§0. Przypomnienie

Oznaczenie.
$[i, j] := \{k \in \mathbb{Z} \mid i \leq k \leq j\}$ dla $i, j \in \mathbb{Z}$.

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 $ab = 1$.

Oznaczenie.
Zbiór elementów odwracalnych pierścienia R oznaczamy $R^\times$.

Uwaga.
Jeśli R jest pierścieniem, to zbiór $R^\times$ jest grupą ze względu na mnożenie.

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 nie ma elementów nieodwracalnych.

Definicja.
Podzbiór I pierścienia R nazywamy ideałem, 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).

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

$$(a_1, \ldots, a_n) := (\{a_1, \ldots, a_n\}).$$

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.

Uwaga.

Jeśli S jest podpierścieniem pierścienia R, to funkcja $S \to R$, $s \mapsto s$, jest monomorfizmem. Z drugiej strony, jeśli $\varphi : S \to R$ jest monomorfizmem pierścieni, to funkcja $S \to \operatorname{Im}\varphi$, $s \mapsto \varphi(s)$, jest poprawnie określona i jest izomorfizmem pierścieni.

Definicja.

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

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

Definicja.

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

$$J \text{ jest ideałem pierścienia } R \wedge I \subset J \implies J = I \vee J = R.$$

Uwaga.

Każdy ideał maksymalny jest pierwszy.

Uwaga.

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

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

Uwaga.
Jeśli dziedzina R jest podpierścieniem ciała K, $a, b \in R$ oraz $a \neq 0$, to $a \mid b$ wtedy i tylko wtedy, gdy $a^{-1}b \in R$ (i wtedy $\frac{b}{a} = a^{-1}b$).

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

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, $a \in R^\times$. Zatem $a \approx 1$ wtedy i tylko wtedy, gdy element $a \in R^\times$.

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) $a \in R^\times$ wtedy i tylko wtedy, gdy $a \mid c$ dla wszystkich elementów $c \in R$,

(6) $a \in R^\times$ wtedy i tylko wtedy, gdy $(a) = R$.

Dowód.

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

(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 $c \in R^\times$.
Jeśli $a = cb$ dla elementu $c \in R^\times$, 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) Zauważmy, że $a \in R^\times$ wtedy i tylko wtedy, gdy $a \approx 1$, a więc wtedy i tylko wtedy, gdy $(a) = (1) = R$.

Uwaga.

Konsekwencją punktu (1) powyższego stwierdzenia jest fakt, że jeśli $a \mid b, c$ dla $a, b, c \in R$, to $a \mid b + c$ oraz $a \mid rc$ dla dowolnego $r \in R$.

Definicja.

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

Uwaga.

Warunek

(0) jeśli $a \mid p$, to $a \approx p$ lub $a \in R^\times$,

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 liczba $|p|$ 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

$$a \mid p \implies a \approx p \vee a \in R^{\times},$$

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 $p_i \approx q_{\sigma(i)}$ dla $i = 1, \ldots, k$.

Przykład.

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

Lemat 1.3.

Jeśli p, q_1, …, 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 z jednoznacznością rozkładu R jest nierozkładalny. Musimy pokazać, że jeśli $p \mid ab$, to $p \mid a$ lub $p \mid b$. Jeśli $a = 0$ lub $b = 0$, to teza jest oczywista. Podobnie jest, gdy $a \in R^\times$ lub $b \in R^\times$. 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 $\{1, \ldots, k\}$ 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 $a \in R^\times$ taki, że $q_l = ap_k$. Wtedy $p_1 \cdots p_{k-1} p_k = q_1 \cdots q_{l-1} a p_k$.

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 1.1 (4) i Stwierdzenie 1.2 (5)) 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 $I_1, I_2, \ldots$ są ideałami dziedziny ideałów głównych R takimi, że $I_i \subset I_{i+1}$ dla wszystkich $i = 1, 2, \ldots$, to istnieje $k > 0$ takie, że $I_i = I_k$ dla wszystkich $i = k, k+1, \ldots$.

Dowód.

Niech $I := \bigcup_{i \geq 1} I_i$. Wtedy zbiór I jest ideałem pierścienia 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 $a = p_1 \cdots p_k$.

Uwaga.

Jeśli elementy $b, c \in R$ są nieodwracalne oraz $b, c \notin S$, to $bc \notin S$.

Lemat 1.8.

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

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 $(a) \subsetneq (c)$. Zauważmy ponadto, że elementy b i c są nieodwracalne, zatem $b \in S$ lub $c \in S$ na mocy wcześniejszej uwagi.

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 $I_i := (f^i(a))$ dla $i = 1, 2, \ldots$. Wtedy $I_i \subsetneq I_{i+1}$ dla wszystkich $i = 1, 2, \ldots$, 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 będzie ideałem pierścienia R. Musimy pokazać, że istnieje element $a \in R$ taki, że $I = (a)$. Gdy $I = 0$, to teza jest oczywista, załóżmy zatem, że $I \neq 0$. Wybierzmy element $a \in I$ taki, że $\varphi(a) = \min\{\varphi(b) \mid b \in I, b \neq 0\}$. Pokażemy, że $I = (a)$. 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.
$\mathbb{Z}[\frac{1+\imath\sqrt{19}}{2}]$ jest dziedziną ideałów głównych, która nie jest dziedziną Euklidesa.

LEMAT 1.12.
Niech a będzie niezerowym elementem dziedziny z rozkładem R oraz p_1, $\ldots$, $p_k \in R$ parami niestowarzyszonymi elementami nierozkładalnymi. Jeśli dla każdego elementu nierozkładalnego $q \in R$ takiego, że $q \mid a$, istnieje $j \in \{1, \ldots, k\}$ takie, że $q \approx p_j$, to istnieją wykładniki $\alpha_1, \ldots, \alpha_k \geq 0$ oraz element $b \in R^\times$ takie, że

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

DOWÓD.
Jeśli $a \in R^\times$, to $b := a$ oraz $\alpha_i := 0$ dla $i = 1, \ldots, k$. Jeśli element $a \notin R^\times$, 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 $b_i \in R^\times$ oraz $j_i \in [1, k]$ takie, że $q_i = b_i p_{j_i}$. Wtedy $b := b_1 \cdots b_l$ oraz $\alpha_j := |\{i \in [1, l] \mid j_i = j\}|$ dla $j = 1, \ldots, k$.

Lemat 1.13.

Jeśli R jest dziedziną z jednoznacznością rozkładu, element $u \in R$ jest odwracalny, elementy $p_1, \ldots, p_k \in R$ są nierozkładalne i parami niestowarzyszone, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$, i $a \mid u p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ dla elementu $a \in R$, to istnieją wykładniki $\beta_i \in [0, \alpha_i]$, $i \in [1, k]$, oraz element $v \in R^\times$ takie, że

$$a = v p_1^{\beta_1} \cdots p_k^{\beta_k}.$$

Dowód.

Niech $q \in R$ będzie elementem nierozkładalnym takim, że $q \mid a$. Wtedy $q \mid u p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Ponieważ q jest elementem pierwszym, więc istnieje $i \in [1, k]$ takie, że $q \mid p_i$ ($q \nmid u$ oraz $q \nmid p_i^{\alpha_i}$ jeśli $\alpha_i = 0$, gdyż $q \notin R^\times$). Ponieważ element p_i jest nierozkładalny, więc $q \approx p_i$. Z poprzedniego lematu wynika zatem, że istnieją element $v \in R^\times$ oraz wykładniki $\beta_1, \ldots, \beta_k \in \mathbb{N}$ takie, że $a = v p_1^{\beta_1} \cdots p_k^{\beta_k}$. Gdyby $\beta_i > \alpha_i$ dla pewnego $i \in [1, k]$, to $p_i \mid u p_1^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k}$, co prowadziłoby do wniosku, że $p_i \mid p_j$ dla pewnego $j \neq i$, a więc do sprzeczności.

Lemat 1.14.

Jeśli R jest dziedziną z jednoznacznością rozkładu, elementy $u, b \in R$ są odwracalne, elementy $p_1, \ldots, p_k \in R$ są nierozkładalne i parami niestowarzyszone, $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \in \mathbb{N}$, oraz

$$u p_1^{\alpha_1} \cdots p_k^{\alpha_k} = v p_1^{\beta_1} \cdots p_k^{\beta_k}$$

to $u = v$ oraz $\alpha_i = \beta_i$ dla wszystkich $i \in [1, k]$.

Dowód.

Indukcja ze względu na $\alpha_1 + \cdots + \alpha_k$.

Definicja.

Niech a_i, $i \in I$, będą elementami dziedziny R. Element $d \in R$ nazywamy największym wspólnym dzielnikiem elementów a_i, $i \in I$, wtedy i tylko wtedy, gdy spełnione są następujące warunki:

(1) $d \mid a_i$ dla wszystkich $i \in I$,

(2) jeśli $b \mid a_i$ dla wszystkich $i \in I$, to $b \mid d$.

Uwaga.

Jeśli element d dziedziny R jest największym wspólnym dzielnikiem elementów a_i, $i \in I$, dziedziny R, to element $c \in R$ jest największym wspólnym dzielnikiem elementów a_i, $i \in I$, wtedy i tylko wtedy, gdy $c \approx d$.

Przykład.

Nie istnieje największy wspólny dzielnik elementów 4 i $2+2\imath\sqrt{3}$ w dziedzinie $\mathbb{Z}[\imath\sqrt{3}]$.

Definicja.

Jeśli 1 jest największym wspólnym dzielnikiem elementów a_i, $i \in I$, dziedziny R, to mówimy, że elementy a_i, $i \in I$, 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

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

dla elementów $u_1, \ldots, u_k \in R^\times$, parami niestowarzyszonych elementów nierozkładalnych $p_1, \ldots, p_l$ oraz wykładników $\alpha_{i,j} \in \mathbb{N}$, $i \in [1,k]$, $j \in [1,l]$, 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 dziedziną ideałów głównych, to element $a \in R$ jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_k$ wtedy i tylko wtedy, gdy

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

Dowód.

(1) Wynika bezpośrednio z Lematu 1.13.

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

Uwaga.

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

Uwaga.

Jeśli a, b ic są elementami dziedziny z jednoznacznością rozkładu R, przy czym elementy a i b oraz elementy a i c są względnie pierwsze, to elementy a i bc są względnie pierwsze.

Uwaga.

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

Dowód.

Ponieważ $d \mid a_i$ dla wszystkich $i \in [1, k]$, więc $\frac{d}{b}$ jest wspólnym dzielnikiem elementów $\frac{a_1}{b}, \ldots, \frac{a_k}{b}$. Ponadto, jeśli element $c \in R$ jest wspólnym dzielnikiem elementów $\frac{a_1}{b}, \ldots, \frac{a_k}{b}$, to bc jest wspólnym dzielnikiem elementów $a_1, \ldots, a_k$, więc $bc \mid d$, skąd $c \mid \frac{d}{b}$, co kończy dowód.

Uwaga.

Jeśli element d jest największym wspólnym dzielnikiem elementów $a_1, \ldots, a_k$ dziedziny R z jednoznacznością rozkładu, to dla dowolnego elementu $a \in R$ element ad 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 $\frac{c}{a} \approx d$, co kończy dowód.

Uwaga.

Jeśli $a = qb + r$ dla $a, b, q, r \in R$, to $(a, b) = (b, r)$.

Uwaga.

