CIAŁO FUNKCJI WYMIERNYCH

Ciało ułamków pierścienia całkowitego:

Niech R będzie pierścieniem całkowitym. Na zbiorze $R \times (R \setminus \{0\})$ wprowadźmy relację równoważności:

$$\mathcal{F} := \{((a,b),(c,d)) \in (R \times (R \setminus \{0\}))^2 \mid ad = bc\}.$$

Zwrotność i symetryczność tej relacji są oczywiste. Dla sprawdzenia przechodniości, załóżmy że $ad = bc$ i $cy = dx$. Mnożąc drugie równanie przez b otrzymujemy $cyb = dxb$. Podstawiając bc z pierwszego równania dostajemy $day = dxb$. Stąd $d(ay - xb) = 0$. Ale $d \neq 0$ i w R nie ma dzielników zera. Zatem $ay = bx$, co udowadnia przechodniość.

$F_R := (R \times R \setminus \{0\}) / \mathcal{F}$ jest przemiennym pierścieniem ze względu na działania dane wzorami: $[(a,b)] \cdot [(c,d)] = [(ac, bd)]$, $[(a,b)] + [(c,d)] = [(ad + bc, bd)]$. Elementem

neutralnym ze względu na mnożenie jest $[(1,1)]$ a ze względu na dodawanie $[(0,1)]$. Dalej, $-[(a,b)] = [(-a,b)]$. Mamy $[(a,b)] = [(0,1)] \iff a = 0$. Zatem $\boxed{\forall [(a,b)] \neq 0 \; \exists [(a,b)]^{-1} = [(b,a)]}$. Dlatego F_R jest ciałem. Nazywamy je ciałem ułamków.

Odwzorowanie $R \ni r \mapsto [(r,1)] \in F_R$ jest injektywnym homomorfizmem pierścieni. Dla $R = \mathbb{Z}$ mamy $F_{\mathbb{Z}} =: \mathbb{Q}$.

Ciałem funkcji wymiernym nad nieskończonym pierścieniem całkowitym R nazywamy ciało ułamków pierścienia całkowitego wielomianów $F_{R[X]}$. Elementy $F_{R[X]}$ nazywamy funkcjami wymiernymi nad R. Zauważmy że dowolny injektywny homomorfizm $R \xhookrightarrow{f} S$ pomiędzy pierścieniami całkowitymi indukuje (injektywny) homomorfizm pomiędzy ciałami ułamków zadany wzorem $F_R \ni [(a,b)] \longmapsto [(f(a), f(b))] \in F_S$. Zatem dla nieskończonego pierścienia całkowitego R, odwzorowanie $F_{R[X]} \ni \frac{\alpha}{\beta} := [(\alpha,\beta)] \mapsto \frac{f_\alpha}{f_\beta} \in F_{t_{R[X]}}$ jest izomorfizmem ciał. Ułamki $\frac{f_\alpha}{f_\beta}$ nie są elemen-

tami $Map(R,R)$, ale jeśli $R=K$ jest ciałem, to mamy

$$K\setminus\{\text{wszystkie pierwiastki } \beta\} \ni r \longmapsto \frac{f_\alpha(r)}{f_\beta(r)} \in K$$

Stwierdzenie: Niech K będzie nieskończonym ciałem (o dowolnej charakterystyce). Wtedy $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'} \in F_{K[X]}$

$\Leftrightarrow \forall r \in K\setminus\{\text{wszystkie pierwiastki } \beta, \beta'\}: \frac{f_\alpha(r)}{f_\beta(r)} = \frac{f_{\alpha'}(r)}{f_{\beta'}(r)}$.

Dowód: Zakładając prawą stronę otrzymujemy wielomian $\alpha * \beta' - \beta * \alpha'$ o nieskończonej ilości różnych pierwiastków. Z twierdzenia o stopniu wielomianu musi być on wielomianem zerowym. Stąd $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'}$. Implikacja odwrotna jest trywialna. ∎

Dlatego ułamki $\frac{\alpha}{\beta}$ utożsamiamy z odpowiednimi odwzorowaniami i nazywamy funkcjami wymiernymi.

