Wykład 12
Ważne pierścienie

1 Dzielenie wielomianów

Definicja 12.1. Niech P będzie pierścieniem, który może nie być dziedziną całkowitości. Powiemy, że w pierścieniu $P[x]$ jest wykonalne dzielenie z resztą przez wielomian $f \in P[x]$, jeżeli dla każdego wielomianu $g \in P[x]$ istnieje dokładnie jedna para (q, r) wielomianów $q, r \in P[x]$ taka, że $g = q \cdot f + r$ oraz $st(r) < st(f)$.

Uwaga 12.2. Ponieważ $st(0) = -\infty$, więc w powyższej definicji $f \neq 0$. Ponadto wielomian r nazywamy *resztą*, zaś q nazywamy *niepełnym ilorazem* z dzielenia wielomianu g przez wielomian f.

Twierdzenie 12.3. *Dla dowolnego pierścienia P i dla dowolnego wielomianu $f \in P[x]$ równoważne są warunki:*

(i) w pierścieniu $P[x]$ jest wykonalne dzielenie z resztą przez wielomian f;

(ii) najstarszy współczynnik wielomianu f jest elementem odwracalnym w P.

Dowód. Niech $st(f) = n$ i niech a będzie najstarszym współczynnikiem wielomianu f. $(i) \Rightarrow (ii)$. Jeżeli a jest dzielnikiem zera w pierścieniu P, to istnieje $0 \neq b \in P$ takie, że $b \cdot a = 0$. Wtedy $st(bf) < n$ oraz $bf = b \cdot f + 0 = 0 \cdot f + bf$ i $(b, 0) \neq (0, bf)$ oraz $st(0) < n$, więc mamy sprzeczność. Zatem a jest elementem regularnym w pierścieniu P. Z założenia istnieją wielomiany $q, r \in P[x]$ takie, że $x^n = q \cdot f + r$ oraz $st(r) < n$. Stąd $q \neq 0$ i ze Stwierdzenia 11.1 mamy, że $st(q \cdot f) = st(q) + st(f) = st(q) + n > st(r)$, więc $n = st(q) + n$, czyli $st(q) = 0$. Zatem $q \in P$ i $q \neq 0$ oraz ze Stwierdzenia 11.1 najstarszym współczynnikiem wielomianu $q \cdot f + r$ jest qa, więc $qa = 1$, skąd $a \in P^*$.

$(ii) \Rightarrow (i)$. Istnieje $b \in P$ takie, że $ab = 1$ i a jest elementem regularnym w pierścieniu P. Niech $q_1, q_2, r_1, r_2 \in P[x]$ będą takie, że $st(r_1), st(r_2) < n$ oraz $q_1 \cdot f + r_1 = q_2 \cdot f + r_2$. Wtedy $(q_1 - q_2) \cdot f = r_2 - r_1$. Ale ze Stwierdzenia 11.1 jest $st((q_1 - q_2) \cdot f) = st(q_1 - q_2) + st(f) = st(q_1 - q_2) + n$ oraz $st(r_2 - r_1) < n$, więc stąd $st(q_1 - q_2) = -\infty$, czyli $q_1 - q_2 = 0$. Zatem $r_2 - r_1 = 0$ oraz $r_2 = r_1$ i $q_2 = q_1$, a więc $(q_2, r_2) = (q_1, r_1)$. W ten sposób wykazaliśmy jednoznaczność reszty i niepełnego ilorazu.

Załóżmy teraz, że pewien wielomian z $P[x]$ nie jest podzielny z resztą przez wielomian f. Wtedy istnieje wielomian $g \in P[x]$ najniższego stopnia m niepodzielny z resztą przez wielomian f. Jeżeli $m < n$, to $g = 0 \cdot f + g$ i mamy sprzeczność. Zatem $m \geq n$. Niech c będzie najstarszym współczynnikiem wielomianu g i niech $h = g - cbx^{m-n}f$. Ponieważ ze Stwierdzenia 11.1 jest $st(cbx^{m-n}f) = m - n + n = m$ i najstarszy współczynnik wielomianu $cbx^{m-n}f$ jest równy $cba = c \cdot 1 = c$, więc $st(h) < m$. Z minimalności m wynika, że istnieją

wielomiany $q_1, r \in P[x]$ takie, że $h = q_1 \cdot f + r$ i $st(r) < n$, skąd $g = (cbx^{m-n} + q_1) \cdot f + r$. Zatem mamy sprzeczność. $\square$

Uwaga 12.4. Algorytm dzielenia wielomianów z resztą znany ze szkoły średniej jest dobry dla dowolnego pierścienia wielomianów.

