

13. WYKŁAD 13: WARTOŚĆ WIELOMIANU, PIERWIĄSTKI WIELOMIANU, FUNKCJA WIELOMIANOWA. WIELOMIANY WIELU ZMIENNYCH.

13.1. Wartość wielomianu, pierwiastki wielomianu, funkcja wielomianowa.

Twierdzenie 13.1 (własność uniwersalna pierścienia wielomianów). *Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R .*

(1) *Pierścień R ma następującą własność:*

$\forall P$ – pierścień $\forall r \in P \forall \phi : R \rightarrow P$ – homomorfizm $\exists! \psi : R[x] \rightarrow P [\psi(x) = r \wedge \psi \upharpoonright_R = \phi]$.

(2) *Dla dowolnego rozszerzenia $R \subset S$ oraz elementu $s \in S \setminus R$ takiego, że $S = R[s]$, jeżeli*

$\forall P$ – pierścień $\forall r \in P \forall \phi : R \rightarrow P$ – homomorfizm $\exists! \psi : S \rightarrow P [\psi(x) = r \wedge \psi \upharpoonright_R = \phi]$.

to $S \cong R[x]$ i izomorfizm $\alpha : R[x] \rightarrow S$ jest jednoznacznie wyznaczony przez warunki

$$\alpha(x) = s \text{ oraz } \alpha \upharpoonright_R = \text{id}_R.$$

Dowód. (1) Ustalmy pierścień P , element $r \in P$ i homomorfizm $\phi : R \rightarrow P$. Zdefiniujemy odwzorowanie $\psi : R[x] \rightarrow P$ wzorem

$$\psi \left(\sum_{k=0}^n a_k x^k \right) = \sum_{k=0}^n \phi(a_k) r^k.$$

Bez trudu sprawdzamy, że ψ jest homomorfizmem. Ponadto $\psi(x) = r$ oraz $\psi(a) = \phi(a)$, dla $a \in R$.

Pokażemy, że ψ jest wyznaczony jednoznacznie. Istotnie, załóżmy, że $\psi_1 : R[x] \rightarrow P$ oraz $\psi_2 : R[x] \rightarrow P$ są dwoma homomorfizmami spełniającymi warunki

$$\psi_1(x) = r \wedge \psi_1 \upharpoonright_R = \phi$$

oraz

$$\psi_2(x) = r \wedge \psi_2 \upharpoonright_R = \phi.$$

Wówczas dla $\sum_{k=0}^n a_k x^k \in R[x]$:

$$\begin{aligned} \psi_1 \left(\sum_{k=0}^n a_k x^k \right) &= \sum_{k=0}^n \psi_1(a_k) (\psi_1(x))^k = \sum_{k=0}^n \psi_1(a_k) r^k \\ &= \sum_{k=0}^n \psi_2(a_k) r^k = \sum_{k=0}^n \psi_2(a_k) (\psi_2(x))^k \\ &= \psi_2 \left(\sum_{k=0}^n a_k x^k \right). \end{aligned}$$

(2) Ustalmy pierścień S , $R \subset S$ i niech $s \in S \setminus R$. Załóżmy, że

$\forall P$ – pierścień $\forall r \in P \forall \phi : R \rightarrow P$ – homomorfizm $\exists! \psi : S \rightarrow P [\psi(x) = r \wedge \psi \upharpoonright_R = \phi]$.

Wobec udowodnionej już części twierdzenia istnieje dokładnie jeden homomorfizm $\psi_1 : R[x] \rightarrow S$ taki, że

$$\psi_1(x) = s \wedge \psi_1 \upharpoonright_R = \text{id}_R.$$

Wobec założenia istnieje dokładnie jeden homomorfizm $\psi_2 : S \rightarrow R[x]$ taki, że

$$\psi_2(s) = x \wedge \psi_2 \upharpoonright_R = \text{id}_R.$$

Pokażemy, że $\psi_2 \circ \psi_1 = id_{R[x]}$. Istotnie, dla $\sum_{k=0}^n a_k x^k \in R[x]$:

$$\begin{aligned} \psi_2 \circ \psi_1 \left(\sum_{k=0}^n a_k x^k \right) &= \psi_2 \left(\sum_{k=0}^n \psi_1(a_k) (\psi_1(x))^k \right) = \psi_2 \left(\sum_{k=0}^n a_k s^k \right) \\ &= \sum_{k=0}^n \psi_2(a_k) (\psi_2(s))^k = \sum_{k=0}^n a_k x^k. \end{aligned}$$

Analogicznie pokazujemy, że $\psi_1 \circ \psi_2 = id_S$. □

Definicja 13.1. Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R .

