Wykład 13
Rozkłady elementów pierścienia na czynniki

1 Elementy nierozkładalne w pierścieniach $\mathbb{Z}[x]$ i $\mathbb{Q}[x]$

Twierdzenie 13.1. *Niech p będzie liczbą pierwszą i niech $f, g \in \mathbb{Z}[x]$. Jeżeli $p \mid f \cdot g$, to $p \mid f$ lub $p \mid g$.*

Dowód. Z założenia istnieje $h \in \mathbb{Z}[x]$ takie, że $f \cdot g = p \cdot h$. Z Przykładu 10.32 i z Twierdzenia 11.15 przekształcenie $T\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ dane wzorem

$$T(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) = [a_n]_p x^n + [a_{n-1}]_p x^{n-1} + \ldots + [a_1]_p x + [a_0]_p$$

jest homomorfizmem pierścieni o jądrze (p). Stąd $T(f)\cdot T(g) = 0$ w pierścieniu $\mathbb{Z}_p[x]$. Ale $\mathbb{Z}_p$ jest ciałem, gdyż p jest liczbą pierwszą, więc z Twierdzenia 11.4, $\mathbb{Z}_p[x]$ jest dziedziną całkowitości, skąd $T(f) = 0$ lub $T(g) = 0$, czyli $f \in (p)$ lub $g \in (p)$. Zatem $p \mid f$ lub $p \mid g$ w pierścieniu $\mathbb{Z}[x]$. □

Definicja 13.2. Powiemy, że wielomian

$$f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$$

jest *pierwotny*, jeżeli $st(f) \geq 1$ oraz $(a_0, a_1, \ldots, a_n) = 1$, tzn. jeżeli nie istnieje liczba pierwsza p taka, że $p \mid f$ w pierścieniu $\mathbb{Z}[x]$.

Z Twierdzenia 13.1 wynika od razu następujący

Lemat 13.3 (Gaussa). *Iloczyn wielomianów pierwotnych jest wielomianem pierwotnym.* □

Twierdzenie 13.4. *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem pierwotnym. Wówczas równoważne są warunki:*

(i) f jest nierozkładalny w pierścieniu $\mathbb{Z}[x]$,

(ii) f jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$.

Dowód. Ponieważ f jest wielomianem pierwotnym, więc $st(f) = n \geq 1$. $(ii) \Rightarrow (i)$. Załóżmy, że f jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$. Jeżeli $f = g \cdot h$ dla pewnych $g, h \in \mathbb{Z}[x]$, to $g \in \mathbb{Q}^*$ lub $h \in \mathbb{Q}^*$, skąd $g \in \mathbb{Z} \setminus \{0\}$ lub $h \in \mathbb{Z} \setminus \{0\}$. Można zakładać, że $g \in \mathbb{Z} \setminus \{0\}$. Jeśli $g \notin \mathbb{Z}^* = \{1, -1\}$, to $|g| > 1$, więc istnieje liczba pierwsza p taka, że $p|g$ w pierścieniu $\mathbb{Z}$, skąd $p|f$ w pierścieniu $\mathbb{Z}[x]$ i mamy sprzeczność. Zatem $g \in \mathbb{Z}^*$, skąd wynika, że f jest nierozkładalny w pierścieniu $\mathbb{Z}[x]$.

$(i) \Rightarrow (ii)$. Załóżmy teraz, że f jest nierozkładalny w pierścieniu $\mathbb{Z}[x]$. Załóżmy, że f nie jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$. Istnieją wtedy wielomiany $g, h \in \mathbb{Q}[x]$ dodatnich stopni takie, że $f = g \cdot h$. Wtedy istnieją liczby naturalne k, l takie, że $kg, lh \in \mathbb{Z}[x]$ oraz $(kl)f = (kg) \cdot (lh)$. Istnieje zatem najmniejsza liczba naturalna s taka, że wielomian sf jest iloczynem dwóch wielomianów $\phi, \psi \in \mathbb{Z}[x]$ dodatnich stopni. Jeżeli $s > 1$, to istnieje liczba pierwsza p taka, że $p \mid s$. Wtedy z Twierdzenia 13.1, $p \mid \phi$ lub $p \mid \psi$ w pierścieniu $\mathbb{Z}[x]$. Bez zmniejszania ogólności możemy zakładać, że $p \mid \phi$. Wtedy $\frac{s}{p} f = (\frac{\phi}{p}) \cdot \psi$ i mamy sprzeczność z minimalnością s. Zatem $s = 1$ oraz $f = \phi \cdot \psi$. Ale $st(\phi), st(\psi) \geq 1$ oraz $(\mathbb{Z}[x])^* = \mathbb{Z}^* = \{1, -1\}$, więc mamy sprzeczność z nierozkładalnością wielomianu f w pierścieniu $\mathbb{Z}[x]$. $\square$

