

Konstrukcja pierścienia wielomianów jednej zmiennej.

Definicja i uwaga:

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, przyjmiemy 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 $g = b_0 + b_1x + \dots + b_mx^m$:

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

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

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 przemiennym z jedynką. Pierścień ten będziemy nazywali **pierścieniem wielomianów** zmiennej x o współczynnikach z pierścienia R i będziemy oznaczali przez $R[x]$.

Uwaga

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:

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. Oczywiste.
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

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

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

5. Wynika wprost z (4).

Wniosek

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

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x].$$

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 (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 $l = 1$, $q = b_m$,
 $r = a_n g - b_m f$. 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 $\deg(r_1) < \deg(f)$.

Położmy

$$g_1 = a_n g - b_m x^{m-n} f.$$

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

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

lub równoważnie

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

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

Wniosek

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. Oczywiste.
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 (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

$$g = q_1 \cdot f + r_1, \deg(r_1) < \deg f, q_1, r_1 \in R[x],$$

$$g = q_2 \cdot f + r_2, \deg(r_2) < \deg f, q_2, r_2 \in R[x].$$

Stąd

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

lub równowaznie

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

Wobec Uwagi ??

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

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

$$r_2 = r_1.$$



Wniosek

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

Definicja

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.

Wartość wielomianu,
pierwiastki wielomianu,
funkcja wielomianowa.

Twierdzenie (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 $\exists ! \psi : R[x] \rightarrow P$

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 $\exists ! \psi : S \rightarrow P[\psi$

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

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

Dowód:

(1) Ustalmy pierścień P , element $r \in P$ i homomorfizm $\phi : R \rightarrow P$. Zdefiniujmy 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, założmy, 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 $\sum_{k=0}^n a_k x^k \in R[x]$:

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

(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 $\exists ! \psi : S \rightarrow P[\psi(x) =$

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

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

Pokażemy, że $\psi_2 \circ \psi_1 = \text{id}_{R[x]}$. 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 $\psi_1 \circ \psi_2 = \text{id}_S$.

Definicja:

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 **miejsцем 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

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

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

Istotnie, wobec Twierdzenia 0.3 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 (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 .

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

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

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.
- (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:

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

Stąd:

$$\begin{array}{llll} a_0 & = & \sum_{k=0}^n a_k a^k - b_0 a & \Rightarrow f(a) = \sum_{k=0}^n a_k a^k = a_0 + ab_0 \\ a_1 & = & b_0 - b_1 a & \Rightarrow b_0 = a_1 + ab_1 \\ & \vdots & & \vdots \\ a_{n-1} & = & b_{n-2} - b_{n-1} a & \Rightarrow b_{n-2} = a_{n-1} + ab_{n-1} \\ a_n & = & b_{n-1} & \Rightarrow b_{n-1} = a_n. \end{array}$$

Definicja

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

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.

Twierdzenie (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 $m > 1$ założmy, 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

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

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

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

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

$$q_1(a_m) = 0.$$

Założmy, 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

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

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 $l = k_m$.

Wniosek

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 $r \in R$, $f(r) \neq 0$;
4. jeśli R jest nieskończony, to jedyny homomorfizm $\psi : R[x] \rightarrow R^R$ definiujący pierścień funkcji wielomianowych jest różnowartościowy.

Dowód:

(1) Wobec Uwagi ?? 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

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

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

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

Ponieważ dla $a \in R$:

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

więc $f \equiv 0$.

Wielokrotne pierwiastki
wielomianów.
Różniczkowanie wielomianów.

Definicja

Niech F będzie ciałem. Wielomian $f \in F[x]$ nazywamy **rozdzielczym**, gdy w każdym rozszerzeniu L ciała F ma on wyłącznie pierwiastki jednokrotne.

Twierdzenie (o wzorach Viete'y²)

Niech R będzie pierścieniem całkowitym, niech $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in R[x]$ będzie wielomianem unormowanym. Niech $x_1, \dots, x_n \in R$ będą wszystkimi (uwzględniając krotności) pierwiastkami f w pierścieniu R . Wówczas:

$$\begin{aligned} a_{n-1} &= -(x_1 + \dots + x_n), \\ &\vdots \\ a_{n-k} &= (-1)^k \sum_{i_1, \dots, i_k} x_{i_1} \cdot \dots \cdot x_{i_k}, \\ &\vdots \\ a_0 &= (-1)^n x_1 \cdot \dots \cdot x_n. \end{aligned}$$

²F. Viete (1540-1603) – matematyk i prawnik francuski.

Dowód.

Dowód otrzymujemy porównując współczynniki przy kolejnych potęgach x 'a w równości:

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - x_1) \cdot (x - x_2) \cdot \dots \cdot (x - x_n).$$



Definicja

Niech R będzie pierścieniem, niech

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in R[x]$ będzie wielomianem. Wielomian

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in R[x]$$

nazywamy **pochodną** wielomianu f . Wielomian

$f^{(k)}(x) = f'(f^{(k-1)}(x))$, gdzie $f^{(1)}(x) = f'(x)$, nazywamy **k -tą pochodną** wielomianu f .

Definicja

Niech R będzie pierścieniem, niech $f_1, f_2, \dots, f_n \in R[x]$.

Wielomian

$$\det \begin{bmatrix} f_1 & f_2 & f_3 & \dots & f_n \\ f'_1 & f'_2 & f'_3 & \dots & f'_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f_1^{(n-1)} & f_2^{(n-1)} & f_3^{(n-1)} & \dots & f_n^{(n-1)} \end{bmatrix}$$

nazywamy **wrońskianem**³ wielomianów $f_1, f_2, \dots, f_n \in R[x]$.