Uwaga 12.5. Wielomian $f \in P[x]$ o najstarszym współczynniku równym 1 nazywamy *wielomianem unormowanym*. Ponieważ $1 \in P^*$, więc z Twierdzenia 12.3 w pierścieniu $P[x]$ jest wykonalne dzielenie z resztą przez wielomiany unormowane.

Twierdzenie 12.6. (Bezout). *Dla dowolnego wielomianu $g \in P[x]$ i dla dowolnego $a \in P$ reszta z dzielenia wielomianu g przez dwumian $x - a$ jest równa $g(a)$, tzn. istnieje wielomian $q \in P[x]$ taki, że $g = q \cdot (x - a) + g(a)$.*

Dowód. Z Uwagi 12.5 istnieją $q, r \in P[x]$ takie, że $g = q \cdot (x - a) + r$ i $st(r) < 1 = st(x - a)$. Stąd $r \in P$ i na mocy Wniosku 11.14, $g(a) = q(a) \cdot (a - a) + r = r$, czyli $r = g(a)$ i $g = q \cdot (x - a) + g(a)$. $\square$

Definicja 12.7. Niech $f, g \in P[x]$. Powiemy, że wielomian f dzieli wielomian g w pierścieniu $P[x]$ i piszemy $f \mid g$, jeżeli istnieje wielomian $h \in P[x]$ taki, że $g = f \cdot h$.

Wniosek 12.8. *Dla dowolnego wielomianu $g \in P[x]$ i dla dowolnego $a \in P$ mamy*

$$x - a \mid g \text{ w pierścieniu } P[x] \Leftrightarrow g(a) = 0.$$

Dowód. Jeżeli $x - a \mid g$ w pierścieniu $P[x]$, to istnieje $q \in P[x]$ takie, że $g = q \cdot (x - a)$, skąd na mocy Wniosku 11.14, $g(a) = q(a) \cdot (a - a) = 0$. Na odwrót, niech $g(a) = 0$. Wtedy z Twierdzenia 12.6 istnieje $q \in P[x]$ takie, że $g = q \cdot (x - a)$, czyli $x - a \mid g$. $\square$

Stwierdzenie 12.9. *Niech $a_1, \ldots, a_n$ będą parami różnymi elementami dziedziny całkowitości P. Wówczas dla dowolnego wielomianu $f \in P[x]$ równoważne są warunki:*

(i) $(x - a_1) \cdot \ldots \cdot (x - a_n) \mid f$ w pierścieniu $P[x]$;

(ii) $f(a_1) = \ldots = f(a_n) = 0$.

Dowód. $(i) \Rightarrow (ii)$. Z założenia istnieje $h \in P[x]$ taki, że $f = h \cdot (x - a_1) \cdot \ldots \cdot (x - a_n)$, skąd na mocy Wniosku 11.14, $f(a_i) = h(a_i) \cdot (a_i - a_1) \cdot \ldots \cdot (a_i - a_i) \cdot \ldots \cdot (a_i - a_n) = 0$ dla $i = 1, \ldots, n$.

$(ii) \Rightarrow (i)$. Stosujemy indukcję względem n. Dla $n = 1$ teza wynika od razu z Wniosku 12.8. Załóżmy, że teza zachodzi dla pewnego naturalnego n i niech $a_1, \ldots, a_{n+1}$ będą parami różnymi elementami pierścienia P takimi, że $f(a_1) = \ldots = f(a_{n+1}) = 0$. Wtedy z założenia indukcyjnego istnieje $g \in P[x]$ takie, że $f = g \cdot (x - a_1) \cdot \ldots \cdot (x - a_n)$. Ale na mocy Wniosku 11.14, $0 = f(a_{n+1}) = g(a_{n+1}) \cdot (a_{n+1} - a_1) \cdot \ldots \cdot (a_{n+1} - a_n)$, więc ponieważ P jest dziedziną całkowitości, to $g(a_{n+1}) = 0$ i z Wniosku 12.8 istnieje $h \in P[x]$ taki, że $g = h \cdot (x - a_{n+1})$. Zatem $f = h \cdot (x - a_1) \cdot \ldots \cdot (x - a_n) \cdot (x - a_{n+1})$, czyli $(x - a_1) \cdot \ldots \cdot (x - a_{n+1}) \mid f$. $\square$