Twierdzenie 13.5. *Niech P będzie dziedziną całkowitości. Wielomian unormowany $f \in P[x]$ jest elementem rozkładalnym w pierścieniu $P[x]$ wtedy i tylko wtedy, gdy istnieją wielomiany unormowane $g, h \in P[x]$ dodatnich stopni takie, że $f = g \cdot h$.*

Dowód. $\Rightarrow$. Z założenia istnieją wielomiany niezerowe nieodwracalne $g_1, h_1 \in P[x]$ takie, że $f = g_1 \cdot h_1$. Zatem na mocy Twierdzenia 11.5, $st(g_1), st(h_1) \geq 1$. Niech a będzie najstarszym współczynnikiem wielomianu g_1, zaś b niech będzie najstarszym współczynnikiem wielomianu h_1. Wtedy ze Stwierdzenia 11.1 i tego, że wielomian f jest unormowany, $1 = ab$, skąd $a, b \in P^*$. Zatem oraz bg_1, ah_1 są wielomianami unormowanymi dodatnich stopni i $(bg_1) \cdot (ah_1) = (ab)(g_1 \cdot h_1) = g_1 \cdot h_1 = f$.

$\Leftarrow$. Z założenia $f = gh$ dla pewnych unormowanych wielomianów $g, h \in P[x]$. Stąd $g, h \neq 0$ i $st(g), st(h) > 0$. Ale na mocy Twierdzenia 11.5, $(P[x])^* = P^*$, więc $g, h \notin (P[x])^*$. Zatem f jest elementem rozkładalnym w pierścieniu $P[x]$. $\square$

Twierdzenie 13.6 (kryterium Eisensteina). *Niech $f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ będzie wielomianem pierwotnym stopnia $n \geq 1$. Jeżeli istnieje liczba pierwsza p taka, że $p \nmid a_n$, $p \mid a_i$ dla $i = 0, 1, \ldots, n-1$ oraz $p^2 \nmid a_0$, to f jest nierozkładalny w pierścieniach $\mathbb{Q}[x]$ i $\mathbb{Z}[x]$.*

Dowód. Dla $n = 1$ teza jest oczywista na mocy pierwotności wielomianu f. Niech dalej $n \geq 2$ i załóżmy, że f jest rozkładalny w $\mathbb{Q}[x]$. Wtedy z Twierdzenia 13.4, f jest rozkładalny w pierścieniu $\mathbb{Z}[x]$. Z pierwotności f wynika, że istnieją wielomiany $g, h \in \mathbb{Z}[x]$ dodatnich stopni takie, że $f = g \cdot h$. Niech $g = b_s x^s + b_{s-1} x^{s-1} + \ldots + b_1 x + b_0$, $b_s \neq 0$ oraz $h = c_r x^r + c_{r-1} x^{r-1} + \ldots + c_1 x + c_0$, $c_r \neq 0$. Wtedy $s + r = n$ i $c_r b_s = a_n$ oraz $b_0 c_0 = a_0$. Stąd z pierwszości p, $p \mid b_0$ lub $p \mid c_0$. Bez zmniejszania ogólności rozważań możemy zakładać, że $p \mid b_0$. Ponieważ $p^2 \nmid a_0$, więc stąd $p \nmid c_0$. Ponadto $p \nmid a_n$, więc $p \nmid b_s$ i $p \nmid c_r$. Istnieje zatem największa nieujemna liczba całkowita $k \leq s - 1$ taka, że $p \mid b_i$ dla wszystkich $i = 0, 1, \ldots, k$. Ponadto $k + 1 \leqslant s < n$, więc $p \mid a_{k+1} = \sum_{i=0}^{k+1} b_i c_{k+1-i} = \sum_{i=0}^{k} b_i c_{k+1-i} + b_{k+1} c_0$. Ale $p \mid b_i$ dla $i = 0, 1, \ldots, k$, więc $p \mid b_{k+1} c_0$ i $p \nmid c_0$, czyli $p \mid b_{k+1}$ i

