{Z} = b + mn\mathbb{Z} \Rightarrow mn \mid a - b \Rightarrow m \mid a - b \Rightarrow a + m\mathbb{Z} = b + m\mathbb{Z}.$$

Łatwo teraz sprawdzamy, że $f$ jest homomorfizmem pierścieni. Jak zauważyliśmy w przykładzie 1.2.6, wynika stąd, że każdy $\mathbb{Z}_m$ moduł staje się $\mathbb{Z}_{mn}$ modułem, w szczególności wolny $\mathbb{Z}_m-$moduł $\mathbb{Z}_m$ staje się $\mathbb{Z}_{mn}-$modułem, jeśli działanie zewnętrzne na $\mathbb{Z}_m$ określimy następująco:

$$(a + mn\mathbb{Z})(b + m\mathbb{Z}) = f(a + mn\mathbb{Z})(b + m\mathbb{Z}) = (a + m\mathbb{Z})(b + m\mathbb{Z}) = ab + m\mathbb{Z}.$$

Stwierdzamy teraz, że $\mathbb{Z}_{mn}-$moduł $\mathbb{Z}_m$ nie jest modułem wolnym. Rzeczywiście, ponieważ $n > 1$ mamy $mn \nmid m$ i wobec tego $m + mn\mathbb{Z} \neq mn\mathbb{Z}$ oraz dla każdego elementu $a + m\mathbb{Z}$ modułu $\mathbb{Z}_m$ mamy

$$(m + mn\mathbb{Z})(a + m\mathbb{Z}) = ma + m\mathbb{Z} = m\mathbb{Z}.$$

Oznacza to, że każdy jednoelementowy podzbiór $\mathbb{Z}_{mn}-$modułu $\mathbb{Z}_m$ jest liniowo zależny i wobec tego ten moduł nie ma bazy. Tak więc $\mathbb{Z}_{mn}-$moduł $\mathbb{Z}_m$ nie jest wolny, ale okazuje się, że przy dodatkowym założeniu $\mathrm{nwd}(m, n) = 1$ jest on modułem projektywnym. Wynika to ze znanego w elementarnej teorii liczb faktu, iż pierścień reszt $\mathbb{Z}_{mn}$ jest izomorficzny z iloczynem kartezjańskim pierścieni $\mathbb{Z}_m$ i $\mathbb{Z}_n$ (o ile $\mathrm{nwd}(m, n) = 1$). Izomorfizm ten jest określony następująco:

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n, \quad a + mn\mathbb{Z} \mapsto (a + m\mathbb{Z}, a + n\mathbb{Z}).$$

Z przykładu 4.1.1 wynika, że $Re_1 = \mathbb{Z}_{mn}(1, 0) \cong \mathbb{Z}_m$ jest $\mathbb{Z}_{mn}-$ modułem projektywnym. Zatem izomorficzny z $Re_1$ moduł $\mathbb{Z}_m$ także jest projektywny.

## 4.2 Moduły projektywne nad pierścieniami lokalnymi

Przykład 4.1.1 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 $R$ nazywa się lokalnym, jeśli ma dokładnie jeden ideał maksymalny. Rozpoczniemy od pewnego uściślenia własności **(SP)** charakteryzującej moduły projektywne w przypadku modułów skończenie generowanych nad dowolnymi pierścieniami.

LEMAT **4.2.1.** *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

$$P \subset \sum_{i\in J} Re_i =: F_0.$$

Mamy więc $F := P \oplus N$ oraz $P \subset F_0$, zatem na podstawie prawa modularności (zadanie **14**) mamy

$$F_0 = F_0 \cap F = F_0 \cap (P + N) = P + (F_0 \cap N).$$

Ponieważ $P \cap N = 0$ więc tym bardziej $P \cap (F_0 \cap N) = 0$ i wobec tego $F_0 = P \oplus (N \cap F_0)$. 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 **4.2.1.** *Skończenie generowany $R-$moduł $P$ jest projektywny wtedy i tylko wtedy gdy istnieje $R-$moduł $Q$ i liczba naturalna $n$ takie, że*

$$P \oplus Q \cong R^n.$$

Niech teraz $R$ będzie pierścieniem lokalnym i $\mathfrak{m}$ niech będzie jedynym ideałem maksymalnym pierścienia $R$. Wtedy wszystkie elementy pierścienia $R$ nie należące do $\mathfrak{m}$ są odwracalne. Pierścień ilorazowy $R/\mathfrak{m} =: K$ jest ciałem, nazywanym ciałem reszt pierścienia lokalnego $R$. Warstwę $a + \mathfrak{m} \in R/\mathfrak{m}$ będziemy oznaczać $\bar{a}$. Zatem $^{-}: R \to K$ jest homomorfizmem kanonicznym.

W dowodzie poniższego twierdzenia istotną rolę gra możliwość przejścia od modułu wolnego nad pierścieniem lokalnym $R$ o randze $n$ do przestrzeni wektorowej nad ciałem reszt $K$ o wymiarze $n$ poprzez zastosowanie homomorfizmu kanonicznego do współrzędnych kombinacji liniowych elementów bazowych modułu wolnego. Objaśnimy więc najpierw tę konstrukcję.

Niech $R$ i $K$ będą pierścieniami i niech $f : R \to K$ będzie surjektywnym homomorfizmem pierścieni (na przykład, $R$ jest pierścieniem lokalnym, $K$ jego ciałem reszt i $f$ homomorfizmem kanonicznym). Jeśli $F$ jest $R-$modułem wolnym z bazą $\{e_1, \ldots, e_n\}$ oraz $\bar{F}$ jest $K-$modułem wolnym z bazą $\{\bar{e}_1, \ldots, \bar{e}_n\}$ to definiujemy odwzorowanie

$$\bar{f} : F \to \bar{F}, \quad \bar{f}(\sum x_i e_i) = \sum f(x_i)\bar{e}_i.$$

Z łatwością sprawdzamy, że $\bar{f}$ jest surjektywnym homomorfizmem addytywnych grup abelowych, ale oczywiście nie jest homomorfizmem modułów (gdyż $F$ i $\bar{F}$ są modułami nad różnymi pierścieniami). Ponadto, $\bar{f}$ jest bijekcją wtedy i tylko wtedy gdy $f$ jest bijekcją. Dalej, jeśli $P$ jest podmodułem modułu $F$, to addytywna grupa $\bar{f}(P)$ jest faktycznie podmodułem modułu $\bar{F}$.

Twierdzenie **4.2.1.** *Jeśli $R$ jest pierścieniem lokalnym, to każdy skończenie generowany projektywny $R-$moduł jest modułem wolnym.*

*Dowód.* Niech $P$ będzie skończenie generowanym $R-$modułem projektywnym. Na podstawie lematu 4.2.1 istnieje skończenie generowany $R-$moduł projektywny $Q$, taki że

$$F := P \oplus Q \cong R^n.$$

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 $\bar{F} \cong K^n$ nad ciałem reszt $K$ pierścienia lokalnego $R$. W tej przestrzeni $\bar{P}$ i $\bar{Q}$ są podprzestrzeniami wektorowymi i z pewnością mamy

$$\bar{F} = \bar{P} + \bar{Q}.$$

Nie możemy natomiast twierdzić, że $\bar{F} = \bar{P} \oplus \bar{Q}$ gdyż podprzestrzenie $\bar{P}$ i $\bar{Q}$ mogą mieć wspólne niezerowe elementy. Tym niemniej, dla pewnej podprzestrzeni $Q_1$ przestrzeni $\bar{Q}$ mamy

$$\bar{F} = \bar{P} \oplus Q_1.$$

Rzeczywiście, każdą bazę $\{v_1, \ldots, v_r\}$ podprzestrzeni $\bar{P} \cap \bar{Q}$ można uzupełnić do bazy $\{v_1, \ldots, v_r, v_{r+1}, \ldots, v_\ell\}$ podprzestrzeni $\bar{P}$ i do bazy $\{v_1, \ldots, v_r, w_{r+1}, \ldots, w_s\}$ podprzestrzeni $\bar{Q}$. Wtedy $\{v_1, \ldots, v_r, v_{r+1}, \ldots, v_\ell, w_{r+1}, \ldots, w_s\}$ jest bazą przestrzeni $\bar{F}$. Jeśli zatem $Q_1 := \mathsf{lin}\{w_{r+1}, \ldots, w_s\}$, to $Q_1 \subseteq \bar{Q}$ oraz $\bar{F} = \bar{P} \oplus Q_1$.

Obierzmy teraz $m_1, \ldots, m_\ell \in P$ oraz $m_{\ell+1}, \ldots, m_n \in Q$ tak by $\bar{m}_1, \ldots, \bar{m}_\ell$ tworzyły bazę podprzestrzeni $\bar{P}$ oraz $\bar{m}_{\ell+1}, \ldots, \bar{m}_n$ tworzyły bazę podprzestrzeni $Q_1$. Wtedy, wobec $\bar{F} = \bar{P} \oplus Q_1$, 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

$$m_i = \sum_{j=1}^{n} b_{ij} e_j, \quad i = 1, \ldots, n, \tag{4.1}$$

gdzie $B = [b_{ij}] \in M_n(R)$ jest macierzą przejścia od bazy $\{e_j\}$ modułu wolnego $F$ do zbioru $\{m_i\}$ elementów modułu $F$. Zauważamy teraz, że poddając równości (4.1) działaniu homomorfizmu kanonicznego otrzymamy

$$\bar{m}_i = \sum_{j=1}^{n} \bar{b}_{ij} \bar{e}_j, \quad i = 1, \ldots, n.$$

Tym razem macierz $\bar{B} = [\bar{b}_{ij}] \in M_n(K)$ jest macierzą przejścia od bazy $\{\bar{e}_1, \ldots, \bar{e}_n\}$ 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 $^- : R \to K$. Ponieważ $R$ jest pierścieniem lokalnym i $\mathfrak{m}$ jest jego jedynym ideałem maksymalnym wynika stąd, że $\det B$ jest elementem odwracalnym w pierścieniu $R$. Wobec tego z równości (4.1) 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

$$m = a_1 m_1 + \cdots + a_\ell m_\ell + q, \quad a_i \in R,\ q \in Q.$$

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. □

## 4.3 Bazy dualne

W algebrze liniowej znana jest dobrze konstrukcja bazy dualnej dla danej bazy przestrzeni wektorowej $V$ nad ciałem $K$. Jeśli $\{v_i : i \in I\}$ jest bazą przestrzeni $V$, to rozpatrujemy funkcjonały liniowe $\varphi_i : V \to K$ takie, że

$$\varphi_i(v_j) = \delta_{ij}, \quad i, j \in I. \tag{4.2}$$

Zbiór funkcjonałów $\{\varphi_i : i \in I\}$ jest liniowo niezależny, gdyż jeśli

$$x_1\varphi_1 + \cdots + x_n\varphi_n = 0$$

dla pewnych $x_1, \ldots, x_n \in K$, to dla każdego $i$, $1 \leqslant i \leqslant n$, mamy

$$0 = (x_1\varphi_1 + \cdots + x_n\varphi_n)(v_i) = x_1\varphi_1(v_i) + \cdots + x_n\varphi_n(v_i) = x_i\varphi_i(v_i) = x_i.$$

Ponadto, jeśli przestrzeń $V$ ma wymiar skończony $n = |I|$, to funkcjonały $\varphi_1, \ldots, \varphi_n$ tworzą bazę przestrzeni dualnej $V^* = \mathsf{Hom}_K(V, K)$ (przestrzeni funkcjonałów liniowych na przestrzeni $V$) zwaną *bazą dualną* dla bazy $\{v_1, \ldots, v_n\}$. Rzeczywiście, funkcjonały $\varphi_1, \ldots, \varphi_n$ rozpinają przestrzeń $V^*$, gdyż dla dowolnego $\varphi \in V^*$, jeśli $\varphi(v_i) = x_i$, to wobec $(x_1\varphi_1 + \cdots + x_n\varphi_n)(v_i) = x_i$ funkcjonały $\varphi$ oraz $x_1\varphi_1 + \cdots + x_n\varphi_n$ działają tak samo na wektorach bazy przestrzeni $V$, wobec tego są równe,

$$\varphi = x_1\varphi_1 + \cdots + x_n\varphi_n.$$

Podsumujmy te uwagi w formie następującego twierdzenia.