Ze Stwierdzenia 12.9 i ze Stwierdzenia 11.1 otrzymujemy natychmiast następujący

Wniosek 12.10. *Niech P będzie dziedziną całkowitości i niech $n \in \mathbb{N}$. Wówczas każdy wielomian $f \in P[x]$ stopnia n posiada co najwyżej n różnych pierwiastków w pierścieniu P.* $\square$

Wniosek 12.11. *Niech P będzie nieskończoną dziedziną całkowitości. Wówczas wielomiany $f, g \in P[x]$ równe funkcyjnie są równe.*

Dowód. Z założenia $f(a) = g(a)$ dla każdego $a \in P$, więc na mocy Wniosku 11.14, $(f-g)(a) = 0$ dla każdego $a \in P$. Stąd wielomian $f - g$ ma nieskoczenie wiele pierwiastków w pierścieniu P. Zatem z Wniosku 12.10, $f - g = 0$, czyli $f = g$. $\square$

Stwierdzenie 12.12. *Niech A będzie podpierścieniem dziedziny całkowitości P oraz niech najstarszy współczynnik wielomianu $f \in A[x]$ będzie odwracalny w A. Wówczas dla dowolnego $g \in A[x]$ z tego, że $f \mid g$ w pierścieniu $P[x]$ wynika, że $f \mid g$ w pierścieniu $A[x]$.*

Dowód. Z założenia istnieje $h \in P[x]$ takie, że $g = h \cdot f$. Z Twierdzenia 12.3 istnieją $q, r \in A[x]$ takie, że $g = q \cdot f + r$ i $st(r) < st(f)$. Zatem w pierścieniu $P[x]$ jest $h \cdot f + 0 = q \cdot f + r$, więc z Twierdzenia 12.3, $r = 0$ i $h = q$. Stąd $g = q \cdot f$ i $f \mid g$ w pierścieniu $A[x]$. $\square$

Twierdzenie 12.13. *Niech $f \in P[x]$ będzie wielomianem stopnia $n \geq 1$ o najstarszym współczynniku odwracalnym w pierścieniu P. Wówczas dla ideału $I = (f) = \{f \cdot g : g \in P[x]\}$ pierścienia $P[x]$ mamy*

$$P[x]/I = \{a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + I : a_0, a_1, \ldots, a_{n-1} \in P\} \tag{1}$$

oraz dla dowolnych $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in P$:

$$a_0 + \ldots + a_{n-1}x^{n-1} + I = b_0 + \ldots + b_{n-1}x^{n-1} + I \Leftrightarrow \forall_{i=0,\ldots,n-1}\ a_i = b_i. \tag{2}$$

Dowód. Niech $g \in P[x]$. Wtedy z Twierdzenia 12.3 istnieją $q, r \in P[x]$ takie, że $st(r) < n$ oraz $g = q \cdot f + r$, skąd $g - r = q \cdot f \in I$, więc $g + I = r + I$. Ponadto istnieją $a_0, a_1, \ldots, a_{n-1} \in P$ takie, że $r = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, co dowodzi wzoru (1).

We wzorze (2) implikacja $\Leftarrow$ jest oczywista. Załóżmy, że $a_0, \ldots, a_{n-1}, b_0, \ldots, b_{n-1} \in P$ i $a_0 + \ldots + a_{n-1}x^{n-1} + I = b_0 + \ldots + b_{n-1}x^{n-1} + I$. Wtedy $(a_0 + \ldots + a_{n-1}x^{n-1}) - (b_0 + \ldots + b_{n-1}x^{n-1}) \in I$, więc istnieje $g \in P[x]$ takie, że $r = (a_0 - b_0) + \ldots + (a_{n-1} - b_{n-1})x^{n-1} = g \cdot f$, skąd $0 = g \cdot f + (-r) = 0 \cdot f + 0$, więc z Twierdzenia 12.3, $-r = 0$, czyli $a_i = b_i$ dla $i = 0, 1, \ldots, n-1$. $\square$

Przykład 12.14. Zbudujemy tabelkę mnożenia warstw w pierścieniu $\mathbb{Z}_2[x]/I$ dla $I = (x^2 + x + 1)$ i uzasadnimy, że ten pierścień jest ciałem 4-elementowym.

