§0. Przypomnienie

Definicja.
Zbiór R z działaniami $+, \cdot : R \times R \to R$, wyróżnionymi elementami $0, 1 \in R$ i operacją $- : R \to R$ nazywamy pierścieniem, jeśli spełnione są następujące warunki:

(1) $\forall a, b, c \in R : a + (b + c) = (a + b) + c$,

(2) $\forall a \in R : a + 0 = a = 0 + a$,

(3) $\forall a \in R : a + (-a) = 0 = (-a) + a$,

(4) $\forall a, b \in R : a + b = b + a$,

(5) $\forall a, b, c \in R : a(bc) = (ab)c$,

(6) $\forall a \in R : a \cdot 1 = a = 1 \cdot a$,

(7) $\forall a, b \in R : ab = ba$,

(8) $\forall a, b, c \in R : a(b + c) = ab + ac \wedge (a + b)c = ac + bc$.

Definicja.
Element a pierścienia R nazywamy dzielnikiem zera, jeśli $a \neq 0$ oraz istnieje element $b \in R$, $b \neq 0$, taki, że $ab = 0$.

Definicja.
Pierścień R nazywamy dziedziną (całkowitości), jeśli $0 \neq 1$ oraz w pierścieniu R nie ma dzielników zera.

Stwierdzenie.
Jeśli a, b i c są elementami dziedziny R takimi, że $ac = bc$ oraz $c \neq 0$, to $a = b$.

Definicja.
Element a pierścienia R nazywamy odwracalnym, jeśli istnieje element $b \in R$ taki, że $ab = 1$.

Definicja.
Element a pierścienia R nazywamy nieodwracalnym, jeśli $a \neq 0$ oraz element a nie jest odwracalny.

Definicja.
Pierścień R nazywamy ciałem, jeśli $0 \neq 1$ oraz w pierścieniu R każdy niezerowy element jest odwracalny.

Definicja.
Podzbiór I pierścienia R nazywamy ideałem (piszemy $I \lhd R$), jeśli spełnione są następujące warunki:

(1) $0 \in I$,

(2) $a, b \in I \implies a + b \in I$,

(3) $a \in R \wedge b \in I \implies ab \in I$.

Definicja.
Ideał I pierścienia R nazywamy właściwym, jeśli $I \neq R$.

Definicja.
Najmniejszy ideał pierścienia R zawierający podzbiór $X \subset R$ nazywamy ideałem generowanym przez zbiór X i oznaczamy (X).

Definicja.
Ideał I pierścienia R nazywamy głównym, jeśli istnieje element $a \in R$ taki, że $I = (a)$.

Definicja.
Dziedzinę R nazywamy dziedziną ideałów głównych, jeśli wszystkie ideały w pierścieniu R są główne.

Oznaczenie.
Niech X i Y będą podzbiorami pierścienia R, $a \in R$. Definiujemy

$$X + Y := \{x + y \mid x \in X, y \in Y\},$$
$$a + X := \{a + x \mid x \in X\},$$
$$Xa := \{xa \mid x \in X\}.$$

Stwierdzenie.
Jeśli $a_1, \ldots, a_n$ są elementami pierścienia R, to

$$(a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n.$$

Definicja.
Podzbiór S pierścienia R nazywamy podpierścieniem, jeśli spełnione są następujące warunki:

(1) $0, 1 \in S$,

(2) $a, b \in S \implies a + b, ab \in S$,

(3) $a \in S \implies -a \in S$.

Definicja.
Niech R i S będą pierścieniami. Funkcję $\varphi : R \to S$ nazywamy homomorfizmem pierścieni jeśli

$$\varphi(0) = 0, \qquad \varphi(a+b) = \varphi(a) + \varphi(b),$$
$$\varphi(1) = 1, \qquad \varphi(ab) = \varphi(a)\varphi(b),$$

dla dowolnych elementów $a, b \in R$.

Definicja.
Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to jądrem homomorfizmu φ nazywamy zbiór

$$\operatorname{Ker}\varphi := \{a \in R \mid \varphi(a) = 0\}.$$

Uwaga.
Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to zbiór $\operatorname{Ker}\varphi$ jest ideałem pierścienia R.

Definicja.
Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to obrazem homomorfizmu φ nazywamy zbiór

$$\operatorname{Im}\varphi := \{\varphi(a) \mid a \in R\}.$$

Uwaga.
Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to zbiór $\operatorname{Im}\varphi$ jest podpierścieniem pierścienia S.

Definicja.
Homomorfizm pierścieni $\varphi : R \to S$ nazywamy monomorfizmem, jeśli funkcja φ jest injekcją.

Uwaga.
Homomorfizm pierścieni $\varphi : R \to S$ jest monomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker}\varphi = 0 := \{0\}$.

Definicja.
Homomorfizm pierścieni $\varphi : R \to S$ nazywamy epimorfizmem, jeśli funkcja φ jest surjekcją.

Uwaga.
Homomorfizm pierścieni $\varphi : R \to S$ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{Im}\varphi = S$.

Definicja.
Homomorfizm pierścieni $\varphi : R \to S$ nazywamy izomorfizmem, jeśli istnieje homomorfizm $\psi : S \to R$ taki, że $\psi\varphi = \mathrm{Id}_R$ i $\varphi\psi = \mathrm{Id}_S$.

Uwaga.
Homomorfizm pierścieni $\varphi : R \to S$ jest izomorfizmem wtedy i tylko wtedy, gdy jest monomorfizmem i epimorfizmem.

Definicja.
Jeśli I jest ideałem pierścienia R, to w zbiorze $R/I := \{a + I \mid a \in R\}$ definiujemy działania

$$(a + I) + (b + I) := (a + b) + I,$$
$$(a + I)(b + I) := ab + I.$$

Definicje te są poprawne oraz definiują w zbiorze R/I strukturę pierścienia, z elementami wyróżnionymi $0 + I$ i $1 + I$, oraz operacją $-(a + I) := -a + I$, nazywanego pierścieniem ilorazowym. Odwzorowanie

$$R \to R/I, a \mapsto a + I,$$

jest epimorfizmem pierścieni, który nazywany naturalnym rzutowaniem.

Definicja.
Ideał I pierścienia R nazywamy pierwszym, jeśli $I \neq R$ oraz spełniony jest warunek

$$ab \in I \implies a \in I \vee b \in I.$$

Uwaga.
Ideał I pierścienia R jest pierwszy wtedy i tylko wtedy, gdy pierścień R/I jest dziedziną.

Definicja.
Ideał I pierścienia R nazywamy maksymalnym, jeśli $I \neq R$ oraz spełniony jest warunek

$$J \lhd R \wedge I \subset J \implies J = I \vee J = R.$$

Uwaga.
Ideał I pierścienia R jest maksymalny wtedy i tylko wtedy, gdy pierścień R/I jest ciałem.

Uwaga.
Każdy ideał maksymalny jest pierwszy.

Uwaga.

Jeśli I jest ideałem właściwym pierścienia R, to istnieje ideał maksymalny J pierścienia R taki, że $I \subset J$.

Motywacja — teoria podzielności

Twierdzenie.

Jeśli $n \in \mathbb{N}$, $n \geq 2$, to istnieją jednoznacznie wyznaczone liczby pierwsze $p_1 < \cdots < p_k$, $k \geq 1$, oraz wykładniki $\alpha_1, \ldots, \alpha_k > 0$ takie, że

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Twierdzenie.

Jeśli $f \in \mathbb{C}[X]$ jest wielomianem unormowanym stopnia dodatniego, to istnieją jednoznacznie wyznaczone (z dokładnością do porządku) unormowane wielomiany $f_1, \ldots, f_k$, $k \geq 1$, stopnia 1 takie, że

$$f = f_1 \cdots f_k.$$

Motywacja — teoria modułów

Twierdzenie.

Jeśli G jest skończenie generowaną grupą abelową, to istnieją jednoznacznie wyznaczone liczby pierwsze $p_1 < \cdots < p_k$, $k \geq 0$, oraz wykładniki $\alpha \geq 0$, $\alpha_{i,1} \geq \cdots \geq \alpha_{i,l_i} > 0$, $l_i > 0$, $i = 1, \ldots, k$, takie, że

$$G \simeq \mathbb{Z}^{\alpha} \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} \mathbb{Z}_{p_i^{\alpha_{i,j}}}.$$

Literatura

(1) Thomas Hungerford, Algebra.

(2) Karlheinz Spindler, Abstract Algebra with Applications, vol. II, Rings and Fields.

(3) Jerzy Browkin, Teoria ciał.

§1. Teoria podzielności w dziedzinach

Założenie.
Przez cały paragraf R oznaczać będzie dziedzinę.

Definicja.
Mówimy, że element $a \in R$ dzieli element $b \in R$ (piszemy $a \mid b$), jeśli istnieje element $c \in R$ taki, że $b = ca$.

Oznaczenie.
Jeśli $a, b, c \in R$, $a \neq 0$, to $\frac{b}{a} := c$ (przypomnijmy, że element c jest jednoznacznie wyznaczony).

Przykład.
Jeśli $a \in R$, to $a \mid a$ ($\frac{a}{a} = 1$), $1 \mid a$ ($\frac{a}{1} = a$) oraz $a \mid 0$ ($\frac{0}{a} = 0$).

Uwaga.
Jeśli $a, b, c \in R$, $a \mid b$ oraz $b \mid c$, to $a \mid c$.

Definicja.
Mówimy, że elementy $a, b \in R$ są stowarzyszone (piszemy $a \approx b$), jeśli $a \mid b$ i $b \mid a$.

Przykład.
Niech $a, b \in \mathbb{Z}$. Wtedy $a \approx b$ wtedy i tylko wtedy, gdy $a = \pm b$.

Przykład.
Jeśli $a \in R$, to $a \mid 1$ wtedy i tylko wtedy, gdy element a jest odwracalny. Zatem $a \approx 1$ wtedy i tylko wtedy, gdy element a jest odwracalny.

Przykład.
Jeśli $a \in R$, to $0 \mid a$ wtedy i tylko wtedy, gdy $a = 0$. Zatem $a \approx 0$ wtedy i tylko wtedy, gdy $a = 0$.

Stwierdzenie 1.1.

Jeśli $a, b \in R$, to:

(1) $a \mid b$ wtedy i tylko wtedy, gdy $(b) \subset (a)$,

(2) $a \approx b$ wtedy i tylko wtedy, gdy $(a) = (b)$,

(3) $\approx$ jest relacją równoważności,

(4) $a \approx b$ wtedy i tylko wtedy, gdy istnieje element odwracalny $c \in R$ taki, że $a = cb$,

(5) element a jest odwracalny wtedy i tylko wtedy, gdy $a \mid c$ dla wszystkich elementów $c \in R$,

(6) element a jest odwracalny wtedy i tylko wtedy, gdy $(a) = R$.

Dowód.

(1) $a \mid b \Leftrightarrow \exists c \in R : b = ca \Leftrightarrow b \in Ra = (a) \Leftrightarrow (b) \subset (a)$.

(2) Wynika natychmiast z punktu (1).

(3) Wynika natychmiast z punktu (2).

(4) Gdy $a = 0$, to teza jest oczywista, więc załóżmy, że $a \neq 0$.
Jeśli $a \approx b$, to istnieją elementy $c, d \in R$ takie, że $a = cb$ oraz $b = da$. Wtedy $a = (cd)a$, więc $cd = 1$, zatem element c jest odwracalny.
Jeśli $a = cb$ dla elementu odwracalnego $c \in R$, to oczywiście $b \mid a$. Ponadto istnieje element $d \in R$ taki, że $dc = 1$. Wtedy $b = dcb = da$, więc $a \mid b$, zatem $a \approx b$.

(5) Teza wynika z faktu, że $a \mid c$ dla dowolnego elementu $c \in R$ wtedy i tylko wtedy, gdy $a \mid 1$

(6) Element a jest odwracalny wtedy i tylko wtedy, gdy $a \approx 1$, a więc wtedy i tylko wtedy, gdy $(a) = (1) = R$.

Definicja.

Element $p \in R$ nazywamy nierozkładalnym, jeśli element p jest nieodwracalny oraz, jeśli $a \mid p$, to $a \approx p$ lub element a jest odwracalny.

Uwaga.

Ostatni warunek powyższej definicji jest równoważny każdemu z dwóch poniższych warunków:

(1) jeśli $p = ab$, to jeden z elementów a i b jest odwracalny,

(2) jeśli $p = ab$, to $a \approx p$ lub $b \approx p$.

Definicja.

Element $p \in R$ nazywamy pierwszym, jeśli element p jest nieodwracalny oraz, jeśli $p \mid ab$, to $p \mid a$ lub $p \mid b$.

Przykład.

$p \in \mathbb{Z}$ jest elementem nierozkładalnym wtedy i tylko wtedy, gdy jest elementem pierwszym, oraz wtedy i tylko wtedy, gdy jedna z liczb p i $-p$ jest pierwsza.

Przykład.

Niech $\mathbb{Z}[\sqrt{5}] := \{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\}$. Wtedy 2 jest elementem nierozkładalnym w dziedzinie $\mathbb{Z}[\sqrt{5}]$, ale nie jest elementem pierwszym.

Stwierdzenie 1.2.

Jeśli $p \in R$, $p \neq 0$, to:

(1) element p jest pierwszy wtedy i tylko wtedy, gdy ideał (p) jest pierwszy,

(2) element p jest nierozkładalny wtedy i tylko wtedy, gdy $(p) \neq R$ oraz spełniony jest warunek

$$(p) \subset (a) \implies (a) = (p) \vee (a) = R,$$

(3) jeśli element p jest pierwszy, to element p jest nierozkładalny,

(4) jeśli R jest dziedziną ideałów głównych oraz element p jest nierozkładalny, to element p jest pierwszy,

(5) jeśli element p jest pierwszy oraz $q \approx p$, to element q jest pierwszy,

(6) jeśli element p jest nierozkładalny oraz $q \approx p$, to element q jest nierozkładalny.

Dowód.

(1) Zauważmy, iż warunek, że element p nieodwracalny, jest równoważny warunkowi $(p) \neq R$ na mocy Stwierdzenia 1.1 (6). Podobnie, warunek

$$p \mid ab \implies p \mid a \vee p \mid b$$

jest równoważny warunkowi

$$ab \in (p) \implies a \in (p) \vee b \in (p)$$

na mocy Stwierdzenia 1.1 (1).

