

12. WYKŁAD 12: KONSTRUKCJA PIERŚCIEŃ WIELOMIANÓW JEDNEJ ZMIENNEJ.

Definicja i Uwaga 12.1. Niech R będzie dowolnym pierścieniem. **Wielomianem** zmiennej x o współczynnikach w pierścieniu R będziemy nazywali wyrażenie o postaci

$$a_0 + a_1x + \dots + a_nx^n,$$

gdzie $n \in \mathbb{N}$ oraz $a_0, \dots, a_n \in R$.

Dwa wielomiany uważamy za **równe** wtedy i tylko wtedy, gdy różnią się tylko o składniki postaci $0 \cdot x_i$, gdzie $i \in \mathbb{N}$.

Będziemy mówili, że wielomian $f = a_0 + a_1x + \dots + a_nx^n$ jest **stopnia** n , gdy $a_n \neq 0$. Umowa ta nie określa stopnia wielomianu 0, przyjmujemy więc dodatkowo, że stopniem wielomianu 0 jest $-\infty$. Stopień wielomianu f będziemy oznaczać przez $\deg(f)$.

Wielomiany stopnia 1 będziemy nazywać **liniowymi**, a wielomiany stopnia 2 **kwadratowymi**.

Dla wielomianu $f = a_0 + a_1x + \dots + a_nx^n$ współczynnik a_n nazywamy **najstarszym** (lub **największym**) współczynnikiem. Jeżeli najstarszy współczynnik równy jest 1, to wielomian f nazywamy **unormowanym**.

W zbiorze wszystkich wielomianów zmiennej x o współczynnikach z pierścienia R definiujemy dodawanie $+$ i mnożenie $\cdot$, kładąc dla dowolnych wielomianów $f = a_0 + a_1x + \dots + a_nx^n$ oraz $g = b_0 + b_1x + \dots + b_mx^m$:

$$f + g = \begin{cases} (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n + b_{n+1}x^{n+1} + \dots + b_mx^m, & \text{gdy } m > n, \\ (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n, & \text{gdy } m = n, \\ (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_m + b_m)x^m + b_{m+1}x^{m+1} + \dots + b_nx^n, & \text{gdy } m < n. \end{cases}$$

$$f \cdot g = c_0 + c_1x + \dots + c_{n+m}x^{n+m},$$

gdzie

$$c_i = \sum_{k=0}^i a_{i-k}b_k,$$

dla $i \in \{0, \dots, n+m\}$. Ponadto wyróżniamy wielomian 0 jako element neutralny dodawania oraz wielomian 1 jako element neutralny mnożenia. Wówczas zbiór wszystkich wielomianów zmiennej x o współczynnikach z pierścienia R z tak określonymi działaniami i wyróżnionymi elementami jest pierścieniem przemennym z jedyneką. Pierścień ten będziemy nazywali **pierścieniem wielomianów** zmiennej x o współczynnikach z pierścienia R i będziemy oznaczali przez $R[x]$.

Uwaga 12.1. Przy liczeniu stopni wielomianów przyjmujemy następującą umowę notacyjną:

- $\forall n \in \mathbb{N} (n > -\infty)$,
- $(-\infty) + (-\infty) = -\infty$,
- $\forall n \in \mathbb{N} (-\infty + n = -\infty)$.

Uwaga 12.2. Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Wówczas:

$$(1) \deg(f + g) \leq \max\{\deg(f), \deg(g)\};$$

(2) *jeśli*

$$\deg(f) \neq \deg(g),$$

to

$$\deg(f + g) = \max\{\deg(f), \deg(g)\};$$

(3) $\deg(fg) \leq \deg(f) + \deg(g);$ (4) *jeśli*

$$f \neq 0 \wedge g \neq 0 \wedge (a_n \text{ jest regularny} \vee b_m \text{ jest regularny}),$$