Twierdzenie **4.3.1.** *Dla dowolnej przestrzeni wektorowej $V$ nad ciałem $K$ istnieje monomorfizm $V \to V^*$ przeprowadzający dowolną bazę $\{v_i : i \in I\}$ przestrzeni $V$ na liniowo niezależny zbiór funkcjonałów dualnych $\{\varphi_i : i \in I\}$ spełniających warunki* (4.2)*. Jeśli wymiar przestrzeni $V$ jest skończony, to ten monomorfizm jest izomorfizmem przestrzeni wektorowych.*

*Dowód.* Przyporządkowanie $v_i \mapsto \varphi_i$ ma jednoznaczne przedłużenie do homomorfizmu przestrzeni wektorowych $V \to V^*$ na podstawie twierdzenia 3.1.1. □

Zauważmy teraz, że jeśli $v = \sum x_i v_i$, to $\varphi_i(v) = x_i$ i wobec tego mamy jednoznaczne przedstawienie

$$v = \sum \varphi_i(v)v_i \quad \text{dla każdego} \quad v \in V.$$

Pokażemy, że pewien wariant tej własności baz przestrzeni wektorowej $V$ i przestrzeni dualnej $V^*$ 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 grupą abelową i jeśli $R$ jest pierścieniem przemiennym, to z mnożeniem homomorfizmów przez skalary jako działaniem zewnętrznym jest $R-$modułem (zob. rozdział 1.4). W dalszym ciągu zakładamy, że $R$ jest pierścieniem przemiennym i wobec tego $M^*$ nazywamy *modułem dualnym* modułu $M$.

**Przykład 4.3.1.** Dla $R-$modułu $R$ mamy izomorfizm $R-$modułów $R \cong R^*$. Rzeczywiście, jeśli $\varphi \in R^*$ oraz $\varphi(1) = a$, to dla każdego $x \in R$ mamy $\varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = ax$. Stąd łatwo wynika, że odwzorowanie

$$R^* \to R, \quad \varphi \mapsto \varphi(1)$$

jest izomorfizmem $R-$modułów.

Pokażemy najpierw, 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). Rozpoczniemy od następującego lematu.

LEMAT **4.3.1.** *Dla dowolnych $R-$modułów $M$ i $N$, mamy izomorfizm*

$$(M \oplus N)^* \cong M^* \oplus N^*.$$

*Dowód.* Dla $\varphi \in (M \oplus N)^*$ i wszystkich $m \in M, n \in N$ mamy

$$\varphi(m,n) = \varphi((m,0)+(0,n)) = \varphi(m,0) + \varphi(0,n).$$

Interpretujemy $\varphi(m,0)$ jako wartość na $m$ funkcjonału $\varphi(\ \ ,0) \in M^*$, który jest zacieśnieniem $\varphi|_M$ funkcjonału $\varphi$ do $M$, i podobnie interpretujemy $\varphi(0,n)$. Możemy wobec tego określić odwzorowanie

$$\Phi : (M \oplus N)^* \to M^* \oplus N^*, \qquad \Phi(\varphi) = (\varphi|_M, \varphi|_N).$$

Oczywiście $\Phi$ jest homomorfizmem modułów. Pokażemy teraz, że homomorfizm $\Phi$ jest injektywny. Należy więc pokazać, że $\ker \Phi = 0$. Wynika to z następujących równoważności:

$$\begin{aligned}
\varphi \in \ker \Phi &\iff \varphi|_M = 0 \in M^* \quad \text{i} \quad \varphi|_N = 0 \in N^* \\
&\iff \varphi(m,0) = 0 \quad \text{i} \quad \varphi(0,n) = 0 \quad \text{dla wszystkich } m \in M, n \in N \\
&\iff \varphi(m,n) = 0 \quad \text{dla wszystkich } m \in M, n \in N \\
&\iff \varphi = 0 \in (M \oplus N)^*.
\end{aligned}$$

Pozostaje pokazać, że homomorfizm $\Phi$ jest surjektywny. Niech $\varphi_1 \in M^*$, $\varphi_2 \in N^*$. Wtedy

$$\varphi : M \oplus N \to R, \quad \varphi(m,n) = \varphi_1(m) + \varphi_2(n)$$

jest funkcjonałem liniowym, $\varphi \in (M \oplus N)^*$. Ponadto $\varphi|_M = \varphi_1$, $\varphi|_N = \varphi_2$. Zatem

$$\Phi(\varphi) = (\varphi|_M, \varphi|_N) = (\varphi_1, \varphi_2)$$

co dowodzi surjektywności homomorfizmu $\Phi$. □

**Przykład 4.3.2.** Stosując wielokrotnie lemat 4.3.1 oraz przykład 4.3.1, otrzymamy dla każdej liczby naturalnej $n$ następujący izomorfizm:

$$(R^n)^* = (R \oplus \cdots \oplus R)^* \cong R^* \oplus \cdots \oplus R^* = (R^*)^n \cong R^n.$$

WNIOSEK **4.3.1.** *Jeśli $M$ jest skończenie generowanym modułem projektywnym, to $M^*$ jest także skończenie generowanym modułem projektywnym.*

*Dowód.* Na podstawie wniosku 4.2.1 istnieje moduł $N$ i liczba naturalna $n$ takie, że $M \oplus N \cong R^n$. Zatem na podstawie lematu 4.3.1 i przykładu 4.3.2 mamy

$$M^* \oplus N^* \cong (M \oplus N)^* \cong (R^n)^* \cong R^n.$$

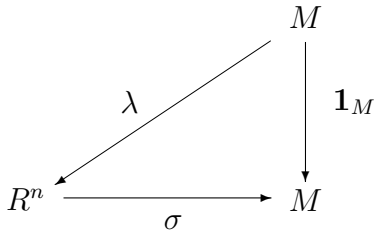
$M^*$ jest więc składnikiem prostym modułu wolnego $R^n$, zatem $M^*$ jest modułem projektywnym. Ponadto, $M^*$ jako składnik prosty $R^n$ jest homomorficznym obrazem $R^n$, zatem jest modułem skończenie generowanym. □

TWIERDZENIE **4.3.2.** *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*

$$m = \sum_{i=1}^{n} \varphi_i(m) m_i \quad \text{dla każdego} \quad m \in M. \tag{4.3}$$

(c) *Istnieją zbiór generatorów $\{m_1, \ldots, m_n\}$ modułu $M$ i zbiór $\{\varphi_1, \ldots, \varphi_n\} \subset M^*$ takie, że zachodzi* (4.3).

*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 3.1.2). A więc istnieje epimorfizm $\sigma : R^n \to M$ i możemy obrać $\sigma$ 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 $\{e_1, \ldots, e_n\}$ modułu $R^n$. Wtedy dla każdego elementu $r = \sum_{i=1}^{n} x_i e_i \in R^n$ mamy

$$r = \sum_{i=1}^{n} \pi_i(r) e_i$$

a więc w szczególności 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

$$\begin{aligned} m = \sigma\lambda(m) = \sigma(\sum_{i=1}^{n} \pi_i(\lambda(m)) e_i) &= \sum_{i=1}^{n} \pi_i(\lambda(m)) \sigma(e_i) \\ &= \sum_{i=1}^{n} \pi_i(\lambda(m)) m_i \\ &= \sum_{i=1}^{n} \varphi_i(m) m_i. \end{aligned}$$

(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 $\sigma$ 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 $\tau$ rozszczepia $\sigma$ i wobec tego $M$ jest składnikiem prostym $R^n$. To dowodzi (a). □

Zbiory generatorów $\{m_1, \ldots, m_n\}$ 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.

Wniosek **4.3.2.** *Niech $M$ będzie $R-$modułem projektywnym. Dla każdego $m \in M$, $m \neq 0$, istnieje funkcjonał $\varphi \in M^*$ taki, że $\varphi(m) \neq 0$.*

*Dowód.* Podamy dowód tylko w przypadku skończenie generowanych modułów projektywnych. Możemy wtedy wykorzystać twierdzenie 4.3.2. Ponieważ $m \neq 0$, jeden z funkcjonałów $\varphi_i$ spełniających (4.3) nie znika na $m$. □

## 4.4 Ideały projektywne

Każdy ideał $\mathcal{I}$ pierścienia $R$ jest $R-$modułem. Podamy tutaj charakteryzacje tych ideałów, które są $R-$modułami wolnymi lub projektywnymi.

Twierdzenie **4.4.1.** *Ideał $\mathcal{I}$ pierścienia $R$ jest $R-$modułem wolnym wtedy i tylko wtedy gdy $\mathcal{I}$ jest ideałem głównym.*

*Dowód.* Jeśli $\mathcal{I}$ jest modułem wolnym, to musi mieć bazę jednoelementową, gdyż każde dwa elementy ideału $\mathcal{I}$ są liniowo zależne nad $R$. Wynika to z równości $ba - ab = 0$ dla dowolnych $a, b \in \mathcal{I}$. Jeśli zatem $\mathcal{I}$ jest wolny to jest ideałem głównym. Na odwrót, ideał główny $\mathcal{I} = Ra$ jest $R-$modułem wolnym z bazą $\{a\}$. □

Pokażemy teraz, że twierdzenie o bazach dualnych pozwala sformułować przejrzysty warunek konieczny i wystarczający na to by ideał $\mathcal{I}$ pierścienia całkowitego $R$ był $R-$modułem projektywnym.

Twierdzenie **4.4.2.** *Niech $R$ będzie pierścieniem całkowitym i niech $K$ będzie ciałem ułamków pierścienia $R$. Ideał skończenie generowany $\mathcal{I}$ pierścienia $R$ jest $R-$modułem projektywnym wtedy i tylko wtedy gdy jest spełniony następujący warunek:*

**(IP)** *Istnieje zbiór generatorów $a_1, \ldots, a_n$ ideału $\mathcal{I}$ i elementy $x_1, \ldots, x_n \in K$ takie, że $x_i\mathcal{I} \subseteq R$ oraz*

$$x_1 a_1 + \cdots + x_n a_n = 1.$$

*Dowód.* Pokażemy najpierw, że warunek **(IP)** pociąga projektywność ideału $\mathcal{I}$. Zakładając **(IP)** możemy określić odwzorowania

$$\varphi_i : \mathcal{I} \to R, \quad \varphi_i(a) = x_i a \quad \text{dla wszystkich} \quad a \in \mathcal{I}.$$

Tutaj założenie, że $x_i\mathcal{I} \subseteq R$ gwarantuje, że wartości $\varphi_i$ należą do $R$. Odwzorowania $\varphi_i$ są oczywiście funkcjonałami liniowymi na $R-$module $\mathcal{I}$ i na podstawie **(IP)** każdy element $a \in \mathcal{I}$ ma przedstawienie postaci

$$a = \sum_{i=1}^{n} x_i a a_i = \sum_{i=1}^{n} \varphi_i(a) a_i.$$

Na podstawie twierdzenia 4.3.2 o bazach dualnych skończenie generowany $R-$moduł $\mathcal{I}$ jest projektywny.