Jeśli R jest dziedziną Euklidesa, to największy wspólny dzielnik możemy znajdować korzystając z algorytmu Euklidesa.

§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

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

Definicja.
Wielomiany Q i H z powyższego twierdzenia nazywamy ilorazem i resztą z dzielenia wielomianu F przez wielomian G, odpowiednio.

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

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

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

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

Twierdzenie 2.3 (Twierdzenie o reszcie).
Jeśli $F \in R[X]$ oraz $a \in R$, to resztą z dzielenia wielomianu F przez wielomian $X - a$ jest $F(a)$.

Dowód.
Niech Q i H będą ilorazem i resztą z dzielenia wielomianu F przez wielomian $X - a$, odpowiednio. Wtedy $\deg H < \deg(X - a) = 1$, więc

$$H = H(a) = F(a) - (a - a)Q(a) = F(a),$$

co kończy dowód.

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

Wniosek 2.4.
Jeśli $F \in R[X]$, to element $a \in R$ jest pierwiastkiem wielomianu F wtedy i tylko wtedy, gdy $X - a \mid F$.

Wniosek 2.5.
Jeśli $F \in R[X]$, $F \neq 0$, to wielomian F ma co najwyżej $\deg F$ parami różnych pierwiastków.

Dowód.
Niech $n := \deg F$ oraz niech $a_1, \ldots, a_m \in R$ parami różnymi będą pierwiastkami wielomianu F. Indukcyjnie pokażemy, że $(X - a_1) \cdots (X - a_i) \mid F$ dla wszystkich $i \in [1, m]$, skąd $m \leq n$, co zakończy dowód. Oczywiście $X - a_1 \mid F$. Załóżmy teraz, że $i \in [2, m]$. Z założenie indukcyjnego istnieje wielomian $G \in R[X]$ taki, że $F = (X - a_1) \cdots (X - a_{i-1})G$. Wtedy

$$0 = F(a_i) = (a_i - a_1) \cdots (a_i - a_{i-1})G(a_i),$$

skąd $G(a_i) = 0$, a więc $X - a_i \mid G$, co kończy dowód.

Przykład.
Wielomian $X^3 \in \mathbb{Z}_8[X]$ ma 4 pierwiastki w pierścieniu $\mathbb{Z}_8$.

Wniosek 2.6.
Jeśli G jest skończoną podgrupą grupy $R^\times$, to grupa G jest cykliczna.

Dowód.
Niech $n := |G|$ oraz $m := \max\{|a| \mid a \in G\}$. Musimy pokazać, że $n = m$.

Oczywiście $m \leq n$. Pokażemy teraz, że $a^m = 1$ dla wszystkich elementów $a \in G$. Ponieważ wielomian $X^m - 1$ ma co najwyżej m parami różnych pierwiastków w dziedzinie R, więc to zakończy dowód. Ustalmy element $a \in G$ taki, że $|a| = m$, oraz niech $b \in G$ i $l := |b|$. Niech

$$m = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \qquad \text{oraz} \qquad l = p_1^{\beta_1} \cdots p_k^{\beta_k}$$

dla $p_1 < \cdots < p_k \in \mathbb{P}$ oraz $\alpha_1, \ldots, \alpha_k, \beta_1, \cdots, \beta_k \in \mathbb{N}$. Definiujemy

$$m' := p_1^{\gamma_1} \cdots p_k^{\gamma_k} \qquad \text{oraz} \qquad l' = p_1^{\sigma_1} \cdots p_k^{\sigma_k},$$

gdzie

$$\gamma_i := \begin{cases} \alpha_i & \alpha_i \geq \beta_i, \\ 0 & \alpha_i < \beta_i, \end{cases} \qquad \text{oraz} \qquad \sigma_i := \begin{cases} 0 & \alpha_i \geq \beta_i, \\ \beta_i & \alpha_i < \beta_i, \end{cases}$$

dla $i \in [1, k]$. Zauważmy, że $(m', l') = 1$. Wtedy $|a'b'| = m'l'$ dla $a' := a^{\frac{m}{m'}}$ i $b' := b^{\frac{l}{l'}}$. Istotnie, zauważmy najpierw, że $|a'| = m'$ i $|b'| = l'$, zatem $(a'b')^{m'l'} = 1$. Ponadto, jeśli $(a'b')^k = 1$ dla pewnego $k \in \mathbb{Z}$, to $(a')^k = (b')^{-k}$, więc $1 = (a')^{km'} = (b')^{-km'}$, skąd $l' \mid km'$ i ostatecznie $l' \mid k$. Analogicznie $m' \mid k$, zatem $l'm' \mid k$. Mamy

$$m'l' = p_1^{\max(\alpha_1, \beta_1)} \cdots p_k^{\max(\alpha_k, \beta_k)} = \operatorname{lcm}(m, l),$$

zatem $\operatorname{lcm}(m, l) = m$, skąd $l \mid m$, co kończy dowód.

Przykład.
Grupa $\mathbb{Z}_8^\times$ nie jest grupą cykliczną.

Uwaga.
Z powyższego wniosku wynika, że jeśli F jest ciałem skończonym, to grupa $F^\times$ jest cykliczna.

Uwaga.
Każda skończona dziedzina jest ciałem.

Konstrukcja.
Definiujemy

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

gdzie

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

Oznaczamy

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

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

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

Powyższe definicje są poprawne. 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, które nazywamy ciałem ułamków dziedziny R. Funkcja

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

jest monomorfizmem pierścieni. Odtąd będziemy utożsamiać obraz tego przekształcenia z dziedziną R i traktować dziedzinę R jako podpierścień ciała K. Zauważmy, że jeśli $a = bc$ dla $a, b, c \in R$ i $b \neq 0$, to $\frac{a}{b} = \frac{c}{1} = c$.

Stwierdzenie 2.7.

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.

Uwagi.

(1) Jeśli $F \in R[X]$, to $F \in (R[X])^\times$ wtedy i tylko wtedy, gdy $\deg F = 0$ oraz $F \in R^\times$.

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

(3) Jeśli $u \in R^\times$ oraz $a \in R$, to wielomian $uX + a$ jest nierozkładalny w dziedzinie $R[X]$.

PRZYKŁADY.

(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 PIERWOTNYM, jeśli elementy $a_k, \ldots, a_0$ są względnie pierwsze.

UWAGA.

Jeśli R jest dziedziną z jednoznacznością rozkładu oraz $F \in R[X]$, to istnieją wielomian pierwotny $F_1 \in R[X]$ oraz element $a \in R$ takie, $F = aF_1$. 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 pierwotny.

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 pierwotny $F_1 \in R[X]$ takie, że $aF = bF_1$. Oczywiście, gdy $F \neq 0$, to $b \neq 0$.

UWAGA.

Jeśli R jest dziedziną z jednoznacznością rozkładu, wielomian $F \in R[X]$ jest pierwotny oraz $F = GH$ dla wielomianów $GH \in R[X]$, to wielomiany G i H są pierwotne.

LEMAT 2.8 (GAUSS).

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

DOWÓD.

Niech

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

i

$$G = b_l X^l + b_{l-1} X^{l-1} + \cdots + b_0.$$

Wtedy

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

gdzie

$$c_m = a_0 b_m + a_1 b_{m-1} + \cdots + a_m b_0,\ m \in [0, k+l],$$

przy czym $a_i = 0$ dla $i > k$ oraz $b_j = 0$ dla $j > l$. Ustalmy element nierozkładalny $p \in R$. 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 $p \nmid a_{i_0} b_{j_0}$. Z dowolności elementu p wynika, że wielomian FG jest pierwotny.

Lemat 2.9.

Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K. Jeśli wielomiany $F, G \in R[X]$ są pierwotne 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 $u \in R^\times$ taki, że $a = bu$. Wtedy $bG = aF = buF$, skąd $G = uF$, co kończy dowód.

Lemat 2.10.

Niech R będzie dziedziną z jednoznacznością rozkładu z ciałem ułamków K. Jeśli wielomian $F \in R[X]$ jest pierwotny, 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 pierwotny 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 $a, b, c, d \in R$ oraz wielomiany pierwotne $G_1, H_1 \in R[X]$ 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 pierwotne, 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 $G, H \in R[X]$. Ponieważ wielomian F jest nierozkładalny w dziedzinie $K[X]$, więc bez straty ogólności można założyć, że $\deg G = 0$, tzn. $G \in R$. Stąd $G \mid 1$, gdyż wielomian F jest pierwotny, zatem element $G \in R^\times = (R[X])^\times$.

Lemat 2.11.

Niech R będzie dziedziną z jednoznacznością rozkładu. Jeśli wielomian $F \in R[X]$ jest pierwotny 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. Ponieważ $\deg F > 0$, więc z Wniosku 2.2 wynika, że istnieją wielomiany nierozkładalne $F_1, \ldots, F_k \in K[X]$ takie, że $F = F_1 \cdots F_k$. Ustalmy niezerowe elementy $a_1, b_1, \ldots, a_k, b_k \in R$ oraz wielomiany pierwotne $G_1, \ldots, G_k \in R[X]$ takie, że $a_iF_i = b_iG_i$ dla $i \in [1, k]$. 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 Lematów 2.8 oraz 2.9. Ponieważ wielomiany $G_1, \ldots, G_k$ są nierozkładalne na mocy poprzedniego lematu, to kończy dowód.

Wniosek 2.12.

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

Dowód.

Ustalmy wielomian nieodwracalny $F \in R[X]$. Istnieją element $a \in R$ oraz

wielomian pierwotny $F_1 \in R[X]$ 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 $F_1 = G_1 \cdots G_k$. Jeśli wielomian F jest pierwotny, to możemy założyć, że $a = 1$, a więc $F = G_1 \cdots G_k$. W przeciwnym wypadku element a jest nieodwracalny, więc istnieją elementy nierozkładalne $a_1, \ldots, a_l \in R$ takie, że $a = a_1 \cdots a_l$, co kończy dowód.

Lemat 2.13.

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

Dowód.

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 pierwotne $G_1, H_1 \in R[X]$ 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 2.9). W szczególności $F \mid G_1$, a więc także $F \mid G$ w dziedzinie $R[X]$.

Lemat 2.14.

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 pierwotne $G_1, H_1 \in R[X]$ 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 pierwotny, a więc nierozkładalny w dziedzinie $K[X]$ na mocy Lematu 2.10, 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 2.13.

Wniosek 2.15.

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 2.16.
Jeśli R jest dziedziną z jednoznacznością rozkładu oraz $k \geq 1$, to pierścień $R[X_1, \ldots, X_k]$ jest dziedziną z jednoznacznością rozkładu.

Wniosek 2.17.
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 2.18 (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 pierwotnym 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 pierwotne. 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 G jest pierwotny, więc istnieje $l \in \mathbb{N}$ takie, że $p \nmid b_l$. Niech $l_0 := \min\{l \mid p \nmid b_l\}$. 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 $\deg G = k$ i $\deg H = 0$. Ponadto pierwotność wielomianu H implikuje, że $H \in R^\times = R[X]^\times$.

Wniosek 2.19 (Kryterium Eisensteina II).
Niech R będzie dziedziną z jednoznacznością rozkładu z 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 pierwotny $F_1 \in R[X]$ 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 $a_i = ab_i$ dla wszystkich $i \in [0, k]$). Z poprzedniego twierdzenia wielomian F_1 jest nierozkładalny w dziedzinie $R[X]$, a więc także w dziedzinie $K[X]$ na mocy Lematu 2.10. Ponieważ element a jest odwracalny w ciele K, więc oznacza to, że wielomian F jest nierozkładalny w dziedzinie $K[X]$.