- (1) Dla dowolnego pierścienia P i jego elementu $r \in P$ oraz homomorfizmu $\phi : R \rightarrow P$, jedyne przedłużenie $\psi : R[x] \rightarrow P$ homomorfizmu ϕ takie, że

$$\psi(x) = r \text{ oraz } \psi|_R = \phi$$

nazwamy **wartością wielomianów**, a jego wartość dla wielomianu $f \in R[x]$, $\psi(f)$, **wartością wielomianu f w punkcie $r \in R$** . Jeżeli wartość wielomianu f w punkcie $r \in R$ jest równa 0, to punkt $r \in R$ nazywamy **miejszem zerowym** (lub **pierwiastkiem**) f . Najczęściej rozważamy przypadek, gdy $R = P$ oraz $\phi = id_P$. Wówczas

$$\psi(f) = \psi \left(\sum_{k=0}^n a_k x^k \right) = \sum_{k=0}^n a_k r^k.$$

- (2) Dla pierścienia R^R i jego elementu $id_R \in R^R$ oraz homomorfizmu $\phi : R \rightarrow R^R$ danego wzorem

$$\phi(a) = \text{const}.a, \text{ dla } a \in R,$$

obraz $\psi(R[x])$ poprzez jedyne przedłużenie $\psi : R[x] \rightarrow R^R$ homomorfizmu ϕ takie, że

$$\psi(x) = id_R \text{ oraz } \psi|_R = \phi$$

nazwamy **pierścieniem funkcji wielomianowych** o współczynnikach z R , a jego elementy **funkcjami wielomianowymi**.

Definicja i Uwaga 13.1. Niech R, P będą pierścieniami, a $\phi : P \rightarrow R$ homomorfizmem pierścieni. Wówczas istnieje dokładnie jeden homomorfizm $\psi : R[x] \rightarrow P[y]$ taki, że

$$\psi(x) = y \text{ oraz } \psi|_R = \phi.$$

Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy, a jeśli ϕ jest surjektywny, to ψ jest surjektywny. Homomorfizm ψ nazywamy **homomorfizmem pierścieni wielomianów indukowanym przez homomorfizm współczynników**.

Dowód. Pokażemy, że istnieje dokładnie jeden homomorfizm $\psi : R[x] \rightarrow P[y]$ taki, że

$$\psi(x) = y \text{ oraz } \psi|_R = \phi.$$

Istotnie, wobec Twierdzenia 13.1 wystarczy wziąć $P = P[y]$ oraz $r = y$.

Założmy, że ϕ jest różnowartościowy. Pokażemy, że ψ jest różnowartościowy. Istotnie, ustalmy $f = \sum_{k=0}^n a_k x^k \in \ker \psi$. Wówczas

$$\begin{aligned} 0 &= \psi(f) = \psi\left(\sum_{k=0}^n a_k x^k\right) \\ &= \sum_{k=0}^n \psi(a_k)(\psi(x))^k = \sum_{k=0}^n \phi(a_k)y^k, \end{aligned}$$

a zatem $\phi(a_k) = 0$, $k \in \{0, \dots, n\}$, czyli $a_k \in \ker \phi$, $k \in \{0, \dots, n\}$. Ponieważ ϕ jest różnowartościowy, więc $a_k = 0$, $k \in \{0, \dots, n\}$, a zatem $f = 0$.

Założmy, że ϕ jest surjektywny. Pokażemy, że ψ jest surjektywny. Istotnie, ustalmy $g = \sum_{k=0}^n b_k y^k \in P[x]$. Ponieważ ϕ jest surjektywny, więc $b_k = \phi(a_k)$, dla pewnego $a_k \in R$, $k \in \{0, \dots, n\}$. Wówczas

$$\begin{aligned} g &= \sum_{k=0}^n b_k y^k = \sum_{k=0}^n \phi(a_k)y^k \\ &= \sum_{k=0}^n \psi(a_k)(\psi(x))^k = \psi\left(\sum_{k=0}^n a_k x^k\right). \end{aligned}$$

□

Twierdzenie 13.2 (Bézout¹). *Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto $f \in R[x]$ oraz $a \in R$. Wówczas a jest pierwiastkiem wielomianu f wtedy i tylko wtedy, gdy $x - a$ dzieli f .*

Dowód. ($\Rightarrow$): Załóżmy, że $f(a) = 0$. Dzieląc z resztą f przez $x - a$ otrzymujemy

$$f(x) = q(x) \cdot (x - a) + r(x) \text{ gdzie } q, r \in R[x] \text{ oraz } \deg r < \deg(x - a) = 1.$$

Tym samym $\deg r \in \{-\infty, 0\}$, więc r jest wielomianem stałym. Ponadto

$$0 = f(a) = q(a) \cdot (a - a) + r(a),$$

skąd $r(a) = 0$. Zatem $x - a$ dzieli f .