Załóżmy teraz, że $\mathcal{I}$ jest $R-$modułem projektywnym. Na podstawie twierdzenia o bazach dualnych istnieje zbiór generatorów $a_1, \ldots, a_n \in \mathcal{I}$ oraz funkcjonały liniowe $\varphi_1, \ldots, \varphi_n : \mathcal{I} \to R$ takie, że dla każdego $a \in \mathcal{I}$ mamy przedstawienie

$$a = \sum_{i=1}^{n} \varphi_i(a) a_i. \tag{4.4}$$

Zauważmy, że dla dowolnych $a, b \in \mathcal{I}$ i dla dowolnego funkcjonału $\varphi_i$ mamy

$$b\varphi_i(a) = \varphi_i(ba) = \varphi_i(ab) = a\varphi_i(b).$$

Zatem dla każdych $a, b \in \mathcal{I}$, $ab \neq 0$, mamy

$$\frac{\varphi_i(a)}{a} = \frac{\varphi_i(b)}{b}, \quad i = 1, 2, \ldots, n.$$

Z przedstawienia (4.4) otrzymujemy teraz

$$1 = \sum_{i=1}^{n} \frac{\varphi_i(a)}{a} a_i.$$

Dla $x_i := \frac{\varphi_i(a)}{a}$ mamy ponadto $x_i b = \frac{\varphi_i(a)}{a} \cdot b = \varphi_i(b) \in R$ dla każdego $b \in \mathcal{I}$. Zatem $x_i\mathcal{I} \subseteq R$ i wobec tego spełniony jest warunek **(IP)**. □

Wykorzystując twierdzenie 4.4.2 wskażemy teraz typowy przykład skończenie generowanego modułu projektywnego, który nie jest modułem wolnym.

**Przykład 4.4.1.** Niech $R = \mathbb{Z}[\sqrt{-5}\,] = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\}$ i niech $\mathcal{I}$ będzie ideałem pierścienia $R$ generowanym przez liczby 2 i $1 + \sqrt{-5}$:

$$\mathcal{I} = (2, 1 + \sqrt{-5}\,) = 2R + (1 + \sqrt{-5}\,)R.$$

Zauważmy najpierw, że $\mathcal{I}$ jest ideałem właściwym pierścienia $R$, to znaczy $\mathcal{I} \neq R$. W przeciwnym razie $1 \in \mathcal{I}$, zatem istnieją $\alpha, \beta \in R$ takie, że

$$2\alpha + (1 + \sqrt{-5}\,)\beta = 1.$$

Mnożąc tę równość stronami przez $1 - \sqrt{-5}$ otrzymujemy

$$2(1 - \sqrt{-5}\,)\alpha + 6\beta = 1 - \sqrt{-5},$$

skąd wynika, że 2 dzieli $1-\sqrt{-5}$ w pierścieniu $R$, sprzeczność. A więc $\mathcal{I} \neq R$.
Pokażemy teraz, że $\mathcal{I}$ jest projektywnym $R-$modułem. Zgodnie z twierdzeniem 4.4.2 wystarczy wskazać równość

$$x_1a_1 + x_2a_2 = 1$$

gdzie $x_1, x_2 \in K = \mathbb{Q}(\sqrt{-5}\,)$, $a_1 = 2, a_2 = 1+\sqrt{-5}$ oraz $x_i\mathcal{I} \subseteq R$. Wobec równości

$$(-1)\cdot 2 + \tfrac{1}{2}(1-\sqrt{-5}\,)\cdot(1+\sqrt{-5}\,) = 1$$

możemy przyjąć

$$x_1 = -1, \quad x_2 = \tfrac{1}{2}(1-\sqrt{-5}\,).$$

Musimy jedynie sprawdzić, że $x_i\mathcal{I} \subseteq R$. Oczywiście wystarczy pokazać, że iloczyny generatorów ideału $\mathcal{I}$ przez $x_2$ należą do $R$. Jest jasne, że $2\cdot x_2 = 1-\sqrt{-5} \in R$. Natomiast

$$(1+\sqrt{-5})\cdot x_2 = \tfrac{1}{2}(1+\sqrt{-5})\cdot(1-\sqrt{-5}\,) = 3 \in R.$$

Wobec tego $\mathcal{I}$ jest $R-$modułem projektywnym na podstawie twierdzenia 4.4.2.
Pozostaje pokazać, że $\mathcal{I}$ nie jest wolnym $R-$modułem. Na podstawie twierdzenia 4.4.1, jeśli $\mathcal{I}$ jest wolny to jest ideałem głównym. Najpierw zauważmy, że $\mathcal{I} \neq R$. Rzeczywiście, Jeśli $\mathcal{I} = R$, to $1 \in \mathcal{I}$, zatem

$$2(x+y\sqrt{-5}\,) + (1+\sqrt{-5}\,)(s+t\sqrt{-5}\,) = 1$$

dla pewnych $x, y, s, t \in \mathbb{Z}$. Stąd $2x+s-5t = 1$ oraz $2y+s+t = 0$ i po dodaniu stronami otrzymamy $2x+2y+2s-4t = 1$, sprzeczność.
Przypuśćmy, że $\mathcal{I} = (a) = Ra$. Ponieważ $2, 1+\sqrt{-5} \in \mathcal{I}$ więc istnieją $\alpha, \beta \in R$ takie, że

$$2 = \alpha a, \quad 1+\sqrt{-5} = \beta a.$$

Obliczając normy otrzymujemy

$$4 = N(\alpha)N(a), \quad 6 = N(1+\sqrt{-5}) = N(\beta)N(a).$$

Tutaj $N(a) > 1$, gdyż w przeciwnym razie $a \in R$ byłby elementem odwracalnym i wobec tego $\mathcal{I} = (a) = R$, sprzeczność. Zauważmy też, że norma liczby $x+y\sqrt{-5} \in R$ jest równa $x^2+5y^2$, zatem nie może być równa 2 ani 3. Stąd wynika, że $N(\alpha) = N(\beta) = 1$ i wobec tego $4 = N(a), 6 = N(a)$, sprzeczność. Zatem $\mathcal{I}$ nie jest ideałem głównym i także nie jest wolnym $R-$modułem.

**Uwaga 4.4.1.** Przykład 4.4.1 jest bardzo typowy dla ideałów w pierścieniach liczbowych. Jeśli $K$ jest dowolnym skończonym rozszerzeniem ciała liczb wymiernych $\mathbb{Q}$ (w naszym przykładzie $K = \mathbb{Q}(\sqrt{-5}\,)$) i $R$ jest pierścieniem wszystkich liczb algebraicznych całkowitych w ciele $K$ (w naszym przykładzie $R = \mathbb{Z}[\sqrt{-5}\,]$), to można pokazać, że *każdy* ideał $\mathcal{I}$ pierścienia $R$ jest $R-$modułem projektywnym. Ponadto, $\mathcal{I}$ jest wolnym $R-$modułem wtedy i tylko wtedy gdy jest ideałem głównym.

# Rozdział 5

# Dualność

Ostatnie zmiany 14.12.2004 r.

## 5.1 Dualność w przestrzeniach wektorowych

Niech $V$ będzie przestrzenią wektorową nad ciałem $K$. Przestrzeń $V^* = \mathsf{Hom}_K(V, K)$ wszystkich *funkcjonałów liniowych* $\alpha : V \to K$ nazywamy *przestrzenią dualną* przestrzeni $V$ (lub przestrzenią sprzężoną z $V$). W rozdziale 3.3 ustaliliśmy już, że jeśli $\{v_i : i \in I\}$ jest bazą przestrzeni $V$, to funkcjonały liniowe $\varphi_i : V \to K$ spełniające

$$\varphi_i(v_j) = \delta_{ij}, \quad i, j \in I$$

są liniowo niezależne i jeśli $V$ jest skończenie wymiarowa, to tworzą bazę przestrzeni dualnej $V^*$. Zatem (na podstawie twierdzenia 3.1.1) istnieje dokładnie jeden monomorfizm przestrzeni wektorowych

$$\Lambda : V \to V^*$$

taki, że $\Lambda(v_i) = \varphi_i$ dla $i \in I$. Ponadto, monomorfizm ten jest izomorfizmem, jeśli $V$ ma skończony wymiar. Mamy więc następujące twierdzenie (zob. twierdzenie 4.3.1).

Twierdzenie **5.1.1.** *Jeśli $V$ jest dowolną przestrzenią wektorową, to istnieje monomorfizm $V \to V^*$. Jeśli $V$ jest skończenie wymiarową przestrzenią wektorową, to przestrzenie $V$ i $V^*$ są izomorficzne.*

Każda przestrzeń wektorowa ma swoją przestrzeń dualną. W szczególności więc jeśli $V$ jest dowolną przestrzenią wektorową, to przestrzeń $V^*$ ma swoją przestrzeń dualną $(V^*)^*$, którą będziemy oznaczać $V^{**}$ i nazywać *przestrzenią bidualną* przestrzeni $V$. Zatem

$$V^{**} = \mathsf{Hom}_K(V^*, K)$$

jest przestrzenią wszystkich funkcjonałów liniowych na przestrzeni $V^*$ (funkcjonałów liniowych na przestrzeni $V$). Zauważmy najpierw, że jeśli przestrzeń $V$ ma skończony wymiar $n$, to $\dim_K V^* = n$ na podstawie twierdzenia 5.1.1 i na podstawie tego samego twierdzenia także przestrzenie $V^*$ i $V^{**}$ są izomorficzne, mają więc ten sam wymiar. Zatem jeśli $V$ ma skończony wymiar, to

$$\dim_K V = \dim_K V^* = \dim_K V^{**}$$

i wobec tego mamy izomorfizmy przestrzeni wektorowych $V \cong V^* \cong V^{**}$.
Na pierwszy rzut oka elementy przestrzeni bidualnej wydają się bardzo skomplikowane, tymczasem jednak istnieje bardzo prosty i naturalny sposób wskazania funkcjonałów liniowych na przestrzeni $V^*$. Niech bowiem $v \in V$ będzie ustalonym wektorem przestrzeni $V$. Wiążemy z nim funkcję

$$\widehat{v} : V^* \to K, \quad \widehat{v}(\alpha) = \alpha(v).$$

$\widehat{v}$ jest funkcjonałem liniowym na przestrzeni $V^*$, gdyż dla dowolnych funkcjonałów $\alpha, \beta \in V^*$ i dowolnych $a, b \in K$ mamy

$$\widehat{v}(a\alpha + b\beta) = (a\alpha + b\beta)(v) = a\alpha(v) + b\beta(v) = a\widehat{v}(\alpha) + b\widehat{v}(\beta).$$

A więc $\widehat{v}$ jest elementem przestrzeni bidualnej $V^{**}$ przestrzeni $V$. Mamy teraz odwzorowanie

$$\lambda : V \to V^{**}, \qquad \lambda(v) = \widehat{v}, \tag{5.1}$$

które jest homomorfizmem przestrzeni wektorowych. Rzeczywiście, dla $a, b \in K$ oraz $v, w \in V$ mamy

$$\lambda(av + bw) = \widehat{av + bw}$$

oraz dla każdego $\alpha \in V^*$,

$$(\widehat{av + bw})(\alpha) = \alpha(av + bw) = a\alpha(v) + b\alpha(w) = a\widehat{v}(\alpha) + b\widehat{w}(\alpha) = (a\widehat{v} + b\widehat{w})(\alpha).$$

Zatem

$$\lambda(av + bw) = \widehat{av + bw} = a\widehat{v} + b\widehat{w} = a\lambda(v) + b\lambda(w).$$

Homomorfizm $\lambda : V \to V^{**}$ ma następującą fundamentalną własność.