mamy sprzeczność z maksymalnością k. Oznacza to, że wielomian f jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$ i na mocy Twierdzenia 13.4, f jest nierozkładalny w pierścieniu $\mathbb{Z}[x]$. $\square$

Wniosek 13.7. *W pierścieniu $\mathbb{Q}[x]$ istnieją wielomiany nierozkładalne dowolnego dodatniego stopnia.*

Dowód. Dla naturalnych n wielomian $f_n = x^n + 2$ jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$ na mocy kryterium Eisensteina przy $p = 2$. $\square$

2 Elementy pierwsze

Definicja 13.8. Element a dziedziny całkowitości P nazywamy *elementem pierwszym* w P, jeżeli $a \neq 0$, $a \notin P^*$ oraz dla dowolnych $x, y \in P$ z tego, że $a \mid xy$ wynika, że $a \mid x$ lub $a \mid y$.

Twierdzenie 13.9. *Każdy element pierwszy dziedziny całkowitości P jest elementem nierozkładalnym w P.*

Dowód. Niech p będzie elementem pierwszym dziedziny całkowitości P. Wtedy $p \neq 0$ i $p \notin P^*$. Weźmy dowolne $x, y \in P$ takie, że $p = xy$. Wtedy $p \mid xy$, więc $p \mid x$ lub $p \mid y$. Zatem $x = pt$ lub $y = pt$ dla pewnego $t \in P$. Stąd $p = pty$ lub $p = xpt$, więc $1 = ty$ lub $1 = xt$, czyli $y \in P^*$ lub $x \in P^*$. Zatem p jest elementem nierozkładalnym w pierścieniu P. $\square$

Przykład 13.10. Podamy przykład elementu nierozkładalnego, który nie jest elementem pierwszym. Proste sprawdzenie pokazuje, że $P = \mathbb{Z} + (x^2)$ jest podpierścieniem pierścienia $\mathbb{Z}[x]$. Stąd P jest dziedziną całkowitości i $P^* \subseteq (\mathbb{Z}[x])^* = \{1, -1\}$, skąd $P^* = \{1, -1\}$. Ponadto $P = \{a_0 + a_2x^2 + \ldots + a_nx^n : a_0, a_2, \ldots, a_n \in \mathbb{Z}, n \in \mathbb{N}_0\}$, więc $x \notin P$ oraz $x^k \in P$ dla $k = 2, 3, \ldots$. Stąd $x^2 \neq 0$, $x^2 \notin P^*$. Ponadto $x^2 | x^3 \cdot x^3$ w P, bo $x^6 = x^2 \cdot x^4$ i $x^4 \in P$, ale x^2 nie dzieli x^3, bo inaczej $x^3 = x^2 f$ dla pewnego $f \in P$, skąd $f = x$ i $x \in P$, sprzeczność. Zatem x^2 nie jest elementem pierwszym w P. Weźmy dowolne $u, v \in P$ takie, że $x^2 = u \cdot v$. Wtedy $2 = st(u) + st(v)$, a ponieważ w P nie ma wielomianu stopnia 1, więc $st(u) = 0$ i $st(v) = 2$ lub $st(u) = 2$ i $st(v) = 0$. Jeśli $st(u) = 0$ i $st(v) = 2$, to $u \in \mathbb{Z}$ i $v = ax^2 + b$ dla pewnych $a, b \in \mathbb{Z}$, skąd $1 = u \cdot a$, więc $u = \pm 1$, czyli $u \in P^*$. Jeśli zaś $st(u) = 2$ i $st(v) = 0$, to rozumując podobnie uzyskamy, że $v \in P^*$. Wobec tego x^2 jest elementem nierozkładalnym w P.