Na mocy Twierdzenia 12.13 każdy element pierścienia $\mathbb{Z}_2[x]/I$ można jednoznacznie zapisać w postaci $a+bx+I$ dla pewnych $a, b \in \mathbb{Z}_2$. Ponieważ $\mathbb{Z}_2 = \{0, 1\}$, więc pierścień $\mathbb{Z}_2[x]/I$ ma dokładnie $2 \cdot 2 = 4$ elementy i są nimi warstwy: $0+I$, $1+I$, $x+I$, $1+x+I$. Ale $x^2+x+1 \in I$, więc $x^2+I = -1-x+I = 1+x+I$, bo $-1 = 1$ w $\mathbb{Z}_2$. Stąd $(x+I)\cdot(x+I) = x^2+I = 1+x+I$, $(x+I)\cdot(1+x+I) = x(1+x)+I = x+x^2+I = x+1+x+I = 1+I$, bo $x+x = (1+1)x = 0 \cdot x = 0$, gdyż $1+1 = 0$ w $\mathbb{Z}_2$. Dalej, $(1+x+I)\cdot(1+x+I) = (1+x)^2+I = 1+x^2+I = 1+1+x+I = x+I$, bo $2x = (1+1)x = 0 \cdot x = 0$. Uwzględniając to, że $0+I$ jest elementem zerowym, a $1+I$ jest jedynką pierścienia $\mathbb{Z}_2[x]/I$ mamy następującą tabelkę mnożenia w tym pierścieniu:

$\cdot$	$0+I$	$1+I$	$x+I$	$1+x+I$
$0+I$	$0+I$	$0+I$	$0+I$	$0+I$
$1+I$	$0+I$	$1+I$	$x+I$	$1+x+I$
$x+I$	$0+I$	$x+I$	$1+x+I$	$1+I$
$1+x+I$	$0+I$	$1+x+I$	$1+I$	$x+I$

z której wynika, że każdy niezerowy element pierścienia 4-elementowego $\mathbb{Z}_2[x]/I$ jest elementem odwracalnym. Stąd pierścień $\mathbb{Z}_2[x]/I$ jest ciałem 4-elementowym.

2 Dziedziny ideałów głównych

Definicja 12.15. *Dziedziną ideałów głównych* (w skrócie: d.i.g.) nazywamy dziedzinę całkowitości, w której każdy ideał jest ideałem głównym.

Przykład 12.16. Na mocy Przykładu 10.9 pierścień liczb całkowitych $\mathbb{Z}$ jest dziedziną ideałów głównych. Ponadto z Zagadki 1 z wykładu 10 wynika, że **każdy podpierścień ciała liczb wymiernych jest dziedziną ideałów głównych**.

Przykład 12.17. Ze Stwierdzenia 10.4 wiemy, że wszystkimi ideałami ciała K są $\{0\} = (0)$ i $K = (1)$. Zatem **każde ciało jest dziedziną ideałów głównych**.

Twierdzenie 12.18. *Dla dowolnego ciała K pierścień $K[x]$ jest dziedziną ideałów głównych.*

Dowód. Z Twierdzenia 11.4 pierścień $K[x]$ jest dziedziną całkowitości. Niech $I \lhd K[x]$. Jeśli $I = \{0\}$, to $I = (0)$. Niech dalej $I \neq \{0\}$. Wtedy w zbiorze $I \setminus \{0\}$ istnieje wielomian f minimalnego stopnia n. Stąd $(f) \subseteq I$, bo $f \in I$. Jeżeli $g \in I$, to z Twierdzenia 12.3 istnieją $q, r \in K[x]$ takie, że $g = q \cdot f + r$ i $st(r) < n$. Ale $r = g - q \cdot f \in I$, więc z minimalności n jest $r = 0$, czyli $g = q \cdot f \in (f)$. Zatem $I \subseteq (f)$ i ostatecznie $I = (f)$. $\square$

Twierdzenie 12.19. *W dziedzinie ideałów głównych każdy niezerowy ideał pierwszy jest ideałem maksymalnym.*

