PIERŚCIEŃ WIELOMIANÓW

Piotr M. Hajac
Uniwersytet Warszawski

Wykład 6, 6.11.2013

Typeset by Jakub Szczepanik.

Plan

1. Co to są wielomiany i jak się je mnoży?
2. Co to jest stopień wielomianu i jak go używać?
3. Jak dzielić wielomian przez wielomian?
4. Czym się różnią wielomiany od funkcji wielomianowych?
5. Jak faktoryzować wielomian na prostsze wielomiany?

Wielomiany

Definition

Pierścieniem wielomianowym nad pierścieniem R nazywamy pierścień monoidalny $R[\mathbb{N}]$, gdzie $\mathbb{N}$ jest monoidem liczb naturalnych ze względu na dodawanie. Elementy pierścienia wielomianów nazywamy wielomianami.

Kluczowym wielomianem jest $x \in R[\mathbb{N}]$ zdefiniowany wzorem

$$\boxed{x(m) := \begin{cases} 1 & \text{dla } m = 1 \\ 0 & \text{dla } m \neq 1 \end{cases}}.$$

Obliczmy $x^n := (\underbrace{x * \ldots * x}_{n\text{-razy}})$:

$$(\underbrace{x * \ldots * x}_{n\text{-razy}})(m) = \sum_{\substack{m_1, \ldots, m_n \in \mathbb{N}, \\ m_1 + \ldots + m_n = m}} x(m_1) \ldots x(m_n) = \begin{cases} 1 & \text{dla } m = n \\ 0 & \text{dla } m \neq n \end{cases}.$$

Ogólna postać wielomianu

Naturalne jest oznaczenie przez x^0 elementu neutralnego ze względu na splatanie, bo wtedy

$$x^0(m) = \begin{cases} 1 & \text{dla } m = 0 \\ 0 & \text{dla } m \neq 0 \end{cases}.$$

Widać że $\forall\, \alpha \in R[\mathbb{N}]$:

$$\boxed{\alpha = \sum_{k=0}^{n} \alpha(k) x^k}, \quad \text{gdzie } \; (r\beta)(m) := r\beta(m).$$

Istotnie, $\left(\sum_{k=0}^{n} \alpha(k)x^k\right)(m) = \sum_{k=0}^{n} \alpha(k)x^k(m) = \alpha(m)$.
Pierścień R jest podpierścieniem $R[\mathbb{N}]$ przez włożenie

$$R \ni r \longmapsto rx^0 \in R[\mathbb{N}].$$

Element neutralny x^0 zazwyczaj oznaczamy przez 1, a R utożsamiamy z jego obrazem w $R[\mathbb{N}]$.

Mnożenie wielomianów

Dwa dowolne wielomiany możemy wymnożyć w następująco:

$$\begin{aligned}\left(\sum_{k=0}^{m} r_k x^k\right) * \left(\sum_{l=0}^{n} s_l x^l\right) &= \sum_{k=0}^{m}\sum_{l=0}^{n} \left(r_k x^k\right) * \left(s_l x^l\right) \\ &= \sum_{k=0}^{m}\sum_{l=0}^{n} r_k s_l (x^k * x^l) \\ &= \sum_{k=0}^{m}\sum_{l=0}^{n} r_k s_l x^{k+l} \\ &= \sum_{N=0}^{m+n} \left(\sum_{k=0}^{N} r_k s_{N-k}\right) x^N.\end{aligned}$$

Dla $N = m + n$ suma $\sum_{k=0}^{N} r_k s_{N-k}$ ma tylko jeden element, bo tylko dla $k = m$ indeks przy r jest $\leqslant m$ i indeks przy s jest $\leqslant n$. Zatem współczynnik przy najwyższej potędze x to $r_m s_n$.