Twierdzenie 13.11. *Dla dowolnego niezerowego elementu p dziedziny całkowitości P równoważne są warunki:*

(i) p jest elementem pierwszym w P,

(ii) ideał (p) jest pierwszy w P.

Dowód. $(i) \Rightarrow ii)$. Z założenia $p \notin P^*$, więc $1 \notin (p)$, czyli $(p) \neq P$. Niech $a, b \in P$ będą takie, że $ab \in (p)$. Wtedy $p \mid ab$, więc z pierwszości p, $p \mid a$ lub $p \mid b$, czyli $a \in (p)$ lub $b \in (p)$. Zatem (p) jest ideałem pierwszym w P.

$(ii) \Rightarrow (i)$. Z założenia $(p) \neq P$, więc $1 \notin (p)$, czyli $p \notin P^*$. Ponadto z założenia $p \neq 0$. Weźmy dowolne $x, y \in P$ takie, że $p \mid xy$. Wtedy $xy \in (p)$, więc z pierwszości ideału (p), $x \in (p)$ lub $y \in (p)$, czyli $p \mid x$ lub $p \mid y$. Zatem p jest elementem pierwszym w pierścieniu P. $\square$

Stwierdzenie 13.12. *Niech f będzie automorfizmem dziedziny całkowitości P i niech $a \in P$. Wówczas:*

(a) $a \in P^* \Leftrightarrow f(a) \in P^*$,

(b) a jest rozkładalny w $P \Leftrightarrow f(a)$ jest rozkładalny w P,

(c) a jest nierozkładalny w $P \Leftrightarrow f(a)$ jest nierozkładalny w P,

(d) a jest elementem pierwszym w $P \Leftrightarrow f(a)$ jest elementem pierwszym w P.

Dowód. (a). Niech $a \in P^*$. Wtedy istnieje $b \in P$ takie, że $a \cdot b = 1$. Stąd $f(a \cdot b) = f(1)$, a więc $f(a) \cdot f(b) = 1$, skąd $f(a) \in P^*$. Ponadto f^{-1} jest automorfizmem pierścienia P, więc jeśli $f(a) \in P^*$, to $a = f^{-1}(f(a)) \in P^*$.

(b). Niech a będzie rozkładalny w P. Wtedy istnieją niezerowe elementy nieodwracalne $x, y \in P$ takie, że $a = x \cdot y$. Stąd $f(a) = f(x) \cdot f(y)$. Ponadto $Ker(f) = \{0\}$, gdyż f jest automorfizmem, więc $f(x), f(y) \neq 0$ oraz na mocy (a), $f(x), f(y) \notin P^*$. Zatem $f(a)$ jest rozkładalny w P. Implikacja odwrotna wynika z pierwszej części dowodu (b) i z tego, że f^{-1} jest automorfizmem P.

(c). Niech a będzie nierozkładalny w P. Wtedy $a \neq 0$ i $a \notin P^*$, więc $f(a) \neq 0$ i z (a), $f(a) \notin P^*$. Jeśli $f(a)$ jest rozkładalny w P, to z (b), a jest rozkładalny w P, sprzeczność. Zatem $f(a)$ jest nierozkładalny w P. Implikacja odwrotna wynika z pierwszej części dowodu (c) i z tego, że f^{-1} jest automorfizmem P.

(d). Niech a będzie elementem pierwszym w P. Wtedy $a \neq 0$ i $a \notin P^*$, więc $f(a) \neq 0$ i z (a), $f(a) \notin P^*$. Weźmy dowolne $x, y \in P$ takie, że $f(a) | x \cdot y$. Wtedy $x \cdot y = f(a) \cdot b$ dla pewnego $b \in P$. Ale f jest "na", więc $x = f(u)$, $y = f(v)$ i $b = f(w)$ dla pewnych $u, v, w \in p$. Zatem $f(u \cdot v) = f(a \cdot w$, skąd $u \cdot v = a \cdot w$, bo f jest "1-1". Z pierwszości elementu a mamy, że $a | u$ lub $a | v$. Jeśli $a | u$, to $u = a \cdot t$ dla pewnego $t \in P$, więc $x = f(u) = f(a) \cdot f(t)$, skąd $f(a) | x$. Jeśli zaś $a | v$, to podobnie uzyskamy, że $f(a) | y$. Zatem $f(a)$ jest elementem pierwszym w P. Implikacja odwrotna wynika z pierwszej części dowodu (d). $\square$