Dowód. Niech $I \neq \{0\}$ będzie ideałem pierwszym dziedziny ideałów głównych P. Wówczas $I \neq P$ i istnieje $a \in P$ takie, że $I = (a)$. Ale $I \neq \{0\}$, więc $a \neq 0$. Niech $J \lhd P$ i $I \subset J$. Wówczas istnieje $b \in P$ takie, że $J = (b)$. Gdyby $b \in I$, to $J = (b) \subseteq I$, skąd $I = J$ i mamy sprzeczność. Zatem $b \notin I$. Dalej, $a \in (a) = I \subseteq J = (b)$, więc istnieje $t \in P$ takie, że $a = b \cdot t$. Stąd $b \cdot t \in I$ i $b \notin I$, więc z pierwszości ideału I, $t \in I$ i istnieje $x \in P$ takie, że $t = a \cdot x$. Zatem $a = b \cdot a \cdot x$ i $a \neq 0$ oraz P jest dziedziną, więc $1 = b \cdot x \in J$, skąd $J = P$. Zatem I jest ideałem maksymalnym pierścienia P. $\square$

Z Twierdzeń 12.18 i 12.19 mamy natychmiast następujący

Wniosek 12.20. *Dla dowolnego ciała K każdy niezerowy ideał pierwszy pierścienia $K[x]$ jest ideałem maksymalnym pierścienia $K[x]$.* $\square$

Twierdzenie 12.21. *Jeżeli $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ są ideałami dziedziny ideałów głównych P, to istnieje n takie, że $I_n = I_{n+1} = I_{n+2} = \ldots$.*

Dowód. Niech $I = \bigcup_{k=1}^{\infty} I_k$. Wtedy $I_k \subseteq I$ dla $k = 1, 2, \ldots$, skąd $I \neq \emptyset$. Weźmy dowolne $x, y \in I$. Wtedy istnieją $k, l \in \mathbb{N}$ takie, że $x \in I_k$, $y \in I_l$, więc dla $m = \max\{k, l\}$ mamy, że $x, y \in I_m$, skąd $x - y \in I_m$, czyli $x - y \in I$. Ponadto dla $a \in P$ jest $ax \in I_k$, więc $ax \in I$. Zatem $I \lhd P$ i P jest d.i.g., więc istnieje $c \in P$ takie, że $I = (c)$. Wtedy $c \in I$, więc istnieje $n \in \mathbb{N}$ takie, że $c \in I_n$, skąd $I = (c) \subseteq I_n \subseteq I_k \subseteq I$ dla wszystkich $k \geq n$. Zatem $I_n = I_k$ dla wszystkich $k \geq n$. $\square$

3 Arytmetyka dziedzin całkowitości

Od tej pory o wszystkich omawianych pierścieniach będziemy zakładali, że są one dziedzinami całkowitości.

Definicja 12.22. Niech a, b będą elementami pierścienia P. Powiemy, że a dzieli b w pierścieniu P, jeżeli istnieje $t \in P$ takie, że $b = a \cdot t$. Piszemy wtedy $a \mid b$.

Przykład 12.23. Niech $k \in \mathbb{Z}$, $f \in \mathbb{Z}[x]$. Pokażemy, że $k \mid f$ w $\mathbb{Z}[x]$ wtedy i tylko wtedy, gdy k dzieli (w pierścieniu $\mathbb{Z}$) wszystkie współczynniki wielomianu f. Mamy, że $f = a_0 + a_1 x + \ldots + a_n x^n$ dla pewnych $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ i pewnego $n \in \mathbb{N}_0$. Jeśli $k | a_i$ w pierścieniu $\mathbb{Z}$ dla każdego $i = 0, 1, \ldots, n$, to istnieją liczby całkowite $b_0, b_1, \ldots, b_n$ takie, że $a_i = k \cdot b_i$ dla $i = 0, 1, \ldots, n$. Stąd $f = k \cdot g$, gdzie $g = b_0 + b_1 x + \ldots + b_n x^n \in \mathbb{Z}[x]$, więc $k | f$ w pierścieniu $\mathbb{Z}[x]$.

Na odwrót, załóżmy, że $k | f$ w pierścieniu $\mathbb{Z}[x]$. Wtedy istnieje $h \in \mathbb{Z}[x]$ takie, że $f = k \cdot h$. Ale $h = c_0 + c_1 x + \ldots + c_m x^m$ dla pewnych $c_0, c_1, \ldots, c_m \in \mathbb{Z}$ i pewnego $m \in \mathbb{N}_0$, więc stąd $a_0 + a_1 x + \ldots + a_n x^n = k \cdot c_0 + (k \cdot c_1)x + \ldots + (k \cdot c_m)x^m$. Wobec tego dla każdego $i = 0, 1, \ldots, n$ mamy, że $a_i = k \cdot c_i$, czyli $k | a_i$. Zatem k dzieli (w pierścieniu $\mathbb{Z}$)

wszystkie współczynniki wielomianu f.