(2) Musimy sprawdzić, że warunek

$$a \mid p \implies a \approx p \vee \text{element } a \text{ jest odwracalny},$$

jest równoważny warunkowi

$$(p) \subset (a) \implies (a) = (p) \vee (a) = R,$$

co wynika ze Stwierdzenia 1.1 (1), (2) oraz (6).

(3) Przypuśćmy, że element p jest pierwszy. Musimy pokazać, że jeśli $p = ab$, to $a \approx p$ lub $b \approx p$. Ponieważ element p jest pierwszy, więc w powyższej sytuacji $p \mid a$ lub $p \mid b$. W pierwszym przypadku $p \approx a$, w drugim zaś $p \approx b$.

(4) Jeśli R jest dziedziną ideałów głównych oraz element p jest nierozkładalny, to ideał (p) jest maksymalny na mocy punktu (2), więc jest także pierwszy, zatem element p jest pierwszy na mocy punktu (1).

(5) Wynika ze Stwierdzenia 1.1 (2) oraz punktu (1) (zauważmy, że $q \neq 0$, gdyż $p \neq 0$).

(6) Wynika ze Stwierdzenia 1.1 (2) oraz punktu (2) (zauważmy, że $q \neq 0$, gdyż $p \neq 0$).

Definicja.

Dziedzinę R nazywamy dziedziną z rozkładem, jeśli dla każdego nieodwracalnego elementu $a \in R$, istnieją elementy nierozkładalne $p_1, \ldots, p_k \in R$, takie, że $a = p_1 \cdots p_k$.

Definicja.

Dziedzinę z rozkładem R nazywamy dziedziną z jednoznacznością rozkładu, jeśli dla dowolnych elementów nierozkładalnych $p_1, \ldots, p_k$, $q_1, \ldots, q_l \in R$ takich, że $p_1 \cdots p_k = q_1 \cdots q_l$, mamy $k = l$ oraz istnieje permutacja σ zbioru $\{1, \ldots, k\}$ taka, że $p_i \approx q_{\sigma(i)}$, $i = 1, \ldots, k$.

Przykład.

Pierścień $\mathbb{Z}[\sqrt{5}]$ jest dziedziną z rozkładem, która nie dziedziną z jednoznacznością rozkładu.

Lemat 1.3.

Jeśli p, $q_1, \ldots, q_k$ są elementami nierozkładalnymi dziedziny z jednoznacznością rozkładu R takimi, że $p \mid q_1 \cdots q_k$, to istnieje $i \in \{1, \ldots, k\}$ takie, że $p \mid q_i$.

Dowód.

Istnieje element $a \in R$ taki, że $pa = q_1 \cdots q_k$. Oczywiście $a \neq 0$. Jeśli element a jest odwracalny, to element pa jest nierozkładalny na mocy Stwierdzeń 1.1 (4) oraz 1.2 (6), więc z jednoznaczności rozkładu wynika, że $k = 1$ i $p \approx pa = q_1$. W szczególności $p \mid q_1$. Jeśli element a jest nieodwracalny, to istnieją elementy nierozkładalne $p_1, \ldots, p_l \in R$ takie, że $a = p_1 \cdots p_l$. Wtedy $pp_1 \cdots p_l = q_1 \cdots q_k$, więc z jednoznaczności rozkładu wynika, że $p \approx q_i$ dla pewnego $i \in \{1, \ldots, k\}$. W szczególności $p \mid q_i$, co kończy dowód.

Lemat 1.4.

W dziedzinie z jednoznacznością rozkładu element jest pierwszy wtedy i tylko wtedy, gdy jest nierozkładalny.

Dowód.

Wiemy już, że elementy pierwsze są nierozkładalne (Stwierdzenie 1.2 (3)). Przypuśćmy, że element p dziedziny R z jednoznacznością rozkładu jest nierozkładalny. Musimy pokazać, że jeśli $p \mid ab$, to $p \mid a$ lub $a \mid b$. Jeśli $a = 0$ lub $b = 0$, to teza jest oczywista. Podobnie jest, gdy jeden z elementów a i b jest odwracalny. Zatem możemy założyć, że elementy a i b są nieodwracalne. Wtedy istnieją elementy nierozkładalne $q_1, \ldots, q_k, q_{k+1}, \ldots, q_{k+l} \in R$, $k, l > 0$, takie, że $a = q_1 \cdots q_k$ oraz $b = q_{k+1} \cdots q_{k+l}$. Wtedy $p \mid q_1 \cdots q_{k+l}$, więc na mocy poprzedniego lematu istnieje $i \in \{1, \ldots, k + l\}$ takie, że $p \mid q_i$. Jeśli $i \leq k$, to $p \mid a$, w przeciwnym wypadku $p \mid b$.

Lemat 1.5.

Jeśli elementy $p_1, \ldots, p_k, q_1, \ldots, q_l \in R$ są pierwsze oraz $p_1 \cdots p_k = q_1 \cdots q_l$, to $k = l$ oraz istnieje permutacja σ zbioru $\{1, \ldots, k\}$ zbioru taka, że $p_i \approx q_{\sigma(i)}$ dla $i = 1, \ldots, k$.

Dowód.

Indukcja ze względu na k.

Ponieważ $p_k \mid q_1 \cdots q_l$, więc $p_k \mid q_i$ dla pewnego $i \in \{1, \ldots, l\}$. Bez straty ogólności możemy założyć, że $i = l$. Ponieważ, element q_l jest nierozkładalny na mocy Stwierdzenia 1.2 (3), więc $p_k \approx q_l$, zatem na mocy Stwierdzenia 1.1 (4) istnieje element odwracalny $a \in R$ taki, że $q_l = ap_k$. Wtedy $p_1 \cdots p_{k-1}p_k = q_1 \cdots q_{l-1}ap_k$.

Załóżmy najpierw, że $k = 1$. Gdyby $l > 1$, to otrzymalibyśmy, że $1 = q_1 \cdots q_{l-1}a$, co jest niemożliwe, gdyż element q_1 jest nieodwracalny. Zatem $l = 1$, co kończy dowód w tym przypadku.

Załóżmy teraz, że $k > 1$. Gdyby $l = 1$, to podobnie jak wcześniej wykorzystując równość $p_1 \cdots p_{k-1} = a$ otrzymalibyśmy sprzeczność. Zatem $l > 1$. Definiujemy $q'_1 := q_1, \ldots, q'_{l-2} := q_{l-2}, q'_{l-1} := q_{l-1}a$. Wtedy elementy $q'_1, \ldots, q'_{l-1}$ są pierwsze (Stwierdzenie 1.2 (6)) oraz $p_1 \cdots p_{k-1} = q'_1 \cdots q'_{l-1}$. Z założenia indukcyjnego $k-1 = l-1$ oraz istnieje permutacja σ zbioru $\{1, \ldots, k-1\}$ taka, że $p_i \approx q'_{\sigma(i)} \approx q_{\sigma(i)}$ dla $i = 1, \ldots, k-1$, co kończy dowód.

Wniosek 1.6.

Dziedzina z rozkładem R jest dziedziną z jednoznacznością rozkładu wtedy i tylko wtedy, gdy każdy element nierozkładalny w dziedzinie R jest pierwszy.

Uwaga.

Istnieją przykłady dziedzin, w których każdy element nierozkładalny jest pierwszy, ale które nie są dziedzinami z rozkładem.

Lemat 1.7.

Jeśli I_1, I_2, ... są ideałami dziedziny ideałów głównych R takimi, że $I_i \subset I_{i+1}$ dla $i = 1, 2, \ldots$, to istnieje $k > 0$ takie, że $I_i = I_k$ dla $i = k, k+1, \ldots$.

Dowód.

Niech $I := \bigcup_{i \geq 1} I_i$. Wtedy $I \lhd R$ (!). Pierścień R jest dziedziną ideałów głównych, więc istnieje element $a \in R$ taki, że $I = (a)$. Istnieje $k > 0$ takie, że $a \in I_k$. Wtedy $I_i \subset I = (a) \subset I_k \subset I_i$ dla $i = k, k+1, \ldots$, co kończy dowód.

Oznaczenie.

Niech S będzie zbiorem takich elementów nieodwracalnych $a \in R$, dla których nie istnieją elementy nierozkładalne $p_1, \ldots, p_k \in R$ takie, że $a = p_1 \cdots p_k$.

Lemat 1.8.
Istnieje funkcja $f : S \to S$ taka, że $(a) \subsetneq (f(a))$ dla każdego $a \in S$.

Dowód.
Ustalmy element $a \in S$. Element a nie jest nierozkładalny, więc istnieją elementy $b, c \in R$ takie, że $a = bc$ oraz $b, c \not\approx a$. W szczególności $(a) \subsetneq (b)$ oraz $(a) \subsetneq (c)$. Ponadto $b \in S$ lub $c \in S$.

Lemat 1.9.
Jeśli pierścień R jest dziedziną ideałów głównych, to pierścień R jest dziedziną z rozkładem.

Dowód.
Musimy pokazać, że $S = \varnothing$. Przypuśćmy, że $S \neq \varnothing$ oraz ustalmy element $a \in S$. Niech $I_i := (f^{i-1}(a))$ dla $i = 1, 2, \ldots$. Wtedy $I_i \subsetneq I_{i+1}$ dla $i = 1, 2, \ldots$, co jest sprzeczne z Lematem 1.7.

Twierdzenie 1.10.
Jeśli pierścień R jest dziedziną ideałów głównych, to pierścień R jest dziedziną z jednoznacznością rozkładu.

Dowód.
Ponieważ każdy element nierozkładalny dziedziny R jest pierwszy na mocy Stwierdzenia 1.2 (4), więc teza wynika z poprzedniego lematu oraz Wniosku 1.6.

Definicja.
Dziedzinę R nazywamy dziedziną Euklidesa, jeśli istnieje funkcja $\varphi : R \to \mathbb{N}$ taka, że

(1) $\varphi(a) = 0$ wtedy i tylko wtedy, gdy $a = 0$,

(2) jeśli $a, b \in R$ i $b \neq 0$, to istnieją elementy $c, d \in R$ takie, że $a = cb + d$ oraz $\varphi(d) < \varphi(b)$.

Przykład.
Dowolne ciało K wraz z funkcją $K \to \mathbb{N}$, $a \mapsto 1$, gdy $a \neq 0$, oraz $a \mapsto 0$, gdy $a = 0$, jest dziedziną Euklidesa.

Przykład.
$\mathbb{Z}$ wraz z funkcją $\mathbb{Z} \to \mathbb{N}$, $n \mapsto |n|$, jest dziedziną Euklidesa.

Przykład.
$\mathbb{Z}[\imath]$ wraz z funkcją $\mathbb{Z}[\imath] \to \mathbb{N}$, $a + b\imath \mapsto a^2 + b^2$, jest dziedziną Euklidesa.

Twierdzenie 1.11.

Każda dziedzina Euklidesa jest dziedziną ideałów głównych. W szczególności, każda dziedzina Euklidesa jest dziedziną z jednoznacznością rozkładu.

Dowód.

Niech $I \lhd R$. Możemy założyć, że $I \neq 0$. Wybierzmy element $a \in I$ taki, że $\varphi(a) = \min\{\varphi(b) \mid b \in I, b \neq 0\}$. Wtedy $I = (a)$. Istotnie, oczywiście $(a) \subset I$. Z drugiej strony, gdy $b \in I$, to istnieją elementy $c, d \in R$ takie, że $b = ca + d$ i $\varphi(d) < \varphi(a)$. Wtedy $d = b - ca \in I$, więc z wyboru elementu a wynika, że $d = 0$. Zatem $b = ca \in Ra = (a)$, co kończy dowód.

Przykład.

$\mathbb{Z}[\frac{1+\sqrt{19}i}{2}]$ jest dziedziną ideałów głównych, która nie jest dziedziną Euklidesa.

Lemat 1.12.

Niech a będzie niezerowym elementem dziedziny z rozkładem R. Załóżmy, że elementy $p_1, \ldots, p_k \in R$ są nierozkładalne oraz takie, że jeśli element $q \in R$ jest nierozkładalny oraz $q \mid a$, to istnieje j takie, że $q \approx p_j$. W powyższej sytuacji istnieją wykładniki $\alpha_1, \ldots, \alpha_k \geq 0$ oraz element odwracalny $b \in R$ takie, że

$$a = bp_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Dowód.

Jeśli element a jest odwracalny, to $b := a$ oraz $\alpha_i := 0$, $i = 1, \ldots, k$. Jeśli element a jest nieodwracalny, to istnieją elementy nierozkładalne $q_1, \ldots, q_l \in R$ takie, że $a = q_1 \cdots q_l$. Z własności elementów $p_1, \ldots, p_k$ wynika, że dla każdego $i = 1, \ldots, l$ istnieją element nierozkładalny $b_i \in R$ oraz $j_i \in \{1, \ldots, k\}$ takie, że $q_i = b_i p_{j_i}$. Wtedy $b := b_1 \cdots b_k$ oraz $\alpha_j := |\{i \in \{1, \ldots, l\} \mid j_i = j\}|$.

Lemat 1.13.

Jeśli R jest dziedziną z jednoznacznością rozkładu, element $a \in R$ jest odwracalny, elementy $p_1, \ldots, p_k \in R$ są nierozkładalne i parami niestowarzyszone, $\alpha_1, \ldots, \alpha_k \geq 0$, i $b \mid ap_1^{\alpha_1} \cdots p_k^{\alpha_k}$, to istnieją wykładniki $\beta_i \in \{0, \ldots, \alpha_i\}$, $i = 1, \ldots, k$, oraz element nierozkładalny $c \in R$ takie, że

$$b = cp_1^{\beta_1} \cdots p_k^{\beta_k}.$$

Dowód.