Ze Stwierdzenia 13.12 i ze Stwierdzenia 11.16 wynika od razu następujący

Wniosek 13.13. *Niech a będzie elementem dziedziny całkowitości P. Wówczas wielomian $f \in P[x]$ jest nierozkładalny w $P[x]$ wtedy i tylko wtedy, gdy wielomian $f(x - a)$ jest nierozkładalny w $P[x]$.* $\square$

Przykład 13.14. Sprawdzimy czy wielomian $f = x^4 + 1$ jest nierozkładalny w pierścieniu $\mathbb{Q}[x]$. Zauważmy, że $f(x-1) = (x-1)^4 + 1 = x^4 - 4x^3 + 6x^2 - 4x + 1 + 1 = x^4 - 4x^3 + 6x^2 - 4x + 2$, więc z kryterium Eisensteina przy $p = 2$ wielomian $f(x-1)$ jest nierozkładalny w $\mathbb{Q}[x]$. Zatem z Wniosku 13.13 wielomian f jest nierozkładalny w $\mathbb{Q}[x]$.

Twierdzenie 13.15. *Dla elementu a dziedziny ideałów głównych P równoważne są warunki:*

(i) a jest elementem pierwszym w P,

(ii) a jest elementem nierozkładalnym w P,

(iii) $a \neq 0$ i (a) jest ideałem maksymalnym pierścienia P,

(iv) $a \neq 0$ i (a) jest ideałem pierwszym pierścienia P,

(v) $a \neq 0$ i pierścień ilorazowy $P/(a)$ jest dziedziną całkowitości,

(vi) $a \neq 0$ i pierścień ilorazowy $P/(a)$ jest ciałem.

Dowód. Implikacja $(i) \Rightarrow (ii)$ wynika od razu z Twierdzenia 13.9. Udowodnimy implikację $(ii) \Rightarrow (iii)$. Z założenia mamy, że $a \neq 0$ i $a \notin P^*$, skąd $1 \notin (a)$, więc $(a) \neq P$. Niech $I \lhd P$ oraz $(a) \subset I$. Wtedy istnieje $b \in I$ takie, że $I = (b)$, więc $(a) \subset (b)$. Zatem $b \mid a$ i istnieje $t \in P$ takie, że $a = bt$. Stąd z nierozkładalności a, $b \in P^*$ lub $t \in P^*$. Jeśli $t \in P^*$, to $a \sim b$, skąd $(a) = (b)$ i mamy sprzeczność. Zatem $b \in P^*$, skąd $1 \in (b)$, czyli $(b) = P$. Zatem (a) jest ideałem maksymalnym w P. Implikacja $(iii) \Rightarrow (iv)$ wynika od razu z Wniosku 10.16. Implikacja $(iv) \Rightarrow (v)$ wynika od razu z Twierdzenia 10.14. Dla dowodu implikacji $(v) \Rightarrow (vi)$ załóżmy, że $a \neq 0$ i pierścień ilorazowy $P/(a)$ jest dziedziną całkowitości. Wtedy z Twierdzenia 10.14, (a) jest ideałem pierwszym pierścienia P. Ale $(a) \neq \{0\}$, więc na mocy Twierdzenia 12.19 ideał (a) jest maksymalny. Zatem z Twierdzenia 10.15 pierścień ilorazowy $P/(a)$ jest ciałem. Pozostaje udowodnić imlikację $(vi) \Rightarrow (i)$. Z naszych założeń wynika na mocy Twierdzenia 10.14, że (a) jest ideałem pierwszym pierścienia P. Ale $a \neq 0$, więc z Twierdzenia 13.11, a jest elementem pierwszym w P. $\square$

