

12. WYKŁAD 12: ROZSZERZENIE CIAŁA O PIERWIASTEK WIELOMIANU. CIAŁO ROZKŁADU WIELOMIANU. CIAŁO ALGEBRAICZNIE DOMKNIĘTE.

12.1. Rozszerzenie ciała o pierwiastek wielomianu. Ciało rozkładu wielomianu.

Twierdzenie 12.1 (Kroneckera). *Niech F będzie ciałem, niech $f \in F[x]$. Wówczas istnieje rozszerzenie L ciała F takie, w którym f ma pierwiastek.*

Dowód. Niech f_1 będzie czynnikiem nierozkładalnym wielomianu f . Wówczas $(f_1) \triangleleft F[x]$ jest ideałem maksymalnym w rodzinie ideałów głównych $F[x]$, a więc ideałem maksymalnym, ponieważ $F[x]$ jest pierścieniem ideałów głównych. Wobec tego pierścień ilorazowy $F[x]/(f_1)$ jest ciałem. Tym samym złożenie homomorfizmów kanonicznych $u : F \rightarrow F[x]/(f_1)$ dane wzorem

$$u(a) = a + (f_1)$$

jest zanurzeniem, jako nietrywialny homomorfizm ciał. Tym samym ciało $L = F[x]/(f_1)$ jest rozszerzeniem ciała F . Powiedzmy, że $f_1(x) = a_0 + a_1x + \dots + a_nx^n$ i niech $\alpha = x + (f_1) \in L$. Wówczas $f_1(\alpha) = a_0 + a_1(x + (f_1)) + \dots + a_n(x + (f_1))^n = f_1 + (f_1) = 0_L$. $\square$

Definicja 12.1. *Niech F będzie ciałem, niech $f_1 \in F[x]$. Rozszerzenie L ciała F nazywamy **rozszerzeniem o pierwiastek a wielomianu f** gdy $L = F(a)$ ¹⁷.*

Przykłady:

- (1) Rozważmy ciało $\mathbb{R}$ i wielomian $x^2 + 1 \in \mathbb{R}[x]$. Wówczas ciało $\mathbb{C}$ jest rozszerzeniem ciała $\mathbb{R}$ o pierwiastek i wielomianu $x^2 + 1$, $\mathbb{C} = \mathbb{R}(i)$.

Twierdzenie 12.2. *Niech F i L będą ciałami, niech $\phi : F \rightarrow L$ będzie izomorfizmem. Niech $\bar{\phi} : F[x] \rightarrow L[x]$ będzie izomorfizmem indukowanym przez ϕ . Niech $f \in F[x]$ będzie wielomianem nierozkładalnym, niech α będzie pierwiastkiem f , a β pierwiastkiem $\bar{\phi}(f)$. Wówczas $\bar{\phi}(f)$ jest wielomianem nierozkładalnym oraz istnieje izomorfizm $\psi : F(\alpha) \rightarrow L(\beta)$ taki, że $\psi|_F = \phi$ oraz $\psi(\alpha) = \beta$.*

Dowód. Bez trudu sprawdzamy, że $\bar{\phi}(f)$ jest wielomianem nierozkładalnym. Zdefiniujmy odwzorowanie $\phi_1 : F[x] \rightarrow F(\alpha)$ wzorem $\phi_1(g) = g(\alpha)$. Jak łatwo zauważyć, jest to homomorfizm. Ponadto $(f) \subset \ker \phi_1$ i ponieważ f jest nierozkładalny, więc (f) jest maksymalny i stąd $(f) = \ker \phi_1$. Wobec twierdzenia o izomorfizmie $F[x]/(f) \cong \text{Im} \phi_1$. Ponadto $F \subset \text{Im} \phi_1$ oraz $\alpha \in \text{Im} \phi_1$, więc $\text{Im} \phi_1 = F(\alpha)$. W szczególności udowodniliśmy, że istnieje izomorfizm $\psi_1 : F[x]/(f) \rightarrow F(\alpha)$.