($\Leftarrow$): Załóżmy, że $f(x) = q(x) \cdot (x - a)$, dla pewnego $q \in R[x]$. Wówczas

$$0 = q(a) \cdot (a - a) = f(a).$$

□

Wniosek 13.1. *Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto $f \in R[x]$ oraz $a \in R$. Wówczas:*

- (1) $f(x) = q(x) \cdot (x - a) + f(a)$, dla pewnego $q \in R[x]$;
- (2) (schemat Hornera) jeżeli $f = \sum_{k=0}^n a_k x^k$, to

$$f(x) = \left(\sum_{k=0}^{n-1} b_k x^k\right) \cdot (x - a) + (a_0 + ab_0),$$

gdzie

$$b_{n-1} = a_n \text{ oraz } b_k = a_{k+1} + ab_{k+1} \text{ dla } k \in \{n-2, \dots, 0\}.$$

Dowód. (1) Porównaj dowód twierdzenia Bézout.

¹E. Bézout (1730-1780) – matematyk francuski.

(2) Wobec udowodnionej już części twierdzenia:

$$\sum_{k=0}^n a_k x^k = q(x) \cdot (x - a) + \sum_{k=0}^n a_k a^k.$$

Niech $q = \sum_{k=0}^{n-1} b_k x^k$. Wówczas:

$$\begin{aligned} \sum_{k=0}^n a_k x^k &= \left(\sum_{k=0}^{n-1} b_k x^k \right) \cdot (x - a) + \sum_{k=0}^n a_k a^k \\ &= b_0 x + b_1 x^2 + \dots + b_{n-1} x^n \\ &\quad - b_0 a - b_1 x a - \dots - b_{n-1} x^{n-1} a + \sum_{k=0}^n a_k a^k \\ &= \left(\sum_{k=0}^n a_k a^k - b_0 a \right) + (b_0 - b_1 a) x + \dots + (b_{n-2} - b_{n-1} a) x^{n-1} + b_{n-1} x^n. \end{aligned}$$

Stąd:

$$\begin{array}{llll} a_0 &= \sum_{k=0}^n a_k a^k - b_0 a &\Rightarrow f(a) &= \sum_{k=0}^n a_k a^k = a_0 + a b_0 \\ a_1 &= b_0 - b_1 a &\Rightarrow b_0 &= a_1 + a b_1 \\ \vdots &&\vdots &\vdots \\ a_{n-1} &= b_{n-2} - b_{n-1} a &\Rightarrow b_{n-2} &= a_{n-1} + a b_{n-1} \\ a_n &= b_{n-1} &\Rightarrow b_{n-1} &= a_n. \end{array}$$

□

Definicja 13.2. Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto $f \in R[x]$ oraz $a \in R$. Element $a \in R$ nazywamy **pierwiastkiem k -krotnym** wielomianu f , gdy f jest podzielny przez $(x - a)^k$, ale nie jest podzielny przez $(x - a)^{k+1}$.

Lemat 13.1. Niech R będzie dowolnym pierścieniem, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto $f \in R[x]$ oraz $a \in R$. Wówczas a jest pierwiastkiem k -krotnym wielomianu f wtedy i tylko wtedy, gdy istnieje wielomian $q \in R[x]$ taki, że $f(x) = (x - a)^k \cdot q(x)$ oraz $q(a) \neq 0$.

Dowód. ($\Rightarrow$): Załóżmy, że istnieją wielomiany $q_1, q_2, r_2 \in R[x]$ takie, że

$$f(x) = q_1(x) \cdot (x - a)^k$$

oraz

$$f(x) = q_2(x) \cdot (x - a)^{k+1} + r_2(x) \text{ gdzie } r_2(a) \neq 0.$$

Przypuśćmy, że $q_1(a) = 0$. Wówczas, wobec twierdzenia Bézout:

$$q_1(x) = q_3(x) \cdot (x - a).$$

Zatem

$$f(x) = q_3(x) \cdot (x - a)^{k+1}$$

co jest sprzecznością wobec jednoznaczności dzielenia z resztą.

