Wykład 11
Pierścienie wielomianów

1 Konstrukcja pierścienia wielomianów

Niech P będzie dowolnym niezerowym pierścieniem. Oznaczmy przez $P[x]$ zbiór wszystkich nieskończonych ciągów

$$f = (f_0, f_1, f_2, \ldots) \tag{1}$$

takich, że $f_i \in P$ dla $i = 0, 1, \ldots$ oraz $0 = f_k = f_{k+1} = f_{k+2} = \ldots$ dla pewnego k.

Elementy zbioru $P[x]$ nazywamy *wielomianami* zmiennej x o współczynnikach z pierścienia P. Przyjmujemy umowę, że jeśli wielomian nazywa się g, to $g = (g_0, g_1, \ldots)$, czyli $g_0, g_1, \ldots$ są jego kolejnymi współczynnikami. Przy tych oznaczeniach dla wielomianów $f, g \in P[x]$ mamy

$$f = g \iff f_i = g_i \text{ dla każdego } i = 0, 1, 2, \ldots. \tag{2}$$

Wielomian $0 = (0, 0, \ldots)$ nazywamy *zerowym*, zaś $1 = (1, 0, 0, \ldots)$ nazywamy *jedynkowym*. Jeżeli $0 = f_1 = f_2 = \ldots$, to wielomian f nazywamy *stałym*. *Wyrazem wolnym* wielomianu f postaci (1) jest współczynnik f_0. Jeżeli $f \neq 0$, to istnieje największe n takie, że $f_n \neq 0$ i wówczas n nazywamy *stopniem wielomianu* f i piszemy $st(f) = n$, zaś f_n nazywamy *najstarszym współczynnikiem* tego wielomianu. Ponadto przyjmujemy, że $st(0) = -\infty$ oraz $-\infty < n$ dla $n = 0, 1, \ldots$ i $(-\infty) + n = (-\infty) + (-\infty) = -\infty$ dla $n = 0, 1, \ldots$.

Jeżeli $f, g \in P[x]$, to istnieją $k, l \in \mathbb{N}_0$ takie, że $f_j = 0$ dla wszystkich $j > k$ oraz $g_j = 0$ dla wszystkich $j > l$. Zatem dla wszystkich $j > \max\{k, l\}$ jest $f_j + g_j = 0$, skąd $(f_0 + g_0, f_1 + g_1, \ldots) \in P[x]$. Możemy więc zdefiniować w naturalny sposób *sumę wielomianów* $f, g \in P[x]$ jako wielomian $f + g = (f_0 + g_0, f_1 + g_1, \ldots)$. Wówczas z naszych rozważań mamy, że dla dowolnych wielomianów $f, g \in P[x]$:

$$st(f + g) \leqslant \max\{st(f), st(g)\}. \tag{3}$$

Jeżeli zaś $st(f) < st(g)$, to oczywiście $st(f + g) = st(g)$.

Z określenia dodawania wielomianów łatwo wynika, że system algebraiczny $(P[x], +, 0)$ jest grupą abelową, przy czym *wielomianem przeciwnym* do wielomianu f jest wielomian $-f = (-f_0, -f_1, \ldots)$.

Iloczynem wielomianów $f, g \in P[x]$ nazywamy ciąg

$$f \cdot g = (f_0g_0, f_0g_1 + f_1g_0, f_0g_2 + f_1g_1 + f_2g_0, \ldots). \tag{4}$$

Zatem dla każdego $n = 0, 1, \ldots$

$$(f \cdot g)_n = \sum_{i=0}^{n} f_i g_{n-i} = \sum_{i+j=n} f_i g_j. \tag{5}$$

Zauważmy, że $f \cdot g \in P[x]$. Rzeczywiście, istnieją $k, l \in \mathbb{N}_0$ takie, że $f_i = 0$ dla wszystkich $i > k$ oraz $g_j = 0$ dla wszystkich $j > l$. Weźmy dowolne $n > k + l$ oraz $i, j \in \mathbb{N}_0$ takie, że $i + j = n$. Jeśli $i > k$, to $f_i = 0$, więc $f_i g_j = 0$; jeśli zaś $i \leqslant k$, to $j = n - i \geqslant n - k > k + l - k = l$, więc $g_j = 0$, czyli $f_i g_j = 0$. Stąd dla $n > k + l$ jest $(f \cdot g)_n = \sum_{i+j=n} f_i g_j = 0$ i $f \cdot g \in P[x]$.