§3. Zastosowania teorii podzielności w teorii liczb

Definicja.

Mówimy, że $n \in \mathbb{Z}$ jest bezkwadratowa, jeśli $n \neq 1$ i nie istnieje $p \in \mathbb{P}$ taka, że $p^2 \mid n$.

Oznaczenie.

Jeśli $n \in \mathbb{Z}$ jest liczbą bezkwadratową, to $\mathbb{Z}[\sqrt{n}] := \{x + y\sqrt{n} \mid x, y \in \mathbb{Z}\}$.

Definicja.

Jeśli $n \in \mathbb{Z}$ jest liczbą bezkwadratową, to normą elementu $\pi = x + y\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$ nazywamy $N(\pi) := x^2 - ny^2$.

Uwaga.

Jeśli $n \in \mathbb{Z}$ jest liczbą bezkwadratową i dziedzina $\mathbb{Z}[\sqrt{n}]$ jest dziedziną z jednoznacznością rozkładu, to $n \not\equiv 1 \pmod 4$.

Twierdzenie 3.1.

Jeśli $n \in \mathbb{Z}$ jest liczbą bezkwadratową taką, że dziedzina $\mathbb{Z}[\sqrt{n}]$ jest dziedziną z jednoznacznością rozkładu, to dla $p \in \mathbb{P}$ następujące warunki są równoważne:

(1) Istnieje $\pi \in \mathbb{Z}$ taka, że $z^2 \equiv n \pmod p$.

(2) p nie jest elementem pierwszym w dziedzinie $\mathbb{Z}[\sqrt{n}]$.

(3) p jest iloczynem dwóch elementów dziedziny $\mathbb{Z}[\sqrt{n}]$, których normy są równe $\pm p$.

(4) Istnieje $\pi \in \mathbb{Z}[\sqrt{n}]$ o normie $\pm p$.

Dowód.

(1) $\Rightarrow$ (2): Jeśli istnieje $z \in \mathbb{Z}$ taka, że $z^2 \equiv n \pmod p$, to $p \mid (z - \sqrt{n})(z + \sqrt{n})$, ale $p \nmid z \pm \sqrt{n}$.

(2) $\Rightarrow$ (3): Zauważmy, że $N(p) = p^2$. Ponieważ p nie jest elementem pierwszym oraz $\mathbb{Z}[\sqrt{n}]$ jest dziedziną z jednoznacznością rozkładu, więc teza jest oczywista (zauważmy, że $N(\alpha\beta) = N(\alpha)N(\beta)$).

(3) $\Rightarrow$ (4): Oczywiste.

(4) $\Rightarrow$ (1): Przypuśćmy, że $x^2 - ny^2 = \pm p$ dla $x, y \in \mathbb{Z}$. Łatwo zauważyć, że $p \nmid y$ (istotnie, w przeciwnym wypadku $p \mid x$, więc $p^2 \mid x^2 - ny^2 = \pm p$), zatem istnieje $z \in \mathbb{Z}$ taka, że $yz \equiv 1 \pmod p$. Wtedy $(xz)^2 \equiv n \pmod p$, co kończy dowód.

Lemat 3.2.

Dziedzina $\mathbb{Z}[\imath]$ jest dziedziną z jednoznacznością rozkładu.

Dowód.

Ćwiczenie.

Uwaga.
Jeśli $p \in \mathbb{N}_+$, $p \geq 2$, i $(p-1)! \equiv -1 \pmod{p}$, to $p \in \mathbb{P}$.

Lemat 3.3 (Twierdzenie Wilsona).
Jeśli $p \in \mathbb{P}$, to $(p-1)! \equiv -1 \pmod{p}$.

Dowód.
Zauważmy, że jeśli $k, l \in [2, p-2]$ oraz $kl \equiv 1 \pmod{p}$, to $k \neq l$, zatem

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

Wniosek 3.4 (Fermat).
Jeśli $p \in \mathbb{P}$, to istnieją $x, y \in \mathbb{Z}$ takie, że $x^2 + y^2 = p$ wtedy i tylko wtedy, gdy $p = 2$ lub $p \equiv 1 \pmod{4}$.

Dowód.
Zauważmy najpierw, że jeśli $x, y \in \mathbb{Z}$, to $(x^2+y^2) \bmod 4 \in \{0, 1, 2\}$, zatem nie istnieją $x, y \in \mathbb{Z}$ takie, że $x^2+y^2 = p$, gdy $p \equiv 3 \pmod{4}$. Oczywiście takie x i y istnieją, gdy $p = 2$ (równoważnie, $p \equiv 2 \pmod{4}$), i nie jest możliwe, aby $p \equiv 0 \pmod{4}$). Załóżmy zatem, że $p \equiv 1 \pmod{4}$. Na mocy poprzedniego twierdzenia musimy pokazać, że istnieje $z \in \mathbb{Z}$ takie, że $z^2 \equiv -1 \pmod{p}$. Weźmy

$$z := \Big(\frac{p-1}{2}\Big)!.$$

Ponieważ $p \equiv 1 \pmod{4}$, więc $2 \mid \frac{p-1}{2}$, skąd

$$z = (-1)^{\frac{p-1}{2}} \Big(\frac{p-1}{2}\Big)! = (-1) \cdots \Big(-\frac{p-1}{2}\Big) \equiv (p-1) \cdots \Big(p - \frac{p-1}{2}\Big) \pmod{p},$$

więc

$$z^2 \equiv (p-1)! \equiv -1 \pmod{p}.$$

Definicja.
Jeśli $p \in \mathbb{P}$ i $a \in \mathbb{Z}$, $p \nmid a$, to mówimy, że a jest resztą kwadratową modulo p, jeśli istnieje $x \in \mathbb{Z}$ taka, że $x^2 \equiv a \pmod{p}$.

Oznaczenie.
Jeśli $p \in \mathbb{P}$, to

$$\mathscr{S}_p := \{a \in \mathbb{Z}_p^\times \mid a \text{ jest resztą kwadratową modulo } p\}.$$

Lemat 3.5.
Jeśli $p \in \mathbb{P}$, $p \neq 2$, to $|\mathscr{S}_p| = \frac{p-1}{2}$.

Dowód.
Rozważmy funkcję $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ daną wzorem $f(a) := a^2 \bmod p$. Wtedy $f(\mathbb{Z}_p^\times) = \mathscr{S}_p$. Ponadto, $|f^{-1}(a)| = 2$ dla każdego $a \in \mathscr{S}_p$. Istotnie, jeśli $x^2 \equiv a \pmod p$ dla $x \in \mathbb{Z}_p^\times$, to $x - p \in \mathbb{Z}_p^\times$, $x - p \neq x$, oraz $(x-p)^2 \equiv a \pmod p$, więc $|f^{-1}(a)| \geq 2$. Ponadto, $|f^{-1}(a)| \leq 2$ na mocy Wniosku 2.5.

Lemat 3.6.
Jeśli $p \in \mathbb{P}$, $a, b \in \mathbb{Z}_p^\times$, to

(1) $ab \bmod p \in \mathscr{S}_p$, jeśli $a, b \in \mathscr{S}_p$ lub $a, b \notin \mathscr{S}_p$,

(2) $ab \bmod p \notin \mathscr{S}_p$, jeśli $a \in \mathscr{S}_p$ lub $b \notin \mathscr{S}_p$.

Dowód.
Dla $p = 2$ tezy są oczywiste, załóżmy zatem, że $p \neq 2$. Oczywiście, jeśli $a, b \in \mathscr{S}_p$, to $ab \bmod p \in \mathscr{S}_p$. Ponadto, gdy $a \in \mathscr{S}_p$ oraz $ax \equiv 1 \pmod p$ dla $x \in \mathscr{S}_p$, to $x \in \mathscr{S}_p$. W konsekwencji, jeśli $a \in \mathscr{S}_p$ i $b \notin \mathscr{S}_p$, to $ab \pmod p \notin \mathscr{S}_p$ (istotnie, $b \equiv (ab)x \pmod p$ dla x jak wyżej).

Załóżmy zatem, że $a \notin \mathscr{S}_p$ i rozważmy funkcję $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ daną wzorem $f(b) := ab \bmod p$. Łatwo zauważyć, że funkcja f jest bijekcją. Ponadto z wcześniejszych rozważań wynika, że $f(\mathscr{S}_p) \subset \mathbb{Z}_p^\times \setminus \mathscr{S}_p$. Ponieważ $|\mathscr{S}_p| = |\mathbb{Z}_p^\times \setminus \mathscr{S}_p|$ na mocy poprzedniego lematu, więc $f(\mathscr{S}_p) = \mathbb{Z}_p^\times \setminus \mathscr{S}_p$, skąd $f(\mathbb{Z}_p^\times \setminus \mathscr{S}_p) = \mathscr{S}_p$, a to oznacza, że jeśli $b \notin \mathscr{S}_p$, to $ab \pmod p \in \mathscr{S}_p$.

Definicja.
Jeśli $p \in \mathbb{P}$, $a \in \mathbb{Z}$, $p \nmid a$, to symbolem Legendre'a a modulo p nazywamy

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \in \mathscr{S}_p, \\ -1 & a \notin \mathscr{S}_p. \end{cases}$$

Wniosek 3.7.
Jeśli $p \in \mathbb{P}$, to symbol Legendre'a jest homomorfizmem grup $\mathbb{Z}_p^\times \to \{\pm 1\}$.

Twierdzenie 3.8 (Kryterium Eulera).
Jeśli $p \in \mathbb{P}$, $p \neq 2$, $a \in \mathbb{Z}$, $p \nmid a$, to a jest resztą kwadratową modulo p wtedy i tylko wtedy, gdy $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

Dowód.
Jeśli istnieje $x \in \mathbb{Z}$ takie, że $x^2 \equiv a \pmod p$, to oczywiście $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$ na mocy twierdzenia Fermata (oczywiście $(x, p) = 1$). Załóżmy teraz, że $a^{\frac{p-1}{2}} \equiv 1 \pmod p$. Wiemy, że grupa $\mathbb{Z}_p^\times$ jest cykliczna (Wniosek 2.6). Niech $b \in \mathbb{Z}_p^\times$ będzie generatorem grupy $\mathbb{Z}_p^\times$. Ustalmy $k \in \mathbb{Z}$ takie, że $a \equiv b^k$

$(\mathrm{mod}\ p)$. Wtedy $b^{k\frac{p-1}{2}} \equiv 1\ (\mathrm{mod}\ p)$, więc $p-1 \mid k\frac{p-1}{2}$, co implikuje, że $2 \mid k$, skąd $a \equiv (b^{\frac{k}{2}})^2\ (\mathrm{mod}\ p)$.

Wniosek 3.9.
Jeśli $p \in \mathbb{P}$, $p \neq 2$, $a \in \mathbb{Z}$, $p \nmid a$, to

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Dowód.
Wobec powyższego twierdzenia wystarczy zauważyć, że na mocy twierdzenia Fermata $a^{\frac{p-1}{2}} \equiv \pm 1\ (\mathrm{mod}\ p)$.