Rozkład funkcji wymiernych na ułamki proste:

Mówimy że $\beta \in R[X]$ dzieli $\alpha \in R[X] \Leftrightarrow$ $\exists\, \gamma \in R[X]: \alpha = \beta * \gamma$. Największym wspólnym dzielnikiem $\alpha_1 \in R[X]$ i $\alpha_2 \in R[X]\setminus\{0\}$ nazywamy $gcd(\alpha_1, \alpha_2) \in R[X] \Leftrightarrow$

① $\gcd(\alpha_1, \alpha_2)$ dzieli α_1 i α_2,

② β dzieli α_1 i $\alpha_2 \Rightarrow \beta$ dzieli $\gcd(\alpha_1, \alpha_2)$,

③ $\gcd(\alpha_1, \alpha_2)(\deg(\gcd(\alpha_1, \alpha_2))) = 1$.

Twierdzenie (Algorytm Euklidesa): Niech K będzie (nieskończonym) ciałem. Wtedy

$$\forall \alpha_1 \in K[\mathbb{N}] \setminus \{0\}, \alpha_2 \in K[\mathbb{N}] \; \exists! \; \gcd(\alpha_1, \alpha_2) \in K[\mathbb{N}]$$

Dowód: Jeśli $\alpha_2 = 0$, to $\gcd(\alpha_1, \alpha_2) = \alpha_1 (\deg(\alpha))^{-1} \alpha_1$.

Jeśli $\deg \alpha_2 = 0$ lub $\deg \alpha_1 = 0$, to $\gcd(\alpha_1, \alpha_2) = 1$. Załóżmy więc że $\deg(\alpha_1) \geq \deg(\alpha_2) > 0$. Korzystając z twierdzenia o dzieleniu wielomianów i odwracalności elementów z $K \setminus \{0\}$, dostajemy $\alpha_1 = \beta_2 * \alpha_2 + \alpha_3$. Jeśli $\alpha_3 = 0$, to $\gcd(\alpha_1, \alpha_2) = \alpha_2 (\deg(\alpha_2))^{-1} \alpha_2$.

Jeśli $\alpha_3 \neq 0$, to $\deg(\alpha_3) < \deg(\alpha_2)$. Teraz dzielimy α_2 przez α_3 otrzymując $\alpha_2 = \beta_3 * \alpha_3 + \alpha_4$.

Procedurę kontynuujemy aż do momentu gdy $\alpha_4 = \beta_{k+1} * \alpha_{k+1}$. (Procedura jest skończona bo $\deg(\alpha_2) < \omega$ i $0 \leq \deg(\alpha_{k+1}) < \deg(\alpha_k)$.)

Podstawiając wzory kolejno do siebie otrzymujemy $\alpha_1 = \beta * \alpha_{k+1}$ i $\alpha_2 = \tilde{\beta} * \alpha_{k+1}$. Jeśli γ

dzieli równocześnie α_1 i α_2, to dzieli również α_3. Jeśli dzieli α_2 i α_3, to dzieli α_4, itd. Zatem γ dzieli α_{n+1}. Stąd $\gcd(\alpha_1, \alpha_2) = \alpha_{n+1}(\deg(\alpha_{n+1}))^{-1}\alpha_{n+1}$. Załóżmy teraz że mamy dwa największe wspólne podzielniki γ i γ'. Wtedy $\gamma = \beta' * \gamma'$ i $\gamma' = \beta * \gamma$. Zatem $\gamma = \beta' * \beta * \gamma$, skąd wynika że $\deg(\beta) = 0$. Teraz z równości $\gamma' = \beta * \gamma$ wynika że $1 = \gamma'(\deg(\gamma')) =$

$= \beta\,\gamma(\deg(\gamma)) = \beta \cdot 1 = \beta$. Zatem $\gamma = \gamma'$. ∎

Lemat: $\left(\alpha_1 \in K[\mathbb{N}] \setminus \{0\} \text{ i } \alpha_2 \in K[\mathbb{N}]\right) \Rightarrow$

$\exists\, \beta_1, \beta_2 \in K[\mathbb{N}]: \boxed{\beta_1 * \alpha_1 + \beta_2 * \alpha_2 = \gcd(\alpha_1, \alpha_2)}$.