Uwaga 12.24. Dla dowolnych elementów a, b pierścienia P równoważne są warunki: (i) $a \mid b$, (ii) $b \in (a)$, (iii) $(b) \subseteq (a)$.

Dowód. $(i) \Rightarrow (ii)$. Istnieje $t \in P$ takie, że $b = at$, skąd $b \in (a)$.

$(ii) \Rightarrow (iii)$. Istnieje $t \in P$ takie, że $b = at$, skąd dla $x \in P$, $bx = atx \in (a)$, czyli $(b) \subseteq (a)$.

$(iii) \Rightarrow (i)$. Ponieważ $b \in (b)$ i $(b) \subseteq (a)$, więc $b \in (a)$ i istnieje $t \in P$ takie, że $b = at$, skąd $a \mid b$. $\square$

Definicja 12.25. Powiemy, że elementy a, b pierścienia P są *stowarzyszone* w P i piszemy $a \sim b$, jeżeli $a \mid b$ i $b \mid a$ w P.

Uwaga 12.26. Dla dowolnych elementów a, b pierścienia P równoważne są warunki: (i) $a \sim b$, (ii) $(a) = (b)$, (iii) $\exists_{u \in P^*}\ a = bu$, (iv) $\exists_{v \in P^*}\ b = av$.

Dowód. Z Uwagi 12.24 mamy, że $(a) = (b) \Leftrightarrow [(a) \subseteq (b)$ i $(b) \subseteq (a)] \Leftrightarrow (b \mid a$ i $a \mid b) \Leftrightarrow a \sim b$. Dalej, dla $u \in P^*$ istnieje $v \in P^*$ takie, że $uv = 1$, skąd wynika natychmiast równoważność warunków (iii) i (iv).

$(i) \Rightarrow (iii)$. Niech $a \sim b$. Wtedy $a \mid b$ i $b \mid a$, więc istnieją $x, y \in P$ takie, że $b = ax$ i $a = by$. Jeśli $b = 0$, to $a = 0 \cdot y = 0$ i wystarczy wziąć $u = 1$. Jeśli zaś $b \neq 0$, to $b = byx$, skąd $1 = yx$, więc $y \in P^*$ i wystarczy wziąć $u = y$.

$(iii) \Rightarrow (i)$. Niech $a = bu$ dla pewnego $u \in P^*$. Wtedy $b \mid a$ i istnieje $v \in P^*$ takie, że $b = av$, skąd $a \mid b$. Zatem $a \sim b$. $\square$

Uwaga 12.27. Z Uwagi 12.26 otrzymujemy od razu, że $\sim$ jest relacją równoważności w zbiorze P.

Definicja 12.28. Element a pierścienia P nazywamy *elementem rozkładalnym*, jeżeli istnieją niezerowe elementy nieodwracalne $x, y \in P$ takie, że $a = x \cdot y$.

Przykład 12.29. Wielomian $f \in K[x]$, gdzie K jest ciałem, jest elementem rozkładalnym w $K[x]$ wtedy i tylko wtedy, gdy f jest iloczynem dwóch wielomianów $g, h \in K[x]$ dodatnich stopni, gdyż $(K[x])^* = K \setminus \{0\}$. Jeżeli $st(f) > 1$ i istnieje $a \in K$ takie, że $f(a) = 0$, to z Twierdzenia Bezout istnieje $g \in K[x]$ takie, że $f = g \cdot (x - a)$. Wtedy $st(f) = st(g) + 1$, więc $st(g) > 0$ i f jest elementem rozkładalnym w $K[x]$.

Definicja 12.30. Niezerowy element nieodwracalny a pierścienia P nazywamy *elementem nierozkładalnym*, jeżeli a nie jest elementem rozkładalnym, tzn. dla dowolnych $x, y \in P$ z tego, że $a = x \cdot y$ wynika: $x \in P^*$ lub $y \in P^*$.

Przykład 12.31. Niech K będzie ciałem i $f \in K[x]$. Jeżeli $st(f) = 1$ oraz $g, h \in K[x]$ są takie, że $f = g \cdot h$, to $1 = st(g) + st(h)$, skąd $st(g) = 0$ lub $st(h) = 0$, czyli $g \in (K[x])^*$

lub $h \in (K[x])^*$. Zatem każdy wielomian $f \in K[x]$ stopnia 1 jest nierozkładalny w $K[x]$.