Niech $q \in R$ będzie elementem nierozkładalnym takim, że $q \mid b$. Wtedy $q \mid ap_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Ponieważ q jest elementem pierwszym, więc istnieje $i \in \{1, \ldots, k\}$ takie, że $q \mid p_i$ ($q \nmid a$, gdyż element q nie jest odwracalny). Ponieważ element p_i jest nierozkładalny, więc $q \approx p_i$. Z poprzedniego lematu wynika zatem, że istnieją element odwracalny $c \in R$ oraz wykładniki $\beta_1, \ldots, \beta_k \geq 0$ takie, ze $b = cp_1^{\beta_1} \cdots p_k^{\beta_k}$. Gdyby $\beta_i > \alpha_i$ dla pewnego i, to $p_i \mid ap_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}$, co prowadziłoby do wniosku, że $p_i \mid p_j$ dla $j \neq i$, a więc do sprzeczności.

Wniosek 1.14.

Jeśli R jest dziedziną z jednoznacznością rozkładu, elementy $a, b \in R$ są nieodwracalne, elementy $p_1, \ldots, p_k \in R$ są nierozkładalne i parami niestowarzyszone, $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \geq 0$, oraz

$$ap_1^{\alpha_1} \cdots p_k^{\alpha_k} = bp_1^{\beta_1} \cdots p_k^{\beta_k}$$

to $a = b$ oraz $\alpha_i = \beta_i$, $i = 1, \ldots, k$.

Definicja.

Niech X będzie podzbiorem dziedziny R. Element $a \in R$ nazywamy największym wspólnym dzielnikiem elementów zbioru X wtedy i tylko wtedy, gdy spełnione są następujące warunki:

(1) $a \mid b$ dla wszystkich $b \in X$,

(2) jeśli $c \mid b$ dla wszystkich $b \in X$, to $c \mid a$.

Uwaga.

Jeśli element a dziedziny R jest największym wspólnym dzielnikiem elementów zbioru $X \subset R$, to element $b \in R$ jest największym wspólnym dzielnikiem elementów zbioru X wtedy i tylko wtedy, gdy $b \approx a$.

Definicja.

Jeśli 1 jest największym wspólnym dzielnikiem elementów zbioru $X \subset R$, to mówimy, że elementy zbioru X są względnie pierwsze.

Stwierdzenie 1.15.

Niech $a_1, \ldots, a_k$ będą elementami dziedziny z jednoznacznością rozkładu R.

(1) Istnieje największy wspólny dzielnik elementów $a_1, \ldots, a_k$. Dokładniej, jeśli

$$a_i = b_i p_1^{\alpha_{i,1}} \cdots p_l^{\alpha_{i,l}}, \quad i = 1, \ldots, k,$$

dla elementów nieodwracalnych $b_1, \ldots, b_k$, parami niestowarzyszonych elementów nierozkładalnych $p_1, \ldots, p_l$ oraz wykładników $\alpha_{i,j} \geq 0$, $i = 1, \ldots, k$, $j = 1, \ldots, l$, to

$$p_1^{\min(\alpha_{1,1},\ldots,\alpha_{k,1})} \cdots p_l^{\min(\alpha_{1,l},\ldots,\alpha_{k,l})}$$

jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_k$.

(2) Jeśli R jest dziedzina ideałów głównych, to element $b \in R$ jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_k$ wtedy i tylko wtedy, gdy

$$(b) = (a_1) + \cdots + (a_k).$$

Dowód.

(1) Wynika bezpośrednio z Lematu 1.13.

(2) Teza wynika z obserwacji, że $c \mid a_i$, $i = 1, \ldots, k$, wtedy i tylko wtedy, gdy $(c) \supseteq (a_1) + \cdots + (a_k)$.

Uwaga.

Jeśli elementy a i b dziedziny z jednoznacznością rozkładu są względnie pierwsze i $a \mid bc$, to $a \mid c$.

Uwaga.

Niech $b \in R$ będzie największym wspólnym dzielnikiem elementów $a_1, \ldots, a_k \in R$. Jeśli element $c \in R$, $c \neq 0$, jest wspólnym dzielnikiem elementów $a_1, \ldots, a_k$, to element $\frac{b}{c}$ jest największym wspólnym dzielnikiem elementów $\frac{a_1}{c}, \ldots, \frac{a_k}{c}$.

Dowód.

Ponieważ $b \mid a_i$ dla $i = 1, \ldots, k$, więc $\frac{b}{c}$ jest wspólnym dzielnikiem elementów $\frac{a_1}{c}, \ldots, \frac{a_k}{c}$. Ponadto, jeśli d jest wspólnym dzielnikiem elementów $\frac{a_1}{c}, \ldots, \frac{a_k}{d}$, to dc jest wspólnym dzielnikiem elementów $a_1, \ldots, a_k$, więc $dc \mid b$, skąd $d \mid \frac{b}{c}$, co kończy dowód.

Uwaga.

Niech $a_1, \ldots, a_k$ będą elementami dziedziny z jednoznacznością rozkładu R. Jeśli element $b \in R$ jest największym wspólnym dzielnikiem elementów a_1, $\ldots$, a_k, to dla dowolnego elementu $a \in R$ element ab jest największym wspólnym dzielnikiem elementów aa_1, $\ldots$, aa_k.

Dowód.

Jeśli $a = 0$, to teza jest oczywista. Załóżmy zatem, że $a \neq 0$. Niech c będzie największym wspólnym dzielnikiem elementów aa_1, $\ldots$, aa_k. Wtedy z poprzedniej uwagi wynika, że element $\frac{c}{a}$ jest największym wspólnym dzielnikiem elementów a_1, $\ldots$, a_k, zatem $\frac{c}{a} \approx b$, co kończy dowód.

§2. Teoria podzielności w pierścieniach wielomianów

Założenie.
Przez cały paragraf R oznaczać będzie dziedzinę.

Twierdzenie 2.1 (Algorytm dzielenia).
Jeśli $F, G \in R[X]$, $G \neq 0$, oraz współczynnik wiodący wielomianu G jest odwracalny, to istnieją jednoznacznie wyznaczone wielomiany $Q, H \in R[X]$ takie, że

$$F = QG + H \quad \text{i} \quad \deg P < \deg H.$$

Dowód.
Istnienie wielomianów Q i H udowodnimy poprzez indukcję ze względu na $\deg F$. Jeśli $\deg F < \deg G$, to kładziemy $Q := 0$ i $P := F$. Przypuśćmy teraz, że $k := \deg F \geq \deg G =: l$. Niech a będzie współczynnikiem wiodącym wielomianu F oraz niech b będzie współczynnikiem wiodącym wielomianu G. Dla $c := b^{-1}a$ mamy $\deg(F - cX^{k-l}G) < \deg F$, więc na mocy założenia indukcyjnego istnieją wielomiany $Q, H \in R[X]$ takie, że

$$F - cX^{k-l}G = QG + H \quad \text{i} \quad \deg H < \deg G.$$

Wtedy $F = (cX^{n-m} + Q)G + H$.

Dla dowodu jednoznaczności załóżmy, że

$$Q_1G + H_1 = Q_2G + H_2$$

dla $Q_1, Q_2, H_1, H_2 \in R[X]$, przy czym $\deg H_1, \deg H_2 < \deg G$. Wtedy $(Q_1 - Q_2)G = H_2 - H_1$, więc

$$\deg(Q_1 - Q_2) + \deg G = \deg((Q_1 - Q_2)G) = \deg(H_2 - H_1) < \deg G,$$

co jest możliwe tylko, gdy $\deg(Q_1 - Q_2) = -\infty$, więc $Q_1 = Q_2$, skąd też $H_1 = H_2$.

Wniosek 2.2.
Jeśli K jest ciałem, to pierścień $K[X]$ jest dziedziną Euklidesa. W szczególności, pierścień $K[X]$ jest dziedziną ideałów głównych oraz dziedziną z jednoznacznością rozkładu.

Dowód.
Wystarczy rozważyć funkcję $K[X] \to \mathbb{N}$, $F \mapsto 2^{\deg F}$.

Wniosek 2.3 (Twierdzenie o reszcie).
Jeśli $F \in R[X]$ oraz $a \in R$, to istnieje wielomian $Q \in R[X]$ taki, że

$$F = (X - a)Q + F(a). \quad \square$$

Definicja.

Mówimy, że element $a \in R$ jest pierwiastkiem wielomianu $F \in R[X]$, jeśli $F(a) = 0$.

Twierdzenie 2.4.

Jeśli $F \in R[X]$, to element $a \in R$ jest pierwiastkiem wielomianu F wtedy i tylko wtedy, gdy $X - a \mid F$.

Dowód.

Jeśli element $a \in R$ jest pierwiastkiem wielomianu F, to $X - a \mid F$ na mocy powyższego wniosku. Z drugiej strony, gdy $X - a \mid F$, to istnieje wielomian $Q_1 \in R[X]$ taki, że $F = Q_1(X - a)$. Z poprzedniego wniosku wiemy też, że istnieje wielomian $Q_2 \in R[X]$ taki, że $F = Q_2(X - a) + F(a)$. Ponieważ $\deg 0, \deg F(a) < \deg(X - a)$, więc z Twierdzenia 2.1 wynika, że $F(a) = 0$.

Konstrukcja.

Definiujemy

$$K := (R \times R \setminus \{0\})/\sim$$

gdzie

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

Oznaczamy

$$\tfrac{a}{b} := [(a, b)]_\sim.$$

W zbiorze K definiujemy działania $+$ i $\cdot$ wzorami

$$\tfrac{a}{b} + \tfrac{c}{d} := \tfrac{ad+bc}{bd},$$
$$\tfrac{a}{b} \cdot \tfrac{c}{d} := \tfrac{ac}{bd}.$$

Zbiór K wraz z powyższymi działaniami, elementami wyróżnionymi $\frac{0}{1}$ i $\frac{1}{1}$, oraz operacją $\frac{a}{b} \mapsto \frac{-a}{b}$, jest ciałem, który nazywamy ciałem ułamków dziedziny R. Funkcja

$$R \ni a \mapsto \tfrac{a}{1} \in K$$

jest monomorfizmem pierścieni. Odtąd będziemy utożsamiać obraz tego przekształcenia z dziedziną R i traktować dziedzinę R jako podpierścień ciała K. Zauważmy, że jeśli $a = bc$, to $\frac{a}{b} = \frac{c}{1} = c$.

STWIERDZENIE 2.5.

Niech R będzie dziedziną z jednoznacznością rozkładu, $F \in R[X]$ i $k := \deg F > 0$. Niech a_k będzie współczynnikiem wiodącym wielomianu F i niech a_0 będzie wyrazem wolnym wielomianu F. Jeśli elementy $b, c \in R$, $c \neq 0$, są względnie pierwsze oraz $\frac{b}{c}$ jest pierwiastkiem wielomianu F, to $b \mid a_0$ i $c \mid a_k$.

DOWÓD.

Niech

$$F = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_1 X + a_0.$$

Równość $F(\frac{b}{c}) = 0$ implikuje równości

$$-a_0 c^k = b(a_k b^{k-1} + a_{k-1} b^{k-2} c + \cdots + a_1 c^{k-1}),$$
$$-a_k b^k = c(a_{k-1} b^{k-1} + \cdots + a_1 b c^{k-2} + a_0 c^{k-1}),$$

co kończy dowód.

UWAGA.(1) Wielomian $F \in R[X]$ jest elementem odwracalnym w dziedzinie $R[X]$ wtedy i tylko wtedy, gdy $\deg F = 0$ oraz element F jest odwracalny w dziedzinie R.

(2) Jeśli element a jest nierozkładalny w dziedzinie R, to wielomian a jest nierozkładalny w dziedzinie $R[X]$.

(3) Jeśli element $a \in R$ jest odwracalny oraz $b \in R$, to wielomian $aX + b$ jest nierozkładalny w dziedzinie $R[X]$.

PRZYKŁAD.

(1) Wielomian $2X + 2$ jest rozkładalny w dziedzinie $\mathbb{Z}[X]$, ale jest nierozkładalny w dziedzinie $\mathbb{Q}[X]$.

(2) Wielomian $X^2 + 1$ jest nierozkładalny w dziedzinie $\mathbb{R}[X]$, ale jest rozkładalny w dziedzinie $\mathbb{C}[X]$.

DEFINICJA.

Niech R będzie dziedziną z jednoznacznością rozkładu oraz

$$F = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_0 \in R[X].$$

Wielomian F nazywamy PRYMITYWNYM, jeśli elementy $a_k, \ldots, a_0$ są względnie pierwsze.

Uwaga.

Jeśli R jest dziedziną z jednoznacznością rozkładu oraz $F \in R[X]$, to istnieje wielomian prymitywny $F_1 \in R[X]$ oraz element $a \in R$ taki, $F = aF_1$. Oczywiście $a \neq 0$, gdy $F \neq 0$.

Uwaga.

Jeśli R jest dziedziną z jednoznacznością rozkładu oraz wielomian $F \in R[X]$ jest nierozkładalny stopnia dodatniego, to wielomian F jest prymitywny.

Uwaga.

Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K. Dla wielomianu $F \in K[X]$ istnieją elementy $a, b \in R[X]$, $a \neq 0$, oraz wielomian prymitywny $F_1 \in R[X]$ takie, że $aF = bF_1$. Oczywiście, gdy $F \neq 0$, to $b \neq 0$.

Lemat 2.6 (Gauss).

Jeśli R jest dziedziną z jednoznacznością rozkładu oraz wielomiany $F, G \in R[X]$ są prymitywne, to wielomian FG jest prymitywny.

Dowód.

Niech

$$F = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_0,$$
$$G = b_l X^l + b_{l-1} X^{l-1} + \cdots + b_0.$$

Wtedy

$$FG = c_{k+l} X^{k+l} + c_{k+l-1} X^{k+l-1} + \cdots + c_0,$$

gdzie

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0.$$

Ustalmy element nierozkładalny $p \in R[X]$. Istnieją $i_0, j_0 \geq 0$ takie, że

$$p \mid a_0, \ldots, a_{i_0-1},\ p \nmid a_{i_0},\ p \mid b_0, \ldots, b_{j_0-1},\ p \nmid b_{j_0}.$$

Wtedy $p \nmid c_{i_0+j_0}$, gdyż p jest elementem pierwszym. Istotnie $p \mid a_i b_j$ dla $(i, j) \neq (i_0, j_0)$, $i + j = i_0 + j_0$, oraz $p \nmid a_{i_0} b_{i_0}$. Z dowolności elementu p wynika, że wielomian FG jest prymitywny.