Jeżeli $f_i = 0$ dla $i = 1, 2, \ldots$ to ze wzoru (5) mamy

$$(f_0, 0, 0, \ldots) \cdot (g_0, g_1, \ldots) = (f_0 g_0, f_0 g_1, f_0 g_2, \ldots). \tag{6}$$

Jeżeli zaś $f_1 = 1$ oraz $f_i = 0$ dla $i = 0, 2, 3, \ldots$ to ze wzoru (5) wynika, że

$$(0, 1, 0, 0, \ldots) \cdot (g_0, g_1, \ldots) = (0, g_0, g_1, \ldots). \tag{7}$$

Niech teraz $f, g \in P[x] \setminus \{0\}$ i $n = st(f)$, $m = st(g)$. Wtedy z wcześniejszych wyliczeń mamy, że $(f \cdot g)_k = 0$ dla wszystkich $k > n + m$. Stąd i z (5) mamy

$$\forall_{f,g \in P[x]}\ st(f \cdot g) \leqslant st(f) + st(g). \tag{8}$$

Stwierdzenie 11.1. *Niech $f, g \in P[x] \setminus \{0\}$ będą takie, że najstarszy współczynnik wielomianu f lub najstarszy współczynnik wielomianu g jest elementem regularnym pierścienia P. Wtedy $st(f \cdot g) = st(f) + st(g)$ oraz najstarszy współczynnik wielomianu $f \cdot g$ jest iloczynem najstarszych współczynników wielomianów f i g.*

Dowód. Oznaczmy $n = st(f)$, $m = st(g)$. Weźmy dowolne $i, j \in \mathbb{N}_0$ takie, że $i + j = n + m$. Jeśli $i < n$, to $j = n + m - i > m$, skąd $g_j = 0$ oraz $f_i g_j = 0$. Jeśli $i > n$, to $f_i = 0$, więc $f_i g_j = 0$. Zatem ze wzoru (5), $(f \cdot g)_{n+m} = f_n g_m \neq 0$, bo $f_n \neq 0$, $g_m \neq 0$ oraz f_n lub g_m jest elementem regularnym. Stąd ze wzoru (8) wynika teza naszego stwierdzenia. □

Wniosek 11.2. *Jeżeli P jest dziedziną całkowitości, to dla dowolnych $f, g \in P[x]$*

$$st(f \cdot g) = st(f) + st(g). \ \square$$

Ze wzorów (4) i (5) wynika od razu, że mnożenie wielomianów jest przemienne. Natomiast ze wzoru (6) wynika od razu, że $1 = (1, 0, 0, \ldots)$ jest elementem neutralnym mnożenia wielomianów.

Teraz udowodnimy, że mnożenie wielomianów jest rozdzielne względem ich dodawania oraz mnożenie wielomianów jest łączne. W tym celu weźmy dowolne $f, g, h \in P[x]$. Wtedy dla $n \in \mathbb{N}_0$ mamy

$$(f \cdot (g+h))_n = \sum_{i+j=n} f_i (g+h)_j = \sum_{i+j=n} f_i (g_j + h_j) =$$

$$= \sum_{i+j=n} (f_i g_j + f_i h_j) = \sum_{i+j=n} f_i g_j + \sum_{i+j=n} f_i h_j = (f \cdot g)_n + (f \cdot h)_n,$$

skąd $f \cdot (g+h) = f \cdot g + f \cdot h$.

Ponadto $((f \cdot g) \cdot h)_n = \sum\limits_{i+j=n} (f \cdot g)_i h_j = \sum\limits_{i+j=n} \sum\limits_{s+t=i} (f_s g_t) h_j = \sum\limits_{s+t+j=n} (f_s g_t) h_j = \sum\limits_{s+t+j=n} f_s (g_t h_j)$ oraz $(f \cdot (g \cdot h))_n = \sum\limits_{s+k=n} f_s (g \cdot h)_k = \sum\limits_{s+k=n} \sum\limits_{t+j=k} f_s (g_t h_j) = \sum\limits_{s+t+j=n} f_s (g_t h_j)$, więc $f \cdot (g \cdot h) = (f \cdot g) \cdot h$. W ten sposób udowodniliśmy następujące

Twierdzenie 11.3. *System algebraiczny* $(P[x], +, \cdot, 0, 1)$ *tworzy pierścień.*

Ten pierścień nazywamy *pierścieniem wielomianów zmiennej* x o współczynnikach z pierścienia P.

