

CIAŁO FUNKCJI WYMIERNYCH

Piotr M. Hajac
Uniwersytet Warszawski

Wykład 7, 13.11.2013

Typeset by Jakub Szczepanik.

Ułamki pierścienia całkowitego

Cel: Wprowadzenie pojęcia funkcji wymiernej i udowodnienie istnienia jej rozkładu na ułamki proste.

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

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

Zaiste, zwrotność i symetryczność tej relacji są oczywiste. Dla sprawdzenia przechodniości, załóżmy że $ad = bc$ i $cy = dx$.

Mnożąc drugie równanie przez b otrzymujemy $c y b = d x b$.

Podstawiając bc z pierwszego równania dostajemy $d a y = d x b$. Stąd $d(ay - xb) = 0$. Ale $d \neq 0$ i w R nie ma dzielników zera. Zatem $ay = bx$, co udowadnia przechodniość.

Elementy zbioru $F_R := (R \times R \setminus \{0\})/\mathcal{F}$ nazywamy **ułamkami** pierścienia R .

Ciało ułamków pierścienia całkowitego

Twierdzenie

Niech R będzie pierścieniem całkowitym. Następujące wzory definiują działania na F_R :

- ① $[(a, b)] + [(c, d)] = [(ad + bc, bd)],$
- ② $[(a, b)] \cdot [(c, d)] = [(ac, bd)].$

Elementami neutralnymi dla tych działań są odpowiednio $[(0, 1)]$ i $[(1, 1)]$. Ze względu na te działania i elementy neutralne, F_R jest ciałem. (Nazywamy je **ciałem ułamków**.)

Dowód: Sprawdzenie że powyższe wzory definiują łączne i przemienne działania na F_R z prawami rozdzielności i odpowiednimi elementami neutralnymi jest proste. Ze względu na dodawanie F_R jest grupą, bo dla dowolnego $[(a, b)]$ mamy $-[(a, b)] = [(-a, b)]$. Dalej, $[(a, b)] = [(0, 1)] \Leftrightarrow a = 0$ implikuje że $[(a, b)] \neq 0 \Rightarrow [(a, b)]^{-1} := [(b, a)] \in F_R$. To kończy dowód że F_R jest ciałem, bo $[(b, a)][(a, b)] = [(ba, ab)] = [(1, 1)]$. $\square$

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

Ciało funkcji wymiernych

Definicja

Ciałem ułamków wymiernych nad pierścieniem całkowitym R nazywamy ciało ułamków $F_{R[\mathbb{N}]}$ pierścienia całkowitego wielomianów $R[\mathbb{N}]$. Elementy $F_{R[\mathbb{N}]}$ nazywamy **ułamkami wymiernymi** nad R .

Zauważmy że dowolny injektywny homomorfizm $R \xrightarrow{h} S$ pomiędzy pierścieniami całkowitymi indukuje injektywny homomorfizm pomiędzy ciałami ułamków: $F_R \ni [(a, b)] \mapsto [(h(a), h(b))] \in F_S$.
Zatem dla nieskończonego pierścienia całkowitego R , odwzorowanie

$$F_{R[\mathbb{N}]} \ni \frac{\alpha}{\beta} := [(\alpha, \beta)] \longmapsto \frac{f_\alpha}{f_\beta} := [(f_\alpha, f_\beta)] \in F_{f(R[\mathbb{N}])}$$

jest izomorfizmem ciał.

Definicja

Niech R będzie nieskończonym pierścieniem całkowitym. Ciało $F_{f(R[\mathbb{N}])}$ nazywamy **ciałem funkcji wymiernych**, a jego elementy **funkcjami wymiernymi**.