Lemat 2.7.

Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K. Jeśli wielomiany $F, G \in R[X]$ są prymitywne w pierścieniu $R[X]$, to wielomiany F i G są stowarzyszone w pierścieniu $R[X]$ wtedy i tylko wtedy, gdy wielomiany F i G są stowarzyszone w pierścieniu $K[X]$.

Dowód.

Oczywiście jeśli wielomiany F i G są stowarzyszone w pierścieniu $R[X]$, to są stowarzyszone w pierścieniu $K[X]$.

Przypuśćmy, że wielomiany F i G są stowarzyszone w pierścieniu $K[X]$. Wtedy istnieją elementy niezerowe $a, b \in R$ takie, że $aF = bG$. Elementy a i b są stowarzyszone w dziedzinie R, gdyż a jest największym wspólnym dzielnikiem współczynników wielomianu aF, zaś b jest największym wspólnym dzielnikiem współczynników wielomianu bG. Zatem istnieje element odwracalny $u \in R$ taki, że $a = bc$. Wtedy $bG = aF = bcF$, skąd $G = cF$, co kończy dowód.

Lemat 2.8.

Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K. Jeśli wielomian $F \in R[X]$ jest prymitywny, to wielomian F jest nierozkładalny w dziedzinie $R[X]$ wtedy i tylko wtedy, gdy wielomian F jest nierozkładalny w dziedzinie $K[X]$.

Dowód.

Załóżmy, że wielomian F jest nierozkładalny w dziedzinie $R[X]$. Ponieważ wielomian F jest prymitywny i nieodwracalny w dziedzinie $R[X]$, więc jest nieodwracalny w dziedzinie $K[X]$. Załóżmy, że $F = GH$ dla pewnych wielomianów $G, H \in K[X]$. Oczywiście $G, H \neq 0$. Ustalmy niezerowe elementy a, b, c i d dziedziny R oraz wielomiany prymitywne $G_1, H_1 \in R[X]$ takie, że $aG = cG_1$ oraz $bH = dH_1$. Wtedy $abF = cdG_1H_1$, więc wielomiany F i G_1H_1 są stowarzyszone w dziedzinie $K[X]$. Ponieważ wielomiany F i G_1H_1 są prymitywne, więc na mocy poprzedniego lematu są one stowarzyszone w dziedzinie $R[X]$. Nierozkładalność wielomianu F w dziedzinie $R[X]$ oznacza, że $\deg G = \deg G_1 = 0$ lub $\deg H = \deg H_1 = 0$, co kończy dowód tej implikacji.

Załóżmy, że wielomian F jest nierozkładalny w dziedzinie $K[X]$. Oczywiście wtedy wielomian F jest nieodwracalny w dziedzinie $R[X]$. Załóżmy zatem, że $F = GH$ dla pewnych wielomianów $G, H \in R[X]$. Wtedy, bez straty ogólności można założyć, że $\deg G = 0$, tzn. $G \in R$. Wtedy $G \mid 1$, więc element G jest odwracalny w pierścieniu R, a więc także w pierścieniu $R[X]$.

Lemat 2.9.

Niech R będzie dziedziną z jednoznacznością rozkładu. Jeśli wielomian $F \in R[X]$ jest prymitywny i $\deg F > 0$, to istnieją wielomiany nierozkładalne $G_1, \ldots, G_k \in R[X]$ takie, że $F = G_1 \cdots G_k$.

Dowód.

Niech K będzie ciałem ułamków dziedziny R. Z Wniosku 2.2 wynika, że istnieją wielomiany nierozkładalne $G_1, \ldots, G_k \in K[X]$ takie, że $F = G_1 \cdots G_k$. Ustalmy niezerowe elementy a_1, b_1, …, a_k, $b_k \in R$ oraz wielomiany prymitywne G_1, …, $G_k \in R[X]$ takie, że $a_i G_i = b_i G_i$ dla $i = 1, \ldots, k$. Wtedy

$$a_1 \cdots a_k F = b_1 \cdots b_k G_1 \cdots G_k,$$

zatem wielomiany F oraz $G_1 \cdots G_k$ są stowarzyszone w dziedzinie $K[X]$, a więc także w dziedzinie $R[X]$ na mocy Lematu 2.7. Ponieważ wielomiany G_1, …, G_k są nierozkładalne na mocy poprzedniego lematu, to kończy dowód.

Wniosek 2.10.

Jeśli R jest dziedziną z jednoznacznością rozkładu, to $R[X]$ jest dziedziną z rozkładem.

Dowód.

Ustalmy wielomian nieodwracalny $F \in R[X]$. Istnieją element $a \in R$ oraz wielomian prymitywny $F_1 \in R[X]$ takie, że $F = aF_1$. Jeśli $\deg F = 0$, to możemy założyć, że $F_1 = 1$, i element a jest nieodwracalny. Ponieważ R jest dziedziną z rozkładem, więc istnieją elementy $a_1, \ldots, a_l \in R$ nierozkładalne w dziedzinie R (a więc także w dziedzinie $R[X]$) takie, że $F = a = a_1 \cdots a_l$. Gdy $\deg F > 0$, to z poprzedniego lematu wiemy, że istnieją wielomiany nierozkładalne $G_1, \ldots, G_k \in R[X]$ takie, że $F = G_1 \cdots G_k$. Jeśli element a jest odwracalny, to możemy założyć, że $a = 1$, a więc $F = G_1 \cdots G_k$. W przeciwnym wypadku istnieją elementy nierozkładalne $a_1, \ldots, a_l \in R$ takie, że $a = a_1 \cdots a_l$, co kończy dowód.

Lemat 2.11.

Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K. Jeśli wielomian $F \in R[X]$ jest prymitywny, $G \in R[X]$ i $F \mid G$ w dziedzinie $K[X]$, to $F \mid G$ w dziedzinie $R[X]$.

Dowód.

Oczywiście, gdy $G = 0$, to teza jest oczywista. Załóżmy zatem, że $G \neq 0$. Istnieje wielomian $H \in K[X]$, $H \neq 0$ taki, że $FH = G$. Wiemy, że istnieją niezerowe elementy $a, b, c \in R$ oraz wielomiany prymitywne $G_1, H_1 \in R[X]$ takie, że $aH = bH_1$ oraz $G = cG_1$. Wtedy $bFH_1 = acG_1$, więc wielomiany FH_1 i G_1 są stowarzyszone w dziedzinie $K[X]$, zatem także w dziedzinie $R[X]$ (Lemat 2.7). W szczególności $F \mid G_1$, a więc także $F \mid G$ w dziedzinie $R[X]$.

Lemat 2.12.

Jeśli R jest dziedziną z jednoznacznością rozkładu oraz wielomian $F \in R[X]$ jest nierozkładalny, to wielomian F jest pierwszy.

Dowód.

Przypuśćmy, że $F \mid GH$. Ustalmy elementy $a, b \in R$ oraz wielomiany prymitywne $G_1, H_1 \in R[X]$ takie, że $G = aG_1$ i $H = bH_1$. Wtedy ab jest największym wspólnym dzielnikiem współczynników wielomianu $GH = abG_1H_1$, więc jeśli $\deg F = 0$, to $F \mid ab$. Ponieważ w tym przypadku element F jest nierozkładalny, zatem pierwszy, w dziedzinie R, więc $F \mid a$ lub $F \mid b$, co implikuje, że $F \mid G$ lub $F \mid H$. Gdy $\deg F > 0$, to wielomian F jest prymitywny, a więc nierozkładalny w dziedzinie $K[X]$ na mocy Lematu 2.8, gdzie K jest ciałem ułamków dziedziny R. Ponieważ pierścień $K[X]$ jest dziedziną z jednoznacznością rozkładu (Wniosek 2.2), więc wielomian F jest pierwszy w dziedzinie $K[X]$, skąd $F \mid G$ lub $F \mid H$ w dziedzinie $K[X]$. Zatem teza wynika z Lematu 2.11.

Wniosek 2.13.

Jeśli R jest dziedziną z jednoznacznością rozkładu, to pierścień $R[X]$ jest dziedziną z jednoznacznością rozkładu.

Dowód.

Przypomnijmy, że na mocy Wniosku 1.6 dziedziny z jednoznacznością rozkładu to dziedziny z rozkładem, w których elementy nierozkładalne są pierwsze.

Wniosek 2.14.

Niech R będzie dziedziną z jednoznacznością rozkładu oraz $k \geq 1$, to pierścień $R[X_1, \ldots, X_k]$ jest dziedziną z jednoznacznością rozkładu.

Wniosek 2.15.
Jeśli K jest ciałem oraz $k \geq 1$, to pierścień $K[X_1, \ldots, X_k]$ jest dziedziną z jednoznacznością rozkładu.

Przykład.
Pierścień $\mathbb{Z}[X]$ jest dziedziną z jednoznacznością rozkładu, która nie jest dziedziną ideałów głównych.

Twierdzenie 2.16 (Kryterium Eisensteina I).
Niech R będzie dziedziną z jednoznacznością rozkładu. Jeśli

$$F = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_0 \in R[X],$$

$k \geq 1$, jest wielomianem prymitywnym oraz istnieje element nierozkładalny $p \in R$ taki, że

$$p \nmid a_k,\ p \mid a_{k-1},\ \ldots,\ p \mid a_0,\ p^2 \nmid a_0,$$

to wielomian F jest nierozkładalny w pierścieniu $R[X]$.

Dowód.
Przypuśćmy, że $F = GH$ dla $G \in R[X]$. Zauważmy, że wielomiany G i H są prymitywne. Zapiszmy

$$G = b_i X^i + \cdots + b_0, \qquad H = c_j X^j + \cdots + c_0.$$

Wtedy $p \mid b_0 c_0$ oraz $p^2 \nmid b_0 c_0$, więc bez straty ogólności możemy założyć, że $p \mid b_0$ oraz $p \nmid c_0$. Ponieważ wielomian H jest prymitywny, więc $l_0 := \min\{l \mid p \nmid b_l\}$ jest dobrze zdefiniowane. Wtedy $p \nmid b_{l_0} c_0 + b_{l_0-1} c_1 + \cdots + b_0 c_{l_0} = a_{l_0}$, więc $l_0 = k$, skąd $\deg G = k$, $\deg H = 0$. Ponadto prymitywność wielomianu F implikuje, że element H jest odwracalny w pierścieniu R, a więc także w pierścieniu $R[X]$.

Wniosek 2.17 (Kryterium Eisensteina II).
Niech R będzie dziedziną z jednoznacznością rozkładu i ciałem ułamków K. Jeśli

$$F = a_k X^k + a_{k-1} X^{k-1} + \cdots + a_0 \in R[X],$$

$k \geq 1$, oraz istnieje element nierozkładalny $p \in R$ taki, że

$$p \nmid a_k,\ p \mid a_{k-1},\ \ldots,\ p \mid a_0,\ p^2 \nmid a_0,$$

to wielomian F jest nierozkładalny w pierścieniu $K[X]$.

Dowód.
Ustalmy element $a \in R$ oraz wielomian prymitywny $F_1 \in R[X]$ takie, że $F = aF_1$. Jeśli

$$F_1 = b_k X^k + b_{k-1} X^{k-1} + \cdots + b_0,$$

to

$$p \nmid b_k,\ p \mid b_{k-1},\ \ldots,\ p \mid b_0,\ p^2 \nmid b_0,$$

gdyż $p \nmid a$ (zauważmy, że $a_i = ab_i$, $i = 0, \ldots, k$). Z poprzedniego twierdzenia wielomian F_1 jest nierozkładalny w dziedzinie $R[X]$, a więc także w dziedzinie $K[X]$ na mocy Lematu 2.8. Ponieważ element a jest odwracalny w ciele K, więc oznacza to, że wielomian F jest nierozkładalny w dziedzinie $K[X]$.

§3. Moduły i ich homomorfizmy

Założenie.
Przez cały paragraf R oznaczać będzie pierścień.

Definicja.
R-modułem nazywamy grupę abelową M wraz z funkcją $R \times M \to M$, $(r, m) \mapsto rm$, taką że spełnione są następujące warunki:

(1) $\forall r \in R,\ m, n \in M : r(m+n) = rm + rn$,

(2) $\forall r, s \in R,\ m \in M : (r+s)m = rm + sm$,

(3) $\forall r, s \in R,\ m \in M : r(sm) = (rs)m$,

(4) $\forall m \in M : 1m = m$.

Uwaga.
Jeśli M jest R-modułem, to dla dowolnych elementów $r \in R$, $m \in M$ oraz $k \in \mathbb{Z}$ zachodzą równości:

$$r0 = 0, \qquad 0m = 0, \qquad k(rm) = r(km), \qquad (-r)m = -(rm) = r(-m).$$

Przykład.
Jeśli R jest ciałem, to R-moduły to przestrzenie liniowe nad ciałem R.

Przykład.
$\mathbb{Z}$-moduły to grupy abelowe.

Przykład.
Jeśli I jest ideałem pierścienia R, to I jest R-modułem.

Przykład.
Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to pierścień S jest R-modułem wraz z działaniem $(r, s) \mapsto \varphi(r)s$.

Przykład.
Zbiór $0 := \{0\}$ wraz z działaniem $(r, 0) \mapsto 0$ R-modułem, który nazywamy trywialnym.

Przykład.
Jeśli $\varphi : R \to S$ jest homomorfizmem pierścieni, to każdy S-moduł M jest R-modułem z działaniem $(r, m) \mapsto \varphi(r)m$.

Definicja.
Niech M i N będą R-modułami. Funkcję $f : M \to N$ nazywamy homomorfizmem R-modułów jeśli

$$f(m+n) = f(m) + f(n) \quad \text{i} \quad f(rm) = rf(m)$$

dla dowolnych elementów $m, n \in M$ oraz $r \in R$.

Uwaga.
Jeśli $\varphi : M \to N$ jest homomorfizmem R-modułów, to φ jest homomorfizmem grup abelowych.

Definicja.
Homomorfizm nazywamy monomorfizmem, jeśli jest injekcją.

Definicja.
Homomorfizm nazywamy epimorfizmem, jeśli jest surjekcją.