Wniosek 3.10.
Jeśli $p \in \mathbb{P}$, $p \neq 2$, to

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4}, \\ -1 & p \equiv 3 \pmod{4}. \end{cases}$$

Twierdzenie 3.11 (Lemat Gaussa).
Niech $p \in \mathbb{P}$, $p \neq 2$. Ustalmy zbiór $S \subset \mathbb{Z}_p^\times$ takie, że $|S \cap \{a, p-a\}| = 1$ dla każdego $a \in \mathbb{Z}_p^\times$. Jeśli $a \in \mathbb{Z}_p^\times$, to

$$\left(\frac{a}{p}\right) = (-1)^\omega$$

gdzie $\omega := |(aS \bmod p) \cap (p - S)|$.

Dowód.
Zdefiniujmy funkcję $f : S \to S$ wzorem

$$f(s) := \begin{cases} as \bmod p & as \bmod p \in S, \\ p - (as \bmod p) & p - as \bmod p \in S. \end{cases}$$

Łatwo zauważyć, że funkcja f jest bijekcją, zatem

$$\prod_{s\in S} s = \prod_{s\in S} f(s) \equiv (-1)^\omega \prod_{s\in S} (as) = (-1)^\omega a^{\frac{p-1}{2}} \prod_{s\in S} s \pmod{p},$$

skąd $a^{\frac{p-1}{2}} \equiv (-1)^\omega\ (\mathrm{mod}\ p)$, co kończy dowód wobec Wniosku 3.9.

Wniosek 3.12.
Jeśli $p \in \mathbb{P}$, $p \neq 2$, to

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8}, \\ -1 & p \equiv \pm 5 \pmod{8}. \end{cases}$$

Dowód.

Niech $S := \{1, 3, \ldots, p-2\}$ oraz niech $\omega := |(2S \bmod p) \cap (p - S)|$. Zauważmy, że jeśli $a < \frac{p}{2}$, to $2a \bmod p = 2a = p - (p - 2a) \in (p - S)$. Z drugiej strony, jeśli $a > \frac{p}{2}$, to $2a \bmod p = 2a - p \in S$. Stąd

$$\omega = \left|\left\{a \in S \mid a < \frac{p}{2}\right\}\right| = \begin{cases} \frac{p-1}{4} & p \equiv 1 \pmod 4, \\ \frac{p+1}{4} & p \equiv -1 \pmod 4, \end{cases}$$

co kończy dowód.

Wniosek 3.13.

Jeśli $p \in \mathbb{P}$, $p > 2$, to

$$\left(\frac{-2}{p}\right) = \begin{cases} 1 & p \equiv 1, 3 \pmod 8, \\ -1 & p \equiv -1, -3 \pmod 8. \end{cases}$$

Dowód.

Zauważmy, że

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right).$$

Twierdzenie 3.14 (Kwadratowe Prawo Wzajemności).

Jeśli $p, q \in \mathbb{P}$, $p, q \neq 2$ i $p \neq q$, to

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Dowód.

Niech $S_1 := \{1, \ldots, \frac{p-1}{2}\}$, $S_2 := \{1, \ldots, \frac{q-1}{2}\}$, oraz $\Gamma := S_1 \times S_2$. Z Lematu Gaussa wynika, że $\left(\frac{q}{p}\right) = (-1)^{\omega_1}$, gdzie ω_1 jest ilością $x \in S_1$ takich, że reszta z dzielenia qx przez p nie należy do zbioru S_1. Zauważmy, że ω_1 jest równe ilości par $(x, y) \in \Gamma$ takich, że $-\frac{p}{2} < qx - py \leq 0$. Analogicznie, $\left(\frac{p}{q}\right) = (-1)^{\omega_2}$, gdzie ω_2 jest ilością par $(x, y) \in \Gamma$ takich, że $0 \leq qx - py < \frac{q}{2}$. Ostatecznie, $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\omega}$, gdzie ω jest ilością par $(x, y) \in \Gamma$ takich, że $-\frac{p}{2} < qx - py < \frac{q}{2}$. Rozważmy funkcję $f : \Gamma \to \Gamma$ daną wzorem $f(x, y) := \left(\frac{p+1}{2} - x, \frac{q+1}{2} - y\right)$. Oczywiście, funkcja f jest bijekcją ($f^2 = \mathrm{Id}_\Gamma$). Ponadto, $f(\Gamma_1) = \Gamma_2$, gdzie

$$\Gamma_1 := \left\{(x, y) \in \Gamma \mid qx - py \leq -\frac{p}{2}\right\}$$

i

$$\Gamma_2 := \left\{(x, y) \in \Gamma \mid qx - py \geq \frac{q}{2}\right\}.$$

Stąd

$$\omega = |\Gamma| - |\Gamma_1| - |\Gamma_2| \equiv |\Gamma| \pmod 2,$$

co kończy dowód.

Stwierdzenie 3.15.
Jeśli $p \in \mathbb{P}$, $p > 3$, to

$$\left(\frac{-3}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod 3, \\ -1 & p \equiv 2 \pmod 3. \end{cases}$$

Dowód.
Mamy ciąg równości

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right),$$

co kończy dowód.

Wniosek 3.16.
Jeśli $p \in \mathbb{P}$, $p > 3$, to

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{12}, \\ -1 & p \equiv \pm 5 \pmod{12}, \end{cases}$$

$$\left(\frac{6}{p}\right) = \begin{cases} 1 & p \equiv \pm 1, \pm 5 \pmod{24}, \\ -1 & p \equiv \pm 7, \pm 11 \pmod{24}, \end{cases}$$

$$\left(\frac{-6}{p}\right) = \begin{cases} 1 & p \equiv 1, 5, 7, 11 \pmod{24}, \\ -1 & p \equiv 13, 17, 19, 23 \pmod{24}. \end{cases}$$

Lemat 3.17.
Jeśli $n \in \{-2, 2, 3, 6\}$, to pierścień $\mathbb{Z}[\sqrt{n}]$ jest dziedziną z jednoznacznością rozkładu.

Dowód.
Dla $n \in \{-2, 2, 3\}$ dowód pozostawiamy jako ćwiczenie, zostaje zatem do pokazania, że pierścień $\mathbb{Z}[\sqrt{6}]$ jest dziedziną z jednoznacznością rozkładu.
Ustalmy $a + b\sqrt{6}, c + d\sqrt{6} \in \mathbb{Z}[\sqrt{6}]$ takie, że $c + d\sqrt{6} \neq 0$. Wiadomo, że

$$\frac{a + b\sqrt{6}}{c + d\sqrt{6}} = \frac{ac - 6bd}{c^2 - 6d^2} + \frac{bc - ad}{c^2 - 6d^2}\sqrt{6}.$$

Wybieramy $\alpha, \beta \in \mathbb{Q}$ oraz $m, n \in \mathbb{Z}$ tak, że następujące warunki są spełnione:

$$0 \leq |\beta| \leq \frac{1}{2}, \qquad m + \beta = \frac{bc - ad}{c^2 - 6d^2},$$
$$0 \leq |\alpha| \leq \frac{1}{2} \text{ jeśli } 0 \leq |\beta| < \frac{\sqrt{6}}{6},$$
$$\frac{1}{2} \leq |\alpha| \leq 1 \text{ jeśli } \frac{\sqrt{6}}{6} < |\beta| < \frac{\sqrt{30}}{12}, \qquad n + \alpha = \frac{ac - 6bd}{c^2 - 6d^2},$$
$$1 \leq |\alpha| \leq \frac{3}{2} \text{ jeśli } \frac{\sqrt{30}}{12} < |\beta| \leq \frac{1}{2}.$$

Zauważmy, że $|\alpha^2 - 6\beta^2| < 1$ oraz $(\alpha + \beta\sqrt{6})(c + d\sqrt{6}) \in \mathbb{Z}[\sqrt{6}]$. Wtedy

$$a + b\sqrt{6} = (n + m\sqrt{6})(c + d\sqrt{6}) + (\alpha + \beta\sqrt{6})(c + d\sqrt{6})$$

oraz

$$|N((\alpha + \beta\sqrt{6})(c + d\sqrt{6}))| = |\alpha^2 - 6\beta^2||N(c + d\sqrt{6})| < |N(c + d\sqrt{6})|,$$

zatem $\mathbb{Z}[\sqrt{6}]$ jest dziedziną Euklidesa, co kończy dowód.

Wniosek 3.18.

Jeśli $p \in \mathbb{P}$, to istnieją $x, y \in \mathbb{Z}$ takie, że

(1) $p = x^2 + 2y^2$ wtedy i tylko wtedy, gdy $p = 2$ lub $p \equiv 1, 3 \pmod 8$,

(2) $p = |x^2 - 2y^2|$ wtedy i tylko wtedy, gdy $p = 2$ lub $p \equiv \pm 1 \pmod 8$,

(3) $p = |x^2 - 3y^2|$ wtedy i tylko wtedy, gdy $p = 2, 3$ lub $p \equiv \pm 1 \pmod{12}$,

(4) $p = |x^2 - 6y^2|$ wtedy i tylko wtedy, gdy $p = 2, 3$ lub $p \equiv \pm 1, \pm 5 \pmod{24}$.

Uwaga.

Analogicznymi metodami, ale z wykorzystaniem pierścienia $\mathbb{Z}\left[\frac{1+\imath\sqrt{3}}{2}\right]$, można pokazać dla $p \in \mathbb{P}$ istnieją $x, y \in \mathbb{Z}$ takie, że $p = x^2 + 3y^2$, wtedy i tylko wtedy, gdy $p = 3$ lub $p \equiv 1 \pmod 3$.

Lemat 3.19.

Niech $n \in \mathbb{N}_+$ oraz niech R będzie dziedziną z jednoznacznością rozkładu. Jeśli $a_1 a_2 = u b^n$ dla względnie pierwszych elementów $a_1, a_2 \in R$ oraz elementów $u \in R^\times$ i $b \in R$, to istnieją elementy $v_1, v_2 \in R^\times$ oraz $b_1, b_2 \in R$ takie, że $a_1 = v_1 b_1^n$ oraz $a_2 = v_2 b_2^n$. Jeśli dodatkowo dla każdego elementu $u \in R^\times$ istnieje element $v \in R^\times$ taki, że $u = v^n$, to możemy założyć, że $a_1 = b_1^n$ i $a_2 = b_2^n$.

Dowód.
Ćwiczenie.

Twierdzenie 3.20 (Fermat).
Jeśli $y^2 + 2 = x^3$ dla $x, y \in \mathbb{Z}$, to $x = 3$ i $y = \pm 5$.

Dowód.
Gdyby $2 \mid y$, to $2 \mid x$, skąd $8 \mid x^3 = y^2 + 2$, co jest niemożliwe. Zatem $2 \nmid y$. Policzymy teraz największy wspólny dzielnik elementów $y - \imath\sqrt{2}$ i $y + \imath\sqrt{2}$ w dziedzinie $\mathbb{Z}[\imath\sqrt{2}]$. Zauważmy, że

$$y + \imath\sqrt{2} = (y - \imath\sqrt{2}) + 2\imath\sqrt{2},$$

Ponadto

$$\begin{aligned} y - \imath\sqrt{2} &= \left(-\frac{y-1}{4}\imath\sqrt{2}\right) \cdot (2\imath\sqrt{2}) + (1 - \imath\sqrt{2}), \\ 2\imath\sqrt{2} &= (-1 + \imath\sqrt{2})(1 - \imath\sqrt{2}) - 1, \end{aligned}$$

gdy $y \equiv 1 \pmod 4$, oraz

$$\begin{aligned} y + \imath\sqrt{2} &= \left(-\frac{y+1}{4}\imath\sqrt{2}\right) \cdot (2\imath\sqrt{2}) + (-1 - \imath\sqrt{2}), \\ 2\imath\sqrt{2} &= (-1 - \imath\sqrt{2})^2 + 1, \end{aligned}$$

gdy $y \equiv -1 \pmod 4$, zatem elementy $y - \imath\sqrt{2}$ i $y + \imath\sqrt{2}$ są względnie pierwsze w dziedzinie $\mathbb{Z}[\imath\sqrt{2}]$.