Funkcje wymierne jako funkcje

Ułamki $\frac{f_\alpha}{f_\beta}$ nie są elementami $\text{Map}(R, R)$, ale jeśli $R = K$ jest ciałem, to z $\frac{f_\alpha}{f_\beta}$ możemy stworzyć funkcję:

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

Twierdzenie

Niech K będzie nieskończonym ciałem. Wówczas $\frac{\alpha}{\beta} = \frac{\alpha'}{\beta'} \in F_{K[\mathbb{N}]}$ wtedy i tylko wtedy gdy $\forall r \in K \setminus \{\text{wszystkie pierwiastki } \beta \text{ i } \beta'\} :$
$$\frac{f_\alpha(r)}{f_\beta(r)} = \frac{f_{\alpha'}(r)}{f_{\beta'}(r)} .$$

Dowód: Zakładając drugą równość 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. $\square$

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

Największy wspólny dzielnik

Definicje

Niech K będzie ciałem. Mówimy że

$$\beta \in K[\mathbb{N}] \text{ dzieli } \alpha \in K[\mathbb{N}] \iff \exists \gamma \in K[\mathbb{N}] : \alpha = \beta * \gamma.$$

Największym wspólnym dzielnikiem $\alpha_1 \in K[\mathbb{N}]$ i $\alpha_2 \in K[\mathbb{N}] \setminus \{0\}$ nazywamy $\gcd(\alpha_1, \alpha_2) \in K[\mathbb{N}]$ wtedy i tylko wtedy gdy

- ❶ $\gcd(\alpha_1, \alpha_2)$ dzieli α_1 i α_2 ,
- ❷ β dzieli α_1 i $\alpha_2 \Rightarrow \beta$ dzieli $\gcd(\alpha_1, \alpha_2)$,
- ❸ $\gcd(\alpha_1, \alpha_2)(\deg(\gcd(\alpha_1, \alpha_2))) = 1$ (współczynnik przy najwyższej potędze w wielomianie $\gcd(\alpha_1, \alpha_2)$).

Twierdzenie (Algorytm Euklidesa)

Niech K będzie ciałem. Wtedy

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

Algorytm Euklidesa

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 $\deg(\alpha_1) \geq \deg(\alpha_2) \geq 1$. 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 $\alpha_n = \beta_{n+1} * \alpha_{n+1}$. (Procedura jest skończona bo $\deg(\alpha_2) < \infty$ i $0 \leq \deg(\alpha_{k+1}) < \deg(\alpha_k)$.) Podstawiając wzory kolejno do siebie otrzymujemy $\alpha_1 = \beta * \alpha_{n+1}$ i $\alpha_2 = \tilde{\beta} * \alpha_{n+1}$. Jeśli γ dzieli równocześnie α_1 i α_2 , to dzieli też α_3 . Jeśli γ dzieli równocześnie α_2 i α_3 , to dzieli też α_4 , itd. Zatem γ dzieli α_{n+1} . Stąd $\gcd(\alpha_1, \alpha_2) = \alpha_{n+1}(\deg(\alpha_{n+1}))^{-1}\alpha_{n+1}$.

Założmy teraz że mamy dwa największe wspólne dzielniki 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 $\gamma' = \beta * \gamma$, $\gamma(\deg(\gamma)) = 1$, $\gamma'(\deg(\gamma')) = 1$ wynika że $\beta = 1$. Zatem $\gamma = \gamma'$. □

Lematy o dzielnikach

Lemat

Niech K będzie ciałem. Jeżeli $\alpha_1 \in K[\mathbb{N}] \setminus \{0\}$ i $\alpha_2 \in K[\mathbb{N}]$, to
$$\exists \beta_1, \beta_2 \in K[\mathbb{N}] : \beta_1 * \alpha_1 + \beta_2 * \alpha_2 = \gcd(\alpha_1, \alpha_2).$$

Lemat

Niech K będzie ciałem. Jeżeli $\mu \in K[\mathbb{N}]$ i $\deg(\mu) > 0$, to
$$\forall \varphi \in K[\mathbb{N}] \exists q \in \mathbb{N}, \gamma_j \in K[\mathbb{N}], j \in \{0, \dots, q\} : \varphi = \sum_{j=0}^q \gamma_j * \mu^j,$$

gdzie $\forall j \in \{0, \dots, q\} : \gamma_j = 0$ lub $\deg(\gamma_j) < \deg(\mu)$.