Definicja.
Homomorfizm $f : M \to N$ nazywamy izomorfizmem, jeśli istnieje homomorfizm $g : N \to M$ taki, że $gf = \mathrm{Id}_M$ oraz $fg = \mathrm{Id}_N$.

Definicja.
Mówimy, że moduły M i N są izomorficzne i piszemy $M \simeq N$, jeśli istnieje izomorfizm $M \to N$.

Definicja.
Jądrem homomorfizmu $f : M \to N$ nazywamy zbiór

$$\operatorname{Ker} f := \{m \in M \mid f(m) = 0\}.$$

Definicja.
Obrazem homomorfizmu $f : M \to N$ nazywamy zbiór

$$\operatorname{Im} f := \{f(m) \mid m \in M\}.$$

Uwaga.

(1) Homomorfizm f jest monomorfizmem wtedy i tylko wtedy, gdy $\operatorname{Ker} f = 0 := \{0\}$.

(2) Homomorfizm $f : M \to N$ jest epimorfizmem wtedy i tylko wtedy, gdy $\operatorname{Im} f = N$.

(3) Homomorfizm f jest izomorfizmem wtedy i tylko wtedy, gdy jest monomorfizmem i epimorfizmem.

Przykład.
Dla dowolnych R-modułów M i N funkcja $0 : M \to N$, $m \mapsto 0$, jest homomorfizmem, $\operatorname{Ker} 0 = M$, $\operatorname{Im} 0 = 0$. W szczególności, dla dowolnego R-modułu M mamy jedyne homomorfizmy postaci $0 \to M$ oraz $M \to 0$.

Definicja.
Niech M będzie R-modułem. Podzbiór $N \subset M$ nazywamy podmodułem modułu M, jeśli N jest podgrupą grupy M oraz

$$r \in R,\ m \in N \implies rm \in N.$$

Uwaga.

(1) Jeśli N jest podmodułem R-modułu M, to N jest R-modułem.

(2) Jeśli N jest podmodułem R-modułu M oraz U jest podmodułem modułu N, to U jest podmodułem modułu M.

(3) Jeśli U i V są podmodułami modułu M takimi, że $U \subset V$, to U jest podmodułem modułu V.

Uwaga.
Jeśli N jest podmodułem R-modułu M, to funkcja $N \to M$, $m \mapsto m$, jest monomorfizmem modułów, który nazywamy naturalnym włożeniem.

Przykład.
Jeśli M jest R-modułem, to zbiory 0 i M są podmodułami modułu M.

Przykład.
Podzbiór pierścienia R jest podmodułem modułu R wtedy i tylko wtedy, gdy jest ideałem pierścienia R.

Przykład.
Jeśli $f : M \to N$ jest homomorfizmem R-modułów, to zbiór $\operatorname{Ker} f$ jest podmodułem modułu M, zaś zbiór $\operatorname{Im} f$ jest podmodułem modułu N. Ogólniej, jeśli U jest podmodułem modułu M, to zbiór $f(U)$ jest podmodułem modułu N, oraz gdy V jest podmodułem modułu N, to zbiór $f^{-1}(V)$ jest podmodułem modułu N.

Przykład.
Jeśli m jest elementem R-modułu M oraz I jest ideałem pierścienia R, to zbiór

$$Im := \{rm \mid r \in I\}$$

jest podmodułem modułu M.

Przykład.
Jeśli $r \in R$ oraz N jest podmodułem R-modułu M, to zbiór

$$rN := \{rn \mid n \in N\}$$

jest podmodułem modułu M.

Przykład.
Jeśli U i V są podmodułami R-modułu M, to zbiór

$$U + V := \{u + v \mid u \in U,\ v \in V\}$$

jest podmodułem modułu M.

Przykład.
Jeśli $r \in R$ oraz M jest R-modułem, to zbiór

$$M[r] := \{m \in M \mid rm = 0\}$$

jest podmodułem modułu M.

Przykład.
Jeśli $r \in R$ oraz M jest R-modułem, to zbiór

$$M(r) := \bigcup_{\alpha>0} M[r^\alpha]$$

jest podmodułem modułu M.

Przykład.
Jeśli M_i, $i \in I$, $I \neq \varnothing$, są podmodułami modułu M, to $\bigcap_{i\in I} M_i$ jest podmodułem modułu M.

Obserwacja 3.1.
Jeśli X jest podzbiorem R-modułu M, oraz M_i, $i \in I$, są wszystkimi podmodułami modułu M zawierającymi podzbiór X, to podmoduł $\bigcap_{i\in I} M_i$ jest najmniejszym podmodułem modułu M zawierającym podzbiór X.

Definicja.
Jeśli X jest podzbiorem R-modułu M, to najmniejszy podmoduł modułu M zawierający zbiór X nazywamy podmodułem modułu M generowanym przez zbiór X i oznaczamy RX.

Definicja.
R-moduł M nazywamy skończenie generowanym wtedy i tylko wtedy, gdy istnieje skończony podzbiór $X \subset M$ taki, że $M = RX$.

Definicja.
R-moduł M nazywamy cyklicznym wtedy i tylko wtedy, gdy istnieje element $m \in M$ taki, że $M = R\{m\}$.

Twierdzenie 3.2.
Jeśli $m_1, \ldots, m_k$ są elementami R-modułu M, to

$$R\{m_1, \ldots, m_k\} = Rm_1 + \cdots + Rm_k.$$

Dowód.
Ćwiczenie.

Obserwacja 3.3.
Jeśli R-moduł M jest generowany przez elementy $m_1, \ldots, m_k$ oraz $f : M \to N$ jest homomorfizmem R-modułów, to moduł $\operatorname{Im} f$ jest generowany przez elementy $f(m_1), \ldots, f(m_k)$.

Definicja.
Jeśli N jest podmodułem R-modułu M, to modułem ilorazowym nazywamy zbiór

$$M/N := \{m + N \mid m \in N\},$$

gdzie

$$m + N := \{m + n \mid n \in N\},\ m \in M,$$

wraz z działaniami

$$(m + N) + (n + N) := (m + n) + N,$$
$$r(m + N) := rm + N.$$

Funkcję $M \to M/N$, $m \mapsto m+N$, nazywamy naturalnym rzutowaniem.

Twierdzenie 3.4.
Jeśli N jest podmodułem R-modułu M, to powyższe definicje są poprawne i określają w zbiorze M/N strukturę R-modułu. Naturalne rzutowanie $M \to M/N$ jest epimorfizmem R-modułów z jądrem N.

Dowód.
Ćwiczenie.

Uwaga.
W powyższym dowodzie można wykorzystać fakt, że $m + N = n + N$ wtedy i tylko wtedy, gdy $m - n \in N$.

TWIERDZENIE 3.5.
Jeśli $f : M \to N$ jest homomorfizmem R-modułów, to dla każdego podmodułu U modułu M takiego, że $U \subset \operatorname{Ker} f$, definicja

$$M/U \to N,\ m + U \mapsto f(m),$$

jest poprawna i definiuje homomorfizm o jądrze $\operatorname{Ker} f/U$ oraz obrazie $\operatorname{Im} f$.

DOWÓD.
Ćwiczenie.

WNIOSEK 3.6 (TWIERDZENIA O IZOMORFIZMIE).
(1) Jeśli $f : M \to N$ jest homomorfizmem R-modułów, to funkcja

$$M/\operatorname{Ker} f \to \operatorname{Im} f,\ m + \operatorname{Ker} f \mapsto f(m),$$

jest izomorfizmem R-modułów.

(2) Jeśli U i V są podmodułami R-modułu M, to funkcja

$$U/U \cap V \to (U + V)/V,\ u + U \cap V \mapsto u + V,$$

jest izomorfizmem R-modułów.

(3) Jeśli U i V są podmodułami R-modułu M takimi, że $V \subset U$, to U/V jest podmodułem modułu M/V oraz funkcja

$$(M/V)/(U/V) \to M/U,\ (m + V) + (U/V) \mapsto m + U,$$

jest izomorfizmem R-modułów.

DEFINICJA.
SUMĄ PROSTĄ R-MODUŁÓW $M_1, \ldots, M_k$, oznaczaną $\bigoplus_{i=1}^{k} M_i$ lub $M_1 \oplus \cdots \oplus M_k$ (lub M^k, gdy $M_i = M$ dla $i = 1, \ldots, k$), nazywamy zbiór $M_1 \times \cdots \times M_k$, z działaniami

$$(m_1, \ldots, m_k) + (n_1, \ldots, n_k) := (m_1 + n_1, \ldots, m_k + n_k),$$
$$r(m_1, \ldots, m_k) := (rm_1, \ldots, rm_k).$$

Dla każdego $j = 1, \ldots, k$ definiujemy funkcje

$$\iota_j : M_j \to \bigoplus_{i=1}^{k} M_i, \qquad m \mapsto (0, \ldots, 0, \underbrace{m}_{j\text{-te miejsce}}, 0, \ldots, 0),$$

i

$$\pi_j : \bigoplus_{i=1}^{n} M_i \to M_j, \qquad (m_1, \ldots, m_n) \mapsto m_j,$$

nazywane NATURALNYM WŁOŻENIEM i RZUTOWANIEM, odpowiednio.

Twierdzenie 3.7.

Niech $M_1, \ldots, M_k$ będą R-modułami.

(1) Suma prosta $\bigoplus_{i=1}^{k} M_i$ jest R-modułem.

(2) Dla każdej liczby $j = 1, \ldots, k$ naturalne włożenie $\iota_j : M_j \to \bigoplus_{i=1}^{k} M_i$ jest monomorfizmem R-modułów.

(3) Dla każdej liczby $j = 1, \ldots, k$ naturalne rzutowanie $\pi_j : \bigoplus_{i=1}^{k} M_i \to M_j$ jest epimorfizmem R-modułów.

Dowód.

Ćwiczenie.

Twierdzenie 3.8.

(1) Jeśli $f_j : M_j \to N$, $j = 1, \ldots, k$, są homomorfizmami R-modułów, to istnieje dokładnie jeden homomorfizm $f : \bigoplus_{i=1}^{k} M_i \to N$ taki, że $f\iota_j = f_j$ dla $j = 1, \ldots, k$, gdzie $\iota_j : M_j \to \bigoplus_{i=1}^{n} M_i$, $j = 1, \ldots, n$, są naturalnymi włożeniami. Homomorfizm f dany jest wzorem

$$f(m_1, \ldots, m_k) = f_1(m_1) + \cdots + f_k(m_k).$$

(2) Jeśli $f_j : N \to M_j$, $j = 1, \ldots, k$, są homomorfizmami modułów, to istnieje dokładnie jeden homomorfizm $f : N \to \bigoplus_{i=1}^{k} M_i$ taki, że $\pi_j f = f_j$ dla $j = 1, \ldots, k$, gdzie $\pi_j : \bigoplus_{i=1}^{k} M_i \to M_j$, $j = 1, \ldots, j$, są naturalnymi rzutowaniami. Homomorfizm f dany jest wzorem

$$f(n) = (f_1(n), \ldots, f_k(n)).$$

Dowód.

Ćwiczenie.

Oznaczenie.

Jeśli $f, g : M \to N$ są homomorfizmami R-modułów, to definiujemy funkcję $f + g : M \to N$ wzorem

$$(f + g)(m) := f(m) + g(m),\ m \in M.$$

Obserwacja 3.9.
Niech $f, g : M \to N$ będą homomorfizmami R-modułów.

(1) Funkcja $f + g$ jest homomorfizmem R-modułów.

(2) Dla dowolnego homomorfizmu $h : N \to U$

$$h(f + g) = hf + hg.$$

(3) Dla dowolnego homomorfizmu $h : V \to M$

$$(f + g)h = fh + gh.$$

Obserwacja 3.10.
Jeśli $M_1, \ldots, M_k$ są R-modułami, to

(1) $\pi_j \iota_j = \mathrm{Id}_{M_j}$, $j = 1, \ldots, k$,

(2) $\pi_i \iota_j = 0$, $i \neq j$,

(3) $\iota_1 \pi_1 + \cdots + \iota_k \pi_k = \mathrm{Id}_{\bigoplus_{i=1}^k M_i}$,

gdzie dla każdego $j = 1, \ldots, k$, $\pi_j : \bigoplus_{i=1}^k M_i \to M_j$ jest naturalnym rzutowaniem, zaś $\iota_j : M_j \to \bigoplus_{i=1}^k M_i$ jest naturalnym włożeniem.

Twierdzenie 3.11.
Jeśli M, $M_1, \ldots, M_k$ są R-modułami, to $M \simeq \bigoplus_{i=1}^k M_i$ wtedy i tylko wtedy, gdy istnieją homomorfizmy $f_j : M \to M_j$ i $g_j : M_j \to M$, $j = 1, \ldots, k$, takie, że

(1) $f_j g_j = \mathrm{Id}_{M_j}$, $j = 1, \ldots, k$,

(2) $f_j g_l = 0$, $j \neq l$,

(3) $g_1 f_1 + \cdots + g_k f_k = \mathrm{Id}_M$.

Dowód.
Jeśli homomorfizmy $f_1, \ldots, f_k, g_1, \ldots, g_k$ są takie jak wyżej, to homomorfizm $f : M \to \bigoplus_{i=1}^k M_i$, $f(m) := (f_1(m), \ldots, f_k(m))$, jest izomorfizmem (izomorfizm odwrotny dany jest wzorem $g(m_1, \ldots, m_k) := g_1(m_1) + \cdots + g_k(m_k)$).

Jeśli $f : M \to \bigoplus_{i=1}^k M_i$ i $g : \bigoplus_{i=1}^k M_i \to M$ są wzajemnie odwrotnymi izomorfizmami, to poszukiwane funkcje są postaci $f_j := \pi_j f$ oraz $g_j := g\iota_j$, $j = 1, \ldots, k$, gdzie dla każdego $j = 1, \ldots, k$, $\pi_j : \bigoplus_{i=1}^k M_i \to M_j$ jest naturalnym rzutowaniem, zaś $\iota_j : M_j \to \bigoplus_{i=1}^k M_i$ jest naturalnym włożeniem.

Definicja.
R-moduł N nazywamy składnikiem prostym R-modułu M, jeśli istnieje R-moduł U taki, że $M \simeq N \oplus U$.