Z twierdzeń 13.15 i 12.18 oraz z Wniosku 11.6 otrzymujemy od razu następujący

Wniosek 13.16. *Niech K będzie ciałem i niech $f \in K[x]$. Wówczas równoważne są warunki:*

(i) f jest elementem pierwszym w $K[x]$,

(ii) f jest elementem nierozkładalnym w $K[x]$,

(iii) (f) jest ideałem maksymalnym pierścienia $K[x]$,

(iv) $f \neq 0$ i (f) jest ideałem pierwszym pierścienia $K[x]$,

(v) $f \neq 0$ i pierścień ilorazowy $K[x]/(f)$ jest dziedziną całkowitości,

(vi) pierścień ilorazowy $K[x]/(f)$ jest ciałem. $\square$

3 Dziedziny z jednoznacznością rozkładu

Definicja 13.17. Niech a będzie niezerowym elementem nieodwracalnym dziedziny całkowitości P. Powiemy, że a ma *rozkład jednoznaczny w* P, jeżeli $a = p_1 \cdot \ldots \cdot p_n$ dla pewnych nierozkładalnych elementów $p_1, \ldots, p_n$ pierścienia P oraz jeśli $q_1, \ldots, q_s$ są elementami nierozkładalnymi w P takimi, że $a = q_1 \cdot \ldots \cdot q_s$, to $s = n$ oraz po ewentualnej permutacji indeksów uzyskamy, że $p_i \sim q_i$ dla $i = 1, \ldots, n$.

Definicja 13.18. Powiemy, że dziedzina całkowitości P jest *dziedziną z jednoznacznością rozkładu*, jeżeli każdy niezerowy element nieodwracalny pierścienia P ma rozkład jednoznaczny.

Twierdzenie 13.19. *W dziedzinie z jednoznacznością rozkładu każdy element nierozkładalny jest elementem pierwszym.*

Dowód. Niech p będzie elementem nierozkładalnym dziedziny z jednoznacznością rozkładu P. Weźmy dowolne $x, y \in P$ takie, że $p \mid xy$. Jeśli $x = 0$, to $p \mid x$, jeśli $y = 0$, to $p \mid y$. Możemy zatem dalej zakładać, że $x \neq 0$ i $y \neq 0$. Istnieje $t \in P$ takie, że $xy = tp$. Jeśli $x \in P^*$, to $y = x^{-1}tp$, skąd $p \mid y$. Jeśli $y \in P^*$, to analogicznie $p \mid x$. Niech dalej $x \notin P^*$ i $y \notin P^*$. Wtedy $x = q_1 \cdot \ldots \cdot q_r$, $y = t_1 \cdot \ldots \cdot t_s$ dla pewnych elementów nierozkładalnych $q_1, \ldots, q_r, t_1, \ldots, t_s$ pierścienia P. Zatem $tp = q_1 \cdot \ldots \cdot q_r \cdot t_1 \cdot \ldots \cdot t_s$. Ale w rozkładzie tp na czynniki nierozkładalne występuje p, więc z jednoznaczności rozkładu elementu tp mamy, że $p \sim q_i$ dla pewnego $i \leq r$, skąd $p \mid x$ lub $p \sim t_j$ dla pewnego $j \leqslant s$, skąd $p \mid y$. Zatem p jest elementem pierwszym w pierścieniu P. $\square$

Przykład 13.20. W Przykładzie 13.10 wykazaliśmy, że x^2 jest elementem nierozkładalnym pierścienia $P = \mathbb{Z} + (x^2)$, ale nie jest elementem pierwszym tego pierścienia. Wobec tego na mocy Twierdzenia 13.19 pierścień P nie jest dziedziną z jednoznacznością rozkładu.

Twierdzenie 13.21. *Niech P będzie dziedziną całkowitości, w której każdy element nierozkładalny jest elementem pierwszym. Wówczas równoważne są warunki:*

(i) P jest dziedziną z jednoznacznością rozkładu,

(ii) każdy niezerowy element nieodwracalny pierścienia P jest iloczynem skończonej liczby elementów nierozkładalnych w pierścieniu P.