Stwierdzenie 12.32. *Niech K będzie ciałem i $f \in K[x]$ oraz $st(f) = 2$ lub $st(f) = 3$. Wówczas f jest elementem nierozkładalnym w pierścieniu $K[x]$ wtedy i tylko wtedy, gdy f nie ma pierwiastka w ciele K.*

Dowód. Jeżeli f jest nierozkładalny w $K[x]$, to z Przykładu 12.29, f nie ma pierwiastka w K. Na odwrót, załóżmy, że f nie ma pierwiastka w K. Weźmy dowolne $g, h \in K[x]$ takie, że $f = g \cdot h$ i $st(g) \leq st(h)$. Wtedy $st(f) = st(g) + st(h) \geq 2st(g)$. Ale $st(f) = 2$ lub $st(f) = 3$, więc stąd $st(g) \leq 1$. Jeśli $st(g) = 1$, to $g = ax + b$ dla pewnych $a, b \in P$, $a \neq 0$, czyli $g(-\frac{b}{a}) = 0$, więc też $f(-\frac{b}{a}) = 0$ i mamy sprzeczność. Zatem $st(g) = 0$, czyli $g \in (K[x])^*$ i f jest elementem nierozkładalnym w $K[x]$. □

Przykład 12.33. Z zasadniczego twierdzenia algebry i ze Stwierdzenia 12.32 oraz z Przykładu 12.31 wynika, że wielomianami nierozkładalnymi w pierścieniu $\mathbb{C}[x]$ są dokładnie wielomiany stopnia 1 (tzn. wielomiany liniowe). Wielomian $x^4+4 \in \mathbb{Q}[x]$ nie posiada nawet pierwiastka rzeczywistego, ale jest rozkładalny w $\mathbb{Q}[x]$, bo $x^4 + 4 = (x^2 + 2)^2 - (2x)^2 = (x^2 + 2 - 2x)(x^2 + 2 + 2x)$.

Lemat 12.34. *Jeżeli a jest niezerowym elementem nieodwracalnym pierścienia P takim, że a nie jest iloczynem skończonej liczby elementów nierozkładalnych, to istnieje $b \in P$, które jest niezerowym elementem nieodwracalnym w P i nie jest iloczynem skończonej liczby elementów nierozkładalnych takie, że $(a) \subset (b)$.*

Dowód. Z założenia wynika, że a jest elementem rozkładalnym w P, więc istnieją niezerowe elementy nieodwracalne $x, y \in P$ takie, że $a = xy$. Jeżeli $x = x_1 \cdot \ldots \cdot x_k$, $y = y_1 \cdot \ldots \cdot y_l$, gdzie $x_1, \ldots, x_k, y_1, \ldots, y_l$ są elementami nierozkładalnymi w P, to $a = x_1 \cdot \ldots \cdot x_k \cdot y_1 \cdot \ldots \cdot y_l$, wbrew założeniu. Zatem można zakładać, że x nie jest iloczynem skończonej liczby elementów nierozkładalnych w P. Ponadto $x \mid a$, więc z Uwagi 12.24, $(a) \subseteq (x)$. Jeśli $(a) = (x)$, to z Uwagi 12.26 istnieje $u \in P^*$ takie, że $a = xu$, skąd $xu = xy$, czyli $y = u \in P^*$ i mamy sprzeczność. Zatem $(a) \subset (x)$ i wystarczy wziąć $b = x$. □

Twierdzenie 12.35. *W dziedzinie ideałów głównych P każdy niezerowy element nieodwracalny jest iloczynem skończonej liczby elementów nierozkładalnych.*

Dowód. Gdyby tak nie było, to przez prostą indukcję z Lematu 12.33 znaleźlibyśmy nieskończony ciąg elementów $a_1, a_2, \ldots$ pierścienia P taki, że $(a_1) \subset (a_2) \subset (a_3) \subset \ldots$ co przeczy Twierdzeniu 12.21. □

Wniosek 12.36. *Dla dowolnego ciała K każdy wielomian $f \in K[x]$ dodatniego stopnia jest iloczynem skończonej liczby wielomianów nierozkładalnych w $K[x]$.* □

Twierdzenie 12.37. *Jeżeli $f \in \mathbb{R}[x]$ jest wielomianem nierozkładalnym w pierścieniu*

$\mathbb{R}[x]$, *to* $st(f) = 1$ *lub* $st(f) = 2$.