³J. Hoene-Wroński (1776-1853) – matematyk, filozof, fizyk, prawnik i ekonomista polski, autor prac z zakresu analizy zespolonej.

Uwaga

Niech R będzie pierścieniem, niech $f, g \in R[x]$, niech $a \in R$.
Wówczas:

1. $(f + g)' = f' + g'$,
2. $(af)' = af'$,
3. $(fg)' = f'g + fg'$,
4. $(f^n)' = nf^{n-1}f'$.

Twierdzenie (wzór Leibniza)

Niech R będzie pierścieniem, niech $f, g \in R[x]$. Wówczas

$$(fg)^{(k)} = \sum_{i=0}^k \binom{k}{i} f^{(k-i)} g^{(i)}.$$

Twierdzenie (wzór Maclaurina)

Niech R będzie pierścieniem, niech $f \in R[x]$. Wówczas

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \dots + \frac{f^{(n)}(0)}{n!}x^n,$$

gdzie $n = \deg f$.

Twierdzenie (wzór Taylora)

Niech R będzie pierścieniem, niech $f \in R[x]$, $c \in R$. Wówczas

$$f(x + c) = f(c) + \frac{f'(c)}{1!}x + \frac{f''(c)}{2!}x^2 + \dots + \frac{f^{(n)}(c)}{n!}x^n,$$

gdzie $n = \deg f$.

Twierdzenie

Niech R będzie pierścieniem, niech $f \in R[x]$, $a \in R$. Wówczas

a jest pierwiastkiem k -krotnym f wtedy i tylko wtedy, gdy
$$f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0, f^{(k)}(a) \neq 0.$$

Dowód:

$(\Rightarrow)$: Załóżmy, że a jest k -krotnym pierwiastkiem f . Wobec tego istnieje wielomian $g \in R[x]$ taki, że

$$f(x) = (x - a)^k g(x) \text{ oraz } g(a) \neq 0.$$

Tym samym

$$f'(x) = (x - a)^{k-1} [kg(x) + (x - a)g'(x)] = (x - a)^{k-1} h(x),$$

gdzie $h(a) \neq 0$. Jeżeli $k - 1 > 0$, to

$$f''(x) = (x - a)^{k-2} h_1(x),$$

gdzie $h_1(a) \neq 0$. Postępując indukcyjnie po $k - 1$ krokach otrzymujemy

$$\begin{aligned} f^{(k-1)}(x) &= (x - a)h_{k-2}(x) \text{ oraz } h_{k-2}(x) \neq 0, \\ f^{(k)}(x) &= h_{k-2}(x) + (x - a)h'_{k-2}(x), \end{aligned}$$

a więc $f^{(k)}(a) \neq 0$ oraz $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$,
 $f^{(k)}(a) \neq 0$.

($\Leftarrow$) : Załóżmy, że $f(a) = f'(a) = \dots = f^{(k-1)}(a) = 0$,
 $f^{(k)}(a) \neq 0$. Niech l będzie krotnością pierwiastka a . Gdyby
 $l < k$ lub $l > k$, to otrzymujemy sprzeczność z udowodnioną już
częścią twierdzenia.

Wniosek

*Niech F będzie ciałem, niech $f \in F[x]$ i niech $g \sim NWD(f, f')$.
Wówczas jeśli $a \in F$ jest pierwiastkiem wielokrotnym
wielomianu f , to a jest też pierwiastkiem wielomianu g .*

Dowód.

Założmy, że $g(x) \sim NWD(f(x), f'(x))$. Wówczas istnieją wielomiany $u, v \in F[x]$ takie, że

$$uf + vf' = g.$$

Wobec Twierdzenia 0.10 $f(a) = 0$ oraz $f'(a) = 0$, a zatem $g(a) = 0$. □

Wniosek

Niech F będzie ciałem, niech $f \in F[x]$. Wówczas każdy pierwiastek f (w dowolnym ciele) jest jednokrotny wtedy i tylko wtedy, gdy $NWD(f, f') \sim 1$.

Dowód.

$(\Leftarrow)$: Przypuśćmy, że $a \in F$ jest pierwiastkiem wielokrotnym. Wobec Twierdzenia 0.10 $f(a) = 0$ oraz $f'(a) = 0$, a zatem $x - a \mid f(x)$ oraz $x - a \mid f'(x)$, co daje sprzeczność.

$(\Rightarrow)$: Przypuśćmy, że $NWD(f, f') \sim g \neq 1$. Wówczas $\deg g > 0$ oraz istnieje element $a \in \overline{F}$ taki, że $g(a) = 0$. Zatem $f(a) = 0$ oraz $f'(a) = 0$, więc a jest pierwiastkiem wielokrotnym f , co znów daje sprzeczność. □

Wniosek

Niech F będzie ciałem, niech $f \in F[x]$, niech ponadto $\text{char} F = 0$. Wówczas jeżeli f jest nierozkładalny w $F[x]$, to ma wyłącznie pierwiastki jednokrotne (w dowolnym ciele).

Dowód.

Niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in F[x]$, gdzie $a_n \neq 0$. Wówczas

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \neq 0.$$

Ponadto $\deg f' = n-1$, więc $f \nmid f'$. Ponieważ f jest nierozkładalny, więc $\text{NWD}(f, f') \sim 1$ i wobec udowodnionego powyżej wniosku każdy pierwiastek f w dowolnym ciele jest jednokrotny. □