Podobnie pokazujemy, że istnieje izomorfizm $\psi_2 : L[x]/(\bar{\phi}(f)) \rightarrow L(\beta)$, Zdefiniujmy ponadto odwzorowanie $\psi_0 : F[x]/(f) \rightarrow L[x]/(\bar{\phi}(f))$ wzorem

$$\psi_0(g + (f)) = \bar{\phi}(g) + (\bar{\phi}(f)).$$

Również bezpośrednio sprawdzamy, że ψ_0 jest izomorfizmem. Otrzymujemy następujący diagram:

$$\begin{array}{ccc} F[x]/(f) & \xrightarrow{\psi_0} & L[x]/(\bar{\phi}(f)) \\ \psi_1 \downarrow & & \downarrow \psi_2 \\ F(\alpha) & \xrightarrow{\psi} & L(\beta) \end{array}$$

w którym odwzorowanie $\psi : F(\alpha) \rightarrow L(\beta)$ dane jest wzorem $\psi = \psi_2 \circ \psi_0 \circ \psi_1^{-1}$. Wówczas ψ jest izomorfizmem, $\psi|_F = \phi$ oraz $\psi(\alpha) = \beta$. $\square$

¹⁷Przypomnijmy, że symbolem $F(a)$ oznaczamy najmniejsze ciało zawierające ciało F i element a .

Wniosek 12.1. Niech F będzie ciałem, niech $f \in F[x]$ i niech a będzie pierwiastkiem wielomianu f . Dowolne dwa rozszerzenia ciała F o pierwiastek a wielomianu f są izomorficzne.

Twierdzenie 12.3. Niech F będzie wielomianem, niech $f \in F[x]$. Wówczas istnieje rozszerzenie L ciała F takie, w którym f rozkłada się na czynniki liniowe.

Dowód. Niech $n = \deg f$. Dowód prowadzimy przez indukcję względem n . Gdy $n = 1$ nie ma czego dowodzić. Ustalmy zatem $n > 1$ i założmy, że twierdzenie jest prawdziwe dla wszystkich wielomianów stopnia k , gdzie $k < n$. Wobec twierdzenia Kroneckera istnieje rozszerzenie M ciała F , w którym f ma pierwiastek α . Wówczas $f(x) = (x - \alpha)f_1(x)$, dla pewnego $f_1 \in M[x]$. Ponadto $\deg f_1 < n$, więc istnieje rozszerzenie L ciała M , w którym f_1 rozkłada się na czynniki liniowe. Zatem $F \subset M \subset L$ i f rozkłada się w L na czynniki liniowe. $\square$

Definicja 12.2. Niech F będzie ciałem, niech $f \in F[x]$. Rozszerzenie L ciała F nazywamy **ciałem rozkładu wielomianu f** , gdy $L = F(a_1, \dots, a_n)$ oraz $f(x) = a(x - a_1)(x - a_2) \cdot \dots \cdot (x - a_n)$ jest rozkładem wielomianu f na czynniki liniowe.

Przykłady:

- (2) Rozważmy ciało $\mathbb{Q}$ i wielomian $x^2 - 5 \in \mathbb{Q}[x]$. Wówczas ciało $\mathbb{R}$ jest ciałem, w którym $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$ rozkłada się na czynniki liniowe oraz $\mathbb{Q}(\sqrt{5}, -\sqrt{5}) = \mathbb{Q}(\sqrt{5})$ jest ciałem rozkładu wielomianu $x^2 - 5$.

Twierdzenie 12.4. Niech F i L będą ciałami, niech $\phi : F \rightarrow L$ będzie izomorfizmem. Niech $\bar{\phi} : F[x] \rightarrow L[x]$ będzie izomorfizmem indukowanym przez ϕ . Niech $f \in F[x]$ i niech M będzie ciałem rozkładu wielomianu f , a N ciałem rozkładu wielomianu $\bar{\phi}(f)$. Wówczas istnieje izomorfizm $\psi : M \rightarrow N$ taki, że $\psi|_F = \phi$.