to

$$\deg(fg) = \deg(f) + \deg(g);$$

(5) *jeśli*

$$f \neq 0 \wedge g \neq 0 \wedge R \text{ jest pierścieniem całkowitym},$$

to

$$\deg(fg) = \deg(f) + \deg(g).$$

Dowód. (1) Niech $h = f + g = \sum_{k=0}^{\infty} c_k x^k$, przy czym $c_k = 0$ dla prawie wszystkich $k \in \mathbb{N}$. Ustalmy $k > \max\{n, m\} = \max\{\deg(f), \deg(g)\}$. Wówczas:

$$c_k = a_k + b_k = 0 + 0 = 0.$$

Wobec tego $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.

(2) Oczywiście.

(3) Niech $h = f + g = \sum_{k=0}^{\infty} c_k x^k$, przy czym $c_k = 0$ dla prawie wszystkich $k \in \mathbb{N}$. Ustalmy $k > n + m = \deg(f) + \deg(g)$. Mamy

$$c_k = \sum_{i=0}^k a_{k-i} b^i.$$

Jeżeli $i \in \{0, \dots, m\}$, to $k - i \in \{n + 1, \dots, k\}$, więc $a_{k-i} = 0$. Podobnie, jeżeli $i \in \{m + 1, \dots, k\}$, to $b_i = 0$. Zatem $c_k = 0$, a więc $\deg(fg) \leq \deg(f) + \deg(g)$.

(4) Niech $h = f + g = \sum_{k=0}^{\infty} c_k x^k$, przy czym $c_k = 0$ dla prawie wszystkich $k \in \mathbb{N}$. Mamy

$$\begin{aligned} c_{n+m} &= \sum_{i=0}^{n+m} a_{n+m-i} b^i \\ &= \underbrace{a_{n+m}}_{=0} b_0 + \underbrace{a_{n+m-1}}_{=0} b_1 + \dots + a_n b_m + a_{n-1} \underbrace{b_{m+1}}_{=0} + \dots + a_0 \underbrace{b_{m+n}}_{=0} \\ &= a_n b_m \end{aligned}$$

Ponieważ a_n lub b_m jest regularny, więc $c_{n+m} \neq 0$.

(5) Wynika wprost z (4). □

Wniosek 12.1. Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1 x + \dots + a_n x^n \in R[x].$$

Wówczas:

- (1) *jeśli a_n jest regularny w R , to f jest regularny w $R[x]$;*
- (2) *każdy wielomian unormowany jest elementem regularnym w $R[x]$;*

(3) jeśli R jest całkowity, to $R[x]$ jest całkowity.

Twierdzenie 12.1 (o dzieleniu wielomianów z resztą). Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Wówczas istnieją liczba $l \in \mathbb{N} \cup \{0\}$ oraz wielomiany $q, r \in R[x]$ takie, że

$$a_n^l \cdot g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Dowód. Jeżeli $\deg(g) = m < n = \deg(f)$, to kładziemy $l = 0$, $q = 0$, $r = g$.

Jeżeli $\deg(g) = m = n = \deg(f)$, to $l = 1$, $q = b_m$, $r = a_ng - b_mf$. Istotnie, zauważmy że wówczas $\deg(r) < n = \deg(f)$.

Jeżeli $\deg(g) = m > n = \deg(f)$, to dowód prowadzimy metodą indukcji względem $\deg(g) = m$. Załóżmy, że dla $m' \in \{n+1, \dots, m-1\}$ i dla wielomianów postaci

$$g_1 = b'_0 + b'_1x + \dots + b'_{m'}x^{m'} \in R[x]$$

istnieją liczba $l_1 \in \mathbb{N} \cup \{0\}$ oraz wielomiany $q_1, r_1 \in R[x]$ takie, że

$$a_n^{l_1} \cdot g_1 = q_1 \cdot f + r_1$$

oraz $\deg(r_1) < \deg(f)$. Połóżmy

$$g_1 = a_ng - b_mx^{m-n}f.$$

Wówczas

$$\deg(g_1) \in \{n+1, \dots, m-1\},$$

istnieją liczba $l_1 \in \mathbb{N} \cup \{0\}$ oraz wielomiany $q_1, r_1 \in R[x]$ takie, że