Ponieważ

$$(y + \imath\sqrt{2})(y - \imath\sqrt{2}) = x^3,$$

więc z poprzedniego lematu wynika, że istnieje element $a + b\imath\sqrt{2} \in \mathbb{Z}[\imath\sqrt{2}]$ taki, że $y + \imath\sqrt{2} = (a + b\imath\sqrt{2})^3$ (zauważmy, że $1 = 1^3$ oraz $(-1) = (-1)^3$ są jedynymi elementami odwracalnymi w dziedzinie $\mathbb{Z}[\imath\sqrt{2}]$). Wtedy

$$y = a^3 - 6ab^2 = a(a^2 - 6b^2) \qquad \text{oraz} \qquad 1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2),$$

skąd $b = \pm 1$ i $3a^2 - 2b^2 = \pm 1$, więc w efekcie $a = \pm 1$ i $b = 1$. Ostatecznie $y = \pm 5$ i $x = 3$.

Twierdzenie 3.21 (Fermat).
Jeśli $y^2 + 1 = 2x^3$ dla $x, y \in \mathbb{Z}$, to $x = 1$ i $y = \pm 1$.

Dowód.

Zauważmy najpierw, że $2 \nmid y$. Policzymy teraz największy wspólny dzielnik elementów $y+\imath$ i $y-\imath$ w dziedzinie $\mathbb{Z}[\imath]$. Mamy ciąg równości

$$\begin{aligned} y+\imath &= (y-\imath)+2\imath, \\ y-\imath &= \Big(-\frac{y-1}{2}\imath\Big)\cdot(2\imath)+(1-\imath), \\ 2\imath &= (-1+\imath)(1-\imath)+0, \end{aligned}$$

skąd wynika, że największym wspólnym dzielnikiem elementów $y+\imath$ i $y-\imath$ jest $1-\imath$. Stąd istnieją elementy $\alpha, \beta \in \mathbb{Z}[\imath]$ takie, że

$$y+\imath = (1-\imath)\alpha \qquad \text{i} \qquad y-\imath = (1-\imath)\beta.$$

Oczywiście elementy α i β są względnie pierwsze. Zauważmy, że

$$\alpha\beta = \frac{2x^3}{(1-\imath)^2} = (-\imath x)^3,$$

zatem na mocy Lematu 3.19 istnieje element $a+b\imath \in \mathbb{Z}[\imath]$ taki, że $\alpha = (a+\imath b)^3$, a więc $y+\imath = (1-\imath)(a+\imath b)^3$ (zauważmy, że $1 = 1^3$, $(-1) = (-1)^3$, $\imath = (-\imath)^3$ i $-\imath = \imath^3$ są jedynymi elementami odwracalnymi w dziedzinie $\mathbb{Z}[\imath]$). Wtedy

$$y = a^3 + 3a^2b - 3ab^2 - b^3 = (a-b)(a^2+4ab+b^2)$$

i

$$1 = -a^3 + 3a^2b - 3ab^2 - b^3 = (a+b)(-a^2+4ab-b^2).$$

Stąd $a+b = \pm 1 = -a^2+4ab-b^2$, skąd $a=0$ i $b=-1$ lub $a=-1$ i $b=0$, tzn. $y=\pm 1$ i $x=1$, co kończy dowód.

Twierdzenie 3.22 (Fermat).

Jeśli $y^2+4 = x^3$ dla $x, y \in \mathbb{Z}$, to $x=5$ i $y=\pm 11$ lub $x=2$ i $y=\pm 2$.

Dowód.

Jeśli $2 \mid y$, to $2 \mid x$. Wtedy $(\frac{y}{2})^2 + 1 = 2(\frac{x}{2})^3$, więc z poprzedniego twierdzenia wynika, że $\frac{x}{2} = 1$ oraz $\frac{y}{2} = \pm 1$, tzn. $x=2$ i $y=\pm 2$.

Załóżmy zatem teraz, że elementy x i y są nieparzyste. Policzymy teraz największy wspólny dzielnik elementów $y+2\imath$ i $y-2\imath$ w dziedzinie $\mathbb{Z}[\imath]$. Zauważmy, że

$$(y+2\imath) = (y-2\imath) + 4\imath.$$

Ponadto

$$(y-2\imath) = \left(-\frac{y-1}{4}\imath\right)\cdot(4\imath) + (1-2\imath)$$

gdy $y \equiv 1 \pmod 4$ oraz

$$(y-2\imath) = \left(-\frac{y+1}{4}\imath\right)\cdot(4\imath) + (-1-2\imath)$$

gdy $y \equiv -1 \pmod 4$. Wreszcie

$$4 = -(-1-2\imath)(1-2\imath) - 1,$$

skąd wynika, że elementy $y+2\imath$ i $y-2\imath$ są względnie pierwsze w dziedzinie $\mathbb{Z}[\imath]$.

Ponieważ

$$(y+2\imath)(y-2\imath) = x^3,$$

zatem na mocy Lematu 3.19 istnieje element $a+b\imath \in \mathbb{Z}[\imath]$ taki, że $y+2\imath = (a+b\imath)^3$. Wtedy

$$y = a^3 - 3ab^2 = a(a^2-3b^2) \qquad \text{i} \qquad 2 = 3a^2b - b^3 = b(3a^2-b^2),$$

Drugie równanie oznacza, że $b=1$ i $a=\pm 1$ lub $b=-2$ i $a=\pm 1$, a więc $y=\pm 2$ lub $y=\pm 11$. Ponieważ założyliśmy, że $2 \nmid y$, więc to kończy dowód.

Oznaczenie.
$\varepsilon := \frac{1+\imath\sqrt{3}}{2}$, $\theta := \imath\sqrt{3}$.

Uwaga.
Jeśli $\alpha \in \mathbb{C}$, to $\alpha \in \mathbb{Z}[\varepsilon]$ wtedy i tylko wtedy, gdy $\alpha = \frac{x+y\theta}{2}$ dla $x, y \in \mathbb{Z}$ takich, że $x \equiv y \pmod 2$. [$a+b\varepsilon = \frac{(2a+b)+b\theta}{2}$ oraz $\frac{x+y\theta}{2} = \frac{x-y}{2} + y\varepsilon$]

Lemat 3.23.
Pierścień $\mathbb{Z}[\varepsilon]$ jest dziedziną Euklidesa.

Dowód.
Rozważmy funkcję $N : \mathbb{Z}[\varepsilon] \to \mathbb{N}$, $z \mapsto |z|^2$, tzn. $N(a+b\varepsilon) = a^2+ab+b^2$. Jeśli $a+b\varepsilon, c+d\varepsilon \in \mathbb{Z}[\varepsilon]$ oraz $c+d\varepsilon \neq 0$, to

$$\frac{a+b\varepsilon}{c+d\varepsilon} = \frac{ac+ad+bd}{c^2+cd+d^2} + \frac{bc-ad}{c^2+cd+d^2}\varepsilon.$$

Wybieramy $\alpha, \beta \in \mathbb{Q}$ oraz $m, n \in \mathbb{Z}$ takie, że $0 \leq |\alpha|, |\beta| \leq \frac{1}{2}$,

$$n+\alpha = \frac{ac+ad+bd}{c^2+cd+d^2} \qquad \text{i} \qquad m+\beta = \frac{bc-ad}{c^2+cd+d^2}.$$

Wtedy $\alpha^2+\alpha\beta+\beta^2<1$, $(\alpha+\beta\varepsilon)(c+d\varepsilon)\in\mathbb{Z}[\varepsilon]$,

$$a+b\varepsilon=(n+m\varepsilon)(c+d\varepsilon)+(\alpha+\beta\varepsilon)(c+d\varepsilon)$$

oraz

$$N((\alpha+\beta\varepsilon)(c+d\varepsilon))=(\alpha^2+\alpha\beta+\beta^2)N(c+d\varepsilon)<N(c+d\varepsilon),$$

zatem $\mathbb{Z}[\varepsilon]$ jest dziedziną Euklidesa, co kończy dowód.

Uwaga.
$\theta=\varepsilon^2-\varepsilon^4$ oraz element θ jest nierozkładalny w dziedzinie $\mathbb{Z}[\varepsilon]$.

Uwaga.
$\mathbb{Z}[\varepsilon]^\times=\{1,\varepsilon,\varepsilon^2,\varepsilon^3,\varepsilon^4,\varepsilon^5\}=\{1,\varepsilon,-1+\varepsilon,-1,-\varepsilon,1-\varepsilon\}$.

Lemat 3.24.
Jeśli $\alpha\in\mathbb{Z}[\varepsilon]$, to istnieje $s\in\{-1,0,1\}$ takie, że $\theta\mid\alpha-s$. W szczególności, $\theta\mid\alpha^3-\alpha$.

Dowód.
Niech $\alpha=\frac{a+b\theta}{2}$ dla $a,b\in\mathbb{Z}$ takich, że $a\equiv b\pmod 2$. Istnieje $s\in\{-1,0,1\}$ takie, że $3\mid 2a-s$. Wtedy oczywiście $\theta\mid 2a-s$. Ponieważ $\alpha=\frac{b+a\theta}{2}\theta+2a$, więc kończy to dowód pierwszej części lematu. Druga część lematu wynika z równości

$$\alpha^3-\alpha=\alpha(\alpha-1)(\alpha+1).$$

Lemat 3.25.
Jeśli $\alpha\in\mathbb{Z}[\varepsilon]$ oraz $\theta\mid\alpha\pm1$, to $\theta^4\mid\alpha^3\pm1$.

Dowód.
Przypomnijmy, że $\theta^2=-3$, więc $\theta^4=9$. Jeśli $\alpha=\beta\theta\pm1$ dla $\beta\in\mathbb{Z}[\varepsilon]$, to

$$\alpha^3=\beta^3\theta^3\pm3\beta^2\theta^2+3\beta\theta\pm1=3\theta(\beta-\beta^3)\mp9\beta^2\pm1,$$

co kończy dowód wobec poprzedniego lematu.

Uwaga.
Jeśli elementy $\alpha_1,\alpha_2,\alpha_3\in\mathbb{Z}[\varepsilon]$ są względnie pierwsze, $u_1,u_2,u_3\in\mathbb{Z}[\varepsilon]^\times$, oraz $u_1\alpha_1^3+u_2\alpha_2^3+u_3\alpha_3^3=0$, to elementy α_1, α_2, α_3 są parami względnie pierwsze.

Lemat 3.26.
Jeśli elementy $\alpha_1,\alpha_2,\alpha_3\in\mathbb{Z}[\varepsilon]$ są względnie pierwsze oraz $\alpha_1^3+\alpha_2^3+\alpha_3^3=0$, to istnieje dokładnie jedno $i\in\{1,2,3\}$ takie, że $\theta\mid\alpha_i$.

Dowód.