($\Leftarrow$): Załóżmy, że istnieje wielomian $q \in R[x]$ taki, że $f = (x - a)^k \cdot q(x)$ oraz $q(a) \neq 0$. Niech a będzie pierwiastkiem l -krotnym wielomianu f . Oczywiście $l \geq k$. Przypuśćmy, że $l > k$. Wówczas

$$f(x) = q_2(x) \cdot (x - a)^{k+1}$$

dla pewnego $q_2 \in R[x]$. Stąd

$$q_2(x) \cdot (x - a)^{k+1} = (x - a)^k \cdot q(x)$$

a zatem $q(x) = q_2(x) \cdot (x - a)$, czyli wobec twierdzenia Bézout a jest pierwiastkiem q , czyli $q(a) = 0$, co daje sprzeczność. $\square$

Twierdzenie 13.3 (o rozkładzie wielomianu na czynniki liniowe). *Niech R będzie pierścieniem całkowitym, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto $0 \neq f \in R[x]$ oraz $a_1, \dots, a_m \in R$ będą pierwiastkami wielomianu f o krotnościach $k_1, \dots, k_m$, odpowiednio. Wówczas istnieje wielomian $q \in R[x]$ taki, że*

$$f(x) = (x - a_1)^{k_1} \cdot \dots \cdot (x - a_m)^{k_m} \cdot q(x) \text{ oraz } q(a_i) \neq 0, i \in \{1, \dots, m\}.$$

Dowód. Dowód prowadzimy przez indukcję względem m . Dla $m = 1$ teza wynika wprost z poprzedniego lematu. Dla $m > 1$ załóżmy, że jeśli $a_1, \dots, a_{m-1} \in R$ są pierwiastkami wielomianu f o krotnościach $k_1, \dots, k_{m-1}$, odpowiednio, to istnieje wielomian $q_1 \in R[x]$ taki, że

$$f(x) = (x - a_1)^{k_1} \cdot \dots \cdot (x - a_{m-1})^{k_{m-1}} \cdot q_1(x) \text{ oraz } q_1(a_i) \neq 0, i \in \{1, \dots, m-1\}.$$

Będziemy chcieli pokazać, że istnieje wielomian $q \in R[x]$ taki, że

$$f(x) = (x - a_1)^{k_1} \cdot \dots \cdot (x - a_m)^{k_m} \cdot q(x) \text{ oraz } q(a_i) \neq 0, i \in \{1, \dots, m\}.$$

W tym celu pokażemy najpierw, że a_m jest pierwiastkiem wielomianu q_1 . Istotnie, ponieważ a_m jest pierwiastkiem wielomianu f , więc

$$0 = f(a_m) = (a_m - a_1)^{k_1} \cdot \dots \cdot (a_m - a_{m-1})^{k_{m-1}} \cdot q_1(a_m)$$

i skoro $a_m - a_i \neq 0, i \in \{1, \dots, m-1\}$ i pierścień R jest całkowity, to

$$q_1(a_m) = 0.$$

Załóżmy, że a_m jest pierwiastkiem q_1 o krotności l . Wobec poprzedniego lematu istnieje wielomian $q \in R[x]$ taki, że

$$q_1(x) = (x - a_m)^l q(x) \text{ oraz } q(a_m) \neq 0,$$

a zatem

$$f(x) = (x - a_1)^{k_1} \cdot \dots \cdot (x - a_{m-1})^{k_{m-1}} \cdot (x - a_m)^l \cdot q(x) \text{ oraz } q(a_i) \neq 0, i \in \{1, \dots, m\}.$$

Pozostaje pokazać, że $l = k_m$. Istotnie, oznaczmy

$$q_2(x) = (x - a_1)^{k_1} \cdot \dots \cdot (x - a_{m-1})^{k_{m-1}} \cdot q(x).$$

Wówczas

$$f(x) = (x - a_m)^l q_2(x)$$

i ponadto

$$q_2(a_m) = (a_m - a_1)^{k_1} \cdot \dots \cdot (a_m - a_{m-1})^{k_{m-1}} \cdot q(a_m) \neq 0,$$

skoro $a_m - a_i \neq 0, i \in \{1, \dots, m-1\}$, $q(a_m) \neq 0$ i pierścień R jest całkowity. Tym samym wobec poprzedniego lematu a_m jest l -krotnym pierwiastkiem wielomianu f , a więc $l = k_m$. $\square$

Wniosek 13.2. *Niech R będzie pierścieniem całkowitym, $(R[x], +, \cdot)$ pierścieniem wielomianów zmiennej x o współczynnikach z pierścienia R . Niech ponadto $0 \neq f \in R[x]$. Wówczas:*

(1) jeśli $a_1, \dots, a_m \in R$ będą pierwiastkami wielomianu f o krotnościach $k_1, \dots, k_m$, odpowiednio, to

$$\sum_{i=1}^m k_i \leq \deg(f);$$

(2) jeśli f jest wielomianem stopnia n , to f ma co najwyżej n pierwiastków;

(3) jeśli R jest nieskończony, to dla pewnego $r \in R$, $f(a) \neq 0$;

(4) jeśli R jest nieskończony, to jedyny homomorfizm $\psi : R[x] \rightarrow R^R$ definiujący pierścień funkcji wielomianowych jest różnowartościowy.