Ze wzorów (3) i (6) wynika od razu, że przekształcenie $\phi \colon P \to P[x]$ dane wzorem

$$\phi(a) = (a, 0, 0, \ldots) \tag{9}$$

jest różnowartościowym homomorfizmem pierścieni. Z tego powodu można dokonać utożsamienia

$$(a, 0, 0, \ldots) \equiv a \quad \text{dla} \quad a \in P. \tag{10}$$

Przy takim utożsamieniu P jest podpierścieniem pierścienia $P[x]$.

Wprowadźmy teraz oznaczenie:

$$x = (0, 1, 0, 0, \ldots). \tag{11}$$

Wówczas ze wzoru (7) przez indukcję uzyskamy, że

$$x^n = (0, 0, \ldots, 0, \overset{n}{1}, 0, \ldots) \quad \text{dla} \quad n = 0, 1, \ldots. \tag{12}$$

Rzeczywiście, dla $n = 0$ nasz wzór zachodzi, bo $x^0 = 1 = (\overset{0}{1}, 0, 0, \ldots)$. Załóżmy, że dla pewnego $n \in \mathbb{N}_0$ jest $x^n = (0, 0, \ldots, \overset{n}{1}, 0, \ldots)$. Ponieważ $x^{n+1} = x \cdot x^n$, więc stąd i ze wzoru (7) mamy, że $x^{n+1} = (0, 0, \ldots, 0, \overset{n+1}{1}, 0, \ldots)$, co kończy dowód.

Niech $f \in P[x]$ będzie wielomianem stopnia $n \geq 1$. Wtedy $f_n \neq 0$ oraz $f_i = 0$ dla każdego $i \geqslant n+1$. Ponadto ze wzorów (6) i (12) mamy, że $(f_k, 0, 0, \ldots) \cdot x^k = (0, \ldots, 0, \overset{k}{f_k}, 0, \ldots)$ dla $k = 1, 2, \ldots$, więc $f = (f_0, 0, 0, \ldots) + (0, f_1, 0, \ldots) +$

$\ldots + (0, 0, \ldots, f_n, 0, \ldots) \equiv f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n$. Ponieważ dla wielomianu stałego f jest $f \equiv f_0$, więc dla dowolnego wielomianu $f \in P[x]$ stopnia $n \geq 0$ mamy utożsamienie:

$$f \equiv f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n. \tag{13}$$

Otrzymujemy w ten sposób naturalną notację dla wielomianów z pierścienia $P[x]$. Przy tej notacji możemy powiedzieć, że wielomiany $f, g \in P[x]$ są równe wtedy i tylko wtedy, gdy $st(f) = st(g)$ oraz $f_i = g_i$ dla każdego i.

Twierdzenie 11.4. *Pierścień P jest dziedziną całkowitości wtedy i tylko wtedy, gdy pierścień $P[x]$ jest dziedziną całkowitości.*

Dowód. $\Rightarrow$. Ponieważ P jest podpierścieniem pierścienia $P[x]$ i P jest dziedziną całkowitości, więc $0 \neq 1$ w P, skąd $1 \neq 0$ w $P[x]$. Jeśli $f, g \in P[x]$ są takie, że $f \cdot g = 0$, to z Wniosku 11.2, $-\infty = st(f) + st(g)$, skąd $st(f) = -\infty$ lub $st(g) = -\infty$, czyli $f = 0$ lub $g = 0$. Zatem $P[x]$ jest dziedziną całkowitości.

$\Leftarrow$. Ponieważ $1 \neq 0$ w $P[x]$ i P jest podpierścieniem $P[x]$, więc $1 \neq 0$ w P. Jeśli $f, g \in P$ są takie, że $f \cdot g = 0$, to $f \cdot g = 0$ w $P[x]$, skąd $f = 0$ lub $g = 0$. Zatem P jest dziedziną całkowitości. $\square$