Dowód. Niech $M = F(a_1, \dots, a_n)$, gdzie $f(x) = a(x - a_1) \cdot \dots \cdot (x - a_n)$. Niech $N = L(b_1, \dots, b_m)$, gdzie $\bar{\phi}(f) = b(x - b_1) \cdot \dots \cdot (x - b_m)$. Zmieniając ewentualnie numerację pierwiastków $a_1, \dots, a_n$, założmy, że $a_1, \dots, a_k \notin F$ oraz $a_{k+1}, \dots, a_n \in F$. Dowód prowadzimy przez indukcję względem k .

Jeżeli $k = 0$, to $a_1, \dots, a_n \in F$, a więc $b_1, \dots, b_m \in L$. Wobec tego $F = M$, $L = N$ i skoro $F \cong L$, to $M \cong N$ i izomorfizm ustala $\phi : F \rightarrow L$.

Ustalmy teraz $k > 0$ i założmy prawdziwość twierdzenia dla liczb mniejszych od k . Niech $f_1 \in F[x]$ będzie czynnikiem nierozkładalnym f i niech $f_1(a_k) = 0$. Wówczas $f = f_1 g$, dla pewnego $g \in F[x]$, więc $\bar{\phi}(f) = \bar{\phi}(f_1)\bar{\phi}(g)$. Wobec Twierdzenia 12.2 wielomian $\bar{\phi}(f_1)$ jest nierozkładalny w $L[x]$. Ponieważ $N[x]$ jest pierścieniem z jednoznacznym rozkładem, więc każdy czynnik nierozkładalny wielomianu $\bar{\phi}(f)$ w $N[x]$ jest stowarzyszony z pewnym $x - b_i$. Zatem $\bar{\phi}(f)$ ma pierwiastek b_i dla pewnego $i \in \{1, \dots, m\}$. Wobec Twierdzenia 12.2 istnieje izomorfizm $\sigma : F(a_k) \rightarrow L(b_i)$ taki, że $\sigma|_F = \phi$ oraz $\sigma(a_k) = b_i$. Wobec założenia indukcyjnego istnieje izomorfizm $\psi : M \rightarrow N$ taki, że $\psi|_{F(a_k)} = \sigma$. W szczególności $\psi|_F = \phi$. $\square$

Wniosek 12.2. Niech F będzie ciałem, niech $f \in F[x]$. Wówczas dowolne dwa ciała rozkładu wielomianu f są izomorficzne.

12.2. Ciało algebraicznie domknięte.

Definicja 12.3. Niech F będzie ciałem. Ciało F nazywamy **algebraicznie domkniętym**, gdy każdy wielomian nierozkładalny $f \in F[x]$ jest liniowy.

Twierdzenie 12.5. Niech F będzie ciałem. Następujące warunki są równoważne:

- (1) F jest algebraicznie domknięte;
- (2) każdy wielomian $f \in F[x]$ stopnia dodatniego ma w F co najmniej jeden pierwiastek.

Dowód jest oczywisty.

Twierdzenie 12.6. Niech F będzie ciałem. Wówczas istnieje rozszerzenie L ciała F , które jest ciałem algebraicznie domkniętym.

Dowód. Niech $A = \{f \in F[x] : \deg f > 0\}$ będzie zbiorem wszystkich wielomianów dodatnich stopni o współczynnikach z ciała F , niech $R = F[\{x_f\}_{f \in A}]$ będzie pierścieniem wielomianów o współczynnikach z ciała F i zmiennych indeksowanych wielomianami ze zbioru A , niech ponadto $I = \langle \{f(x_f) : f(x) \in A\} \rangle$ będzie ideałem pierścienia R generowanym przez wszystkie wielomiany ze zbioru A , w których, dla danego wielomianu $f \in A$, zmienną x zastąpiono zmienną x_f .