Gdyby $\theta \nmid \alpha_i$ dla wszystkich $i \in \{1,2,3\}$, to z Lematu 3.24 wynikałoby, że dla każdego $i \in \{1,2,3\}$ istnieje $s_i \in \{-1,1\}$ takie, że $\theta \mid \alpha_i + s_i$. Z Lematu 3.25 wynika, że wtedy $\theta^4 \mid \alpha_i^3 + s_i$ dla wszystkich $i \in \{1,2,3\}$. Ponieważ

$$s_1 + s_2 + s_3 = (\alpha_1^3 + s_1) + (\alpha_2^3 + s_2) + (\alpha_3^3 + s_3) - (\alpha_1^3 + \alpha_2^3 + \alpha_3^3),$$

więc $\theta^4 \mid s_1 + s_2 + s_3$, co jest niemożliwe, gdyż $s_1 + s_2 + s_3 \in \{\pm 1, \pm 3\}$. Jedyność i wynika z powyższej uwagi.

Lemat 3.27.

Jeśli $u_1\alpha_1^3 + u_2\alpha_2^3 + u_3(\theta^n\alpha_3')^3 = 0$ dla $n \in \mathbb{N}_+$ oraz elementów $u_1, u_2, u_3 \in \mathbb{Z}[\varepsilon]^\times$ i $\alpha_1, \alpha_2, \alpha_3' \in \mathbb{Z}[\varepsilon]$ takich, że $\theta \nmid \alpha_1, \alpha_2, \alpha_3'$, to $u_2 = \pm u_1$ i $n \geq 2$.

Dowód.

Na mocy Lematu 3.24 wiemy, że istnieją $s_1, s_2 \in \{-1,1\}$ takie, że $\theta \mid \alpha_1 + s_1$ oraz $\theta \mid \alpha_2 + s_2$. Ponadto z Lematu 3.25 wynika, że w powyższej sytuacji $\theta^4 \mid \alpha_1^3 + s_1$ oraz $\theta^4 \mid \alpha_2^3 + s_2$.

Zauważmy, że $\theta^3 \mid u_1\alpha_1^3 + u_2\alpha_2^3$. Z równości

$$u_1 s_1 + u_2 s_2 = u_1(\alpha_1^3 + s_1) + u_2(\alpha_2^3 + s_2) - (u_1\alpha_1^3 + u_2\alpha_2^3)$$

wynika zatem, że $\theta^3 \mid u_1 s_1 + u_2 s_2$. Ponieważ $N(su_1 + s_2u_2) \leq 4 < 27 = N(\theta^3)$, więc oznacza to, że $s_1u_1 + s_2u_2 = 0$, zatem $u_2 = -\frac{s_2}{s_1}u_1 = \pm u_1$.

Dla dowodu drugiej części zauważmy, że równość $s_1u_1 + s_2u_2 = 0$ implikuje, że $\theta^4 \mid u_1\alpha_1^3 + u_2\alpha_2^3$, gdyż

$$u_1\alpha_1^3 + u_2\alpha_2^3 = u_1(\alpha_1^3 + s_1) + u_2(\alpha_2^3 + s_2) - (s_1u_1 + s_2u_2).$$

Stąd $\theta^4 \mid (\theta^n\alpha_3')^3$, co kończy dowód.

Lemat 3.28.

Jeśli $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = 0$ dla elementów $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}[\varepsilon]$, to istnieje $i \in \{1,2,3\}$ takie, że $\alpha_i = 0$.

Dowód.

Przypuśćmy, że istnieją elementy $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}[\varepsilon]\backslash\{0\}$ takie, że $\alpha_1^3 + \alpha_2^3 + \alpha_3^3 = 0$. Bez straty ogólności możemy założyć, że elementy α_1, α_2 i α_3 są względnie pierwsze. Na mocy Lematu 3.26 możemy wtedy założyć, że $\theta \nmid \alpha_1, \alpha_2$ oraz $\alpha_3 = \theta^n\alpha_3'$ dla $n \in \mathbb{N}_+$ i elementu $\alpha_3' \in \mathbb{Z}[\varepsilon]$ takiego, że $\theta \nmid \alpha_3'$. W szczególności, zbiór X złożony z układów $(\alpha_1, \alpha_2, \alpha_3', u_1, u_2, u_3, n)$ takich, że elementy $\alpha_1, \alpha_2, \alpha_3' \in \mathbb{Z}[\varepsilon]$ są (parami) względnie pierwsze, $u_1, u_2, u_3 \in \mathbb{Z}[\varepsilon]^\times$, $n \in \mathbb{N}_+$, $\theta \nmid \alpha_1, \alpha_2, \alpha_3'$, oraz $u_1\alpha_1^3 + u_2\alpha_2^3 + u_3(\theta^n\alpha_3')^3 = 0$, jest niepusty. Ustalmy układ $(\alpha_1, \alpha_2, \alpha_3', u_1, u_2, u_3, n) \in X$, dla którego wartość n jest minimalna. Możemy

przy tym przyjąć, że $u_1 = 1$. Przypomnijmy, że z poprzedniego lematu wynika, iż $n \geq 2$ oraz $u_2 = \pm u_1 = \pm 1$. Ponadto, jeśli $u_2 = -1$, to dla $\alpha_2' = -\alpha_2$ mamy $\alpha_1^3 + (-\alpha_2')^3 + u_3\alpha_3^3 = 0$, możemy więc przyjąć $u_2 = 1$.

Pokażemy najpierw, że $(\alpha_1 + \varepsilon^{2i}\alpha_2, \alpha_1 + \varepsilon^{2j}\alpha_2) = \theta$ dla dowolnych $i, j \in \{0,1,2\}$, $i \neq j$. Zauważmy, że

$$-u_3\theta^{3n}\alpha_3'^3 = \alpha_1^3 + \alpha_2^3 = (\alpha_1 + \alpha_2)(\alpha_1 + \varepsilon^2\alpha_2)(\alpha_1 + \varepsilon^4\alpha_2),$$

zatem istnieje $k \in \{0,1,2\}$ takie, że $\theta \mid \alpha_1 + \varepsilon^{2k}\alpha_2$, gdyż element θ jest pierwszy. Dodatkowo $\theta \mid \varepsilon^{2l} - \varepsilon^{2k}$ dla wszystkich $l \in \{0,1,2\}$ — istotnie $\theta = \varepsilon^2 - \varepsilon^4$ oraz

$$(*) \quad \varepsilon^{2l} - \varepsilon^{2k} = \begin{cases} -\varepsilon^{2l+2}(\varepsilon^2 - \varepsilon^4) & l - 1 \equiv k \pmod 3, \\ 0 & l \equiv k \pmod 3 \\ +\varepsilon^{2k+2}(\varepsilon^2 - \varepsilon^4) & l + 1 \equiv k \pmod 3, \end{cases}$$

— więc oznacza to, że $\theta \mid \alpha_1 + \varepsilon^{2l}\alpha_2$ dla wszystkich $l \in \{0,1,2\}$, gdyż

$$\alpha_1 + \varepsilon^{2l}\alpha_2 = (\alpha_1 + \varepsilon^{2k}\alpha_2) + (\varepsilon^{2l} - \varepsilon^{2k})\alpha_2.$$

Z drugiej strony, jeśli $\beta \mid \alpha_1 + \varepsilon^{2i}\alpha_2$ i $\beta \mid \alpha_1 + \varepsilon^{2j}\alpha_2$, to $\beta \mid (\varepsilon^{2i} - \varepsilon^{2j})\alpha_2$. Ponieważ elementy β i α_2 są względnie pierwsze (gdyż elementy α_1 i α_2 są względnie pierwsze), więc $\beta \mid \varepsilon^{2i} - \varepsilon^{2j}$, co wobec równości $(*)$ oznacza, że $\beta \mid \varepsilon^2 - \varepsilon^4 = \theta$ i kończy dowód równości $(\alpha_1 + \varepsilon^{2i}\alpha_2, \alpha_1 + \varepsilon^{2j}\alpha_2) = \theta$. Istnieją zatem względnie pierwsze elementy $\beta_1, \beta_2, \beta_3 \in \mathbb{Z}[\varepsilon]$ takie, że

$$\alpha_1 + \alpha_2 = \theta\beta_1, \qquad \alpha_1 + \varepsilon^2\alpha_2 = \theta\beta_2, \qquad \alpha_1 + \varepsilon^4\alpha_2 = \theta\beta_3.$$

Zauważmy, że $\theta^{3n-3} \mid \beta_1\beta_2\beta_3$, zatem bez straty ogólności możemy założyć, że $\beta_3 = \theta^{3n-3}\beta_3'$ dla pewnego elementu $\beta_3' \in \mathbb{Z}[\varepsilon]$ takiego, że $\theta \nmid \beta_3'$, oraz $\theta \nmid \beta_1, \beta_2$. Ponadto z równości $\beta_1\beta_2\beta_3' = u_3(-\alpha_3')^3$ i Lematu 3.19 wynika, że istnieją elementy $v_1, v_2, v_3 \in \mathbb{Z}[\varepsilon]^\times$ oraz $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}[\varepsilon]$ takie, że $\beta_1 = v_1\gamma_1^3$, $\beta_2 = v_2\gamma_2^3$ oraz $\beta_3' = v_3\gamma_3^3$, przy czym $\theta \nmid \gamma_1, \gamma_2, \gamma_3$ oraz elementy γ_1, γ_2 i γ_3 są względnie pierwsze. Zauważmy, że

$$(\alpha_1 + \alpha_2) + \varepsilon^2(\alpha_1 + \varepsilon^2\alpha_2) + \varepsilon^4(\alpha_1 + \varepsilon^4\alpha_2^2) = (\alpha_1 + \alpha_2)(1 + \varepsilon^2 + \varepsilon^4) = 0,$$

skąd

$$v_1\gamma_1^3 + (\varepsilon^2 v_2)\gamma_2^3 + (\varepsilon^4 v_3)(\theta^{n-1}\gamma_3)^3 = 0,$$

tzn. $(\gamma_1, \gamma_2, \gamma_3, v_1, \varepsilon^2 v_2, \varepsilon^4 v_3, n-1) \in X$, co przeczy minimalności n i kończy dowód.

Twierdzenie 3.29.

Nie istnieją $x, y, z \in \mathbb{Z} \setminus \{0\}$ takie, że $x^3 + y^3 = z^3$.

§4. Rozkład prymarny

Założenie.
Przez cały paragraf będziemy zakładać, że R jest pierścieniem.

Definicja.
Ideał właściwy Q pierścienia R nazywamy prymarnym, jeśli dla dowolnych elementów $a, b \in R$ spełniony jest warunek:

$$ab \in Q \wedge b \notin Q \implies \exists\, n \in \mathbb{N} : a^n \in Q.$$

Przykład.
Jeśli p jest elementem pierwszym w dziedzinie R, to ideał (p^n) jest prymarny dla dowolnego $n \in \mathbb{N}_+$.

Definicja.
Mówimy, że ideał I pierścienia R posiada rozkład prymarny, jeśli istnieją ideały prymarne $Q_1, \ldots, Q_n$ pierścienia R takie, że $I = Q_1 \cap \cdots \cap Q_n$.

Przykład.
Jeśli a jest elementem nieodwracalnym w dziedzinie z jednoznacznością rozkładu R, to istnieją parami niestowarzyszone elementy pierwsze $p_1, \ldots, p_n \in R$ oraz $\alpha_1, \ldots, \alpha_n \in \mathbb{N}^+$ takie, że $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$. Wtedy $(a) = (p_1^{\alpha_1}) \cap \cdots \cap (p_n^{\alpha_n})$, zatem ideał (a) posiada rozkład prymarny.