Twierdzenie 11.5. *Jeżeli P jest dziedziną całkowitości, to $(P[x])^* = P^*$.*

Dowód. Niech $f \in (P[x])^*$. Wtedy istnieje $g \in P[x]$ takie, że $f \cdot g = 1$, skąd z Wniosku 11.2, $st(f) + st(g) = 0$, więc $st(f) = st(g) = 0$. Zatem $f, g \in P$ i $f \cdot g = 1$, czyli $f \in P^*$. Jeżeli zaś $f \in P^*$, to istnieje $g \in P$ takie, że $f \cdot g = 1$, skąd $f \in (P[x])^*$. $\square$

Wniosek 11.6. *Pierścień $P[x]$ nigdy nie jest ciałem.*

Dowód. Załóżmy, że dla pewnego pierścienia P pierścień $P[x]$ jest ciałem. Wtedy P jako podpierścień $P[x]$ jest dziedziną całkowitości, więc na mocy Twierdzenia 11.5, $(P[x])^* \subseteq P$. Ale $P[x]$ jest ciałem, więc stąd $x \in P$ i mamy sprzeczność. $\square$

Przykład 11.7. Załóżmy, że w pierścieniu P istnieje niezerowy element a taki, że $a^2 = 0$. Wtedy w pierścieniu $P[x]$ dla każdego $n = 1, 2, \ldots$ mamy, że $(1 + ax^n) \cdot (1 - ax^n) = 1 - a^2 x^{2n} = 1 - 0 \cdot x^{2n} = 1$. Zatem w pierścieniu $P[x]$ istnieją wielomiany odwracalne dowolnego stopnia $n \geqslant 1$. Oznacza to, że dla takich pierścieni P Twierdzenie 11.5 nie jest prawdziwe. Przykładem takiego pierścienia P jest $\mathbb{Z}_4$.

Definicja 11.8. *Wartością wielomianu* $f = f_0 + f_1 x + \ldots + f_n x^n \in P[x]$ w punkcie $a \in P$ nazywamy $f(a) = f_0 + f_1 a + \ldots + f_n a^n$.

Definicja 11.9. *Pierwiastkiem wielomianu* $f \in P[x]$ nazywamy takie $a \in P$, że $f(a) = 0$.

Definicja 11.10. Wielomiany $f, g \in P[x]$ nazywamy *równymi funkcyjnie*, jeżeli

$$f(a) = g(a) \text{ dla każdego } a \in P.$$

Przykład 11.11. Niech p będzie dowolną liczbą pierwszą i niech $P = \mathbb{Z}_p$. Wówczas P jest ciałem i na mocy Małego Twierdzenia Fermata, $a^p = a$ dla każdego $a \in P$. Wobec tego wielomiany $f = x^p$ i $g = x$ są równe funkcyjnie, ale nie są one równe, bo $st(f) = p > 1 = st(g)$. Z tego powodu wielomiany nad dowolnym pierścieniem P nie zawsze mogą być traktowane jako funkcje wielomianowe z pierścienia P w pierścień P.

2 Homomorfizmy na pierścieniach wielomianów

Twierdzenie 11.12. *Niech $f\colon P \to A$ będzie homomorfizmem pierścienia P w pierścień A i niech $a \in A$. Wtedy przekształcenie $F\colon P[x] \to A$ dane wzorem*

$$F((w_0, w_1, \ldots)) = f(w_0) + f(w_1)a + f(w_2)a^2 + \ldots \tag{14}$$

jest homomorfizmem pierścienia $P[x]$ w pierścień A oraz $(Ker(f)) \subseteq Ker(F)$. Jeżeli dodatkowo f jest ,,na", to F też jest ,,na".

Dowód. Ponieważ istnieje n takie, że $w_i = 0$ dla wszystkich $i > n$, więc $f(w_i) = 0$ dla $i > n$ i wzór (14) ma sens. Ze wzoru (14) mamy, że $F(1) = F((1, 0, 0, \ldots)) = f(1) + f(0)a + f(0)a^2 + \ldots = f(1) = 1$ oraz $F(w + u) = F(w) + F(u)$ dla dowolnych $w, u \in P[x]$. Ponadto dla $w, u \in P[x]$ jest $(w \cdot u)_n = \sum\limits_{i+j=n} w_i u_j$ dla $n = 0, 1, \ldots$ oraz istnieje m takie, że dla wszystkich $k > m$: $(w \cdot u)_k = 0$, skąd $f((w \cdot u)_k) = 0$ dla $k > m$. Ponadto