Pokażemy najpierw, że $I \subsetneq R$. Istotnie, przypuśćmy, że $1 \in I$. Wówczas istnieje $n \in \mathbb{N}$, wielomiany $f_1, \dots, f_n \in A$ oraz wielomiany $g_1, \dots, g_n \in R$ takie, że $1 = g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n})$. Niech L będzie ciałem rozkładu wielomianu $f_1 \dots f_n \in F[x]$. Wówczas każdy wielomian $f_i, i \in \{1, \dots, n\}$, ma pierwiastek $a_i \in L, i \in \{1, \dots, n\}$. Wobec tego w ciele L zachodzi równość $1 = g_1 f_1(a_1) + \dots + g_n f_n(a_n) = 0$, co jest sprzecznością.

Ideał I możemy więc rozszerzyć do ideału maksymalnego $\mathfrak{m}$. Niech $F_1 = R/\mathfrak{m}$. Wówczas F_1 jest ciałem i rozpatrując złożenie kanonicznych homomorfizmów otrzymujemy homomorfizm $u : F \rightarrow F_1$ dany wzorem $u(a) = a + \mathfrak{m}$, który tym samym jest zanurzeniem, a w rezultacie F_1 jest rozszerzeniem ciała F . Poza tym dowolny wielomian $f \in F[x]$ stopnia niezerowego ma w F_1 pierwiastek $x_f + \mathfrak{m}$.

Postępując indukcyjnie konstruujemy ciąg rozszerzeń ciał $F \subset F_1 \subset F_2 \subset \dots$ o tej własności, że każdy wielomian $f \in F_i[x]$ ma pierwiastek w ciele F_{i+1} . Niech $F_\infty = \bigcup_{i=1}^\infty F_i$. F_∞ jest ciałem jako suma łańcucha ciał. Jest też ciałem algebraicznie domkniętym, gdyż jeśli $f \in F_\infty[x]$ jest wielomianem dodatniego stopnia, to wówczas $f \in F_i[x]$ dla pewnego $i \in \mathbb{N}$. Wobec tego f ma pierwiastek w ciele F_i , ale $F_i \subset F_\infty$. $\square$

“Najsłynniejszym” ciałem algebraicznie domkniętym jest ciało liczb zespolonych. Twierdzenie orzekające o tym, że $\mathbb{C}$ jest ciałem algebraicznie domkniętym nosi nazwę **zasadniczego twierdzenia algebry**. Po raz pierwszy zostało ono sformułowane przez Girarda w 1629 roku, a pełny dowód jako pierwszy podał Gauss w 1799. Zasadnicze twierdzenie algebry jest “zasadnicze” tylko z historycznego punktu widzenia i obecnie przyjęta nazwa wydaje się dziś nieco przesadzona, pochodzi jednak z czasów, gdy problem rozwiązalności równań algebraicznych był jednym z głównych tematów zainteresowań matematyków. Istnieje całe mnóstwo dowodów zasadniczego twierdzenia – my podamy jeden z nich, korzystający z twierdzenia Weierstrassa.¹⁸ Dowód zasadniczego twierdzenia algebry opiera się na dwóch lematach:

Lemat 12.1. Niech $P(z) = a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z]$, $|a_n| = 1$, niech $p : \mathbb{C} \rightarrow \mathbb{R}$ będzie dana wzorem $p(z) = |P(z)|$. Wówczas p osiąga kres dolny na zbiorze $\mathbb{C}$.

Dowód. Wobec nierówności trójkąta dla modułu:

$$\begin{aligned} p(z) &= |P(z)| = |a_n z^n + \dots + a_1 z + a_0| = |z^n| \cdot \left| a_n + \frac{a_{n-1}}{z} + \dots + \frac{a_0}{z^n} \right| \\ &\geq |z|^n \left(1 - \frac{|a_{n-1}|}{|z|} - \dots - \frac{|a_0|}{|z|^n} \right) \geq |z|^n \left(1 - \frac{n \cdot \max\{|a_i| : i \in \{0, \dots, n-1\}\}}{R} \right), \end{aligned}$$

dla $|z| \geq R \geq 1$. Niech $R = 2(1 + \max\{|a_i| : i \in \{0, \dots, n-1\}\})$. Wówczas $p(z) \geq \frac{1}{2}R^n > |a_0| = p(0)$ dla $|z| \geq R$. Zatem wewnątrz koła $\{z : |z| \leq R\}$ istnieje punkt, w którym wartość p jest mniejsza od wartości