Dowód. (1) Wobec Uwagi 12.2 i Twierdzenia o rozkładzie wielomianu na czynniki liniowe, ponieważ istnieje wielomian $q \in R[x]$ taki, że

$$f(x) = (x - a_1)^{k_1} \cdot \dots \cdot (x - a_m)^{k_m} \cdot q(x) \text{ oraz } q(a_i) \neq 0, i \in \{1, \dots, m\},$$

więc

$$\deg(f) = \sum_{i=1}^m k_i + \deg(q) \geq \sum_{i=1}^m k_i.$$

(2) Oczywiste.

(3) Wobec (2) wielomian f ma co najwyżej $\deg(f)$ pierwiastków, zaś pierścień R jest nieskończony, więc dla pewnego $a \in R$

$$f(a) \neq 0.$$

(4) Niech $\psi : R[x] \rightarrow R^R$ będzie jedynym przedłużeniem homomorfizmu $\phi : R \rightarrow R^R$ danego wzorem

$$\phi(a) = \text{const}.a, \text{ dla } a \in R,$$

takim, że

$$\psi(x) = \text{id}_R \text{ oraz } \psi \upharpoonright_R = \phi.$$

Ustalmy $f = \sum_{k=0}^n a_k x^k \in \ker \psi$. Wówczas

$$0 = \psi(f) = \psi\left(\sum_{k=0}^n a_k x^k\right) = \sum_{k=0}^n \text{const}.a_k \cdot (\text{id}_R)^k.$$

Ponieważ dla $a \in R$:

$$f(a) = \sum_{k=0}^n \text{const}.a_k(a) \cdot (\text{id}_R(a))^k = 0,$$

więc $f \equiv 0$.

□

13.2. Wielomiany wielu zmiennych.

Definicja i Uwaga 13.2. Niech R będzie dowolnym pierścieniem. **Wielomianem** zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R będziemy nazywali wyrażenie postaci

$$\sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n},$$

gdzie $m \in \mathbb{N}$, wskaźniki $i_1, \dots, i_n \in \mathbb{N}$ przebiegają wszystkie liczby nie większe niż m oraz $a_{i_1 \dots i_n} \in R$.

Dwa wielomiany uważamy za **równe**, gdy różnią się jedynie o składniki postaci $0 \cdot x_1^{i_1} \dots x_n^{i_n}$, gdzie $i_1, \dots, i_n \in \mathbb{N}$.

Bedziemy mówili, że wielomian $f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ jest **stopnia** r , gdy istnieje taki różny od zera współczynnik $a_{i_1 \dots i_n}$, że $i_1 + \dots + i_n = r$ i $a_{j_1 \dots j_n} = 0$ o ile $j_1 + \dots + j_n > r$. 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 nazywali **liniowymi**, a wielomiany stopnia 2 **kwadratowymi**.

Wielomian postaci $a \cdot x_1^{i_1} \dots x_n^{i_n}$, gdzie $a \in R$ oraz $i_1, \dots, i_n \in \mathbb{N}$ nazywamy **jednomianem**.

W zbiorze wszystkich wielomianów zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R definiujemy dodawanie $+$ i mnożenie $\cdot$, kładąc dla dowolnych wielomianów $f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ oraz $g = \sum_{j_1, \dots, j_n \leq r} b_{j_1 \dots j_n} x_1^{j_1} \dots x_n^{j_n}$:

$$f + g = \sum_{k_1, \dots, k_n \leq \max\{m, r\}} c_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}$$

gdzie

$$c_{k_1 \dots k_n} = \begin{cases} a_{k_1 \dots k_n} + b_{k_1 \dots k_n}, & \text{gdy } k_1, \dots, k_n \leq \max\{m, r\}, \\ a_{k_1 \dots k_n}, & \text{gdy, dla pewnego wskaźnika } k_i, i \in \{1, \dots, n\}, k_i > r, \text{ ale } k_1, \dots, k_n < m, \\ b_{k_1 \dots k_n}, & \text{gdy, dla pewnego wskaźnika } k_i, i \in \{1, \dots, n\}, k_i > m, \text{ ale } k_1, \dots, k_n < r, \end{cases}$$

oraz

$$f \cdot g = \sum_{k_1, \dots, k_n \leq m+r} c_{k_1 \dots k_n} x_1^{k_1} \dots x_n^{k_n}$$

gdzie

$$c_{k_1 \dots k_n} = \sum_{0 \leq l_1 \leq k_1, \dots, 0 \leq l_n \leq k_n} a_{k_1 - l_1, \dots, k_n - l_n} b_{l_1 \dots l_n}.$$

Ponadto wyróżniamy wielomian 0 jako element neutralny dodawania oraz wielomian 1 jako element neutralny mnożenia. Wówczas zbiór wszystkich wielomianów zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R z tak określonymi działaniami i wyróżnionymi elementami jest pierścieniem przemienym z jedynką. Pierścień ten będziemy nazywali **pierścieniem wielomianów** zmiennych $x_1, \dots, x_n$ o współczynnikach z pierścienia R i będziemy oznaczali przez $R[x_1, \dots, x_n]$.