TWIERDZENIE **5.1.2.** *Homomorfizm $\lambda : V \to V^{**}$ jest monomorfizmem. Jeśli przestrzeń $V$ jest skończenie wymiarowa, to homomorfizm $\lambda$ jest izomorfizmem przestrzeni wektorowych.*

*Dowód.* Pokażemy najpierw, że homomorfizm (5.1) jest różnowartościowy. Niech więc $v \in V$ oraz $\lambda(v) = \widehat{v} = 0 \in V^{**}$. Wtedy

$$\alpha(v) = \widehat{v}(\alpha) = 0$$

dla każdego funkcjonału $\alpha \in V^*$. Stąd wynika, że $v = 0$, gdyż gdyby $v \neq 0$, to istnieje baza $\mathcal{B}$ przestrzeni $V$, do której należy wektor $v$ i wtedy można określić niezerowy funkcjonał liniowy $\varphi$ na $V$, na przykład taki, że $\varphi(v) = 1$ oraz $\varphi(u) = 0$ dla pozostałych wektorów $u$ bazy $\mathcal{B}$. Zatem $\ker \lambda = 0$ co oznacza, że homomorfizm $\lambda$ jest różnowartościowy. Jeśli wymiar przestrzeni $V$ jest skończony, to przestrzenie $V^{**}$ oraz $V$ mają równe wymiary i z różnowartościowości $\lambda$ wynika, że $\lambda$ jest izomorfizmem przestrzeni wektorowych. □

A więc skończenie wymiarowa przestrzeń wektorowa jest naturalnie izomorficzna ze swoją przestrzenią bidualną. Opis funkcjonałów liniowych na przestrzeni $V^*$ jest przy tym zaskakująco prosty. Dla każdego funkcjonału liniowego $\tau : V^* \to K$ istnieje dokładnie jeden wektor $v \in V$ taki, że $\tau(\alpha) = \alpha(v)$ dla wszystkich $\alpha \in V^*$.

Twierdzenia 5.1.1 i 5.1.2 stanowią wzorzec twierdzeń o dualności dla modułów nad dowolnymi pierścieniami. W tym rozdziale pokażemy, że twierdzenia te mają swoje naturalne uogólnienia dla modułów wolnych nad dowolnymi pierścieniami. Pokażemy także, że twierdzenie 5.1.2 ma jeszcze ogólniejszą wersję dla modułów projektywnych nad dowolnymi pierścieniami, natomiast twierdzenie 5.1.1 nie ma już pełnego odpowiednika dla modułów projektywnych.

## 5.2 Homomorfizmy modułów homomorfizmów

Omówimy tutaj pewną ogólną konstrukcję homomorfizmów pomiędzy modułami homomorfizmów, która jako szczególne przypadki obejmuje homomorfizmy indukowane (określone w rozdziale 1.4.1) oraz homomorfizmy transponowane, które wykorzystamy poniżej.

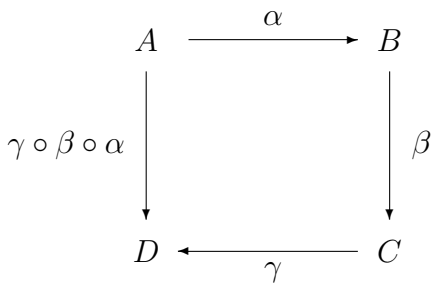
Niech $R$ będzie pierścieniem przemiennym i niech $A, B, C, D$ będą $R-$modułami. Niech

$$\alpha : A \to B, \quad \beta : B \to C, \quad \gamma : C \to D$$

będą homomorfizmami modułów. Wtedy otrzymujemy homomorfizm modułów

$$\gamma \circ \beta \circ \alpha : A \to D.$$

Odpowiedni diagram wygląda następująco:

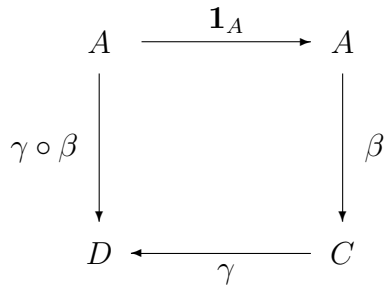



W ten sposób każdemu homomorfizmowi $\beta \in \mathsf{Hom}(B, C)$ możemy przyporządkować homomorfizm $\gamma \circ \beta \circ \alpha \in \mathsf{Hom}(A, D)$. Tak określa się homomorfizm modułów

$$\mathsf{Hom}(\alpha, \gamma) : \mathsf{Hom}(B, C) \to \mathsf{Hom}(A, D), \qquad \mathsf{Hom}(\alpha, \gamma)(\beta) = \gamma \circ \beta \circ \alpha.$$

Sprawdzenie, że $\mathsf{Hom}(\alpha, \gamma)$ jest rzeczywiście homomorfizmem modułów pozostawiamy Czytelnikowi jako łatwe ćwiczenie. Należy zwrócić uwagę na to, że każda para homomorfizmów $\alpha, \gamma$ wyznacza odpowiedni homomorfizm $\mathsf{Hom}(\alpha, \gamma)$. Wykorzystamy tę możliwość w trzech szczególnych sytuacjach.

**Przykład 5.2.1.** Rozważmy szczególny przypadek gdy $A = B$ oraz $\alpha = \mathbf{1}_A$.




Wtedy mamy homomorfizm

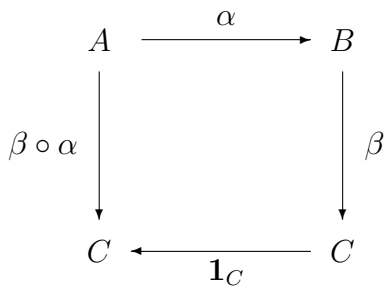
$$\mathsf{Hom}(\mathbf{1}_A, \gamma) : \mathsf{Hom}(A, C) \to \mathsf{Hom}(A, D), \quad \mathsf{Hom}(\mathbf{1}_A, \gamma)(\beta) = \gamma \circ \beta.$$

Ten homomorfizm oznaczyliśmy w rozdziale 1.4.1 symbolem $\gamma_*$ i nazwaliśmy homomorfizmem indukowanym przez homomorfizm $\gamma$. Ponieważ zamierzamy określić

jeszcze jeden homomorfizm pomiędzy modułami homomorfizmów, który także zasługuje na nazwę homomorfizmu indukowanego, homomorfizm $\gamma_*$ możemy nazywać *pierwszym* homomorfizmem indukowanym. A więc dla homomorfizmu $\gamma : C \to D$ mamy

$$\gamma_* : \mathsf{Hom}(A, C) \to \mathsf{Hom}(A, D), \quad \gamma_*(\beta) = \gamma \circ \beta.$$

**Przykład 5.2.2.** Rozważmy szczególny przypadek gdy $C = D$ oraz $\gamma = \mathbf{1}_C$.




Wtedy mamy homomorfizm

$$\mathsf{Hom}(\alpha, \mathbf{1}_C) : \mathsf{Hom}(B, C) \to \mathsf{Hom}(A, C), \quad \mathsf{Hom}(\alpha, \mathbf{1}_C)(\beta) = \beta \circ \alpha.$$

Ten homomorfizm oznaczamy symbolem $\alpha^*$ i także nazywamy homomorfizmem indukowanym przez homomorfizm $\alpha$. Dla rozróżnienia $\gamma_*$ i $\alpha^*$ homomorfizm $\alpha^*$ nazywamy *drugim* homomorfizmem indukowanym. A więc dla homomorfizmu $\alpha : A \to B$ mamy

$$\alpha^* : \mathsf{Hom}(B, C) \to \mathsf{Hom}(A, C), \quad \alpha^*(\beta) = \beta \circ \alpha.$$

Przy pomocy drugiego homomorfizmu indukowanego definiuje się ważne pojęcie modułu *injektywnego*. Mówimy, że moduł $P$ jest injektywny, jeśli dla każdego injektywnego homomorfizmu $f : M \to N$ drugi homomorfizm indukowany

$$f^* : \mathsf{Hom}(N, P) \to \mathsf{Hom}(M, P), \quad f^*(\beta) = \beta \circ f$$

jest epimorfizmem.

Twierdzenie **5.2.1.** *Niech*

$$0 \to M' \xrightarrow{g} M \xrightarrow{f} N \to 0 \tag{5.2}$$

*będzie rozszczepialnym ciągiem dokładnym $R-$modułów i ich homomorfizmów. Wtedy dla dowolnego $R-$modułu $P$ także ciągi*

$$0 \to \mathsf{Hom}(P, M') \xrightarrow{g_*} \mathsf{Hom}(P, M) \xrightarrow{f_*} \mathsf{Hom}(P, N) \to 0 \tag{5.3}$$

$$0 \to \mathsf{Hom}(N, P) \xrightarrow{f^*} \mathsf{Hom}(M, P) \xrightarrow{g^*} \mathsf{Hom}(M', P) \to 0 \tag{5.4}$$

*są dokładne i rozszczepiają się.*

*Szkic dowodu.* Najpierw pokazujemy, że jeśli ciąg (5.2) jest dokładny, to dla każdego $R-$modułu $P$ ciągi

$$0 \to \mathsf{Hom}(P, M') \xrightarrow{g_*} \mathsf{Hom}(P, M) \xrightarrow{f_*} \mathsf{Hom}(P, N)$$

$$0 \to \mathsf{Hom}(N, P) \xrightarrow{f^*} \mathsf{Hom}(M, P) \xrightarrow{g^*} \mathsf{Hom}(M', P)$$

są dokładne. Następnie wykorzystując, że $f$ jest surjekcją i ciąg (5.2) rozszczepia się, pokazujemy, że w ciągu (5.3) homomorfizm $f_*$ jest surjekcją. Dalej, jeśli homomorfizm $\varphi : N \to M$ rozszczepia $f$, to znaczy $f \circ \varphi = \mathbf{1}_N$, to $(f \circ \varphi)_* = f_* \circ \varphi_*$ jest identycznością na module $\mathsf{Hom}(P, N)$, a więc $\varphi_*$ rozszczepia $f_*$. Zatem ciąg (5.3) jest dokładny i rozszczepia się.
Podobnie dowodzi się, że ciąg (5.4) jest dokładny i rozszczepia się. □

**Przykład 5.2.3.** Rozważmy szczególny przypadek gdy $C = D = R$ oraz $\gamma = \mathbf{1}_R$. Wtedy mamy homomorfizm

$$\mathsf{Hom}(\alpha, \mathbf{1}_R) : \mathsf{Hom}(B, R) \to \mathsf{Hom}(A, R), \quad \mathsf{Hom}(\alpha, \mathbf{1}_R)(\beta) = \beta \circ \alpha.$$

Jest to zatem szczególny przypadek drugiego homomorfizmu indukowanego

$$\alpha^* = \mathsf{Hom}(\alpha, \mathbf{1}_C) = \mathsf{Hom}(\alpha, \mathbf{1}_R).$$

Ten homomorfizm oznaczamy symbolem ${}^t\alpha$ i nazywamy transpozycją homomorfizmu $\alpha$. A więc dla homomorfizmu $\alpha : A \to B$ homomorfizmem transponowanym jest homomorfizm

$${}^t\alpha : B^* \to A^*, \qquad {}^t\alpha(\beta) = \beta \circ \alpha.$$

Odnotujmy dwie własności homomorfizmu transponowanego. Po pierwsze, dla homomorfizmu identycznościowego $\mathbf{1}_A : A \to A$ mamy

$${}^t(\mathbf{1}_A)(\beta) = \beta \circ \mathbf{1}_A = \beta.$$

Zatem ${}^t(\mathbf{1}_V)$ jest identycznością na $A^*$.
Po drugie, dla homomorfizmów $\alpha : A \to B,\ \delta : C \to A$, ich złożenia $\alpha \circ \delta : C \to B$ i dla homomorfizmów transponowanych

$${}^t\alpha : B^* \to A^*, \quad {}^t\delta : A^* \to C^*, \quad {}^t(\alpha \circ \delta) : B^* \to C^*$$

mamy

$${}^t(\alpha \circ \delta)(\beta) = \beta \circ (\alpha \circ \delta) = (\beta \circ \alpha) \circ \delta = {}^t\alpha(\beta) \circ \delta = {}^t\delta({}^t\alpha(\beta)) = ({}^t\delta \circ {}^t\alpha)(\beta).$$

A więc

$${}^t(\alpha \circ \delta) = {}^t\delta \circ {}^t\alpha.$$

Zanotujmy także szczególny przypadek twierdzenia 5.2.1.