¹⁸Funkcja ciągła na zbiorze zwartym o wartościach rzeczywistych przyjmuje wartości największą i najmniejszą.

w dowolnym punkcie poza kołem $\{z : |z| \leq R\}$. Wobec tego $\inf\{p(z) : z \in \mathbb{C}\} = \inf\{p(z) : |z| \leq R\}$. Ponieważ koło $\{z \in \mathbb{C} : |z| \leq 1\}$ jest zbiorem zwartym, więc wobec twierdzenia Weierstrassa funkcja p osiąga na nim kres dolny. $\square$

Lemat 12.2. Niech $P(z) = a_n z^n + \dots + a_1 z + a_0 \in \mathbb{C}[z]$, $|a_n| = 1$, niech $p : \mathbb{C} \rightarrow \mathbb{R}$ będzie dana wzorem $p(z) = |P(z)|$. Niech ponadto $p(z_0) = \inf\{p(z) : z \in \mathbb{C}\}$. Wówczas $P(z_0) = 0$.

Dowód. Przypuśćmy, że $P(z_0) \neq 0$, $P(z_0) = m$, $m \in \mathbb{R}_+$. Niech $\rho \in (0, \min\{1, m\})$. Niech $z \in \partial K(z_0, \rho)$ (w ten sposób oznaczamy brzeg koła o środku z_0 i promieniu ρ). Wówczas $z = z_0 + \rho e^{i\theta}$. Mamy:

$$P(z_0 + \rho e^{i\theta}) = \sum_{k=0}^n a_k (z_0 + \rho e^{i\theta})^k = P(z_0) + w_1(z_0) \rho e^{i\theta} + \dots + w_n(z_0) \rho^n e^{in\theta},$$

gdzie $w_1(z_0), \dots, w_n(z_0)$ są pewnymi współczynnikami.

Pokażemy, że dla pewnej liczby $j \in \{1, \dots, n\}$, $w_j(z_0) \neq 0$. Istotnie, przypuśćmy że $w_1(z_0) = \dots = w_n(z_0) = 0$. Wówczas P jest stały na $\partial K(z_0, \rho)$, a więc wielomian $Q(z) = P(z) - P(z_0)$ stopnia dodatniego ma nieskończenie wiele pierwiastków, co jest sprzecznością.

Niech zatem $k = \min\{j \in \{1, \dots, n\} : w_j(z_0) \neq 0\}$. Mamy więc:

$$|P(z_0 + \rho e^{i\theta})| \leq |P(z_0) + w_k(z_0) \rho^k e^{ik\theta}| + (1 + n \cdot \max\{|w_j(z_0)| : j \in \{1, \dots, n\}\}) \rho^{k+1}.$$

Położmy $\theta = \frac{\pi - \text{Arg}(w_k(z_0))}{k}$. Wówczas:

$$|P(z_0 + \rho e^{i \frac{\pi - \text{Arg}(w_k(z_0))}{k}})| \leq |P(z_0)| - |w_k(z_0)| \rho^k + (1 + n \cdot \max\{|w_j(z_0)| : j \in \{1, \dots, n\}\}) \rho^{k+1}.$$

Niech teraz $\rho < \frac{|w_k(z_0)|}{1 + n \cdot \max\{|w_j(z_0)| : j \in \{1, \dots, n\}\}}$. Wówczas:

$$|P(z_0)| - |w_k(z_0)| \rho^k + (1 + n \cdot \max\{|w_j(z_0)| : j \in \{1, \dots, n\}\}) \rho^{k+1} < |P(z_0)| = P(z_0) = m = \inf\{p(z) : z \in \mathbb{C}\},$$

więc $p(z_0 + \rho e^{i \frac{\pi - \text{Arg}(w_k(z_0))}{k}}) < \inf\{p(z) : z \in \mathbb{C}\}$ - sprzeczność. $\square$

Oczywiście z Lematu 12.2 wynika natychmiast zasadnicze twierdzenie algebry.