PIERŚCIEŃ WIELOMIANÓW

(1) Czym się różnią wielomiany od funkcji wielomianowych?

(2) Co to jest stopień wielomianu i jak go wyznaczać?

(3) Jak przy pomocy dzielenia zrozumieć strukturę wielomianu?

(4) Co to są liczby algebraiczne? Liczby które nie są algebraiczne nazywamy przestępnymi. Przykładem liczb przestępnych nad $\mathbb{Q}$ są e i π.

Podstruktury algebraiczne: Niech G będzie półgrupą z działaniem $G \times G \xrightarrow{\circ} G$. Podzbiór $H \subseteq G$ nazywamy podpółgrupą $\Leftrightarrow$ $\circ(H \times H) \subseteq H$ i $H \neq \emptyset$. Jeśli G jest monoidem to podzbiór $H \subseteq G$ nazywamy podmonoidem $\Leftrightarrow$ jest podpółgrupą i $e \in H$. Jeśli G jest grupą, to $H \subseteq G$ nazywamy podgrupą $\Leftrightarrow$ jest podpółgrupą i $x \in H \Rightarrow x^{-1} \in H$. Niech R będzie pierścieniem. Podzbiór $S \subseteq R$ nazywamy podpierścieniem $\Leftrightarrow$ jest podgrupą ze względu na $+$ i podmonoidem ze względu na $\cdot$.

Niech L będzie ciałem. Podzbiór $K \subseteq L$ nazywamy podciałem $\Leftrightarrow$ K jest podpierścieniem L oraz $K \setminus \{0\}$ jest podgrupą $L \setminus \{0\}$.

Pierścień monoidalny: Niech R będzie dowolnym pierścieniem a M dowolnym monoidem. Zbiór

$$R[M] := \{\alpha \in Map(M,R) \mid \alpha(m) \neq 0 \text{ tylko dla skończonej ilości } m \in M\}$$

wyposażony w dodawanie punktowe i mnożenie splotowe $*$ dane wzorem

$$(\alpha * \beta)(m) := \sum_{\substack{(k,l) \in M^2 \\ kl = m}} \alpha(k)\beta(l)$$

jest pierścieniem nazywanym pierścieniem monoidalnym.

Jeśli M jest grupą, to $R[M]$ nazywamy pierścieniem grupowym.

Pierścieniem wielomianowym nad pierścieniem R nazywamy pierścień monoidalny $R[\mathbb{N}]$, gdzie $\mathbb{N}$ jest monoidem liczb naturalnych ze względu na dodawanie. Kluczowy jest $x \in R[\mathbb{N}]$, $x(n) := \begin{cases} 1 & \text{dla } n=1 \\ 0 & \text{dla } n \neq 1 \end{cases}$. Sprawdzamy że $(x*x)(m) = \begin{cases} 1 & \text{dla } m=2 \\ 0 & \text{dla } m \neq 2 \end{cases}$. Podobnie sprawdzamy

że $\underbrace{(X * \dots * X)}_{n\text{-razy}}(m) = \begin{cases} 1 & \text{dla } m = n \\ 0 & \text{dla } m \neq n \end{cases}$. Oznaczmy

$\underbrace{X * \dots * X}_{n\text{-razy}} =: X^n$. 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 $\forall \alpha \in R[IN]\ \exists!\ (r_0, \dots, r_n) \in R^{n+1}$:

$\alpha = \sum_{k=0}^{n} r_k X^k$, gdzie $(r\beta)(m) := r\beta(m)$.

Widać też że $\left(\sum_{k=0}^{m} r_k X^k\right) * \left(\sum_{l=0}^{n} s_l X^l\right) =$

$$= \sum_{k=0}^{m} \sum_{l=0}^{n} (r_k X^k) * (s_l X^l) = \sum_{k=0}^{m} \sum_{l=0}^{n} r_k s_l X^{k+l} =$$

$$= \sum_{N=0}^{m+n} \left(\sum_{k=0}^{N} r_k s_{N-k} \right) X^N.$$ R jest podpierścieniem $R[IN]$ przez utożsamienie $R \ni r \mapsto r X^0 \in R[IN]$

Element neutralny X^0 zazwyczaj oznaczamy przez 1, a R utożsamiamy z jego obrazem w $R[IN]$. Elementy pierścienia $R[IN]$ nazywamy wielomianami nad R.