Uwaga 13.1. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Niech ponadto

$$f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \in R[x_1, \dots, x_n] \text{ oraz } g = \sum_{j_1, \dots, j_n \leq r} b_{j_1 \dots j_n} x_1^{j_1} \dots x_n^{j_n} \in R[x_1, \dots, x_n].$$

Wówczas:

- (1) $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$;
- (2) $\deg(fg) \leq \deg(f) + \deg(g)$;
- (3) jeśli

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

to

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

Wniosek 13.3. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Wówczas jeśli R jest pierścieniem całkowitym, to $R[x_1, \dots, x_n]$ też.

Definicja 13.3. Niech R i P będą dowolnymi pierścieniami, niech $R \subset P$ i niech $S \subset P$ będzie pewnym zbiorem. Zbiór S nazywamy **algebraicznie niezależnym nad R** , jeżeli zbiór

$$\{f \in R[s_1, \dots, s_n] : n \in \mathbb{N}, s_1, \dots, s_n \in S, f \text{ jest jednomianem}\}$$

jest liniowo niezależny nad pierścieniem R .

Twierdzenie 13.4 (własność uniwersalna pierścienia wielomianów wielu zmiennych). Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R .

(1) Pierścień R ma następującą własność:

$$\forall P - \text{pierścień } \forall r_1, \dots, r_n \in P \forall \phi : R \rightarrow P - \text{homomorfizm } \exists! \psi : R[x_1, \dots, x_n] \rightarrow P$$

$$[\psi(x_i) = r_i, i \in \{1, \dots, n\} \wedge \psi \upharpoonright_R = \phi].$$

(2) Dla dowolnego rozszerzenia $R \subset S$ oraz elementów $s_1, \dots, s_n \in S \setminus R$ algebraicznie niezależnych nad R i takich, że $S = R[s_1, \dots, s_n]$, jeżeli

$$\forall P - \text{pierścień } \forall r_1, \dots, r_n \in P \forall \phi : R \rightarrow P - \text{homomorfizm } \exists! \psi : S \rightarrow P$$

$$[\psi(s_i) = r_i, i \in \{1, \dots, n\} \wedge \psi \upharpoonright_R = \phi].$$

to $S \cong R[x_1, \dots, x_n]$ i izomorfizm $\alpha : R[x_1, \dots, x_n] \rightarrow S$ jest jednoznacznie wyznaczony przez warunki

$$\alpha(x_i) = s_i, i \in \{1, \dots, n\} \text{ oraz } \alpha \upharpoonright_R = \text{id}_R.$$

Definicja 13.4. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R .

(1) Dla dowolnego pierścienia P i jego elementu $r \in P$ oraz homomorfizmu $\phi : R \rightarrow P$, jedyne przedłużenie $\psi : R[x_1, \dots, x_n] \rightarrow P$ homomorfizmu ϕ takie, że

$$[\psi(x_i) = r_i, i \in \{1, \dots, n\} \wedge \psi \upharpoonright_R = \phi]$$

nazwamy **wartością wielomianów**, a jego wartość dla wielomianu $f \in R[x_1, \dots, x_n]$, $\psi(f)$, **wartością wielomianu f w punkcie $(r_1, \dots, r_n) \in R^n$** . Jeżeli wartość wielomianu f w punkcie $(r_1, \dots, r_n) \in R^n$ jest równa 0, to punkt $(r_1, \dots, r_n) \in R^n$ nazywamy **miejscem zerowym** (lub **pierwiastkiem**) f . Najczęściej rozważamy przypadek, gdy $R = P$ oraz $\phi = \text{id}_P$. Wówczas

$$\psi(f) = \psi \left(\sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \right) = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} r_1^{i_1} \dots r_n^{i_n}.$$

(2) Dla pierścienia R^{R^n} i jego elementów $\pi_1, \dots, \pi_n \in R^{R^n}$ takich, że

$$\pi_j(a_1, a_2, \dots, a_j, \dots, a_n) = a_j, (a_1, \dots, a_n) \in R^n, j \in \{1, \dots, n\},$$

oraz homomorfizmu $\phi : R \rightarrow R^{R^n}$ danego wzorem

$$\phi(a) = \text{const}.a, \text{ dla } a \in R,$$

obraz $\psi(R[x_1, \dots, x_n])$ poprzez jedyne przedłużenie $\psi : R[x_1, \dots, x_n] \rightarrow R^{R^n}$ homomorfizmu ϕ takie, że

$$\psi(x_i) = \pi_i, i \in \{1, \dots, n\} \text{ oraz } \psi \upharpoonright_R = \phi$$

nazwamy **pierścieniem funkcji wielomianowych** o współczynnikach z R , a jego elementy funkcjami wielomianowymi.