Wniosek 3.12.

R-moduł N jest składnikiem prostym R-modułu M wtedy i tylko wtedy, gdy istnieją homomorfizmy $f : N \to M$ oraz $g : M \to N$ takie, że $gf = \mathrm{Id}_N$.

Dowód.

Jeśli N jest składnikiem prostym R-modułu M, to istnienie stosownych homomorfizmów jest konsekwencją poprzedniego twierdzenia.

Załóżmy zatem, że istnieją homomorfizmy $f : N \to M$ i $g : M \to N$ takie, że $gf = \mathrm{Id}_N$. Pokażemy, że $M \simeq N \oplus \operatorname{Ker} g$. Istotnie, niech $\iota : \operatorname{Ker} g \to M$ będzie naturalnym włożeniem oraz $h : M \to \operatorname{Ker} g$ dane będzie wzorem $h(m) := m - fg(m)$. Wtedy $gf = \mathrm{Id}_N$, $h\iota = \mathrm{Id}_{\operatorname{Ker} g}$, $g\iota = 0$, $hf = 0$ oraz $fg + \iota h = \mathrm{Id}_M$, co kończy dowód wobec poprzedniego twierdzenia.

Twierdzenie 3.13.

Jeśli $M_1, \ldots, M_k$ są podmodułami R-modułu M takimi, że

(1) $M = M_1 + \cdots + M_k$,

(2) $M_i \cap (M_1 + \cdots + M_{i-1} + M_{i+1} + \cdots + M_k) = 0$, $i = 1, \ldots, k$,

to $M \simeq \bigoplus_{i=1}^{k} M_i$.

Dowód.

Z założeń twierdzenia wynika, że dla każdego elementu m istnieją jednoznacznie wyznaczone elementy $m_i \in M_i$, $i = 1, \ldots, k$, takie, że $m = m_1 + \cdots + m_k$. Zatem funkcje $f_j : M \to M_j$, $j = 1, \ldots, k$, dane wzorami

$$f_j(m_1 + \cdots + m_k) := m_j,\ m_i \in M_i,\ i = 1, \ldots, k,$$

$j = 1, \ldots, k$, są poprawnie określone. Ponadto są one homomorfizmami R-modułów oraz $f_j\iota_j = \mathrm{Id}_{M_j}$, $j = 1, \ldots, k$, $f_j\iota_l = 0$, $j \neq l$, i $\iota_1 f_1 + \cdots + \iota_k f_k = \mathrm{Id}_M$, gdzie dla każdego $j = 1, \ldots, k$, $\iota_j : M_i \to M$ jest naturalnym włożeniem. Zatem teza wynika z Twierdzenia 3.11.

Definicja.

W sytuacji opisanej powyższym twierdzeniem mówimy czasami, że moduł M jest wewnętrzną sumą prostą podmodułów $M_1, \ldots, M_k$.

Definicja.

Mówimy, że ciąg homomorfizmów R-modułów

$$M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} M_2 \to \cdots \to M_{k-1} \xrightarrow{f_k} M_k$$

jest dokładny wtedy i tylko wtedy, gdy $\operatorname{Im} f_i = \operatorname{Ker} f_{i+1}$, $i = 1, \ldots, n-1$.

Uwaga.

Ciąg $0 \to M \xrightarrow{f} N$ jest dokładny wtedy i tylko wtedy, gdy f jest monomorfizmem.

Uwaga.
Ciąg $M \xrightarrow{f} N \to 0$ jest dokładny wtedy i tylko wtedy, gdy f jest epimorfizmem.

Przykład.
Dla dowolnych R-modułów M i N ciągi

$$0 \to M \xrightarrow{\iota_1} M \oplus N \xrightarrow{\pi_2} N \to 0$$

i

$$0 \to N \xrightarrow{\iota_2} M \oplus N \xrightarrow{\pi_1} M \to 0$$

są dokładne, gdzie $\iota_1 : M \to M \oplus N$ i $\iota_2 : N \to M \oplus N$ są naturalnymi włożeniami, zaś $\pi_1 : M \oplus N \to M$ i $\pi_2 : M \oplus N \to N$ są naturalnymi rzutowaniami.

Przykład.
Jeśli N jest podmodułem R-modułu M, to ciąg

$$0 \to N \xrightarrow{\iota} M \xrightarrow{\pi} M/N \to 0$$

jest dokładny, gdzie $\iota : N \to M$ jest naturalnym włożeniem, zaś $\pi : M \to M/N$ jest naturalnym rzutowaniem.

Przykład.
Dla dowolnego homomorfizmu $f : M \to N$ ciąg

$$0 \to \operatorname{Ker} f \to M \xrightarrow{f} N \to \operatorname{Coker} f \to 0$$

jest dokładny, gdzie $\operatorname{Coker} f := N/\operatorname{Im} f$ nazywamy kojądrem homomorfizmu f.

Definicja.
Ciąg dokładny

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$$

nazywamy rozszczepialnym, jeśli istnieje izomorfizm $h : V \to U \oplus W$ taki, że $hf = \iota$ oraz $\pi h = g$, gdzie $\iota : U \to U \oplus W$ i $\pi : U \oplus W \to V$ są naturalnym włożeniem i rzutowaniem, odpowiednio.

Lemat 3.14.
Jeśli

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$$

jest ciągiem dokładnym oraz $h : U \oplus W \to V$ jest homomorfizmem takim, że $h\iota = f$ i $gh = \pi$, gdzie $\iota : U \to U \oplus W$ oraz $\pi : U \oplus W \to W$ są naturalnymi włożeniem i rzutowaniem, to homomorfizm h jest izomorfizmem.

Dowód.
Przypuśćmy, że $(u, w) \in \operatorname{Ker} h$. Wtedy mamy

$$w = \pi(u, w) = (gh)(u, w) = 0$$

oraz

$$f(u) = h\iota(u) = h(u, 0) = h(u, w) = 0$$

więc $u = 0$, gdyż f jest monomorfizmem.

Aby pokazać, że h jest epimorfizmem, ustalmy $v \in V$. Niech $w := g(v)$. Wtedy $v - h(0, w) \in \operatorname{Ker} g = \operatorname{Im} f$, więc istnieje element $u \in U$ taki, że $v - h(0, w) = f(u)$, skąd

$$h(u, w) = h(u, 0) + h(0, w) = f(u) + h(0, w) = v.$$

Twierdzenie 3.15.
Ciąg dokładny

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$$

jest rozszczepialny wtedy i tylko wtedy, gdy istnieje homomorfizm $h : W \to V$ taki, że $gh = \mathrm{Id}_W$.

Dowód.
Niech $\iota_1 : U \to U \oplus W$, $\iota_2 : W \to U \oplus W$ i $\pi : U \oplus W \to V$ będą naturalnymi włożeniami i rzutowaniem, odpowiednio.

Jeśli ciąg

$$0 \to U \xrightarrow{f} V \xrightarrow{g} W \to 0$$

jest dokładny oraz $\kappa : V \to U \oplus W$ jest izomorfizmem takim, że $\kappa f = \iota_1$ oraz $\pi\kappa = g$, to dla $h = \kappa^{-1}\iota_2$ mamy $gh = \mathrm{Id}_W$.

Niech $h : W \to V$ będzie homomorfizmem takim, że $gh = \mathrm{Id}_W$, i niech $\kappa : U \oplus W \to V$ będzie homomorfizmem danym wzorem

$$\kappa(u, w) := f(u) + h(w).$$

Wtedy $\kappa\iota_1 = f$ i $g\kappa = \pi$, więc homomorfizm κ jest izomorfizmem na mocy poprzedniego lematu. Ponadto $\kappa^{-1}f = \iota_1$ oraz $\pi\kappa^{-1} = g$, co kończy dowód.

§4. Moduły wolne i projektywne

Założenie.
Przez cały paragraf R oznaczać będzie pierścień, $R \neq 0$.

Oznaczenie.
Dla ustalonego $k \geq 1$ piszemy

$$e_i := (0, \ldots, 0, \underbrace{1}_{i\text{-te miejsce}}, 0, \ldots, 0) \in R^k,$$

$i = 1, \ldots, k$.

Lemat 4.1.
Jeśli $m_1, \ldots, m_k$ są elementami R-modułu M, to istnieje dokładnie jeden homomorfizm $f : R^k \to M$ taki, że $f(e_i) = m_i$, dla $i = 1, \ldots, n$. Homomorfizm f dany jest wzorem

$$f(r_1, \ldots, r_k) = r_1 m_1 + \cdots + r_k m_k,\ r_1, \ldots, r_k \in R,$$

oraz $\operatorname{Im} f = Rm_1 + \cdots + Rm_k$,

Dowód.
Ćwiczenie.

Definicja.
Elementy $m_1, \ldots, m_k$ R-modułu M nazywamy liniowo niezależnymi, jeśli spełniony jest następujący warunek:

$$\forall r_1, \ldots, r_k \in R : r_1 m_1 + \cdots + r_k m_k = 0 \implies r_1 = \cdots = r_k = 0.$$

Przykład.
Elementy $e_1, \ldots, e_k \in R^k$ są liniowo niezależne.

Uwaga.
Jeśli elementy $m_1, \ldots, m_k$ R-modułu M są liniowo niezależne, to elementy $m_{i_1}, \ldots, m_{i_k}$ są liniowo niezależne dla dowolnego ciągu $1 \leq i_1 < \cdots < i_k \leq n$.

Uwaga.
Elementy $m_1, \ldots, m_k$ R-modułu M są liniowo niezależne wtedy i tylko wtedy, gdy homomorfizm przedstawiony w Lemacie 4.1 jest monomorfizmem.

Definicja.
Mówimy, że elementy $m_1, \ldots, m_k$ R-modułu M tworzą bazę modułu M, jeśli są liniowo niezależne oraz $M = Rm_1 + \cdots + Rm_k$.

Lemat 4.2.
Jeśli elementy $m_1, \ldots, m_k$ tworzą bazą R-modułu M, to moduł M jest (wewnętrzną) sumą prostą podmodułów $Rm_1, \ldots, Rm_k$.

Dowód.
Ćwiczenie.

Definicja.
R-moduł M nazywamy (skończenie generowanym) wolnym, jeśli posiada bazę.

Obserwacja 4.3.
Jeśli M jest R-modułem wolnym z bazą $m_1, \ldots, m_k$ oraz $f : M \to N$ jest izomorfizmem R-modułów, to moduł N jest wolny z bazą $f(m_1), \ldots, f(m_k)$.

Przykład.
Jeśli K jest ciałem, to wszystkie (skończenie generowane, tj. skończenie wymiarowe) K-moduły są wolne.

Przykład.
R-moduł R jest wolny z bazą 1.

Obserwacja 4.4.
Jeśli R-moduły M i N są wolne z bazami $m_1, \ldots, m_k$ oraz $n_1, \ldots, n_l$, odpowiednio, to moduł $M \oplus N$ jest wolny z bazą $(m_1, 0), \ldots, (m_k, 0), (0, n_1), \ldots, (0, n_l)$.

Wniosek 4.5.
R-moduł R^k jest wolny z bazą $e_1, \ldots, e_k$.

Wniosek 4.6.
Dla dowolnego skończenie generowanego R-modułu M istnieje wolny R-moduł N oraz epimorfizm $N \to M$.

Dowód.
Wynika z poprzedniego wniosku oraz Lematu 4.1.

Twierdzenie 4.7.
R-moduł M jest wolny z bazą $m_1, \ldots, m_k$ wtedy i tylko wtedy, gdy homomorfizm $R^k \to M$,

$$(r_1, \ldots, r_k) \mapsto r_1 m_1 + \cdots + r_k m_k,$$

jest izomorfizmem.

Dowód.
Ćwiczenie.

Twierdzenie 4.8.

R-moduł M jest wolny z bazą $m_1, \ldots, m_k$ wtedy i tylko wtedy, gdy dla dowolnego R-modułu N oraz elementów $n_1, \ldots, n_k$ istnieje dokładnie jeden homomorfizm $f : M \to N$ taki, że $f(m_i) = n_i$, $i = 1, \ldots, k$.

Dowód.

Z Lematu 4.1 wiemy, że mamy homomorfizm $g : R^k \to M$ dany wzorem

$$g(r_1, \ldots, r_k) := r_1 m_1 + \cdots + r_k m_k.$$

Jeśli moduł M jest wolny z bazą $m_1, \ldots, m_k$, to homomorfizm g jest izomorfizmem na mocy Twierdzenia 4.7. Ustalmy R-moduł N oraz elementy $n_1, \ldots, n_k$. Mamy homomorfizm $h : R^k \to N$ dany wzorem

$$h(r_1, \ldots, r_k) := r_1 n_1 + \cdots + r_k n_k.$$

Wtedy $f := hg^{-1} : M \to N$ jest homomorfizmem takim, że $f(m_i) = n_i$, $i = 1, \ldots, k$.

Ponadto, jeśli $f : M \to N$ jest homomorfizmem takim, że $f(m_i) = n_i$, $i = 1, \ldots, k$, to $fg : R^k \to N$ jest homomorfizmem takim, że $fg(e_i) = n_i$, $i = 1, \ldots, k$. Z Lematu 4.1 wynika, że $fg = h$, więc $f = hg^{-1}$.

Przypuśćmy teraz dla dowolnego R-modułu N oraz elementów $n_1, \ldots, n_k$ istnieje dokładnie jeden homomorfizm $f : M \to N$ taki, że $f(m_i) = n_i$, $i = 1, \ldots, k$. W szczególności istnieje homomorfizm $f : M \to R^k$ taki, że $f(m_i) = e_i$, $i = 1, \ldots, k$. Wtedy

$$gf(m_i) = m_i = \mathrm{Id}_M(m_i), \quad fg(e_i) = e_i = \mathrm{Id}_{R^k}(e_i),$$

$i = 1, \ldots, k$, zatem z powyższego warunku oraz Lematu 4.1 wynika, że $gf = \mathrm{Id}_M$ i $fg = \mathrm{Id}_{R^k}$. Zatem homomorfizm g jest izomorfizmem, co kończy dowód wobec Twierdzenia 4.7.

Oznaczenie.