Lemat: $\left(\mu \in K[\mathbb{N}] \text{ i } \deg(\mu) > 0\right) \Rightarrow$

$\forall\, \varphi \in K[\mathbb{N}]\ \exists\, q \in \mathbb{N} \text{ i } \gamma_j \in K[\mathbb{N}]$, $j \in \{0, \dots, q\}$: $\boxed{\varphi = \sum_{j=0}^{q} \gamma_j * \mu^j}$ i $\forall_{j \in \{0,\dots,q\}}$:

$\gamma_j = 0$ lub $\deg(\gamma_j) < \deg(\mu)$.

Dowód: Zdefiniuj $q := \max\{n \in \mathbb{N} \mid \deg(\mu^n) \leq \deg\varphi\}$.

Wtedy $\varphi = \gamma_q * \mu^q + \varphi_1$, $\varphi_1 = 0$ lub $\deg(\varphi_1) < \deg(\mu^q)$, oraz $\boxed{\varphi_1}$

$\deg(r_q) < \deg(r)$ (bo inaczej $\deg(\varphi) \geq \deg(\mu^{q+1})$, co przeczy definicji q). Jeśli $\varphi_1 = 0$, lemat jest udowodniony. Jeśli $\varphi_1 \neq 0$, to $\max\{h \in \mathbb{N} : \deg(\mu^h) \leq \deg(\varphi_1)\} =: q_1 \leq q-1$. Lemat wynika z iteracji procedury która jest skończona bo $0 \leq \deg(\varphi_{k+1}) < \deg(\mu^{q_k}) \leq \deg(\varphi_k)$. ■

Wielomian $w \in K[\mathbb{N}]$ nazywamy <u>pierwszym</u> $\Leftrightarrow$ (① $\deg(w) > 0$ i ② $w = \beta * \gamma \Rightarrow \deg(\beta)\deg(\gamma) = 0$).

<u>Lemat</u>: $\forall \alpha \in K[\mathbb{N}]$ $\exists$ nieproporcjonalne wielomiany pierwsze $w_1, \dots, w_n$, $k_1, \dots, k_n \in \mathbb{N}$: $\alpha = w_1^{k_1} * \dots * w_n^{k_n}$.

Niech K będzie nieskończonym ciałem. <u>Ułamkiem prostym</u> nazywamy funkcję wymierną postaci $\frac{\alpha}{w^n}$, gdzie w jest wielomianem pierwszym, $\deg(\alpha) < \deg(w)$, $n \in \mathbb{N}$.

<u>Twierdzenie o rozkładzie na ułamki proste:</u>

$\forall \frac{\alpha}{\beta} \in F_{K[\mathbb{N}]}$ $\exists$ nieproporcjonalne wielomiany pierwsze $w_1, \dots, w_n$, $k_1, \dots, k_n \in \mathbb{N}$:

$$\frac{\alpha}{\beta} = \sum_{i=1}^{n} \sum_{j_i=1}^{k_i} \frac{\eta_{j_i}}{w_i^{j_i}},$$

gdzie $\forall j_i$: $\eta_{j_i} = 0$ lub $\deg(\eta_{j_i}) < \deg(w_i)$.

Dowód: Niech $\beta = w_1^{k_1} * \dots * w_n^{k_n}$. Potem indukcja po n. Dla $n=1$ mamy twierdzenie z q-lematu. Krok indukcyjny z $\gcd(w_1^{k_1} \dots w_{n-1}^{k_{n-1}}, w_n^{k_n}) = 1$. ■