Definicja i Uwaga 13.3. Niech R, P będą pierścieniami, a $\phi : P \rightarrow R$ homomorfizmem pierścieni. Wówczas istnieje dokładnie jeden homomorfizm $\psi : R[x_1, \dots, x_n] \rightarrow P[y_1, \dots, y_n]$ taki, że

$$\psi(x_i) = y_i, i \in \{1, \dots, n\} \text{ oraz } \psi \upharpoonright_R = \phi.$$

Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy, a jeśli ϕ jest surjektywny, to ψ jest surjektywny. Homomorfizm ψ nazywamy **homomorfizmem pierścieni wielomianów n zmiennych indukowanym przez homomorfizm współczynników**.

Wniosek 13.4. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Niech ponadto $0 \neq f \in R[x_1, \dots, x_n]$. Wówczas:

- (1) jeśli R jest nieskończony, to dla pewnego $(r_1, \dots, r_n) \in R^n$, $f(r_1, \dots, r_n) \neq 0$;
- (2) jeśli R jest nieskończony, to jedyny homomorfizm $\psi : R[x_1, \dots, x_n] \rightarrow R^{R^n}$ definiujący pierścień funkcji wielomianowych jest różnowartościowy.

Definicja 13.5. Niech $(I, <)$ będzie zbiorem częściowo uporządkowanym. Jeżeli

$$\forall i, j \in I \exists k \in I [i < k \wedge j < k],$$

to wówczas $(I, <)$ nazywamy **zbiorem skierowanym**.

Uwaga 13.2. Niech $(I, <)$ będzie zbiorem skierowanym, niech $\{R_i : i \in I\}$ będzie rodziną pierścieni indeksowaną elementami zbioru I taką, że

$$\forall i, j \in I [(i < j) \Rightarrow (R_i < R_j)].$$

W zbiorze $\bigcup_{i \in I} R_i$ definiujemy działania $+$ oraz $\cdot$ następująco:

- jeśli $a, b \in \bigcup_{i \in I} R_i$, to $a \in R_i$, $b \in R_j$, dla pewnych $i, j \in I$; ponieważ I jest skierowany, więc dla pewnego $k \in I$ zachodzi $i < k$ oraz $j < k$, a zatem $R_i < R_k$ oraz $R_j < R_k$, więc $a, b \in R_k$ i możemy zdefiniować

$$a + b = a +_{R_k} b \text{ oraz } a \cdot b = a \cdot_{R_k} b.$$

Wówczas $(\bigcup_{i \in I} R_i, +, \cdot)$ jest pierścieniem.

Definicja i Uwaga 13.4. Niech R będzie pierścieniem, S pewnym zbiorem, a $\{x_s : s \in S\}$ rodziną zmiennych indeksowaną elementami zbioru S . Dla dowolnego skończonego zbioru $T = \{s_1, \dots, s_n\} \subset S$ definiujemy

$$R_T = R[x_{s_1}, \dots, x_{s_n}].$$

Wówczas $(I, \subset)$, gdzie $I = \{T \subset S : \text{card} T < \infty\}$ jest zbiorem indeksowanym, zaś $\{R_T : T \in I\}$ rodziną pierścieni indeksowaną elementami zbioru I taką, że

$$\forall T_1, T_2 \in I [(T_1 \subset T_2) \Rightarrow (R_{T_1} < R_{T_2})].$$

Wobec poprzedniej uwagi $\bigcup_{T \in I} R_T$ jest pierścieniem. Nazywamy go **pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z R i oznaczamy $R[\{x_s : s \in S\}]$.**

Uwaga 13.3. Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R . Niech ponadto

$$f \in R[\{x_s : s \in S\}] \text{ oraz } g \in R[\{x_s : s \in S\}].$$

Wówczas:

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

- (2) $\deg(fg) \leq \deg(f) + \deg(g)$;
 (3) jeśli

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

to

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

Wniosek 13.5. Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R . Wówczas jeśli R jest pierścieniem całkowitym, to $R[\{x_s : s \in S\}]$ też.

Twierdzenie 13.5 (własność uniwersalna pierścienia wielomianów nieskończenie wielu zmiennych). Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R .