Dowód. Załóżmy, że tak nie jest. Wtedy istnieje $f \in \mathbb{R}[x]$ nierozkładalny w $\mathbb{R}[x]$ taki, że $st(f) \geq 3$. Z zasadniczego twierdzenia algebry $f(z_0) = 0$ dla pewnego $z_0 \in \mathbb{C}$. Ponadto z Przykładu 12.29, $z_0 \notin \mathbb{R}$, więc $z_0 \neq \overline{z_0}$. Ale $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ dla pewnych liczb rzeczywistych $a_0, \ldots, a_n$, więc

$$f(\overline{z_0}) = a_n(\overline{z_0})^n + a_{n-1}(\overline{z_0})^{n-1} + \ldots + a_1\overline{z_0} + a_0 =$$

$$= \overline{a_n z_0^n} + \overline{a_{n-1}z_0^{n-1}} + \ldots + \overline{a_1 z_0} + \overline{a_0} =$$

$$= \overline{a_n z_0^n + a_{n-1}z_0^{n-1} + \ldots + a_1 z_0 + a_0} = \overline{f(z_0)} = \overline{0} = 0.$$

Niech $h = (x - z_0) \cdot (x - \overline{z_0}) = x^2 - (z_0 + \overline{z_0})x + z_0\overline{z_0}$. Ponieważ $z_0 + \overline{z_0}, z_0\overline{z_0} \in \mathbb{R}$, więc $h \in \mathbb{R}[x]$. Ponadto ze Stwierdzenia 12.9 , $h \mid f$ w pierścieniu $\mathbb{C}[x]$. Ale $h, f \in \mathbb{R}[x]$, więc ze Stwierdzenia 12.12, $h \mid f$ w pierścieniu $\mathbb{R}[x]$. Zatem $f = h \cdot g$ dla pewnego $g \in \mathbb{R}[x]$, skąd $st(f) = st(h) + st(g) = 2 + st(g)$. Ale $st(f) \geq 3$, więc $st(g) > 0$, co przeczy temu, że f jest nierozkładalny w $\mathbb{R}[x]$. Zatem $st(f) = 1$ lub $st(f) = 2$. □

Z Twierdzenia 12.37 i z Wniosku 12.36 wynika od razu następujące

Twierdzenie 12.38. *Każdy wielomian dodatniego stopnia o współczynnikach rzeczywistych jest iloczynem skończonej liczby wielomianów o współczynnikach rzeczywistych stopni* ≤ 2. □

Z Przykładu 12.33 i Wniosku 12.36 mamy od razu następujące

Twierdzenie 12.39. *Każdy wielomian dodatniego stopnia o współczynnikach zespolonych jest iloczynem skończonej liczby czynników liniowych.* □

Uwaga 12.40. Na mocy Przykładu 6 wielomian $f = ax^2 + bx + c \in \mathbb{R}[x]$ stopnia 2 jest nierozkładalny w pierścieniu $\mathbb{R}[x]$ wtedy i tylko wtedy, gdy f nie ma pierwiastka w $\mathbb{R}$, czyli gdy $\Delta = b^2 - 4ac < 0$.

Zagadka 1. Czy $3 + \sqrt{2} \mid 16 + 3\sqrt{2}$ w pierścieniu $\mathbb{Z}[\sqrt{2}]$?

Zagadka 2. Czy $3 + 7i \in (1 + i)$ w pierścieniu $\mathbb{Z}[i]$?

Zagadka 3. Niech $P = \mathbb{Z}_5[x]$ oraz $I = (x^2 + x + 1)$. Czy w pierścieniu P/I prawdziwa jest równość:

$$(x^3 + 2x^2 + x + 4 + I) \cdot (2x^2 + 3x + 2 + I) = 1 + I?$$

Zagadka 4. Udowodnij, że w dowolnej dziedzinie całkowitości P element stowarzyszony z elementem rozkładalnym jest elementem rozkładalnym.

Zagadka 5. Udowodnij, że w dowolnej dziedzinie całkowitości P element stowarzyszony z elementem nierozkładalnym jest elementem nierozkładalnym.

Zagadka 6. Wyznacz wszystkie unormowane wielomiany stopnia 3 nierozkładalne w pierścieniu $\mathbb{Z}_3[x]$.

Zagadka 7. Zbuduj tabelkę mnożenia warstw w pierścieniu $\mathbb{Z}_3[x]/I$ dla $I = (x^2 + 1)$ i uzasadnij, że ten pierścień jest ciałem 9-elementowym.