Jeśli I ideałem pierścienia R oraz M jest R-modułem, to przez IM oznaczamy podmoduł modułu M generowany przez wszystkie elementy postaci rm, $r \in I$, $m \in M$.

Lemat 4.9.

Niech I będzie ideałem pierścienia R oraz M R-modułem. Jeśli $M = Rm_1 + \cdots + Rm_k$, to

$$IM = Im_1 + \cdots + Im_k.$$

Dowód.

Wiemy, że $Im_1 + \cdots + Im_k$ jest podmodułem R-modułu M. Łatwo też zauważyć, że $Im_1 + \cdots + Im_k \subset IM$. Dla zakończenia dowodu wystarczy pokazać, że $rm \in Im_1 + \cdots + Im_k$ dla dowolnych $r \in R$ i $m \in M$, co jest łatwym ćwiczeniem.

Lemat 4.10.

Jeśli I jest ideałem pierścienia R oraz M jest R-modułem, to definicja

$$(r + I)(m + IM) := rm + IM$$

jest poprawna i określa w zbiorze M/IM strukturę R/I-modułu.

Dowód.

Ćwiczenie.

Lemat 4.11.

Jeśli I jest ideałem właściwym pierścienia R, M wolnym R-modułem z bazą $m_1, \ldots, m_k$, to R/I-moduł M/IM jest wolny z bazą $m_1+IM, \ldots, m_k+IM$.

Dowód.

Pokażemy najpierw, że elementy $m_1+IM, \ldots, m_k+IM$ generują R/I-moduł M/IM. Jeśli $m+IM \in M/IM$, to istnieją elementy $r_1, \ldots, r_k \in R$ takie, że $m = r_1m_1 + \cdots + r_km_k$, więc

$$\begin{aligned} &m + IM = \\ &(r_1 + I)(m_1 + IM) + \cdots + (r_k + I)(m_k + IM). \end{aligned}$$

Aby sprawdzić, że elementy $m_1 + IM, \ldots, m_k + IM$ są liniowo niezależne, załóżmy, że

$$(r_1 + I)(m_1 + IM) + \cdots + (r_k + I)(m_k + IM) = 0$$

dla pewnych $r_1, \ldots, r_k \in R$. Wtedy istnieją elementy $s_1, \ldots, s_k \in I$ takie, że

$$r_1m_1 + \cdots + r_km_k = s_1m_1 + \cdots + s_km_k.$$

Z liniowej niezależności elementów $m_1, \ldots, m_k$ wynika, że $r_1 = s_1, \ldots, r_k = s_k$, co kończy dowód.

Wniosek 4.12.

Jeśli M jest wolnym R-modułem, to dowolne dwie bazy modułu M są równoliczne.

Dowód.

Niech $m_1, \ldots, m_k$ oraz $n_1, \ldots, n_l$ będą dwoma bazami modułu M. Ustalmy ideał maksymalny I pierścienia R. Wtedy moduł M/IM jest wolnym R/I-modułem z bazami $m_1 + IM, \ldots, m_k + IM$ oraz $n_1 + IM, \ldots, n_l + IM$. Ponieważ R/I jest ciałem, więc $k = l$, co kończy dowód.

Definicja.

Jeśli M jest wolnym R-modułem, to liczbę elementów dowolnej bazy modułu M nazywamy rangą modułu M oraz oznaczamy $\operatorname{rk}_R M$.

Obserwacja 4.13.

Jeśli M i N są wolnymi R-modułami, to $M \oplus N$ jest wolnym R-modułem oraz $\operatorname{rk}_R(M \oplus N) = \operatorname{rk}_R M + \operatorname{rk}_R N$ (patrz Obserwacja 4.4).

Stwierdzenie 4.14.
Jeśli M i N są wolnymi R-modułami, to $M \simeq N$ wtedy i tylko wtedy, gdy $\mathrm{rk}_R M = \mathrm{rk}_R N$.

Dowód.
Jeśli $f : M \to N$ jest izomorfizmem oraz elementy $m_1, \ldots, m_k$ tworzą bazę modułu M, to elementy $f(m_1), \ldots, f(m_k)$ tworzą bazę modułu N (Obserwacja 4.3).

Załóżmy teraz, że elementy $m_1, \ldots, m_k$ tworzą bazę modułu M oraz elementy $n_1, \ldots, n_k$ tworzą bazę modułu N. Z Twierdzenia 4.8 wiemy, że istnieją homomorfizmy $f : M \to N$ i $g : N \to M$ takie, że $f(m_i) = n_i$ oraz $g(n_i) = m_i$, $i = 1, \ldots, k$. Wtedy $gf(m_i) = m_i$ oraz $fg(n_i) = n_i$, $i = 1, \ldots, k$, więc $gf = \mathrm{Id}_M$ i $fg = \mathrm{Id}_N$ na mocy Twierdzenia 4.8, co kończy dowód.

Definicja.
R-moduł M nazywamy projektywnym, jeśli dla każdego homomorfizmu R-modułów $f : M \to U$ oraz epimorfizmu R-modułów $g : V \to U$ istnieje homomorfizm $h : M \to V$ taki, że $f = gh$.

Twierdzenie 4.15.
Jeśli M jest wolnym R-modułem, to moduł M jest projektywny.

Dowód.
Ustalmy bazę $m_1, \ldots, m_k$ modułu M. Niech $f : M \to U$ będzie homomorfizmem R-modułów oraz niech $g : V \to U$ będzie epimorfizmem R-modułów. Wybierzmy elementy $v_1, \ldots, v_k$ modułu V takie, że $g(v_i) = f(m_i)$, $i = 1, \ldots, k$. Na mocy Twierdzenie 4.8 istnieje homomorfizm $h : M \to V$ taki, że $h(m_i) = v_i$, $i = 1, \ldots, k$. Wtedy $hg(m_i) = f(m_i)$, $i = 1, \ldots, k$, więc $hg = f$ na mocy Twierdzenia 4.8.

Przykład.
$\mathbb{Z}_2$ jest projektywnym $\mathbb{Z}_6$-modułem, który nie jest wolny.

Lemat 4.16.
Jeśli R-moduł M jest projektywny, to każdy ciąg dokładny postaci

$$0 \to U \to V \to M \to 0$$

jest rozszczepialny.

Dowód.
Niech

$$0 \to U \to V \xrightarrow{f} M \to 0$$

będzie ciągiem dokładnym. Z definicji modułu projektywnego wynika, że istnieje homomorfizm $g : M \to V$ taki, że $fg = \mathrm{Id}_M$, co kończy dowód na mocy Twierdzenie 3.15.

§5. Moduły nad dziedzinami ideałów głównych

Założenie.
Przez cały paragraf R oznaczać będzie dziedzinę ideałów głównych.

Przykład.
$\{0, 2\}$ jest podmodułem wolnego $\mathbb{Z}_4$-modułu $\mathbb{Z}_4$, który nie jest wolny.

Obserwacja 5.1.
Jeśli $a \in R$, $a \neq 0$, to $R \simeq Ra$.

Lemat 5.2.
Jeśli M jest podmodułem modułu R, to moduł M jest wolny oraz $\mathrm{rk}_R M \leq 1$.

Dowód.
Jeśli $M = 0$, to teza jest oczywista. Przypuśćmy zatem, że $M \neq 0$. Wtedy istnieje element $a \in R$ taki, że $M = Ra$, co kończy dowód wobec poprzedniej obserwacji.

Twierdzenie 5.3.
Jeśli N jest podmodułem R-modułu wolnego M, to moduł N jest wolny oraz $\mathrm{rk}_R N \leq \mathrm{rk}_R M$.

Dowód.
Niech $m_1, \ldots, m_k$ będzie bazą modułu M. Definiujemy

$$M_i := Rm_1 + \cdots + Rm_i, \quad N_i := N \cap M_i, \qquad i = 0, \ldots, k.$$

Z Wniosku 3.6 (2) wynika, że

$$M_i/M_{i-1} \simeq Rm_i \simeq R, \quad N_i/N_{i-1} \simeq (N_i + M_{i-1})/M_{i-1} \subset M_i/M_{i-1},$$

$i = 1, \ldots, k$, gdyż $N_{i-1} = N_i \cap M_{i-1}$, $i = 1, \ldots, k$. Z poprzedniego lematu wynika zatem, że moduł N_i/N_{i-1} jest wolny oraz $\mathrm{rk}_R N_i/N_{i-1} \leq 1$, $i = 1, \ldots k$. W szczególności $N_i \simeq N_i/N_{i-1} \oplus N_{i-1}$, $i = 1, \ldots, k$ (Twierdzenie 4.15 oraz Lemat 4.16). Przez prostą indukcję otrzymujemy, że

$$N \simeq N_1/N_0 \oplus \cdots \oplus N_k/N_{k-1},$$

co kończy dowód wobec Obserwacji 4.13.

Ćwiczenie.
Jeśli N jest podmodułem skończenie generowanego R-modułu M, generowanego przez k elementów, to moduł N może być generowany przez l elementów dla pewnego $l \leq k$.

Wniosek 5.4.
Skończenie generowany R-moduł M jest wolny wtedy i tylko wtedy, gdy jest projektywny.

Dowód.
$\Rightarrow$: Twierdzenie 4.15.

$\Leftarrow$: Z Wniosku 4.6 wiemy, że istnieje R-moduł wolny N oraz ciąg dokładny

$$0 \to U \to N \to M \to 0.$$

Z Lematu 4.16 wynika, że $N \simeq M \oplus U$, więc moduł M jest (izomorficzny z) podmodułem modułu N, zatem teza wynika z Twierdzenia 5.3.

Definicja.
Jeśli m jest elementem R-modułu M, to anihilatorem elementu m nazywamy zbiór

$$\mathrm{Ann}(m) := \{r \in R \mid rm = 0\}.$$

Uwaga.
Jeśli $f : M \to N$ jest izomorfizmem R-modułów, to $\mathrm{Ann}(m) = \mathrm{Ann}(f(m))$.

Obserwacja 5.5.
Jeśli m jest elementem R-modułu M, to zbiór $\mathrm{Ann}(m)$ jest ideałem pierścienia R.

Definicja.
Jeśli m jest elementem R-modułu M i $\mathrm{Ann}(m) = (r)$, to mówimy, że element m ma rząd r.

Definicja.
Jeśli M jest R-modułem, to podmodułem torsyjnym modułu M nazywamy zbiór

$$M_{\mathrm{tor}} := \{m \in M \mid \mathrm{Ann}(m) \neq 0\}.$$

Obserwacja 5.6.
Jeśli M jest R-modułem, to zbiór M_{tor} jest podmodułem modułu M.

Obserwacja 5.7.
Jeśli R-moduły M i N są izomorficzne, to $M_{\mathrm{tor}} \simeq N_{\mathrm{tor}}$ i $M/M_{\mathrm{tor}} \simeq N/N_{\mathrm{tor}}$.

Definicja.
R-moduł M nazywamy torsyjnym, jeśli $M = M_{\mathrm{tor}}$.

Definicja.
R-moduł M nazywamy beztorsyjnym, jeśli $M_{\mathrm{tor}} = 0$.

Obserwacja 5.8.
R-moduł M jest beztorsyjny wtedy i tylko wtedy, gdy z warunku $rm = 0$ dla $r \in R$ i $m \in M$ wynika, że $r = 0$ lub $m = 0$.

Twierdzenie 5.9.
Skończenie generowany moduł M jest wolny wtedy i tylko wtedy, gdy jest beztorsyjny.

Dowód.
$\Rightarrow$: Oczywiste.

$\Leftarrow$: Jeśli $M = 0$, to teza jest oczywista. Załóżmy, że $M \neq 0$ oraz niech $m_1, \ldots, m_k$ będą generatorami modułu M. Możemy założyć, że istnieje $l \in \{1, \ldots, k\}$ takie, że elementy $m_1, \ldots, m_l$ są liniowo niezależne, oraz dla każdego $i \in \{l+1, \ldots, k\}$ elementy $m_1, \ldots m_l, m_i$, są liniowo niezależne. Niech $N := Rm_1 + \cdots + Rm_l$. Moduł N jest wolny oraz dla każdego $i \in \{l+1, \ldots, k\}$ istnieje element $r_i \in R$, $r_i \neq 0$, taki, że $r_i m_i \in N$. Niech $r := r_{l+1} \cdots r_k$. Wtedy $rM \subset N$, więc moduł rM jest wolny na mocy Twierdzenia 5.3. Ponadto odwzorowanie $M \to rM$, $m \mapsto rm$, jest izomorfizmem, co kończy dowód.

Wniosek 5.10.
Jeśli M jest skończenie generowanym R-modułem, to moduł M/M_{tor} jest wolny oraz $M \simeq M_{\mathrm{tor}} \oplus M/M_{\mathrm{tor}}$.

Dowód.
Moduł M/M_{tor} jest skończenie generowany (jako obraz skończenie generowanego modułu M) oraz beztorsyjny, zatem jest wolny na mocy poprzedniego twierdzenia. Druga część twierdzenia jest konsekwencją zastosowania Twierdzenia 4.16 do ciągu dokładnego

$$0 \to M_{\mathrm{tor}} \to M \to M/M_{\mathrm{tor}} \to 0.$$

Lemat 5.11.

Jeśli M jest skończenie generowanym R-modułem oraz $M \simeq U \oplus V$ dla R-modułu torsyjnego U oraz modułu wolnego V, to $U \simeq M_{\mathrm{tor}}$ oraz $V \simeq M/M_{\mathrm{tor}}$.

Dowód.

Łatwo sprawdzić, że $(U \oplus V)_{\mathrm{tor}} = \{(u, 0) \mid u \in U\} \simeq U$. Druga część tezy wynika z Wniosku 3.6 (1) zastosowanego do kanonicznego rzutowania $U \oplus V \to V$.

Oznaczenie.

Jeśli M jest R-modułem torsyjnym, to definiujemy

$$\mathscr{P}(M) := \{[p]_{\approx} \mid p \in R\text{– pierwszy}, M(p) \neq 0\}.$$

Lemat 5.12.