$$\begin{aligned} F(w \cdot u) &= f(w_0u_0) + f(w_0u_1 + w_1u_0)a + \ldots + f\Big(\sum_{i+j=n} w_iu_j\Big)a^n + \ldots = \\ &= f(w_0)f(u_0) + [f(w_0)f(u_1) + f(w_1)f(u_0)]a + \ldots + \sum_{i+j=n} f(w_i)f(u_j)a^n + \ldots \end{aligned}$$

oraz

$$\begin{aligned} F(w) \cdot F(u) &= [f(w_0) + f(w_1)a + \ldots] \cdot [f(u_0) + f(u_1)a + \ldots] = \\ &= f(w_0)f(u_0) + [f(w_0)f(u_1) + f(w_1)f(u_0)]a + \ldots + \\ &+ [f(w_0)f(u_n) + f(w_1)f(u_{n-1}) + \ldots + f(w_n)f(u_0)]a^n + \ldots \end{aligned}$$

więc $F(w \cdot u) = F(w) \cdot F(u)$ dla dowolnych $w, u \in P[x]$. Zatem F jest homomorfizmem pierścieni. Jeżeli $b \in Ker(f)$, to $f(b) = 0$, więc dla $w \in P[x]$ jest $F(b \cdot w) = F(b) \cdot F(w) = f(b) \cdot F(w) = 0 \cdot F(w) = 0$, skąd $b \cdot w \in Ker(F)$. Zatem $(Ker(f)) \subseteq Ker(F)$. Jeżeli f jest ,,na"i $y \in A$, to istnieje $b \in P$ takie, że $f(b) = y$, skąd $F(b) = F((b, 0, 0, \ldots)) = f(b) + 0 \cdot a + \ldots = y$, więc F jest ,,na". □

Twierdzenie 11.13. *Niech a będzie ustalonym elementem pierścienia P. Wtedy przekształcenie $F\colon P[x] \to P$ dane wzorem $F(w) = w(a)$ dla $w \in P[x]$ jest homomorfizmem pierścienia $P[x]$ na pierścień P o jądrze $(x - a)$. W szczególności*

$$P[x]/(x-a) \cong P.$$

Dowód. Przekształcenie $f\colon P \to P$ dane wzorem $f(p) = p$ dla $p \in P$ jest homomorfizmem pierścienia P ,,na"pierścień P. Zatem na mocy Twierdzenia 11.12, F jest homomorfizmem pierścienia $P[x]$,,na"pierścień P. Zatem z twierdzenia o izomorfizmie $P[x]/Ker(F) \cong P$. Ponadto $F(x-a) = a-a = 0$, więc $x-a \in Ker(F)$, skąd $(x-a) \subseteq Ker(F)$. Niech teraz $w \in Ker(F)$. Wtedy $w = a_0 + a_1x + \ldots + a_nx^n$ dla pewnych $a_0, a_1, \ldots, a_n \in P$ oraz $a_0 + a_1a + \ldots + a_na^n = 0$. Stąd

$$\begin{aligned} w &= (a_0 + a_1x + \ldots + a_nx^n) - (a_0 + a_1a + \ldots + a_na^n) = \\ &= a_1(x-a) + a_2(x^2-a^2) + \ldots + a_n(x^n-a^n). \end{aligned}$$

Ale $x^k - a^k = (x-a)(x^{k-1} + x^{k-2}a + \ldots + xa^{k-2} + a^{k-1})$ dla $k = 1, \ldots, n$, skąd wynika, że $w \in (x-a)$. Zatem $Ker(F) = (x-a)$ oraz $P[x]/(x-a) \cong P$. $\square$

Z Twierdzenia 11.13 i ze Stwierdzenia 10.27 otrzymujemy od razu następujący

Wniosek 11.14. *Niech a będzie ustalonym elementem pierścienia P. Wówczas dla dowolnych wielomianów $w_1, w_2, \ldots, w_n \in P[x]$ zachodzą wzory:*
(i) $(w_1 \cdot w_2 \cdot \ldots \cdot w_n)(a) = w_1(a) \cdot w_2(a) \cdot \ldots \cdot w_n(a)$,
(ii) $(w_1 + w_2 + \ldots + w_n)(a) = w_1(a) + w_2(a) + \ldots + w_n(a)$. $\square$

Twierdzenie 11.15. *Niech $f\colon A \to B$ będzie homomorfizmem pierścienia A w pierścień B. Wówczas przekształcenie $F\colon A[x] \to B[x]$ dane wzorem*

$$F(a_0 + a_1x + \ldots + a_nx^n) = f(a_0) + f(a_1)x + \ldots + f(a_n)x^n \tag{15}$$

dla $a_0, \ldots, a_n \in A$, $n = 0, 1, \ldots$ jest homomorfizmem pierścienia $A[x]$ w pierścień $B[x]$. Ponadto $Ker(F) = (Ker(f))$ oraz jeżeli f jest ,,na", to F też jest ,,na".