Wniosek **5.2.1.** *Jeśli* $0 \to M' \xrightarrow{g} M \xrightarrow{f} N \to 0$ *jest rozszczepialnym ciągiem dokładnym $R-$modułów i ich homomorfizmów to także ciąg*

$$0 \to N^* \xrightarrow{{}^t f} M^* \xrightarrow{{}^t g} M'^* \to 0$$

*jest dokładny i rozszczepia się.*

Zauważmy jeszcze, że dla homomorfizmu transponowanego ${}^t\alpha : B^* \to A^*$ homomorfizmu $\alpha : A \to B$ istnieje także homomorfizm transponowany ${}^t({}^t(\alpha)) : A^{**} \to B^{**}$, który oznaczamy ${}^{tt}\alpha$ i nazywamy *drugą transpozycją* homomorfizmu $\alpha$.

## 5.3 Moduł bidualny

Zbadamy teraz w jakim zakresie rezultaty dotyczące dualności skończenie wymiarowych przestrzeni wektorowych przenoszą się na skończenie generowane moduły nad dowolnym pierścieniem przemiennym $R$. Dla ułatwienia śledzenia analogii konstrukcji zachowamy oznaczenia, które stosowaliśmy dla przestrzeni wektorowych.

Niech więc $V$ będzie modułem nad pierścieniem przemiennym $R$. Moduł $V^* = \mathsf{Hom}_R(V, R)$ wszystkich *funkcjonałów liniowych* $\varphi : V \to R$ nazywamy *modułem dualnym* modułu $V$ (lub modułem sprzężonym z $V$). W rozdziale 3.3 ustaliliśmy już następujące własności modułu dualnego:

- $R^* = \mathsf{Hom}_R(R, R)$ jest izomorficzny z $R-$modułem $R$ (przykład 4.3.1).
- $(R^n)^* \cong R^n$ (przykład 4.3.2).
- Jeśli $V$ jest skończenie generowanym modułem projektywnym, to także $V^*$ jest skończenie generowanym modułem projektywnym (wniosek 4.3.1)
- $(V \oplus U)^* \cong V^* \oplus U^*$ dla dowolnych $R-$modułów $V, U$ (lemat 4.3.1).

Druga z powyższych własności stwierdza, że moduł wolny o skończonej randze jest izomorficzny ze swoim modułem dualnym, co jest uogólnieniem twierdzenia 5.1.1. Takie twierdzenie nie jest już jednak prawdziwe dla skończenie generowanych modułów projektywnych (zob. przykład 5.5.1).

Ustalimy teraz związek między modułem $V$ i jego modułem bidualnym $V^{**}$. Dla dowolnego $R-$modułu $V$ określamy odwzorowanie

$$\lambda_V : V \to V^{**}, \quad \lambda_V(v) = \widehat{v}, \tag{5.5}$$

gdzie $v \in V$ oraz $\widehat{v} : V^* \to R$ jest funkcjonałem liniowym na module $V^*$ określonym następująco:

$$\widehat{v}(\varphi) = \varphi(v) \quad \text{dla} \quad \varphi \in V^*.$$

Odwzorowanie $\lambda_V$ jest homomorfizmem $R-$modułów, gdyż dla dowolnych $a, b \in R$, $u, w \in V$ oraz $\varphi \in V^*$, tak jak w przypadku gdy $V$ jest przestrzenią wektorową, mamy

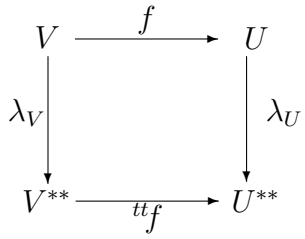
$$\widehat{(av + bw)}(\varphi) = \varphi(av + bw) = a\varphi(v) + b\varphi(w) = a\widehat{v}(\varphi) + b\widehat{w}(\varphi) = (a\widehat{v} + b\widehat{w})(\varphi),$$

skąd

$$\lambda(av + bw) = \widehat{av + bw} = a\widehat{v} + b\widehat{w} = a\lambda(v) + b\lambda(w).$$

Homomorfizm $\lambda_V : V \to V^{**}$ jest określony uniwersalną formułą (5.5) dla każdego modułu $V$. W szczególności, homomorfizm $\lambda_V$ 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 $\lambda_V$ niepotrzebny jest żaden wybór bazy przestrzeni $V$ i w dodatku formuła (5.5) stosuje się do każdego $R-$modułu $V$. Tę nadzwyczajną uniwersalność homomorfizmu $\lambda_V$ podkreśla twierdzenie 5.3.1. Objaśnia ono co rozumiemy przez kanoniczność lub naturalność homomorfizmu $\lambda_V$.

TWIERDZENIE **5.3.1.** *Niech $V, U$ będą modułami nad pierścieniem $R$. Dla każdego homomorfizmu modułów $f : V \to U$ mamy diagram przemienny*




*w którym* ${}^{tt}f$ *jest drugą transpozycją homomorfizmu* $f$*.*

*Dowód.* Pokażemy, że $\lambda_U f(v) = {}^{tt}f\lambda_V(v)$ dla każdego elementu $v \in V$. Przede wszystkim zauważmy, że

$$\lambda_U f(v) = \widehat{f(v)}, \quad \text{gdzie} \quad \widehat{f(v)} : U^* \to R, \quad \widehat{f(v)}(\beta) = \beta(f(v))$$

dla każdego $\beta \in U^*$, oraz

$${}^{tt}f\lambda_V(v) = {}^{tt}f(\widehat{v}), \quad \text{gdzie} \quad \widehat{v} : V^* \to R, \quad \widehat{v}(\alpha) = \alpha(v)$$

dla każdego $\alpha \in V^*$. Ponieważ $\widehat{f(v)}$, ${}^{tt}f(\widehat{v}) \in U^{**}$ są funkcjonałami liniowymi na module $U^*$, więc aby udowodnić, że są one równe bierzemy dowolny funkcjonał $\beta \in U^*$ i sprawdzamy, że

$$\widehat{f(v)}(\beta) = \beta(f(v)) = (\beta \circ f)(v),$$

$${}^{tt}f(\widehat{v})(\beta) = {}^{t}({}^{t}f)(\widehat{v})(\beta) = (\widehat{v} \circ {}^{t}f)(\beta) = \widehat{v}({}^{t}f(\beta)) = \widehat{v}(\beta \circ f) = (\beta \circ f)(v).$$

Dowodzi to przemienności naszego diagramu. □

## 5.4 Dualność w modułach wolnych

Dla modułów wolnych zachodzą obydwa twierdzenia o dualności przestrzeni wektorowych (twierdzenia 5.1.1 oraz 5.1.2).

Twierdzenie **5.4.1.** *Jeśli* $V$ *jest dowolnym modułem wolnym, to istnieje monomorfizm* $V \to V^*$*. Jeśli* $V$ *jest modułem wolnym o skończonej randze, to moduły* $V$ *i* $V^*$ *są izomorficzne.*

*Dowód.* Niech $\mathcal{B} = \{v_i : i \in I\}$ będzie bazą modułu wolnego $V$. Rozpatrujemy funkcjonały liniowe $\varphi_i : V \to R$ takie, że

$$\varphi_i(v_j) = \delta_{ij}, \quad i, j \in I.$$

Funkcjonały $\{\varphi_i : i \in I\}$ są liniowo niezależne, gdyż jeśli

$$x_1\varphi_1 + \cdots + x_n\varphi_n = 0$$

dla pewnych $x_1, \ldots, x_n \in R$, to dla każdego $i$, $1 \leqslant i \leqslant n$, mamy

$$0 = (x_1\varphi_1 + \cdots + x_n\varphi_n)(v_i) = x_1\varphi_1(v_i) + \cdots + x_n\varphi_n(v_i) = x_i\varphi_i(v_i) = x_i.$$

Odwzorowanie $\beta : \mathcal{B} \to V^*$ takie, że $\beta(v_i) = \varphi_i$ ma jednoznaczne przedłużenie do homomorfizmu modułów $\Lambda : V \to V^*$ na podstawie twierdzenia 3.1.1. Ponieważ zbiór $\beta(\mathcal{B})$ jest liniowo niezależny, homomorfizm $\Lambda$ jest monomorfizmem. Dowodzi to pierwszej części twierdzenia.

Załóżmy teraz, że $V$ ma skończoną rangę $n = |I|$. Wtedy funkcjonały $\varphi_1, \ldots, \varphi_n$ rozpinają moduł $V^*$, gdyż dla dowolnego $\varphi \in V^*$, jeśli $\varphi(v_i) = x_i$, to wobec $(x_1\varphi_1 + \cdots + x_n\varphi_n)(v_i) = x_i$ funkcjonały $\varphi$ oraz $x_1\varphi_1 + \cdots + x_n\varphi_n$ działają tak samo na elementach bazy modułu wolnego $V$, wobec tego są równe,

$$\varphi = x_1\varphi_1 + \cdots + x_n\varphi_n.$$

Zatem funkcjonały $\varphi_1, \ldots, \varphi_n$ tworzą bazę modułu $V^*$ zwaną bazą *dualną* dla bazy $v_1, \ldots, v_n$ modułu $V$. Wynika stąd, że $V^*$ jest także modułem wolnym i ma rangę równą randze modułu wolnego $V$. Homomorfizm $\Lambda$ przeprowadza bazę $\mathcal{B}$ modułu $V$ na bazę dualną $\beta(\mathcal{B})$ modułu $V^*$ i wobec tego jest izomorfizmem. □

Zauważmy jeszcze, że dla drugiej części twierdzenia 5.4.1 mamy niezależny dowód. $R-$moduł wolny $V$ rangi $n$ jest izomorficzny z $R^n$ natomiast $V^* \cong (R^n)^* \cong R^n$ na podstawie przykładu 4.3.2.

Twierdzenie **5.4.2.** *Dla każdego modułu wolnego $V$ homomorfizm*

$$\lambda_V : V \to V^{**}, \quad \lambda_V(v) = \widehat{v}$$

*jest monomorfizmem modułów. Jeśli moduł wolny $V$ ma skończoną rangę, to $\lambda_V$ jest izomorfizmem modułów.*

*Dowód.* Przypuśćmy, że $\lambda_V(v) = 0$ dla pewnego niezerowego elementu $v \in V$. Oznacza to, że $\widehat{v}(\beta) = \beta(v) = 0$ dla każdego funkcjonału $\beta \in V^*$.

Niech $\mathcal{B} = \{v_i : i \in I\}$ będzie bazą modułu $V$. Rozpatrujemy funkcjonały liniowe $\varphi_i : V \to R$ takie, że

$$\varphi_i(v_j) = \delta_{ij}, \quad i, j \in I.$$

Jeśli $v = \sum x_i v_i$, to $x_i = \varphi_i(v)$ i skoro $v \neq 0$, to przynajmniej jedna współrzędna $x_i$ nie jest równa zero. Wtedy $\widehat{v}(\varphi_i) = \varphi_i(v) = x_i \neq 0$, wbrew temu, że $\beta(v) = 0$ dla każdego $\beta \in V^*$. Zatem $\ker \lambda_V = 0$ i $\lambda_V$ jest monomorfizmem.