Jeśli m jest niezerowym elementem R-modułu torsyjnego M, to istnieją elementy pierwsze $p_1, \ldots, p_k \in R$ takie, że $[p_1]_{\approx}, \ldots, [p_k]_{\approx} \in \mathscr{P}(M)$ oraz elementy $m_i \in M(p_i)$, $i = 1, \ldots, k$, takie, że

$$m = m_1 + \cdots + m_k.$$

Dowód.

Niech r będzie rzędem elementu m. Wtedy element r jest nieodwracalny. Istnieją element odwracalny $u \in R$, elementy pierwsze $p_1, \ldots, p_k \in R$ oraz wykładniki $\alpha_1, \ldots, \alpha_k > 0$, takie, że

$$r = up_1^{\alpha_1} \cdots p_k^{\alpha_k}.$$

Niech

$$r_i := up_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k},\ i = 1, \ldots, k.$$

Elementy $r_1, \ldots, r_k$ są względnie pierwsze, więc istnieją elementy $s_1, \ldots, s_k \in R$ takie, że

$$s_1 r_1 + \cdots + s_k r_k = 1.$$

Niech $m_i := s_i r_i m$, $i = 1, \ldots, k$. Łatwo sprawdzić, ze $m_i \in M(p_i)$, $i = 1, \ldots, k$, oraz

$$m = m_1 + \cdots + m_k.$$

Ponadto $m_1, \ldots, m_k \neq 0$, więc $[p_1]_{\approx}, \ldots, [p_k]_{\approx} \in \mathscr{P}(M)$. Istotnie, gdyby $m_i = 0$, to $r_i \in \mathrm{Ann}(m)$, więc $r \mid r_i$, co jest niemożliwe.

LEMAT 5.13.

Niech M będzie R-modułem torsyjnym. Jeśli $p_1, \ldots, p_k \in R$ są elementami pierwszymi takimi, że $p_i \not\approx p_j$ dla $i \neq j$, oraz

$$m_1 + \cdots + m_k = 0$$

dla $m_i \in M(p_i)$, $i = 1, \ldots, k$, to

$$m_1 = \cdots = m_k = 0.$$

DOWÓD.

Istnieją wykładniki $\alpha_1, \ldots, \alpha_k > 0$ takie, że $p_i^{\alpha_i} m_i = 0$, $i = 1, \ldots, k$. Dla każdego $i \in \{1, \ldots, k\}$ elementy $p_i^{\alpha_i}$ oraz

$$r_i := p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}$$

są względnie pierwsze, więc istnieją elementy $s_i, t_i \in R$ takie, że $s_i p_i^{\alpha_i} + t_i r_i = 1$. Wtedy

$$m_i = (s_i p_i^{\alpha_i} + t_i r_i) m_i = -t_i r_i (m_1 + \cdots m_{i-1} + m_{i+1} + \cdots + m_k) = 0,$$

co kończy dowód.

STWIERDZENIE 5.14.

Jeśli M jest skończenie generowanym R-modułem torsyjnym, to zbiór $\mathscr{P}(M)$ jest skończony oraz

$$M \simeq \bigoplus_{[p]_\approx \in \mathscr{P}(M)} M(p).$$

DOWÓD.

Załóżmy, że elementy $m_1, \ldots, m_k$ generują moduł M. Z Lematu 5.12 wynika, że możemy założyć, iż istnieją elementy pierwsze $p_1, \ldots, p_k \in \mathscr{P}(M)$ takie, że $m_i \in M(p_i)$, $i = 1, \ldots, k$. Pokażemy, że

$$\mathscr{P}(M) = \{[p_1]_\approx, \ldots, [p_k]_\approx\}.$$

Niech $\{\{[p_1]_\approx, \ldots, [p_k]_\approx\} = \{[q_1]_\approx, \ldots, [q_l]_\approx\}$, gdzie $q_i \not\approx q_j$ dla $i \neq j$. Dla $p \in \mathscr{P}(M)$ ustalmy $m \in M(p)$, $m \neq 0$. Z założeń i Lematu 5.12 wynika, że istnieją elementy $n_i \in M(q_i)$, $i = 1, \ldots, l$, takie, że $m = n_1 + \cdots + n_l$. Ponieważ $m \neq 0$, więc z Lematu 5.13 wynika, że istnieje $i \in \{1, \ldots, l\}$ takie, że $p \approx q_i$, co kończy dowód powyższej równości.

Dla zakończenia dowodu zauważmy, że z Lematów 5.12 i 5.13 wynika, że odwzorowanie

$$\bigoplus_{i=1}^{l} M(q_i) \to M,\ (m_1, \ldots, m_l) \mapsto m_1 + \cdots + m_l,$$

jest izomorfizmem, co kończy dowód.

Obserwacja 5.15.
Jeśli $f : M \to N$ jest izomorfizmem skończenie generowanych R-modułów torsyjnych, to $M(p) \simeq N(p)$ dla dowolnego elementu pierwszego $p \in R$.

Definicja.
Jeśli $p \in R$ jest elementem pierwszym, to R-moduł torsyjny M nazywamy p-torsyjnym, jeśli $M = M(p)$.

Lemat 5.16.
Niech M będzie skończenie generowanym R-modułem torsyjnym, $p_1, \ldots, p_k \in R$ elementami pierwszymi takimi, że $p_i \not\approx p_j$ dla $i \neq j$, oraz $M_1, \ldots, M_k$ niezerowymi modułami p_1-, $\ldots$, p_k-torsyjnymi, odpowiednio. Jeśli

$$M \simeq M_1 \oplus \cdots \oplus M_k,$$

to

$$\mathscr{P}(M) = \{[p_1]_{\approx}, \ldots, [p_k]_{\approx}\}$$

oraz $M_i \simeq M(p_i)$, $i = 1, \ldots, k$.

Dowód.
Łatwo sprawdzić, że w powyższej sytuacji

$$(M_1 \oplus \cdots M_k)(p_i) = \{(0, \ldots, 0, \underbrace{m}_{i\text{-te miejsce}}, 0, \ldots, 0) \mid m \in M_i\} \simeq M_i,$$

$i = 1, \ldots, k$, oraz $(M_1 \oplus \cdots M_k)(p) = 0$ dla elementu pierwszego $p \in R$ takiego, że $p \not\approx p_i$, $i = 1, \ldots, k$, co kończy dowód wobec poprzedniej obserwacji.

Obserwacja 5.17.
Jeśli $p \in R$ jest elementem pierwszym oraz M jest skończenie generowanym R-modułem p-torsyjnym, to istnieje wykładnik $\alpha \in \mathbb{N}$ taki, że $p^\alpha M = 0$.

Obserwacja 5.18.
Niech m będzie elementem R-modułu M oraz niech $p \in R$ będzie elementem pierwszym. Jeśli $p^\alpha m = 0$ dla pewnego $\alpha \in \mathbb{N}$, to $\mathrm{Ann}(m) = (p^\beta)$ dla pewnego $\beta \in \{0, \ldots, i\}$.

LEMAT 5.19.
Niech M będzie skończenie generowanym R-modułem p-torsyjnym. Jeśli $p^\alpha M = 0$ oraz $m \in M$ jest elementem rzędu p^α, to Rm jest składnikiem prostym modułu M.

DOWÓD.
Na mocy Wniosku 3.12 wystarczy skonstruować homomorfizm $f : M \to Rm$ taki, że $f\iota = \mathrm{Id}_{Rm}$, gdzie $\iota : Rm \to M$ jest naturalnym włożeniem. Niech $m_0 := m$, m_1, $\ldots$, m_k będą generatorami modułu M i

$$N_i := Rm_0 + \cdots + Rm_i,\ i = 0, \ldots, k.$$

Dla każdego $i = 0, \ldots, k$, zdefiniujemy indukcyjnie homomorfizm $f_i : N_i \to Rm$ taki, $f_i\iota = \mathrm{Id}_{Rm}$. Wtedy $f := f_k$. Oczywiście $f_0 := \mathrm{Id}_{Rm}$.

Przypuśćmy, że $i \in \{1, \ldots, k\}$ oraz, że homomorfizm $f_{i-1} : N_{i-1} \to Rm$ jest zdefiniowany. Niech $I := \mathrm{Ann}(m_i + N_{i-1})$. Wtedy $(p^\alpha) \subset I$, więc istnieje wykładnik $\beta \in \{1, \ldots, \alpha\}$ taki, że $I = (p^\beta)$. Mamy $p^\beta m_i \in N_{i-1}$, więc istnieje element $a \in R$ taki, że $am = f_{i-1}(p^\beta m_i)$. Ponieważ $p^{\alpha-\beta}am = 0$, więc $a = p^\beta b$ dla pewnego elementu $b \in R$. Wtedy definicja

$$f_i(n + rm_i) := f_{i-1}(n) + rbm,\ n \in N_{i-1},\ r \in R,$$

jest poprawna. Oczywiście $f_i\iota = \mathrm{Id}_{Rm}$.

OBSERWACJA 5.20.
Jeśli $p \in R$ jest elementem pierwszym oraz M jest R-modułem takim, że $pM = 0$, to M jest $R/(p)$-przestrzenią liniową. (Warunek $pM = 0$ oznacza, że $M/(p)M \simeq M$).

OBSERWACJA 5.21.
Jeśli M i N są R-modułami oraz $r \in R$, to

$$(M \oplus N)[r] = M[r] \oplus N[r].$$

OBSERWACJA 5.22.
Jeśli U i V są podmodułami R-modułów M i N odpowiednio, to

$$(M \oplus N)/(U \oplus V) = (M/U) \oplus (N/V).$$

OBSERWACJA 5.23.
Jeśli m jest elementem R-modułu M, to funkcja $R/\mathrm{Ann}(m) \to Rm$, $r + \mathrm{Ann}(M) \mapsto rm$, jest izomorfizmem.

WNIOSEK 5.24.

Jeśli $p \in R$ jest elementem pierwszym i M jest skończenie generowanym R-modułem p-torsyjnym, to istnieją jednoznacznie wyznaczone wykładniki $\alpha_1 \geq \alpha_2 \geq \cdots \geq \alpha_k > 0$ takie, że

$$M \simeq R/(p^{\alpha_1}) \oplus \cdots \oplus R/(p^{\alpha_k}).$$

DOWÓD.

Istnienie wykładników wynika przez indukcję z poprzedniego lematu. Jednoznaczność jest konsekwencją następującego wzoru:

$$\#\{i \in \{1, \ldots, k\} \mid \alpha_i \geq \alpha\} = \dim_{R/(p)} M[p^\alpha]/M[p^{\alpha-1}].$$

(Zauważmy, że

$$(R/(p^\beta))[p^\alpha] = \begin{cases} R/(p^\beta) & \beta < \alpha, \\ (R/(p^\beta))(p^{\beta-\alpha} + (p^\beta)) & \beta \geq \alpha. \end{cases})$$

WNIOSEK 5.25.

Jeśli M jest skończenie generowanym R-modułem, to istnieją jednoznacznie wyznaczone parami różne klasy abstrakcji $[p_1]_\approx, \ldots, [p_k]_\approx$, $k \geq 0$, elementów pierwszych dziedziny R oraz wykładniki $\alpha \geq 0$, $\alpha_{i,1} \geq \cdots \geq \alpha_{i,l_i} > 0$, $l_i > 0$, $i = 1, \ldots, k$, takie, że

$$M \simeq R^\alpha \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} R/(p_i^{\alpha_{i,j}}).$$

DEFINICJA.

Liczbę α występującą w powyższym wniosku nazywamy RANGĄ MODUŁU M, zaś elementy (bardziej dokładnie, klasy abstrakcji elementów) $p_i^{\alpha_{i,j}}$, $i = 1, \ldots, k$, $j = 1, \ldots, l_i$, ELEMENTARNYMI DZIELNIKAMI MODUŁU M.

LEMAT 5.26.

Jeśli I i J są ideałami dziedziny R takimi, że $I + J = R$, to

$$R/I \oplus R/J \simeq R/(I \cap J).$$

DOWÓD.

Rozważmy homomorfizm $f : R \to R/I \oplus R/J$, $a \mapsto (a+I, a+J)$. Pokażemy, że homomorfizm f jest epimorfizmem. Ustalmy elementy $r \in I$ oraz $s \in J$ takie, że $r + s = 1$. Wtedy dla $a, b \in R$ otrzymujemy, że $f(sa + rb) = (a + I, b + J)$. Ponieważ $\operatorname{Ker} f = I \cap J$, więc teza wynika z Wniosku 3.6 (1).

Wniosek 5.27.
Jeśli elementy $r, s \in R$ są względnie pierwsze, to

$$R/(rs) \simeq R/(r) \oplus R/(s).$$

Dowód.
Ze Stwierdzenia 1.15 (2) wynika, że $(r) + (s) = R$. Ponadto łatwo sprawdzić, że nasze założenia implikują, iż $(r) \cap (s) = (rs)$.

Wniosek 5.28.
Jeśli $r = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$ dla elementu odwracalnego $u \in R$, parami niestowarzyszonych elementów pierwszych $p_1, \ldots, p_k \in R$ oraz wykładników $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, to

$$R/(r) \simeq R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k}).$$

Wniosek 5.29.
Jeśli M jest skończenie generowanym R-modułem, to istnieją jednoznacznie wyznaczone klasy abstrakcji $[r_1]_{\approx}$, $\ldots$, $[r_k]_{\approx}$, $k \geq 0$, elementów dziedziny R i wykładnik $\alpha \in \mathbb{N}$, takie, że $r_l \mid r_{l-1} \mid \cdots \mid r_1$ oraz

$$M \simeq R^{\alpha} \oplus R/(r_1) \oplus \cdots \oplus R/(r_l).$$

Dowód.
Jeśli

$$M \simeq R^{\alpha} \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{l_i} R/(p_i^{\alpha_{i,j}}),$$

gdzie $\alpha_{i,1} \geq \cdots \geq \alpha_{i,l_i} > 0$, to

$$r_j := \prod_{i : l_i \geq j} p_i^{\alpha_{i,j}},$$

$j = 1, \ldots, l$, gdzie $l := \max(l_1, \ldots, l_k)$.

Definicja.
Elementy (bardziej dokładnie, klasy abstrakcji elementów) r_i, $i = 1, \ldots, k$, $j = 1, \ldots, l_i$, niezmienniczymi czynnikami modułu M.