Dowód. Ponieważ B jest podpierścieniem pierścienia $B[x]$, więc f jest homomorfizmem pierścienia A w pierścień $B[x]$. Podstawiając $a = x$ w Twierdzeniu 11.12 uzyskamy, że przekształcenie F dane wzorem (15) jest homomorfizmem pierścienia $A[x]$ w pierścień $B[x]$ oraz $(Ker(f)) \subseteq Ker(F)$. Niech $w \in Ker(F)$. Wtedy istnieją $a_0, \ldots, a_n \in A$ takie, że $w = a_0 + a_1x + \ldots + a_nx^n$ oraz $f(a_0) + f(a_1)x + \ldots + f(a_n)x^n = 0$ oraz $f(a_i) \in B$ dla $i = 0, 1, \ldots, n$, skąd $f(a_i) = 0$, czyli $a_i \in Ker(f)$ dla $i = 0, \ldots, n$. Zatem $w \in (Ker(f))$. Stąd $Ker(F) = (Ker(f))$. Załóżmy, że f jest ,,na"i weźmy dowolne $b_0, \ldots, b_n \in B$. Wtedy istnieją $a_0, \ldots, a_n \in A$ takie, że $b_i = f(a_i)$ dla $i = 0, \ldots, n$, skąd $b_0 + b_1x + \ldots + b_nx^n = F(a_0 + a_1x + \ldots + a_nx^n)$, czyli F jest ,,na". $\square$

Stwierdzenie 11.16. *Dla dowolnego elementu a pierścienia P przekształcenie $F\colon P[x] \to P[x]$ dane wzorem $F(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1(x-a) + \ldots + a_n(x-a)^n$ dla $a_0, a_1, \ldots, a_n \in P$, $n \in \mathbb{N}_0$, jest automorfizmem pierścienia $P[x]$. Ponadto $st(w) = st(F(w))$ dla każdego $w \in P[x]$.*

Dowód. Z Twierdzenia 11.12 przekształcenie F jest homomorfizmem pierścieni. Ponadto z tego samego twierdzenia wynika, że przekształcenie $G\colon P[x] \to P[x]$ dane wzorem $G(a_0 + a_1x + \ldots + a_nx^n) = a_0 + a_1(x + a) + \ldots + a_n(x + a)^n$ dla $a_0, a_1, \ldots, a_n \in P$, $n \in \mathbb{N}_0$, jest homomorfizmem pierścieni. Ponadto dla dowolnych $a_0, a_1, \ldots, a_n \in P$, $n \in \mathbb{N}_0$ mamy, że $(G \circ F)(a_0 + a_1x + \ldots + a_nx^n) = G(a_0 + a_1(x - a) + \ldots + a_n(x - a)^n) = G(a_0) + G(a_1(x-a)) + \ldots + G(a_n(x-a)^n) = a_0 + G(a_1) \cdot G(x-a) + \ldots + G(a_n) \cdot [G(x-a)]^n = a_0 + a_1 \cdot (x + a - a) + \ldots + a_n \cdot [(x + a - a)]^n = a_0 + a_1x + \ldots + a_nx^n$, więc $G \circ F = id_{P[x]}$. Podobnie pokazujemy, że $F \circ G = id_{P[x]}$. Zatem G jest przekształceniem odwrotnym do F, skąd F jest bijekcją. Zatem F jest automorfizmem pierścienia $P[x]$.