Załóżmy teraz, że moduł wolny $V$ ma skończoną rangę. W dowodzie poprzedniego twierdzenia pokazaliśmy, że jeśli $V$ jest modułem wolnym o skończonej randze, to $V^*$ jest także modułem wolnym i ma rangę równą randze modułu wolnego $V$. 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. Izomorfizmy te otrzymamy obierając w każdym z wymienionych modułów wolnych bazę i definiując odpowiednie izomorfizmy poprzez ich odpowiednie określenie na bazach modułów. Nasze twierdzenie mówi jednak, że homomorfizm $\lambda_V : V \to V^{**}$ jest izomorfizmem. Okazuje się, że $\lambda_V$ przeprowadza każdą bazę $\mathcal{B}$ modułu $V$ na bazę modułu $V^{**}$ dualną do bazy modułu $V^*$ dualnej z bazą $\mathcal{B}$.
Niech $\{v_1, \ldots, v_n\}$ będzie bazą modułu $V$ i niech $\{\varphi_1, \ldots, \varphi_n\}$ będzie bazą dualną modułu $V^*$. Przypomnijmy, że

$$\lambda_V(v_i) = \widehat{v}_i, \quad \text{gdzie} \quad \widehat{v}_i(\varphi_j) = \varphi_j(v_i) = \delta_{ji}.$$

Zatem $\{\widehat{v}_1, \ldots, \widehat{v}_n\}$ jest bazą modułu $V^{**}$ dualną względem bazy $\{\varphi_1, \ldots, \varphi_n\}$ modułu $V^*$ i homomorfizm $\lambda_V$ przeprowadza bazę $\{v_1, \ldots, v_n\}$ modułu wolnego $V$ na bazę $\{\widehat{v}_1, \ldots, \widehat{v}_n\}$ modułu wolnego $V^{**}$. A więc $\lambda_V$ jest izomorfizmem modułów. □

## 5.5 Dualność w modułach projektywnych

Dla modułów projektywnych nie funkcjonuje pierwsze twierdzenie o dualności mówiące, że moduł jest izomorficzny ze swoim modułem dualnym. Natomiast dla każdego skończenie generowanego modułu projektywnego prawdziwe jest drugie twierdzenie o dualności i dowód tego twierdzenia przedstawimy w tym rozdziale.

**Przykład 5.5.1.** Zasygnalizujemy tutaj istnienie skończenie generowanego modułu projektywnego $P$ takiego, że $P \ncong P^*$. Niestety przykład modułu o takich własnościach wymaga użycia pojęć i faktów wykraczających poza ten wykład. Czytelnik, który zna podstawowe pojęcia teorii pierścieni Dedekinda zaakceptuje poniższe informacje.

Niech $R$ będzie pierścieniem całkowitym i niech $K$ będzie ciałem ułamków pierścienia $R$. *Ideałem ułamkowym* ciała $K$ nazywamy każdy $R-$podmoduł $\mathcal{I}$ ciała $K$ dla którego istnieje różny od zera element $a \in R$ taki, że $a\mathcal{I} \subseteq R$. W szczególności więc każdy ideał $\mathcal{I}$ pierścienia $R$ jest ideałem ułamkowym w $K$ (można wziąć $a = 1$). Definiujemy *iloczyn* ideałów ułamkowych $\mathcal{I}$ oraz $\mathcal{J}$ ciała $K$ podobnie jak iloczyn ideałów pierścienia jako zbiór wszystkich skończonych sum $\sum a_i b_i$, gdzie $a_i \in \mathcal{I}$ oraz $b_i \in \mathcal{J}$. Łatwo stwierdzić, że to mnożenie ideałów ułamkowych jest działaniem przemiennym i łącznym oraz ideał jednostkowy $(1) = R$ jest elementem neutralnym tego działania. Ideały ułamkowe tworzą więc monoid.

Dla każdego ideału ułamkowego $\mathcal{I}$ ciała $K$ kładziemy

$$\mathcal{I}' = \{x \in K : x\mathcal{I} \subseteq R\}.$$

Łatwo sprawdzić, że $\mathcal{I}\mathcal{I}' \subseteq R$ oraz $\mathcal{I}'$ jest ideałem ułamkowym ciała $K$. Jeśli $\mathcal{I}\mathcal{I}' = R$, to ideał $\mathcal{I}$ jest odwracalny w monoidzie ideałów ułamkowych ciała $K$. Piszemy wtedy $\mathcal{I}^{-1}$ zamiast $\mathcal{I}'$. Okazuje się przy tym, że ideał $\mathcal{I}$ jest odwracalny wtedy i tylko wtedy gdy jest projektywnym $R-$modułem. Łatwo stwierdzić, że jeśli $\mathcal{I}$ jest ideałem odwracalnym, to $\mathcal{I}^{-1} \cong \mathcal{I}^* = \mathsf{Hom}_R(\mathcal{I}, R)$.

Weźmy teraz w pierścieniu $R$ ideał $\mathcal{I}$ taki, że $\mathcal{I}^3 = (a) = aR$ jest ideałem głównym, ale $\mathcal{I}$ i $\mathcal{I}^2$ nie są ideałami głównymi. Wtedy $\mathcal{I} \ncong \mathcal{I}^2$ gdyż można udowodnić (jest to szczególny przypadek tak zwanego twierdzenia Steinitza), że jeśli dwa ideały $\mathcal{I}$, $\mathcal{J}$ pierścienia całkowitego są izomorficznymi $R-$modułami, to istnieje element $c \in R$ taki, że $\mathcal{I} = c\mathcal{J}$. Gdyby więc $\mathcal{I} \cong \mathcal{I}^2$, to $\mathcal{I} = c\mathcal{I}^2$, skąd $\mathcal{I}^2 = c\mathcal{I}^3 = (ca)$ jest ideałem głównym, wbrew założeniu. W tej sytuacji mamy

$$\mathcal{I} \ncong \mathcal{I}^2 = (a)\mathcal{I}^{-1} \cong \mathcal{I}^{-1} \cong \mathcal{I}^*,$$

a więc projektywny $R-$moduł $\mathcal{I}$ nie jest izomorficzny z modułem dualnym $\mathcal{I}^*$.

Istnienie ideałów o powyższych własnościach można wskazać w wielu pierścieniach Dedekinda. Pierścień całkowity $R$ jest pierścieniem Dedekinda wtedy i tylko wtedy gdy każdy niezerowy ideał ułamkowy ciała ułamków $K$ pierścienia $R$ jest odwracalny, lub równoważnie, gdy monoid ideałów ułamkowych ciała $K$ jest grupą (zob. J. Browkin, *Teoria ciał*, PWN Warszawa 1977, str. 259). Konkretne przykłady pierścieni Dedekinda otrzymujemy jako pierścienie $R_K$ liczb algebraicznych całkowitych w skończonych rozszerzeniach $K$ ciała liczb wymiernych $\mathbb{Q}$. Jeśli $K = \mathbb{Q}(\sqrt{-23}\,)$, to $R_K = \{a + b\omega : a, b \in \mathbb{Z}\}$, gdzie $\omega = \frac{1}{2}(1 + \sqrt{-23}\,)$ i dla każdego ideału $\mathcal{I}$, który nie jest główny, także ideał $\mathcal{I}^2$ nie jest główny, podczas gdy $\mathcal{I}^3$ jest ideałem głównym (wynika to stąd, że tzw. *liczba klas* ciała $K$ jest równa 3). Tak więc, na przykład, ideał $\mathcal{I} = (2, \omega)$ jest skończenie generowanym $R-$modułem projektywnym, który nie jest izomorficzny z modułem dualnym $\mathcal{I}^*$.

TWIERDZENIE **5.5.1.** *Dla każdego modułu projektywnego $P$ odwzorowanie*

$$\lambda_P : P \to P^{**}, \quad \lambda_P(p) = \widehat{p}$$

*jest monomorfizmem modułów. Jeśli $P$ jest skończenie generowany, to $\lambda_P$ jest izomorfizmem modułów.*

*Pierwszy dowód twierdzenia* 5.5.1. Przedstawimy najpierw dowód injektywności $\lambda_P$. Niech $p \in \ker \lambda_P$. Wtedy $\widehat{p}(\varphi) = \varphi(p) = 0$ dla każdego funkcjonału $\varphi \in P^*$. Na podstawie wniosku 4.3.2 otrzymujemy $p = 0$. Zatem $\ker \lambda_P = 0$ i homomorfizm $\lambda_P$ jest injektywny.

Dla dowodu drugiej części twierdzenia 5.5.1 zakładamy, że $P$ jest skończenie generowanym $R-$modułem projektywnym. Na podstawie lematu 4.2.1 istnieje $R-$moduł $Q$ taki, że moduł $F := P \oplus Q$ jest wolny i ma skończoną rangę. Na podstawie twierdzenia 5.4.2 homomorfizm $\lambda_F : F \to F^{**}$ jest izomorfizmem.
Dowód, że $\lambda_P$ jest izomorfizmem polega na analizie następującego diagramu:

$$\begin{array}{ccc} F = P \oplus Q & \xrightarrow{\lambda_P \oplus \lambda_Q} & P^{**} \oplus Q^{**} \\ \Big\downarrow{\scriptstyle i \oplus j} & & \Big\downarrow{\scriptstyle {}^{tt}i \oplus {}^{tt}j} \\ F & \xrightarrow{\lambda_F} & F^{**} \end{array} \qquad (\bigstar)$$

Objaśnimy najpierw działanie homomorfizmów występujących w diagramie. Dla homomorfizmów $\lambda_P : P \to P^{**}$ oraz $\lambda_Q : Q \to Q^{**}$ (określonych formułą (5.5)) definiujemy

$$\lambda_P \oplus \lambda_Q : P \oplus Q \to P^{**} \oplus Q^{**}, \qquad (\lambda_P \oplus \lambda_Q)(p, q) = (\lambda_P(p), \lambda_Q(q)) = (\widehat{p}, \widehat{q}\,).$$

Dla włożeń $i : P \to P \oplus Q$ oraz $j : Q \to P \oplus Q$ określamy

$$i \oplus j : P \oplus Q \to F, \qquad (i \oplus j)(p, q) = i(p) + j(q) = p + q.$$

Dla włożeń $i : P \to P \oplus Q$ oraz $j : Q \to P \oplus Q$ rozpatrujemy homomorfizmy transponowane

$${}^{t}i : (P \oplus Q)^* \to P^*, \qquad {}^{t}j : (P \oplus Q)^* \to Q^*$$

oraz drugie transpozycje homomorfizmów $i, j$:

$${}^{tt}i : P^{**} \to (P \oplus Q)^{**} = F^{**}, \qquad {}^{tt}j : Q^{**} \to (P \oplus Q)^{**} = F^{**}.$$

Teraz występujący w diagramie ($\bigstar$) homomorfizm określony jest następująco:

$${}^{tt}i \oplus {}^{tt}j : P^{**} \oplus Q^{**} \to (P \oplus Q)^{**} = F^{**}, \qquad ({}^{tt}i \oplus {}^{tt}j)(\alpha, \beta) = {}^{tt}i(\alpha) + {}^{tt}j(\beta).$$

LEMAT **5.5.1.** *Diagram ($\bigstar$) jest przemienny.*

*Dowód.* Zauważmy najpierw, że dla dowolnych $p \in P$, $q \in Q$ mamy

$$\lambda_F((i \oplus j)(p,q)) = \lambda_F(p+q) = \widehat{p+q}$$
$$({}^{tt}i \oplus {}^{tt}j)((\lambda_P \oplus \lambda_Q)(p,q)) = ({}^{tt}i \oplus {}^{tt}j)(\widehat{p},\widehat{q}) = {}^{tt}i(\widehat{p}) + {}^{tt}j(\widehat{q}).$$

Są to elementy modułu $F^{**}$, czyli funkcjonały liniowe na module $F^*$. Pokażemy, że dla każdego funkcjonału $\gamma \in F^*$ mamy równość

$$\widehat{p+q}\,(\gamma) = ({}^{tt}i(\widehat{p}) + {}^{tt}j(\widehat{q}))(\gamma).$$

Rzeczywiście, z jednej strony $\widehat{p+q}\,(\gamma) = \gamma(p+q)$ z drugiej zaś

$$\begin{aligned} {}^{tt}i(\widehat{p})(\gamma) &= {}^{t}({}^{t}i)(\widehat{p})(\gamma) = (\widehat{p} \circ {}^{t}i)(\gamma) = \widehat{p}\,({}^{t}i(\gamma)) \\ &= \widehat{p}\,(\gamma \circ i) = (\gamma \circ i)(p) = \gamma(i(p)) \\ &= \gamma(p) \end{aligned}$$

i podobnie ${}^{tt}j(\widehat{q})(\gamma) = \gamma(q)$, czyli

$$({}^{tt}i(\widehat{p}) + {}^{tt}j(\widehat{q}))(\gamma) = \gamma(p) + \gamma(q) = \gamma(p+q),$$

co dowodzi przemienności diagramu (★). □

Dla dowodu twierdzenia 5.5.1 wystarczy teraz ustalić następujące fakty:

- $i \oplus j$ jest izomorfizmem.
- $\lambda_F$ jest izomorfizmem.
- ${}^{tt}i \oplus {}^{tt}j$ jest izomorfizmem.