$$a_n^{l_1} \cdot g_1 = q_1 \cdot f + r_1 \text{ oraz } \deg(r_1) < \deg(f)$$

czyli

$$a_n^{l_1} \cdot (a_ng - b_mx^{m-n}f) = q_1 \cdot f + r_1 \text{ oraz } \deg(r_1) < \deg(f)$$

lub równoważnie

$$a_n^{l_1+1}g = (q_1 + b_mx^{m-n}) \cdot f + r_1 \text{ oraz } \deg(r_1) < \deg(f).$$

Tym samym kładąc $l = l_1 + 1$, $q = q_1 + a_n^{l_1}b_mx^{m-n}$ oraz $r = r_1$ otrzymujemy tezę. $\square$

Wniosek 12.2. Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Wówczas:

(1) jeśli $a_n = 1$, to istnieją wielomiany $q, r \in R[x]$ takie, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$;

(2) jeśli R jest ciałem, to istnieją wielomiany $q, r \in R[x]$ takie, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Dowód. (1) Oczywiście.

- (2) Jeżeli R jest ciałem, to istnieje element $a_n^{-1} \in R$, a więc taki, że $a_n^{-1}a_n = 1$. Wobec tego istnieją wielomiany $q_1, r_1 \in R[x]$ takie, że

$$g = q_1 \cdot a_n^{-1}f + r_1$$

oraz $\deg(r_1) < \deg(a_n^{-1}f) = \deg(f)$. Zatem kładąc $q = q_1 a_n^{-1}$ oraz $r = r_1$ otrzymujemy tezę □

Twierdzenie 12.2 (o jednoznaczności dzielenia z resztą). *Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto*

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Jeśli a_n jest regularny, to istnieje co najwyżej jedna para takich wielomianów $q, r \in R[x]$, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Dowód. Niech

$$\begin{aligned} g &= q_1 \cdot f + r_1, \deg(r_1) < \deg f, q_1, r_1 \in R[x], \\ g &= q_2 \cdot f + r_2, \deg(r_2) < \deg f, q_2, r_2 \in R[x]. \end{aligned}$$

Stąd

$$0 = (q_1 - q_2)f + (r_1 - r_2),$$

lub równowaznie

$$r_2 - r_1 = (q_1 - q_2)f.$$

Wobec Uwagi 12.2

$$\deg(f) > \max\{\deg(r_1), \deg(r_2)\} - \deg(r_2 - r_1) = \deg((q_1 - q_2)f) = \deg(q_1 - q_2) + \deg(f).$$

Tym samym $\deg(q_1 - q_2) = -\infty$, a więc $q_1 - q_2 = 0$, skąd też $r_2 = r_1$. □

Wniosek 12.3. *Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto*

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

- (1) *Jeżeli R jest całkowity, to istnieje co najwyżej jedna para takich wielomianów $q, r \in R[x]$, że*

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

- (2) *Jeżeli $a_n = 1$, to istnieje dokładnie jedna para takich wielomianów $q, r \in R[x]$, że*

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

- (3) *Jeżeli R jest ciałem, to istnieje dokładnie jedna para takich wielomianów $q, r \in R[x]$, że*

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$.

Definicja 12.1. Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x] \text{ oraz } g = b_0 + b_1x + \dots + b_mx^m \in R[x].$$

Jeżeli istnieje dokładnie jedna para takich wielomianów $q, r \in R[x]$, że

$$g = q \cdot f + r$$

oraz $\deg(r) < \deg(f)$ to mówimy, że w pierścieniu $R[x]$ wykonalne jest **dzielenie z resztą** wielomianu g przez f . Wielomian q nazywamy wówczas **niepełnym ilorazem**, a wielomian r **resztą** z dzielenia.