Jeśli $0 \neq w \in P[x]$, to $w = a_0 + a_1x + \ldots + a_nx^n$ dla pewnych $a_0, a_1, \ldots, a_n \in P$, $a_n \neq 0$ i dla pewnego $n \in \mathbb{N}_0$. Stąd $F(w) = a_0 + a_1(x - a) + \ldots + a_n(x - a)^n$. Ale dla $k \in \mathbb{N}_0$ mamy, że $st((x - a)^k) = k$, skąd $st(a_0 + a_1(x - a) + \ldots + a_{n-1}(x - a)^{n-1}) < n$. Ponadto $a_n \neq 0$, więc $st(a_n(x - a)^n) = n$ i wobec tego $st(F(w)) = n$, czyli $st(F(w)) = st(w)$. W końcu, $st(F(0)) = st(0)$, bo $F(0) = 0$. $\square$

Przykład 11.17. W pierścieniu $\mathbb{Z}_{12}[x]$ znajdziemy ideał maksymalny oraz znajdziemy ideał pierwszy, który nie jest maksymalny. Z Zagadki 7 z Wykładu 10 przekształcenie $a \mapsto [a]_2$ dla $a \in \mathbb{Z}_{12}$ jest homomorfizmem pierścienia $\mathbb{Z}_{12}$ na pierścień $\mathbb{Z}_2$ i jego jądrem jest $(2) = \{0, 2, 4, 6, 8, 10\}$. Zatem z Twierdzenia 11.15 przekształcenie $F\colon \mathbb{Z}_{12}[x] \to \mathbb{Z}_2[x]$ dane wzorem

$$F(a_0 + a_1x + \ldots + a_nx^n) = [a_0]_2 + [a_1]_2x + \ldots + [a_n]_2x^n$$

dla dowolnych $a_0, a_1, \ldots, a_n \in \mathbb{Z}_{12}$ i dowolnego $n \in \mathbb{N}_0$, jest homomorfizmem pierścienia $\mathbb{Z}_{12}[x]$ na pierścień $\mathbb{Z}_2[x]$, który na mocy Twierdzenia 11.4 jest dziedziną całkowitości (gdyż $\mathbb{Z}_2$ jest ciałem, bo 2 jest liczbą pierwszą) i nie jest ciałem na mocy Wniosku 11.6. Ponadto z Twierdzenia 11.15 mamy, że $Ker(F) = (\{0, 2, 4, 6, 8, 10\}) = (2)$. Zatem z Wniosku 10.30 ideał $(2) = \{2 \cdot w : w \in \mathbb{Z}_{12}[x]\}$ jest ideałem pierwszym, ale nie jest ideałem maksymalnym w pierścieniu $\mathbb{Z}_{12}[x]$.

Z Twierdzenia 11.13 mamy, że przekształcenie $g\colon \mathbb{Z}_2[x] \to \mathbb{Z}_2$ dane wzorem $g(w) = w(0)$ dla $w \in \mathbb{Z}_2[x]$, jest homomorfizmem pierścieni i g jest "na". Ze Stwierdzenia 10.24, $G = g \circ F$ jest homomorfizmem pierścienia $\mathbb{Z}_{12}[x]$ na ciało $\mathbb{Z}_2$. Zatem z Wniosku 10.30 ideał $Ker(G)$ jest maksymalny. Ale dla dowolnego wielomianu $w = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}_{12}[x]$ mamy, że $G(w) = g([a_0]_2 + [a_1]_2x + \ldots + [a_n]_2x^n) = [a_0]_2$, więc $Ker(G) = \{a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}_{12}[x] : [a_0]_2 = 0\}$, skąd $Ker(G) = (2, x)$.

Zagadka 1. Podaj przykład pierścienia P i takiego jego właściwego podpierścienia A, że $A \cong P$.

Zagadka 2. Udowodnij, że $(\mathbb{Z}_6[x])^* = \mathbb{Z}_6^*$.

Zagadka 3. Podaj przykład nieskończonego pierścienia P takiego, że $P^* = \{1\}$.

Zagadka 4. Podaj przykład wielomianu odwracalnego $f \in \mathbb{Z}_{75}[x]$ stopnia 2014.

Zagadka 5. W pierścieniu $\mathbb{Z}_{143}[x]$ wskaż ideał maksymalny i ideał pierwszy, który nie jest maksymalny.

Zagadka 6. Udowodnij, że $S = \{a + x^2 f \ : \ a \in \mathbb{Z},\ f \in \mathbb{Z}[x]\}$ jest podpierścieniem pierścienia $\mathbb{Z}[x]$. Czy $x \in S$?

Zagadka 7. Niech P będzie niezerowym pierścieniem skończonym. Znajdź wielomian $f \in P[x]$ dodatniego stopnia taki, że wielomiany f i 0 są równe funkcyjnie.