Rzeczywiście, wobec przemienności diagramu (★) (lemat 5.5.1), wynika stąd, że $\lambda_P \oplus \lambda_Q$ jest izomorfizmem, to zaś pociąga, że $\lambda_P$ jest izomorfizmem.

Z trzech powyższych stwierdzeń pierwsze jest oczywiste, drugie już udowodniliśmy (zob. twierdzenie 5.4.1), trzecie natomiast udowodnimy teraz. Z przedstawienia modułu $F$ jako sumy prostej modułów $P$ i $Q$ wynika, że mamy rozszczepialny ciąg dokładny

$$0 \to Q \xrightarrow{j} F \xrightarrow{\pi} P \to 0 \tag{5.6}$$

gdzie $\pi$ jest rzutowaniem $F$ na składnik prosty $P$. Na podstawie wniosku 5.2.1, następujący ciąg

$$0 \to P^* \xrightarrow{{}^{t}\pi} F^* \xrightarrow{{}^{t}j} Q^* \to 0$$

jest dokładny i rozszczepia się. Stosując jeszcze raz wniosek 5.2.1 do tego ostatniego ciągu otrzymujemy dokładny i rozszczepialny ciąg

$$0 \to Q^{**} \xrightarrow{{}^{tt}j} F^{**} \xrightarrow{{}^{tt}\pi} P^{**} \to 0. \tag{5.7}$$

Pokażemy, że homomorfizmem rozszczepiającym ${}^{tt}\pi$ jest ${}^{tt}i$, to znaczy, że

$${}^{tt}\pi \circ {}^{tt}i = \mathbf{1}_{P^{**}}.$$

Rzeczywiście, dla $\beta \in P^*$ mamy

$$\begin{aligned} ({}^{tt}\pi \circ {}^{tt}i)(\beta) &= {}^{tt}\pi({}^{tt}i(\beta)) = {}^{tt}\pi(\beta \circ {}^{t}i) = \beta \circ ({}^{t}i \circ {}^{t}\pi) \\ &= \beta \circ {}^{t}(\pi \circ i) = \beta \circ {}^{t}(\mathbf{1}_P) = \beta \circ \mathbf{1}_{P^*} \\ &= \beta. \end{aligned}$$

Na podstawie wniosku 2.3.1 mamy rozkład $F^{**} = \operatorname{im} {}^{tt}i \oplus \operatorname{im} {}^{tt}j \cong P^{**} \oplus Q^{**}$ oraz ${}^{tt}i \oplus {}^{tt}j : P^{**} \oplus Q^{**} \to F^{**}$ jest izomorfizmem.

*Drugi dowód twierdzenia* 5.5.1. Tak jak w pierwszym dowodzie zakładamy, że moduł $F := P \oplus Q$ jest wolny i ma skończoną rangę. Niech $i : P \to P \oplus Q$ oraz $j : Q \to P \oplus Q$ będą kanonicznymi włożeniami. Dla dowodu injektywności homomorfizmu $\lambda_P$ rozpatrujemy diagram

$$\begin{array}{ccc} P & \xrightarrow{\ i\ } & F \\ {\scriptstyle \lambda_P}\downarrow & & \downarrow{\scriptstyle \lambda_F} \\ P^{**} & \xrightarrow[{}^{tt}i]{} & F^{**} \end{array}$$

Diagram ten jest przemienny na podstawie twierdzenia 5.3.1. Zatem

$$\lambda_F \circ i = {}^{tt}i \circ \lambda_P.$$

Na podstawie twierdzenia 5.4.2 homomorfizm $\lambda_F : F \to F^{**}$ jest monomorfizmem i oczywiście także włożenie $i$ jest monomorfizmem. Złożenie monomorfizmów jest monomorfizmem, zatem także ${}^{tt}i \circ \lambda_P$ jest monomorfizmem i wobec tego $\lambda_P$ musi być monomorfizmem.

Załóżmy teraz, że moduł projektywny $P$ jest skończenie generowany. Pokażemy, że $\lambda_P$ jest epimorfizmem. Z przedstawienia modułu $F$ jako sumy prostej modułów $P$ i $Q$ wynika, że mamy rozszczepialny ciąg dokładny (5.6):

$$0 \to Q \xrightarrow{\ j\ } F \xrightarrow{\ \pi\ } P \to 0$$

gdzie $\pi$ jest rzutowaniem $F$ na składnik prosty $P$. Tak jak w pierwszym dowodzie otrzymujemy stąd rozszczepialny ciąg dokładny (5.7):

$$0 \to Q^{**} \xrightarrow{\ {}^{tt}j\ } F^{**} \xrightarrow{\ {}^{tt}\pi\ } P^{**} \to 0.$$

Ciągi (5.6) i (5.7) po połączeniu ich homomorfizmami $\lambda_Q, \lambda_F, \lambda_P$ tworzą następujący przemienny diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & Q & \xrightarrow{\ j\ } & F & \xrightarrow{\ \pi\ } & P & \longrightarrow & 0 \\ \downarrow & & \downarrow{\scriptstyle \lambda_Q} & & \downarrow{\scriptstyle \lambda_F} & & \downarrow{\scriptstyle \lambda_P} & & \downarrow \\ 0 & \longrightarrow & Q^{**} & \xrightarrow{\ {}^{tt}j\ } & F^{**} & \xrightarrow{\ {}^{tt}\pi\ } & P^{**} & \longrightarrow & 0 \end{array}$$

Dwa środkowe kwadraty tego diagramu są przemienne na podstawie twierdzenia 5.3.1. Mamy zatem

$${}^{tt}\pi \circ \lambda_F = \lambda_P \circ \pi.$$

Ponieważ moduł wolny $F$ ma skończoną rangę, $\lambda_F$ jest izomorfizmem na podstawie twierdzenia 5.4.2. Homomorfizm ${}^{tt}\pi$ jest surjekcją wobec dokładności ciągu (5.7). Zatem złożenie tych homomorfizmów jest surjekcją i wobec tego złożenie $\lambda_P \circ \pi$ jest surjekcją. Stąd wynika, że $\lambda_P$ także jest surjekcją. Razem z pierwszą częścią twierdzenia oznacza to, że $\lambda_P$ jest izomorfizmem.

# Rozdział 6

# Moduły nad pierścieniami ideałów głównych

Ostatnie zmiany 04.01.2005 r.

## 6.1 Pojęcia wstępne

W tym rozdziale pokażemy, że skończenie generowane moduły nad pierścieniami euklidesowymi są sumami prostymi podmodułów cyklicznych. Wynika stąd, że każdy skończenie generowany moduł projektywny nad pierścieniem euklidesowym jest modułem wolnym. Faktycznie twierdzenia takie są prawdziwe nad pierścieniami ideałów głównych, ale zajmiemy się tylko nieco prostszym przypadkiem pierścieni euklidesowych.

### 6.1.1 Sumy proste

Przypomnijmy, że $R-$moduł $M$ jest *sumą prostą* swoich podmodułów $N_1, \ldots, N_k$,

$$M = N_1 \oplus \cdots \oplus N_k$$

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 $N_i = Rm_i$ jest generowany przez element $m_i \in M$, to fakt, iż $M$ jest sumą prostą podmodułów $N_i$

$$M = Rm_1 \oplus \cdots \oplus Rm_k$$

oznacza dwie rzeczy: po pierwsze, każdy element $m \in M$ można przedstawić w postaci

$$m = a_1 m_1 + \cdots + a_k m_k, \quad a_1, \ldots, a_k \in R \tag{6.1}$$

oraz, po drugie, przedstawienie to jest jednoznaczne w tym sensie, że jeśli mamy inne przedstawienie

$$m = b_1 m_1 + \cdots + b_k m_k, \quad b_1, \ldots, b_k \in R,$$

to $a_1 m_1 = b_1 m_1, \ldots, a_k m_k = b_k m_k$. Nie wymagamy więc jednoznaczności współczynników $a_i \in R$ ale jednoznaczności składników $a_i m_i \in N_i$.

Jeśli $M$ jest $R-$modułem wolnym z bazą $\mathcal{B} = \{m_1, \ldots, m_k\}$, to $M$ jest sumą prostą podmodułów cyklicznych generowanych przez elementy bazowe,

$$M = Rm_1 \oplus \cdots \oplus Rm_k.$$

Tutaj jednoznaczność przedstawienia elementu $m \in M$ w postaci (6.1) ma mocniejszą własność, mianowicie nie tylko składniki $a_i m_i$ są wyznaczone jednoznacznie, ale także współczynniki $a_i$ są wyznaczone jednoznacznie przez element $m$.

### 6.1.2 Minimalne zbiory generatorów

Niech $M$ będzie modułem skończenie generowanym i niech $\{m_1, \ldots, m_k\}$ będzie zbiorem generatorów modułu $M$. Oznacza to, że $M$ jest (zwykłą) sumą podmodułów cyklicznych $Rm_i$:

$$M = Rm_1 + \cdots + Rm_k.$$

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 $M$. Jeśli zatem $\{m_1, \ldots, m_r\}$ jest minimalnym zbiorem generatorów modułu $M$, to $M$ jest sumą $r$ podmodułów cyklicznych

$$M = Rm_1 + \cdots + Rm_r,$$

ale nie jest sumą mniejszej liczby podmodułów cyklicznych.

W przestrzeniach wektorowych minimalne zbiory generatorów są bazami przestrzeni. Tak jest też w skończenie generowanych modułach wolnych, ale wymaga to dość subtelnego dowodu (zob. dowód twierdzenia 6.2.1).

### 6.1.3 Beztorsyjność

Definicja **6.1.1.** Niech $R$ będzie dowolnym pierścieniem i niech $M$ będzie $R-$modułem.
Element $m \in M$ nazywamy elementem *torsyjnym*, jeśli istnieje element $a \in R,\ a \neq 0$ taki, że $am = 0$.
Moduł $M$ nazywamy modułem *torsyjnym*, jeśli każdy element modułu $M$ jest torsyjny.
$R-$moduł $M$ nazywa się modułem *beztorsyjnym*, jeśli jedynym elementem torsyjnym modułu $M$ jest element zerowy $0 \in M$. Zatem $R-$moduł $M$ jest beztorsyjny wtedy i tylko wtedy gdy ma następującą własność: dla $a \in R$, $m \in M$,

$$am = 0 \quad \Rightarrow \quad a = 0 \quad \text{lub} \quad m = 0.$$

**Przykład 6.1.1.** W grupie abelowej $M$ traktowanej jako $\mathbb{Z}-$moduł 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.
Przestrzenie wektorowe nie dostarczają przykładów modułów torsyjnych: każda niezerowa przestrzeń wektorowa $V$ nad ciałem $K$ jest beztorsyjnym $K-$modułem.

Lemat **6.1.1.** *Każdy moduł wolny $F$ nad pierścieniem $R$ bez dzielników zera jest beztorsyjny.*

*Dowód.* Rzeczywiście, jeśli dla pewnego $f \in F$ oraz $0 \neq a \in R$ 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 $R$ ma dzielniki zera, to moduł wolny nad $R$ zawsze zawiera elementy torsyjne. Na przykład, pierścień $R = \mathbb{Z}/6\mathbb{Z}$ traktowany jako $R-$moduł jest modułem wolnym, ale element $2 + 6\mathbb{Z}$ jest elementem torsyjnym gdyż $(3 + 6\mathbb{Z})(2 + 6\mathbb{Z}) = 0 \in \mathbb{Z}/6\mathbb{Z}$.