Dowód: Dla $\varphi = 0$ lemat jest trywialny. Załóżmy więc że $\varphi \neq 0$, i zdefiniujmy $q := \max\{n \in \mathbb{N} \mid \deg(\mu^n) \leq \deg \varphi\}$. Wtedy $\varphi = \gamma_q * \mu^q + \varphi_1$, $\varphi_1 = 0$ lub $\deg(\varphi_1) < \deg(\mu^q)$, $\gamma_q \neq 0$. Mamy też $\deg(\gamma_q) < \deg(\mu)$, 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 niech $\max\{n \in \mathbb{N} \mid \deg(\mu^n) \leq \deg(\varphi_1)\} =: q_1 \leq q - 1$. Lemat wynika z iteracji procedury która jest skończona, bo
$$0 \leq \deg(\varphi_{k+1}) < \deg(\mu^{q_k}) \leq \deg(\varphi_k).$$



Wielomiany pierwsze i ułamki proste

Definicja

Niech R będzie pierścieniem. Wielomian $\omega \in R[\mathbb{N}]$ nazywamy **pierwszym (nieredukowalnym)** wtedy i tylko wtedy gdy

- 1 $\deg(\omega) > 0$,
- 2 $\omega = \beta * \gamma \Rightarrow \deg(\beta) \deg(\gamma) = 0$.

Lemat (o faktoryzacji na czynniki pierwsze)

Niech K będzie ciałem. Jeżeli $\beta \in K[\mathbb{N}] \setminus K$, $\beta(\deg(\beta)) = 1$, to istnieją nieproporcjonalne wielomiany pierwsze $\omega_1, \dots, \omega_n \in K[\mathbb{N}]$ oraz liczby $k_1, \dots, k_n \in \mathbb{N} \setminus \{0\}$ takie że

$$\beta = \omega_1^{k_1} * \dots * \omega_n^{k_n}.$$

Definicja

Niech K będzie nieskończonym ciałem. **Ułamkiem prostym** nazywamy element ciała ułamków wymiernych $F_{K[\mathbb{N}]}$ postaci $\frac{\alpha}{\omega^n}$, gdzie ω jest wielomianem pierwszym, $\deg(\alpha) < \deg(\omega)$, $n \in \mathbb{N} \setminus \{0\}$.

Rozkład na ułamki proste

Twierdzenie (o rozkładzie na ułamki proste)

Niech K będzie nieskończonym ciałem. Dla każdej funkcji wymiernej $\frac{f_\alpha}{f_\beta} \in F_f(K[\mathbb{N}])$, $\alpha, \beta \in K[\mathbb{N}] \setminus \{0\}$, $\deg(\alpha) < \deg(\beta)$, istnieją nieproporcjonalne wielomiany pierwsze $\omega_1, \dots, \omega_n \in K[\mathbb{N}]$, $k_1, \dots, k_n \in \mathbb{N}$:

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

gdzie $\forall j_i \in \{1, \dots, k_i\} : \eta_{j_i} = 0$ lub $\deg(\eta_{j_i}) < \deg(\omega_i)$.

Szkic dowodu: Twierdzenie udowadniamy w izomorficznym ciele ułamków wymiernych. Ponieważ $\frac{\alpha}{\beta} = \frac{\beta(\deg(\beta))^{-1}\alpha}{\beta(\deg(\beta))^{-1}\beta}$, bez straty ogólności możemy założyć że $\beta(\deg(\beta)) = 1$. Wtedy z lematu o faktoryzacji na wielomiany pierwsze mamy $\beta = \omega_1^{k_1} * \dots * \omega_n^{k_n}$, gdzie $\omega_1, \dots, \omega_n$ to nieproporcjonalne wielomiany pierwsze. Dla $n = 1$ twierdzenie wynika z drugiego lematu o dzielnikach. Potem indukcja po n . Krok indukcyjny z $\gcd(\omega_1^{k_1} \dots \omega_{n-1}^{k_{n-1}}, \omega_n^{k_n}) = 1$ i pierwszego lematu o dzielnikach.