Stopień wielomianu

Definition

Stopniem wielomianu nazywamy odwzorowanie

$$R[\mathbb{N}] \setminus \{0\} \ni \sum_{k\in\mathbb{N}} r_k x^k \xrightarrow{\deg} \max\{k \in \mathbb{N} \mid r_k \neq 0\} \in \mathbb{N}.$$

Jeśli R nie ma dzielników zera, tzn. $xy = 0 \Rightarrow (x = 0 \text{ lub } y = 0)$, to stopień wielomianu zadaje homomorfizm monoidów: $\deg(1) = 0$ oraz

$$\forall\, \alpha, \beta \in R[\mathbb{N}] \setminus \{0\} : \quad \boxed{\deg(\alpha * \beta) = \deg \alpha + \deg \beta}\,.$$

Istotnie,

$$\deg\left(\left(\sum_{k=0}^{m} r_k x^k\right) * \left(\sum_{l=0}^{n} s_l x^l\right)\right) = \deg\left(\sum_{N=0}^{m+n}\left(\sum_{k=0}^{N} r_k s_{N-k}\right) x^N\right)$$
$$= m + n = \deg\left(\sum_{k=0}^{m} r_k x^k\right) + \deg\left(\sum_{l=0}^{n} s_l x^l\right).$$

Dzielenie wielomianów

Theorem (o dzieleniu wielomianów)

Niech R będzie pierścieniem bez dzielników zera, $\beta \in R[\mathbb{N}] \setminus \{0\}$. Załóżmy że $\exists\, r \in R : \beta\,(\deg(\beta))\, r = 1 = r\beta\,(\deg(\beta))$. Wtedy

$$\forall\, \alpha \in R[\mathbb{N}]\ \exists!\ (\gamma, \delta) \in R[\mathbb{N}]^2 :$$

$$\boxed{\alpha = \beta * \gamma + \delta}\ \textit{i}\ \Big(\delta = 0\ \textit{lub}\ \deg(\delta) < \deg(\beta)\Big).$$

Dowód: Zauważmy najpierw że, dzięki brakowi dzielników zera, jeżeli $\gamma \neq 0$, to $\beta * \gamma \neq 0$ oraz

$$\deg(\beta * \gamma) = \deg(\beta) + \deg(\gamma) \geqslant \deg(\beta) > \deg(\delta).$$

Stąd $\beta * \gamma + \delta \neq 0$ oraz $\deg(\beta * \gamma + \delta) = \deg(\beta) + \deg(\gamma)$. Zatem, jeżeli $\alpha = 0$, jedynym rozwiązaniem równania $\alpha = \beta * \gamma + \delta$ jest $\gamma = 0$, $\delta = 0$. Podobnie, jeżeli $\deg(\beta) > \deg(\alpha)$, to jedynym rozwiązaniem równania $\alpha = \beta * \gamma + \delta$ jest $\gamma = 0$, $\delta = \alpha$. Załóżmy teraz że $\alpha \neq 0$ i $\deg(\alpha) \geqslant \deg(\beta)$. Niech

$$\alpha_1 := \alpha - \beta * \Big(\beta(\deg(\beta))^{-1}\alpha(\deg(\alpha))x^{\deg(\alpha)-\deg(\beta)}\Big).$$

Ewaluacja wielomianu

Wtedy $\alpha = \beta * \left(\beta(\deg(\beta))^{-1}\alpha(\deg(\alpha))x^{\deg(\alpha)-\deg(\beta)}\right) + \alpha_1$ oraz $\left(\deg(\alpha_1) < \deg(\alpha) \text{ lub } \alpha_1 = 0\right)$. Po skończonej ilości iteracji tej procedury otrzymamy

$$\alpha_k = \beta * \left(\beta(\deg(\beta))^{-1}\alpha_k(\deg(\alpha_k))x^{\deg(\alpha_k)-\deg(\beta)}\right) + \alpha_{k+1},$$