## 6.2 Moduły skończenie generowane

Udowodnimy teraz główne twierdzenie o strukturze skończenie generowanych modułów nad pierścieniami euklidesowymi. Przypomnijmy, że pierścień całkowity $R$ nazywa się euklidesowy, jeśli dla $R$ prawdziwe jest twierdzenie o dzieleniu z resztą (względem odpowiedniej normy euklidesowej $N$). Łatwo dowodzi się, że każdy pierścień euklidesowy jest pierścieniem ideałów głównych. Przykładami pierścieni euklidesowych są pierścień $\mathbb{Z}$ liczb całkowitych (z normą $N(a) = |a|$), pierścień $\mathbb{Z}[i]$ liczb całkowitych Gaussa (z normą $N(a + bi) = a^2 + b^2$) oraz pierścień $K[X]$ wielomianów jednej zmiennej nad dowolnym ciałem $K$ (z normą $N(f) = \deg f$).

Twierdzenie **6.2.1.** *Niech $R$ będzie pierścieniem euklidesowym i niech $M$ będzie skończenie generowanym $R-$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.* 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 $R-$modułów o randze $r - 1$. Niech $\{m_1, \ldots, m_r\}$ będzie minimalnym zbiorem generatorów modułu $M$. Wtedy $M = Rm_1 + \cdots + Rm_r$ jest (zwykłą) sumą podmodułów cyklicznych $Rm_i$. Jeśli ta suma jest sumą prostą, to twierdzenie jest udowodnione. W przeciwnym przypadku istnieją $a_1, \ldots, a_r \in R$ takie, że zachodzi równość

$$a_1 m_1 + \cdots + a_r m_r = 0, \tag{6.2}$$

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 (6.2) 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 (6.2). Udowodnimy teraz dwa pomocnicze fakty stwierdzające własności elementu $a_1$.

Fakt 1. Jeśli

$$b_1 m_1 + \cdots + b_r m_r = 0 \tag{6.3}$$

dla pewnych $b_1, \ldots, b_r \in R$, to $a_1$ dzieli $b_1$.

Jeśli $a_1$ nie dzieli $b_1$, to na podstawie euklidesowości pierścienia $R$ istnieją $q, t \in R$ takie, że

$$b_1 = a_1 q + t, \quad t \neq 0, \quad N(t) < N(a_1).$$

Wtedy z (6.2) otrzymujemy $a_1qm_1 + \cdots + a_rqm_r = 0$ i odejmując tę równość od równości (6.3) mamy

$$(b_1 - a_1q)m_1 + \cdots + (b_r - a_rq)m_r = 0.$$

Tutaj $b_1 - a_1q = t$ 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 (6.2).

Przypuśćmy, że $a_1$ nie dzieli $a_2$. Zatem istnieją $q, t \in R$ takie, że

$$a_2 = a_1q + t, \quad t \neq 0, \quad N(t) < N(a_1).$$

Z równości (6.2) otrzymujemy wtedy

$$a_1(m_1 + qm_2) + tm_2 + a_3m_3 + \cdots + a_rm_r = 0. \tag{6.4}$$

Zauważmy, że $\{m_1 + qm_2, m_2, \ldots, m_r\}$ jest także minimalnym zbiorem generatorów modułu $M$ i równość (6.4), w której występuje 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 $a_3, \ldots, a_r$.

**Uwaga 6.2.1.** Jeśli moduł $M$ jest beztorsyjny, to można szybko zakończyć dowód. Rzeczywiście, na podstawie Faktu 2 istnieją $q_2, \ldots, q_r \in R$ takie, że

$$a_2 = a_1q_2, \ldots, a_r = a_1q_r.$$

Wobec tego równość (6.2) przyjmuje postać

$$a_1(m_1 + q_2m_2 + \cdots + q_rm_r) = 0.$$

Ponieważ moduł $M$ jest beztorsyjny oraz $a_1 \neq 0$ wynika stąd, że

$$m_1 + q_2m_2 + \cdots + q_rm_r = 0$$

a zatem $m_1$ jest kombinacją liniową $m_2, \ldots, m_r$. Wobec tego $\{m_2, \ldots, m_r\}$ jest także zbiorem generatorów modułu $M$ wbrew temu, że $\mathsf{rank}\, M = r$. Ta sprzeczność jest konsekwencją przypuszczenia, że przedstawienie $M = Rm_1 + \cdots + Rm_r$ nie jest postaci $M = Rm_1 \oplus \cdots \oplus Rm_r$. A więc w przypadku skończenie generowanego modułu beztorsyjnego minimalny zbiór generatorów wyznacza rozkład modułu na sumę prostą podmodułów cyklicznych. Zauważmy jeszcze, że ze względu na beztorsyjność $M$ w przedstawieniu elementu $m \in M$ w postaci (6.1) nie tylko składniki $a_im_i$ są wyznaczone jednoznacznie, ale także współczynniki $a_i$ są wyznaczone jednoznacznie przez element $m$. Rzeczywiście, jeśli dla generatora $m_i$ mamy $a_im_i = b_im_i$, to $(a_i - b_i)m_i = 0$ i wobec beztorsyjności $M$ otrzymujemy $a_i = b_i$. Minimalny zbiór generatorów skończenie generowanego modułu beztorsyjnego nad pierścieniem euklidesowym jest więc bazą modułu a moduł jest modułem wolnym.

Powracamy teraz do dowodu twierdzenia w ogólnym przypadku (bez założenia, że moduł $M$ jest beztorsyjny). Na podstawie Faktu 2 istnieją $q_2, \ldots, q_r \in R$ takie, że

$$a_2 = a_1q_2, \ldots, a_r = a_1q_r.$$

Wykorzystamy teraz elementy $q_2, \ldots, q_r \in R$ 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 $M_1 := Rm_1^*$ będzie podmodułem cyklicznym generowanym przez $m_1^*$ oraz niech $N := Rm_2 + \cdots + Rm_r$ 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 $b_1, b_2, \ldots, b_r \in R$ 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 $q \in R$ 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 **6.2.1.** *Każdy skończenie generowany moduł beztorsyjny nad pierścieniem euklidesowym jest modułem wolnym.*

*Dowód.* Zobacz uwagę 6.2.1. □

Wniosek **6.2.2.** *Każdy skończenie generowany moduł projektywny $P$ nad pierścieniem euklidesowym $R$ jest $R-$modułem wolnym.*

*Dowód.* Moduł projektywny $P$ jest składnikiem prostym (a więc podmodułem) pewnego $R-$modułu wolnego, który jest beztorsyjny (lemat 6.1.1). A więc $P$ jest beztorsyjny i wobec tego jest wolny na podstawie wniosku 6.2.1.
Nieco inny argument: Na podstawie twierdzenia 6.2.1, moduł $P$ jest sumą prostą modułów cyklicznych. Natomiast moduł cykliczny $Rm$ dla $0 \neq m \in P$ jest izomorficzny z $R-$modułem $R$. Wynika to stąd, że $P$ jest podmodułem modułu wolnego nad pierścieniem bez dzielników zera i wobec tego $am \neq 0$ dla $0 \neq a \in R$ i $0 \neq m \in P$. Stąd $R \to Rm$, $a \mapsto am$ jest izomorfizmem $R-$modułów. □

**Uwaga 6.2.2.** Można udowodnić ogólniejsze twierdzenie: każdy moduł projektywny nad pierścieniem ideałów głównych jest wolny.

Zanotujmy jeszcze wnioski z twierdzenia 6.2.1 dla $\mathbb{Z}-$modułów.

Wniosek **6.2.3.** *Każda skończenie generowana grupa abelowa jest sumą prostą grup cyklicznych.*

Wniosek **6.2.4.** *Każda skończenie generowana beztorsyjna grupa abelowa jest grupą abelową wolną.*

Wniosek **6.2.5.** *Każda skończona grupa abelowa jest sumą prostą grup cyklicznych.*

# Rozdział 7

# Moduły półproste

Ostatnie zmiany 14.01.2005 r.

## 7.1 Moduły proste i półproste

Rozpatrywaliśmy dotąd uogólnienia pojęcia przestrzeni wektorowej związane z istnieniem baz w przestrzeniach wektorowych. Bezpośrednim uogólnieniem jest pojęcie modułu wolnego, ale jak pokazaliśmy, znaczna część własności modułów wolnych przysługuje też szerszej klasie modułów projektywnych. Przestrzenie wektorowe mają jednak jeszcze inne specjalne własności wyróżniające je wśród modułów. Jedną z nich jest fakt, że każda podprzestrzeń przestrzeni wektorowej jest jej składnikiem prostym. Rzeczywiście, jeśli $U$ jest podprzestrzenią $V$ oraz $U \neq V$, to obieramy jakąkolwiek bazę $\mathcal{B}_1$ podprzestrzeni $U$ i dopełniamy ją zbiorem liniowo niezależnych wektorów $\mathcal{B}_2$ do bazy $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ przestrzeni $V$. Jeśli $W$ jest podprzestrzenią $V$ rozpiętą na $\mathcal{B}_2$, to

$$V = U \oplus W.$$

W tym rozdziale rozpatrujemy moduły, które mają podobną własność.

Definicja **7.1.1.** Moduł $M$ nazywamy *półprostym*, jeśli każdy podmoduł $N$ modułu $M$ jest składnikiem prostym modułu $M$.

Przypomnijmy, że moduł $M$ nazywa się *prosty*, jeśli nie ma właściwych podmodułów, to znaczy jedynymi jego podmodułami są 0 i $M$. Oczywiście każdy moduł prosty jest półprosty.

Lemat **7.1.1.** *Jeśli $M$ jest modułem półprostym, to każdy niezerowy podmoduł modułu $M$ zawiera podmoduł prosty.*

*Dowód.* □

**Przykład 7.1.1.** 1. Każda przestrzeń wektorowa jest modułem półprostym.
2. Skończona grupa abelowa jest $\mathbb{Z}-$modułem półprostym wtedy i tylko wtedy, gdy jej rząd nie dzieli się przez kwadrat żadnej liczby pierwszej.
3. Grupy addytywne $\mathbb{Z}$ i $\mathbb{Q}$ traktowane jako $\mathbb{Z}-$moduły nie są półproste, gdyż w ogóle nie zawierają podmodułów prostych.
4. Homomorficzny obraz modułu półprostego jest modułem półprostym. Każdy moduł ilorazowy modułu półprostego jest modułem półprostym.

## 7.2 Charakteryzacja

TWIERDZENIE **7.2.1.** *Dla $R-$modułu $M$ następujące warunki są równoważne.*
(a) *$M$ jest modułem półprostym.*
(b) *$M$ jest sumą podmodułów prostych.*
(c) *$M$ jest sumą prostą podmodułów prostych.*
(d) *Każdy podmoduł modułu $M$ jest sumą podmodułów prostych.*

*Dowód.* □

## 7.3 Pierścienie półproste

Pierścień $R$ nazywa się *lewostronnie półprosty*, jeśli traktowany jako lewostronny $R-$moduł jest modułem półprostym. Podobnie definiuje się pierścień *prawostronnie półprosty*. Następujące twierdzenie pokazuje, że można mówić po prostu *pierścień półprosty*.

TWIERDZENIE **7.3.1.** *Pierścień $R$ jest lewostronnie półprosty wtedy i tylko wtedy gdy jest prawostronnie półprosty.*

*Dowód.* □

TWIERDZENIE **7.3.2.** *Pierścień $R$ jest półprosty wtedy i tylko wtedy gdy każdy lewostronny i każdy prawostronny $R-$moduł jest projektywny.*

*Dowód.* □