Definicja.
Pierścień R nazywamy noetherowskim, jeśli dla każdego ideału I pierścienia R istnieją elementy $a_1, \ldots, a_n \in R$ takie, że $I = (a_1, \ldots, a_n)$.

Przykład.
Jeśli R jest dziedziną ideałów głównych, to pierścień R jest noetherowski.

Lemat 4.1.
Jeśli I_n, $n \in \mathbb{N}$, są ideałami pierścienia noetherowskiego R takmi, że $I_n \subset I_{n+1}$ dla wszystkich $n \in \mathbb{N}$, to istnieje $k \in \mathbb{N}$ takie, że $I_n = I_k$ dla wszystkich $n \in \mathbb{N}$ takich, że $n \geq k$.

Dowód.
Analogiczny do dowodu Lematu 1.7.

Lemat 4.2.
Jeśli I_i, $i \in I$, $I \neq \varnothing$, są ideałami pierścienia noetherowskiego R, to istnieje $j \in I$ takie, że $I_j = \max\{I_i \mid i \in I\}$, tzn. jeśli $I_j \subset I_i$ dla pewnego $i \in I$, to $I_j = I_i$.

Dowód.
Jeśli dla każdego $i \in I$ istnieje $j_i \in I$ takie, ze $I_i \subsetneq I_{j_i}$, to możemy zdefiniować

funkcję $f : I \to I$ wzorem $f(i) := j_i$. Ustalmy $i_0 \in I$ oraz niech $i_n := f^n(i_0)$ dla $n \in \mathbb{N}$. Wtedy $I_{i_n} \subsetneq I_{i_{n+1}}$ dla wszystkich $n \in \mathbb{N}$, co przeczy poprzedniemu lematowi.

Uwaga.

Powyższy lemat pozwala dowodzić własności ideałów właściwych w pierścieniach noetherowskich przez indukcję noetherowską. Niech (W) będzie własnością ideałów właściwych. Przypuśćmy, że potrafimy udowodnić, że jeśli I jest ideałem pierścienia R takim, że każdy ideału właściwy J pierścienia R taki, że $I \subsetneq J$, posiada własność (W), to ideał I także posiada własność (W). W takiej sytuacji każdy ideał właściwy pierścienia R posiada własność (W). Istotnie, niech $\mathscr{S}$ będzie zbiorem ideałów pierścienia R nie posiadających własności (W). Jeśli $\mathscr{S} \neq \varnothing$, to z poprzedniego lematu wynika, że w zbiorze $\mathscr{S}$ istnieje ideał maksymalny I. Z maksymalności ideału I wynika, że każdy ideał właściwy J pierścienia R taki, że $I \subsetneq J$ posiada własność (W). Z założenia wynika jednak, że wtedy także ideał I posiada własność (W), co prowadzi do sprzeczności.

Twierdzenie 4.3.

Każdy ideał właściwy pierścienia noetherowskiego posiada rozkład prymarny.

Dowód.

Niech R będzie pierścieniem noetherowskim. Udowodnimy twierdzenie przez indukcję noetherowską. Niech I będzie ideałem właściwym pierścienia R takim, że każdy ideał właściwy J pierścienia R taki, że $I \subsetneq J$, posiada rozkład prymarny. Jeśli ideał I jest prymarny, to teza jest oczywista, załóżmy zatem, że ideał I nie jest prymarny. Wtedy istnieją elementy $a, b \in R$ takie, że $ab \in I$, $a \notin I$ oraz $b^n \notin I$ dla wszystkich $n \in \mathbb{N}$. Dla $n \in \mathbb{N}$ niech $I_n := \{r \in R \mid b^n r \in I\}$. Zauważmy, że zbiór I_n jest ideałem pierścienia R dla każdego $n \in \mathbb{N}$. Ponadto $I_0 = I$, $I_1 \neq I$ (gdyż $a \in I_1 \setminus I$) oraz $I_n \subset I_{n+1}$ dla każdego $n \in \mathbb{N}$, zatem na mocy Lematu 4.1 istnieje $k \in \mathbb{N}_+$ takie, że $I_n = I_k$ dla wszystkich $n \in \mathbb{N}$. Niech $J := (b^k) + I$. Oczywiście $I \subset I_k \cap J$. Z drugiej strony, jeśli $r \in I_k \cap J$, to $r = b^k s + c$ dla pewnych $s \in R$ oraz $c \in I$, przy czym $b^k r \in I$. Stąd $b^{2k} s = b^k r - b^k c \in I$, więc $s \in I_{2k} = I_k$. Ostatecznie $b^k s \in I$, skąd $r \in I$, zatem $I = I_k \cap J$. Zauważmy, że $I \subsetneq I_k \subsetneq R$, gdyż $b^k \cdot 1 = b^k \notin I$, a więc $1 \notin I_k$, zatem ideał I_k posiada rozkład prymarny. Podobnie $I \subsetneq J \subsetneq R$, gdyż gdyby $J = R$, to $I = I_k \cap J = I_k$, zatem ideał J także posiada rozkład prymarny. Ponieważ $I = I_k \cap J$, więc ideał I także posiada rozkład prymarny, co kończy dowód.

Definicja.

Radykałem ideału I pierścienia R nazywamy zbiór

$$\operatorname{rad} I := \{r \in R \mid \exists n \in \mathbb{N} : r^n \in I\}.$$

Uwaga.
Jeśli I jest ideałem pierścienia R, to zbiór $\operatorname{rad} I$ jest ideałem pierścienia R.

Uwaga.
Jeśli I jest ideałem właściwym pierścienia R, to $\operatorname{rad} I \neq R$.

Przykład.
Jeśli ideał P pierścienia R jest pierwszy, to $\operatorname{rad} P = P$.

Uwaga.
Ideał właściwy Q pierścienia R jest prymarny wtedy i tylko wtedy, gdy dla dowolnych elementów $a, b \in R$ spełniony jest warunek:

$$ab \in Q \wedge b \notin Q \implies a \in \operatorname{rad} Q.$$

Stwierdzenie 4.4.
Jeśli ideał Q jest prymarny, to ideał $\operatorname{rad} Q$ jest pierwszy.

Dowód.
Przypuśćmy, że $ab \in \operatorname{rad} Q$ oraz $a \notin \operatorname{rad} Q$. Z definicji radykału wynika, że istnieje $n \in \mathbb{N}$ takie, że $a^n b^n \in Q$. Ponieważ $a \notin \operatorname{rad} Q$, więc $a^n \notin Q$, zatem z definicji ideału prymarnego wynika, że istnieje $m \in \mathbb{N}$ takie, że $b^{nm} \in Q$. Stąd $b \in \operatorname{rad} Q$, co kończy dowód.

Definicja.
Niech P będzie ideałem pierwszym pierścienia R. Mówimy, że ideał prymarny Q jest P-prymarny, jeśli $\operatorname{rad} Q = P$.

Przykład.
Jeśli p jest elementem pierwszym w dziedzinie R, to ideał (p^n) jest (p)-prymarny dla dowolnego $n \in \mathbb{N}_+$.

Lemat 4.5.
Jeśli $I_1, \ldots, I_n$ są ideałami pierścienia R, to

$$\operatorname{rad}(I_1 \cap \cdots \cap I_n) = \operatorname{rad} I_1 \cap \cdots \cap \operatorname{rad} I_n.$$

Dowód.
Przypuśćmy najpierw, że $a \in \operatorname{rad}(I_1 \cap \cdots \cap I_n)$. Wtedy istnieje $m \in \mathbb{N}$ takie, że $a^m \in I_1 \cap \cdots \cap I_n$, tzn. $a^m \in I_i$ dla każdego $i \in [1, n]$, zatem $a \in \operatorname{rad} I_i$ dla każdego $i \in [1, n]$.

Przypuśćmy teraz, że $a \in \operatorname{rad} I_1 \cap \cdots \cap \operatorname{rad} I_n$. Wtedy dla każdego $i \in [1, n]$ istnieje $m_i \in [1, n]$ takie, że $a^{m_i} \in I_i$. Stąd dla $m := \max(m_1, \ldots, m_n)$ mamy $a^m \in I_1 \cap \cdots \cap I_n$, więc $a \in \operatorname{rad}(I_1 \cap \cdots \cap I_n)$, co kończy dowód.

UWAGA.

Niech P będzie ideałem pierwszym pierścienia R. Ideał Q pierścienia R jest P-prymarny wtedy i tylko wtedy, gdy $\operatorname{rad} Q = P$ oraz dla dowolnych elementów $a, b \in R$ spełniony jest warunek:

$$ab \in Q \wedge b \notin Q \implies a \in P.$$

STWIERDZENIE 4.6.

Niech P będzie ideałem pierwszym pierścienia R. Jeśli $Q_1, \ldots, Q_n$ są ideałami P-prymarnymi pierścienia R, to ideał $Q_1 \cap \cdots \cap Q_n$ jest P-prymarny.

DOWÓD.

Z poprzedniego lematu wynika, że

$$\operatorname{rad}(Q_1 \cap \cdots \cap Q_n) = \operatorname{rad} Q_1 \cap \cdots \cap \operatorname{rad} Q_n = P \cap \cdots \cap P = P,$$

zatem dla dowodu wystarczy pokazać, że dla dowolnych elementów $a, b \in R$, jeśli $ab \in Q_1 \cap \cdots \cap Q_n$ oraz $a \notin Q_1 \cap \cdots \cap Q_n$, to $b \in P$. Jeśli jednak $i \in [1, n]$ jest takie, że $a \notin Q_i$, to teza wynika z P-prymarności ideału Q_i.

DEFINICJA.

Rozkład prymarny $I = Q_1 \cap \cdots \cap Q_n$ ideału I pierścienia R nazywamy ZREDUKOWANYM, jeśli $\operatorname{rad} Q_i \neq \operatorname{rad} Q_j$ dla wszystkich $i \neq j$, oraz $Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_n \not\subset Q_i$ dla wszystkich $i \in [1, n]$.

TWIERDZENIE 4.7.

Jeśli ideał I posiada rozkład prymarny, to ideał I posiada zredukowany rozkład prymarny.

DOWÓD.

Niech $I = Q_1 \cap \cdots \cap Q_n$ będzie rozkładem prymarnym ideału I. Pokażemy najpierw, że możemy założyć, iż $\operatorname{rad} Q_i \neq \operatorname{rad} Q_j$ dla wszystkich $i \neq j$. Istotnie, gdy $\operatorname{rad} Q_i = \operatorname{rad} Q_j$ dla $i \neq j$, to na mocy poprzedniego lematu możemy zastąpić ideały Q_i i Q_j ideałem $Q_i \cap Q_j$. W oczywisty sposób możemy też założyć, iż drugi warunek z definicji rozkładu zredukowanego jest spełniony.

WNIOSEK 4.8.

Każdy ideał właściwy pierścienia noetherowskiego posiada zredukowany rozkład prymarny.

STWIERDZENIE 4.9.

Niech I będzie ideałem pierścienia R. Jeśli $I \subset P_1 \cup \cdots \cup P_n$ dla ideałów pierwszych $P_1, \ldots, P_n$ pierścienia R, to istnieje $i \in [1, n]$ takie, że $I \subset P_i$.

Dowód.