$\deg(\beta) \leqslant \deg(\alpha_k)$ oraz $\left(\deg(\alpha_{k+1}) < \deg(\beta) \text{ lub } \alpha_{k+1} = 0\right)$. Podstawiając do wzoru na α wszystkie pozostałe wzory otrzymujemy $\alpha = \beta * \gamma + \alpha_{k+1}$. Udowadnia to istnienie rozwiązania. Jedyność wynika z braku dzielników zera. Istotnie, niech $\beta * \gamma + \delta = \beta * \gamma' + \delta'$. Wtedy $\beta * (\gamma - \gamma') = \delta' - \delta$. Zatem, jeżeli $\gamma \neq \gamma'$, to

$$\deg(\beta) \leqslant \deg(\beta) + \deg(\gamma - \gamma') = \deg(\delta' - \delta),$$

co nie jest możliwe. Dlatego $\gamma = \gamma'$, skąd $\delta = \delta'$. $\square$

Ewaluacją w $r \in R$ nazywamy odwzorowanie

$$R[\mathbb{N}] \ni \sum_{k=0}^{n} r_k x^k \overset{\mathrm{ev}_r}{\longmapsto} \mathrm{ev}_r\left(\sum_{k=0}^{n} r_k x^k\right) := \sum_{k=0}^{n} r_k r^k \in R.$$

Jeśli R jest przemienny, to ev_r jest homomorfizmem pierścieni.

Funkcje wielomianowe

Definition

Funkcją wielomianową f_α wielomianu $\alpha \in R[\mathbb{N}]$ nazywamy odwzorowanie $R \ni r \mapsto \boxed{f_\alpha(r) := \mathrm{ev}_r(\alpha)} \in R$.

Definition

Pierścieniem całkowitym (dziedziną całkowitą) nazywamy przemienny pierścień bez dzielników zera.

Theorem

Jeśli R jest nieskończonym pierścieniem całkowitym, to odwzorowanie $R[\mathbb{N}] \ni \alpha \mapsto f_\alpha \in \mathrm{Map}(R, R)$ jest injektywnym homomorfizmem pierścieni.

1. Pierścień $R[\mathbb{N}]$ jest całkowity $\Leftrightarrow$ R jest całkowity.
2. Jeśli R jest przemienny, to $R[\mathbb{N}] \ni \alpha \mapsto f_\alpha \in \mathrm{Map}(R, R)$ jest homomorfizmem pierścieni.
3. Jeśli R jest niezerowym skończonym pierścieniem, to $R[\mathbb{N}] \ni \alpha \mapsto f_\alpha \in \mathrm{Map}(R, R)$ nie jest injekcją, bo $R[\mathbb{N}]$ jest zbiorem nieskończonym a $\mathrm{Map}(R, R)$ skończonym.

Pierwiastki i faktoryzacja

Definition

Pierwiastkiem $\alpha \in R[\mathbb{N}]$ nazywamy $r \in R \Leftrightarrow f_\alpha(r) = 0$.

Theorem

Dla dowolnego pierścienia R, jeśli $r \in R$ jest pierwiastkiem $\alpha \in R[\mathbb{N}]$, to $\exists\, \beta \in R[\mathbb{N}] : \boxed{\alpha = \beta * (x - r)}$.

Dowód: Niech $\alpha =: \sum_{m=0}^{n} \alpha_m x^m$. Zauważmy że

$$\forall\, m \in \mathbb{N} \setminus \{0, 1\} : x^m - r^m = \left(\sum_{k=0}^{m-1} r^k x^{m-1-k} \right) * (x - r).$$

Zatem $\alpha = \alpha - f_\alpha(r) = \sum_{m=0}^{n} \alpha_m (x^m - r^m) = \beta * (x - r)$. □

Corollary

Jeśli R jest pierścieniem całkowitym i $\alpha \in R[\mathbb{N}] \setminus \{0\}$, to α może mieć co najwyżej $\deg(\alpha)$ różnych pierwiastków.

Dowód: Niech $r_1, ..., r_n$ będą różnymi pierwiastkami α. Całkowitość R implikuje faktoryzację $\alpha = \beta * (x - r_1) * ... * (x - r_n)$. Teraz ze wzoru $\deg(\beta * \gamma) = \deg(\beta) + \deg(\gamma)$ mamy $n \leqslant \deg(\alpha)$. □