- (1) Pierścień R ma następującą własność:

$\forall P$ – pierścień $\forall \lambda : \{x_s : s \in S\} \rightarrow P$ – odwzorowanie $\forall \phi : R \rightarrow P$ – homomorfizm $\exists! \psi : R[\{x_s : s \in S\}] \rightarrow P$

$$[\psi \upharpoonright_{\{x_s : s \in S\}} = \lambda \wedge \psi \upharpoonright_R = \phi].$$

- (2) Dla dowolnego rozszerzenia $R \subset R'$ i zbioru $T \subset R'$ algebraicznie niezależnego nad R i takiego, że $R' = R[\{x_t : t \in T\}]$, jeżeli

$\forall P$ – pierścień $\forall \lambda : \{x_t : t \in T\} \rightarrow P$ – odwzorowanie $\forall \phi : R \rightarrow P$ – homomorfizm $\exists! \psi : R' \rightarrow P$

$$[\psi \upharpoonright_{\{x_t : t \in T\}} = \lambda \wedge \psi \upharpoonright_R = \phi].$$

to $R' \cong R[\{x_t : t \in T\}]$ i izomorfizm $\alpha : R[\{x_t : t \in T\}] \rightarrow R'$ jest jednoznacznie wyznaczony przez warunki

$$\alpha(x_t) = t, t \in T \text{ oraz } \alpha \upharpoonright_R = id_R.$$

Definicja 13.6. Niech R będzie dowolnym pierścieniem, S pewnym zbiorem, $R[\{x_s : s \in S\}]$ pierścieniem wielomianów nieskończonej liczby zmiennych ze zbioru $\{x_s : s \in S\}$ o współczynnikach z pierścienia R . Dla dowolnego pierścienia P i odwzorowania $\lambda : \{x_s : s \in S\} \rightarrow P$ oraz homomorfizmu $\phi : R \rightarrow P$, jedyne przedłużenie $\psi : R[\{x_s : s \in S\}] \rightarrow P$ homomorfizmu ϕ takie, że

$$[\psi \upharpoonright_{\{x_s : s \in S\}} = \lambda \wedge \psi \upharpoonright_R = \phi]$$

nazwamy **wartością wielomianów**, a jego wartość dla wielomianu $f \in R[\{x_s : s \in S\}]$, $\psi(f)$, **wartością wielomianu f na zbiorze $\lambda(\{x_s : s \in S\}) \subset P$** . Jeżeli wartość wielomianu f na zbiorze $\lambda(\{x_s : s \in S\}) \subset P$ jest równa 0, to zbiór $\lambda(\{x_s : s \in S\}) \subset P$ nazywamy **miejszem zerowym** (lub **pierwiastkiem**) f . Najczęściej rozważamy przypadek, gdy $R = P$ oraz $\phi = id_P$.

Definicja i Uwaga 13.5. Niech R, P będą pierścieniami, S pewnym zbiorem, a $\phi : P \rightarrow R$ homomorfizmem pierścieni. Wówczas istnieje dokładnie jeden homomorfizm $\psi : R[\{x_s : s \in S\}] \rightarrow P[\{y_s : s \in S\}]$ taki, że

$$\psi(x_s) = y_s, s \in S \text{ oraz } \psi \upharpoonright_R = \phi.$$

Ponadto jeśli ϕ jest różnowartościowy, to ψ jest różnowartościowy, a jeśli ϕ jest surjektywny, to ψ jest surjektywny. Homomorfizm ψ nazywamy **homomorfizmem pierścieni wielomianów n zmiennych indukowanym przez homomorfizm współczynników**.

Definicja 13.7. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Wielomian

$$0 \neq f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \in R[x_1, \dots, x_n]$$

nazywamy **wielomianem jednorodnym stopnia d** (lub **formą stopnia d**) jeżeli

$$\forall i_1, \dots, i_n \leq m [\deg(a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}) = d].$$

Formy stopnia 1 nazywamy **formami liniowymi**, formy stopnia 2 **formami kwadratowymi**, formy stopnia 3 **formami kubicznymi** itd.

Uwaga 13.4. Niech R będzie dowolnym pierścieniem, $(R[x_1, \dots, x_n], +, \cdot)$ pierścieniem wielomianów n zmiennych o współczynnikach z pierścienia R . Wielomian

$$0 \neq f = \sum_{i_1, \dots, i_n \leq m} a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n} \in R[x_1, \dots, x_n]$$

jest wielomianem jednorodnym stopnia d wtedy i tylko wtedy, gdy dla każdego pierścienia P , $R < P$ i dla każdego zbioru $n + 1$ algebraicznie niezależnych nad R elementów $a, b_1, \dots, b_n \in P$ zachodzi równość

$$f(ab_1, \dots, ab_n) = a^d f(b_1, \dots, b_n).$$