Stopniem wielomianu $\sum_{k\in\mathbb{N}} r_k x^k \neq 0$ nazywamy $\max\{k\in\mathbb{N} \mid r_k \neq 0\}$. Jeśli R nie ma dzielników zera (x jest dzielnikiem zera $\iff x\neq 0$ i $\exists y\neq 0 : xy=0$ lub $yx=0$), to stopień wielomianu zadaje homomorfizm monoidów $R[\mathbb{N}]\setminus\{0\} \xrightarrow{\deg} \mathbb{N}$,

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

Ewaluacją wielomianu $\sum_{k=0}^{n} r_k x^k$ **w** r nazywamy $\sum_{k=0}^{n} r_k r^k \in R$. Jeśli R jest przemienny, to ewaluacja zadaje homomorfizm pierścieni: $\forall r\in R$:

$$R[\mathbb{N}] \ni \sum_{k=0}^{n} r_k x^k \xmapsto{ev_r} ev_r\left(\sum_{k=0}^{n} r_k x^k\right) := \sum_{k=0}^{n} r_k r^k \in R.$$

Pierścieniem całkowitym nazywamy przemienny pierścień bez dzielników zera.

Wniosek: $R[\mathbb{N}]$ jest pierścieniem całkowitym $\iff$ R jest pierścieniem całkowitym.

Funkcją wielomianową f_α o współczynnikach $\alpha \in R[\mathbb{N}]$ nazywamy odwzorowanie

$$R \ni r \longmapsto f_\alpha(r) := ev_r(\alpha) \in R,$$

$$R \ni r \longmapsto \sum_{k=0}^{n} r_k r^k \in R.$$ Jeśli R jest przemienny, to $R[\mathbb{N}] \ni \alpha \mapsto f_\alpha \in Map(R,R)$ jest homomorfizmem pierścieni. ($Map(R,R)$ jest tu pierścieniem z działaniami punktowymi.) Jeśli zaś R jest niezerowym skończonym pierścieniem, to odwzorowanie $R[\mathbb{N}] \ni \alpha \mapsto f_\alpha \in Map(R,R)$ nie może być injekcją bo wtedy $R[\mathbb{N}]$ jest zbiorem nieskończonym, a $Map(R,R)$ zbiorem skończonym.

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

Uwaga: W ten sposób utożsamia się pierścień wielomianów z podpierścieniem funkcji wielomianowych.

Twierdzenie o dzieleniu wielomianów:

Niech R będzie pierścieniem całkowitym.

$$\left(\alpha, \beta \in R[\mathbb{N}] \setminus \{0\} \;\wedge\; \exists\, \beta(\deg(\beta))^{-1}\right) \Rightarrow$$

$$\exists!\, (\gamma, \delta) \in R[\mathbb{N}]^2 : \boxed{\alpha = \beta * \gamma + \delta} \;\wedge\; (\delta = 0 \text{ lub } \deg(\delta) < \deg(\beta)).$$

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

Twierdzenie: Dla dowolnego pierścienia R, jeśli $\alpha \in R[\mathbb{N}]$ i $\boxed{f_\alpha(r) = 0}$, to $\exists \beta \in R[\mathbb{N}] : \boxed{\alpha = \beta * (x - r)}$.

Dowód: Niech $\alpha =: \sum_{k=0}^{N} \alpha_k x^k$. Zauważmy że

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

Zatem $\alpha = \alpha - f_\alpha(r) = \sum_{k=0}^{N} \alpha_k (x^k - r^k) = \beta * (x - r)$. ∎

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

Dowód: Połączenie poprzedniego twierdzenia ze wzorem $\deg(\alpha * \beta) = \deg(\alpha) + \deg(\beta)$. ∎

Niech ciało K będzie podciałem ciała L. Liczba $r \in L$ jest **algebraiczna** nad $K \Leftrightarrow \exists \alpha \in K[\mathbb{N}] : f_\alpha(r) = 0$. Ciało K jest **algebraicznie domknięte** $\Leftrightarrow \forall \alpha \in K[\mathbb{N}]\; \exists r \in K : f_\alpha(r) = 0$.