Bez straty ogólności możemy założyć, że $n > 1$ oraz $I \not\subset P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_n$ dla każdego $i \in [1,n]$. Ustalmy elementy $a_1, \ldots, a_n \in I$ takie, że $a_i \notin P_1 \cup \cdots \cup P_{i-1} \cup P_{i+1} \cup \cdots \cup P_n$ dla każdego $i \in [1,n]$. Zauważmy, że $a_i \in P_i$ dla każdego $i \in [1,n]$. Wtedy $a_1 + a_2 \cdots a_n \in I$, zatem istnieje $i \in [1,n]$ takie, że $a_1 + a_2 \cdots a_n \in P_i$. Jeśli $i = 1$, to $a_2 \cdots a_n \in P_1$, a więc istnieje $j \in [2,n]$ takie, że $a_j \in P_1$, co jest niemożliwe. Jeśli natomiast $i \in [2,n]$, to $a_1 \in P_i$, co też jest niemożliwe.

Lemat 4.10.

Niech $I = Q_1 \cap \cdots Q_n$ i $I = Q'_1 \cap \cdots \cap Q'_m$ będą zredukowanymi rozkładami prymarnymi ideału właściwego I pierścienia R. Jeśli ideał $\operatorname{rad} Q_1$ jest maksymalny w zbiorze $\{\operatorname{rad} Q_1, \ldots, \operatorname{rad} Q_n, \operatorname{rad} Q'_1, \ldots, Q'_m\}$, to istnieje $i \in [1,m]$ takie, że $\operatorname{rad} Q_1 = \operatorname{rad} Q'_i$ oraz $Q_2 \cap \cdots \cap Q_n = Q'_1 \cap \cdots \cap Q'_{i-1} \cap Q'_{i+1} \cap \cdots \cap Q'_m$.

Dowód.

Niech $P_i := \operatorname{rad} Q_i$ dla $i \in [1,n]$ oraz $P'_i := \operatorname{rad} Q'_i$ dla $i \in [1,m]$. Niech $\Lambda := \{i \in [1,m] \mid P_1 \neq P'_i\}$. Z maksymalności ideału P_1 wynika, że $P_1 \not\subset P_i$ dla wszystkich $i \in [2,n]$ oraz $P_1 \not\subset P'_i$ dla wszystkich $i \in \Lambda$. Z poprzedniego stwierdzenia wynika zatem, że istnieje element $a \in P_1$ taki, że $a \notin P_i$ dla wszystkich $i \in [2,n]$ oraz $a \notin P'_i$ dla wszystkich $i \in \Lambda$. Wiemy, że istnieje $k \in \mathbb{N}$ takie, że $a^k \in Q_1 \cap \bigcap_{i \in [1,m] \setminus \Lambda} Q'_i$ (gdzie $\bigcap_{i \in [1,m] \setminus \Lambda} Q'_i := R$, gdy $\Lambda = [1,m]$). Niech $J := \{b \in R \mid a^k b \in I\}$. Pokażemy, że

$$J = Q_2 \cap \cdots \cap Q_n \qquad \text{i} \qquad J = \bigcap_{i \in \Lambda} Q'_i,$$

co wobec zredukowalności przedstawień $I = Q_1 \cap \cdots \cap Q_n$ i $I = Q'_1 \cap \cdots \cap Q'_m$ zakończy dowód. Zauważmy najpierw, że jeśli $b \in Q_2 \cap \cdots \cap Q_n$, to $a^k b \in Q_1 \cap Q_2 \cap \cdots \cap Q_n = I$. Analogicznie, gdy $b \in \bigcap_{i \in \Lambda} Q'_i$, to $a^k b \in I$. Przypuśćmy teraz, że $a^k b \in I$. Wtedy $a^k b \in Q_i$, więc $b \in Q_i$ (gdyż $a \notin P_i$) dla każdego $i \in [2,n]$. Analogicznie pokazujemy, że $b \in Q'_i$ dla każdego $i \in \Lambda$, co kończy dowód.

Twierdzenie 4.11.

Jeśli $I = Q_1 \cap \cdots Q_n$ i $I = Q'_1 \cap \cdots \cap Q'_m$ są zredukowanymi rozkładami prymarnymi ideału I pierścienia R, to $n = m$ oraz istnieje permutacja σ zbioru $[1,n]$ taka, że $\operatorname{rad} Q_i = \operatorname{rad} Q'_{\sigma(i)}$ dla każdego $i \in [1,n]$.

Dowód.

Indukcja wykorzystująca powyższy lemat.

Definicja.

Jeśli $I = Q_1 \cap \cdots Q_n$ jest zredukowanym rozkładem prymarnym ideału wła-

ściwego I pierścienia R, to ideały $\operatorname{rad} Q_1, \ldots, \operatorname{rad} Q_n$ nazywamy IDEAŁAMI PIERWSZYMI STOWARZYSZONYMI Z IDEAŁEM I.

Definicja.

Ideał pierwszy P stowarzyszony z ideałem właściwym I pierścienia R nazywamy IZOLOWANYM, jeśli $P' \not\subset P$ dla każdego ideału pierwszego $P' \neq P$ stowarzyszonego z ideałem I.

Twierdzenie 4.12.

Jeśli $I = Q_1 \cap \cdots Q_n$ i $I = Q'_1 \cap \cdots \cap Q'_n$ są zredukowanymi rozkładami prymarnymi ideału I pierścienia R takimi, że $\operatorname{rad} Q_i = \operatorname{rad} Q'_i$ dla każdego $i \in [1, n]$, to $Q_i = Q'_i$ dla każdego $i \in [1, n]$ takiego, że ideał $\operatorname{rad} Q_i$ jest izolowany.

Dowód.

Niech $P_i := \operatorname{rad} Q_i$ dla $i \in [1, n]$. Bez straty ogólności możemy założyć, że ideał P_1 jest izolowany. Wtedy dla każdego $i \in [2, n]$ istnieje element $a_i \in P_i \setminus P_1$. Niech $a := a_2 \cdots a_n$. Zauważmy, że $a \in P_2 \cap \cdots \cap P_n \setminus P_1$. Wtedy istnieje $m \in \mathbb{N}$ takie, że $a^m \in Q_i$ oraz $a^m \in Q'_i$ dla wszystkich $i \in [2, n]$. Pokażemy, że $Q_1 = Q = Q'_1$, gdzie $Q := \{b \in R \mid a^m b \in I\}$. Jeśli $b \in Q_1$, to $a^m b \in Q_1 \cap Q_2 \cap \cdots \cap Q_n = I$, więc $Q_1 \subset Q$. Z drugiej strony, jeśli $a^m b \in I$ dla $b \in R$, to $a^m b \in Q_1$, więc $b \in Q_1$ (gdyż z założenia $a \notin P_1$), zatem $Q \subset Q_1$. Analogicznie pokazujemy, że $Q = Q'_1$, co kończy dowód.

Przykład.

Jeśli K jest ciałem, to ideał (X^2, XY) mam następujące rozkładu prymarne w pierścieniu $K[X, Y]$:

$$(X^2, XY) = (X) \cap (X^2, Y) \qquad \text{i} \qquad (X^2, XY) = (X) \cap (X^2, XY, Y^2).$$

Zauważmy, że $\operatorname{rad}(X) = (X) \subset (X, Y) = \operatorname{rad}(X^2, Y) = (X^2, XY, Y^2)$.

Twierdzenie 4.13 (Hilberta o bazie).

Jeśli pierścień R jest noetherowski, to pierścień $R[X]$ jest noetherowski.

Dowód.

Niech I będzie ideałem pierścienia $R[X]$. Musimy pokazać, że ideał I jest skończenie generowany. Jeśli $I = 0$, to teza jest oczywista, załóżmy zatem, że $I \neq 0$. Niech J będzie podzbiorem pierścienia R złożonym z 0 oraz współczynników wiodących wielomianów należących do ideału I. Wtedy zbiór J jest ideałem pierścienia R, istnieją zatem elementy $a_1, \ldots, a_n \in R$ takie, że $I = (a_1, \ldots, a_n)$. Ustalmy wielomiany $F_1, \ldots, F_n \in I$ takie, że dla wszystkich $i \in [1, k]$ współczynnik wiodący wielomianu F_i jest równy a_i. Bez straty ogólności możemy założyć, że $\deg F_1 = \cdots = \deg F_n =: d$. Dla każdego $k \in [0, d-1]$ niech J_k będzie podzbiorem pierścienia R złożonym z 0

oraz współczynników wiodących wielomianów stopnia k należących do ideału I. Wtedy zbiór J_k jest ideałem pierścienia R, zatem istnieją elementy $a_{k,1}, \ldots, a_{k,n_k} \in R$ takie, że $J_k = (a_{k,1}, \ldots, a_{k,n_k})$. Ustalmy wielomiany $F_{k,1}, \ldots, F_{k,n_k} \in I$ stopnia k takie, że dla każdego $i \in [1, n_k]$ współczynnik wiodący wielomianu $F_{k,i}$ jest równy $a_{k,i}$. Pokażemy, że

$$I = (F_1, \ldots, F_n, F_{d-1,1}, \ldots, F_{d-1,n_{d-1}}, \ldots, F_{0,1}, \ldots, F_{0,n_0}).$$

Jedna inkluzja jest oczywista, wystarczy zatem, że przez indukcję ze względu na $\deg F$ udowodnimy implikację

$$F \in I \Longrightarrow F \in (F_1, \ldots, F_n, F_{d-1,1}, \ldots, F_{d-1,n_{d-1}}, \ldots, F_{0,1}, \ldots, F_{0,n_0}).$$

Jeśli $\deg F = -\infty$, tzn. $F = 0$, to teza jest oczywista, załóżmy zatem, że $k := \deg F \geq 0$ i niech a będzie współczynnikiem wiodącym wielomianu F. Jeśli $k < d$, to istnieją elementy $b_1, \ldots, b_{n_k} \in R$ takie, że $a = b_1 a_{k,1} + \cdots + b_{n_k} a_{k,n_k}$, więc $\deg(F - (b_1 F_{k,1} + \cdots + b_{n_k} F_{k,n_k}) < k$. Analogicznie, gdy $k \geq d$, to istnieją elementy $b_1, \ldots, b_n \in R$ takie, że $a = b_1 a_1 + \cdots + b_n a_n$, więc $\deg(F - (b_1 F_1 + \cdots + b_n F_n) X^{k-d}) < k$. W obu przypadkach możemy więc zastosować założenie indukcyjne, co kończy dowód.

Wniosek 4.14.
Dla dowolnych ciała K oraz $n \in \mathbb{N}_+$ pierścień $K[X_1, \ldots, X_n]$ jest noetherowski.

Wniosek 4.15.
Dla dowolnego $n \in \mathbb{N}_+$ pierścień $\mathbb{Z}[X_1, \ldots, X_n]$ jest noetherowski.

Lemat 4.16.
Jeśli I jest ideałem pierścienia noetherowskiego R, to pierścień R/I jest noetherowski.

Przykład.
Jeśli $n \in \mathbb{Z}$ jest liczba bezkwadratową, to pierścień $\mathbb{Z}[\sqrt{n}]$ jest noetherowski. $[\mathbb{Z}[\sqrt{n}] \simeq \mathbb{Z}[X]/(X^2 - n)]$

Przykład.
W pierścieniu $\mathbb{Z}[\sqrt{5}]$ element 2 jest nierozkładalny, ale nie jest pierwszy. W szczególności ideał (2) nie jest pierwszy. Jest to jednak ideał prymarny oraz $\mathrm{rad}(2) = (2, \sqrt{5} - 1)$. Przypomnijmy, że $2 \cdot 2 = (\sqrt{5} + 1)(\sqrt{5} - 1)$.