Dowód. $(i) \Rightarrow (ii)$. Oczywiste. $(ii) \Rightarrow (i)$. Niech zachodzi (ii), ale nie zachodzi (i). Wtedy istnieje niezerowy element nieodwracalny $a \in P$ rozkładający się na iloczyn najmniejszej liczby elementów nierozkładalnych $p_1, \ldots, p_n$ i nie posiadający jednoznacznego rozkładu w P. Zatem istnieją elementy nierozkładalne $q_1, \ldots, q_s$ pierścienia P takie, że $a = q_1 \cdot \ldots \cdot q_s = p_1 \cdot \ldots \cdot p_n$ oraz nie można spermutować elementów $p_1, \ldots, p_n$ tak aby $p_i \sim q_i$ dla $i = 1, \ldots, n$ lub $n \neq s$. Z założenia $n \leq s$. Jeżeli $n = 1$, to $s = 1$, skąd $q_1 = p_1$ i mamy sprzeczność. Zatem $n > 1$. Ponadto p_n jest elementem pierwszym w P oraz $p_n \mid q_1 \cdot \ldots \cdot q_s$, więc dla pewnego $i \leq s$, $p_n \mid q_i$. Bez zmniejszania ogólności można

zakładać, że $i = s$, tzn. $p_n \mid q_s$. Stąd z nierozkładalności p_n i q_s mamy, że $p_n \sim q_s$, czyli $q_s = p_n u$ dla pewnego $u \in P^*$ oraz $q_1 \cdot \ldots \cdot q_{s-2} \cdot (q_{s-1}u) = p_1 \cdot \ldots \cdot p_{n-1}$. Ale $q_{s-1}u$ jest elementem nierozkładalnym w P, więc z minimalności n mamy, że $n - 1 = s - 1$, skąd $n = s$. Ponadto po ewentualnej permutacji indeksów $p_i \sim q_i$ dla $i = 1, \ldots, n-1$ i $p_n \sim q_s u \sim q_s$. Stąd $p_i \sim q_i$ dla $i = 1, \ldots, n$ i mamy sprzeczność. □

Z twierdzeń 12.35, 13.15 i 13.21 wynika od razu następujący

Wniosek 13.22. *Każda dziedzina ideałw głównych jest dziedziną z jednoznacznością rozkładu.* □

Z Twierdzenia 12.18 i z Przykładu 12.17 oraz z Wniosku 13.22 mamy od razu następujący

Wniosek 13.23. Dla dowolnego ciała K pierścienie K i $K[x]$ są dziedzinami z jednoznacznością rozkładu.

Z Przykładu 12.16 i z Wniosku 13.22 mamy od razu następujący

Wniosek 13.24. Każdy podpierścień ciała $\mathbb{Q}$ jest dziedziną z jednoznacznością rozkładu.

Zagadka 1. Udowodnij, że wielomian stały f jest elementem nierozkładalnym pierścienia $\mathbb{Z}[x]$ wtedy i tylko wtedy, gdy $f = \pm p$ dla pewnej liczby pierwszej p.

Zagadka 2. Udowodnij, że każdy wielomian pierwotny $f \in \mathbb{Z}[x]$ jest iloczynem skończonej liczby elementów nierozkładalnych pierścienia $\mathbb{Z}[x]$.

Zagadka 3. Udowodnij, że każdy niezerowy element nieodwracalny pierścienia $\mathbb{Z}[x]$ jest iloczynem skończonej liczby elementów nierozkładalnych tego pierścienia.

Zagadka 4. Udowodnij, że pierścień $\mathbb{Z}[x]$ jest dziedziną z jednoznacznością rozkładu.

Zagadka 5. Udowodnij, że ideał $(2, x)$ pierścienia $\mathbb{Z}[x]$ nie jest główny.

Zagadka 6. Udowodnij, że w dowolnej dziedzinie całkowitości P element stowarzyszony z elementem pierwszym jest elementem pierwszym.

Zagadka 7. Czy wielomian $f = x^4 - x^2 + 1$ jest nierozkładalny w $\mathbb{Q}[x]$?