

Algebra 2R

a voyage into the unknown

koteczek

~

Spis rzeczy niezbyt mądrych

Wstęp



Wykład: 1: Teoria równań algebraicznych

Przez R, S będziemy oznaczać pierścienie przemienne z $1 \neq 0$, natomiast K, L będziemy rezerwować dla oznaczeń ciał.

1.1 Rozwiązywanie układów równań

Rozważmy funkcje $f_1, \dots, f_m \in R[X_1, \dots, X_n]$. Dla wygody będziemy oznaczać krotki przez \bar{X} , czyli $R[X_1, \dots, X_n] = R[\bar{X}]$. Pojawia się problem: *czy istnieje rozszerzenie pierścieni z jednością $R \subseteq S$ takie, że układ $U : f_1(\bar{X}) = \dots = f_m(\bar{X}) = 0$ ma rozwiązanie w pierścieniu S ?*

Fakt 1.1. $\bar{a} = (a_1, \dots, a_n) \subseteq S$, gdzie S jest rozszerzeniem pierścienia R , jest rozwiązaniem układu równań $U \iff g(\bar{a}) = 0$ dla każdego wielomianu $g \in (f_1, \dots, f_m) \triangleleft R[\bar{X}]$.

Dowód:

\Leftarrow Implikacja jest dość trywialna, jeśli każdy wielomian z (f_1, \dots, f_m) , czyli wytworzony za pomocą sumy i produktu wielomianów f_1, \dots, f_m zeruje się na \bar{a} , to musi zerować się też na każdym z tych wielomianów.

\Rightarrow Rozważamy dwa przypadki:

1. $(f_1, \dots, f_m) \ni b \neq 0$ i $b \in R$.

To znaczy w (f_1, \dots, f_m) mamy pewien niezerowy wyraz wolny. Wtedy mamy wielomian $g \in (f_1, \dots, f_m)$ taki, że $g(\bar{a}) \neq 0$. Ale przecież g jest kombinacją wielomianów f_1, \dots, f_m , która na \bar{a} przyjmuje wartość 0. W takim razie dostajemy układ sprzeczny i przypadek jest do odrzucenia.

2. $(f_1, \dots, f_m) \cap R = \{0\}$. (nie ma wyrazów wolnych różnych od 0)

Teraz wiemy, że układ U jest niesprzeczny, a więc możemy skonstruować pierścień z 1 S będący rozszerzeniem R [$S \supseteq R$] oraz rozwiązanie $\bar{a} \subseteq S$ spełniające nasz układ równań.

Niech $S = R[\bar{X}]/(f_1, \dots, f_m)$ i rozważmy

$$j : R[\bar{X}] \rightarrow S = R[\bar{X}]/(f_1, \dots, f_m)$$

nazywane **przekształceniem ilorazowym**. Po pierwsze, zauważmy, że $j \upharpoonright R$ jest $1 - 1$, bo

$$\ker(j \upharpoonright R) = \ker(j) \cap R = (f_1, \dots, f_m) \cap R = \{0\}$$

i dlatego

$$j \upharpoonright R : R \xrightarrow{\cong} j[R] \subseteq S.$$

Z uwagi na ten izomorfizm, będziemy utożsamiać $R, j[R]$. W takim razie, S jest rozszerzeniem pierścienia R . Czyli mamy rozszerzenie pierścienia R .

Niech

$$\bar{a} = (a_1, \dots, a_n) = (j(X_1), \dots, j(X_n)) \subseteq S,$$

czyli jako potencjalne rozwiązanie rozważamy zbiór obrazów wielomianów stopnia 1 przez wcześniej zdefiniowaną funkcję $j : R[\bar{X}] \rightarrow S$. Tak zdefiniowane \bar{a} jest rozwiązaniem układu U w pierścieniu S , bo dla funkcji wielomianowej (czyli zapisywalnej jako wielomian) $\hat{f}_i \in (f_1, \dots, f_m)$ mamy

$$\hat{f}_i(\bar{a}) = \hat{f}_i(j(X_1), \dots, j(X_n)) = j(\hat{f}_i(X_1, \dots, X_n)) = j(f_i) = 0.$$

TUTAJ TRZEBA POUZASADNIAĆ KILKA RÓWNOŚCI, ALE MOŻE NIE BĘDĘ TEGO ROBIŁA NA AISD

Uwaga 1.2. Skonstruowane powyżej rozwiązanie \bar{a} układu U ma następującą własność uniwersalności:

(☕) Jeżeli $S' \supseteq R$ jest rozszerzeniem pierścienia z 1 i $\bar{a}' = (a'_1, \dots, a'_m) \in S'$ jest rozwiązaniem U w S' , to istnieje jedyny homomorfizm

$$h : R[\bar{a}] \rightarrow R[\bar{a}']$$

taki, że $h \upharpoonright R$ jest identycznością na R i $h(\bar{a}) = \bar{a}'$. Wszystkie rozwiązania układów są homomorficzne.

$$\begin{array}{ccc} R & \xrightarrow{\subseteq} & R[\bar{a}] \subseteq S \\ \downarrow \subseteq & \nearrow h & \\ R[\bar{a}'] \subseteq S' & & \end{array}$$

Tutaj $R[\bar{a}] \subseteq S$ jest **podpierścieniem generowanym przez $R \cup \{\bar{a}\}$** , czyli zbiór:

$$R[\bar{a}] = \{f(\bar{a}) : f(\bar{X}) \in R[\bar{X}]\} \subseteq S$$

Dowód: Niech $I = \{g \in R[\bar{X}] : g(\bar{a}') = 0\} \subseteq S'$. Oczywiście mamy, że $I \triangleleft R[\bar{X}]$, a więc

$$(f_1, \dots, f_m) \subseteq I.$$

Z twierdzenia o faktoryzacji wie

$$\begin{array}{ccc} R[\bar{X}] & \xrightarrow{j} & S = R[\bar{X}]/(f_1, \dots, f_m) \\ \downarrow \phi & \nearrow (\exists ! h) h(\bar{a}) = \bar{a}' & \\ S' \supseteq R[\bar{a}'] & & \end{array}$$

Homomorfizm $\phi : R[\bar{X}] \rightarrow R[\bar{a}']$ określamy wzorem

$$\phi(w) = w(\bar{a}),$$

a homomorfizm j jest jak wyżej odwzorowaniem ilorazowym. Widzimy, że

$$I = \ker(\phi)$$

$$\ker(j) = (f_1, \dots, f_m).$$

Z twierdzenia o homomorfizmie pierścieni dostajemy jedyny homomorfizm

$$h : R[\bar{X}]/(f_1, \dots, f_m) \rightarrow R[\bar{a}]$$

taki, że $h(\bar{a}) = \bar{a}'$.

Uwaga 1.3. Jeśli $I = (f_1, \dots, f_m)$, to $h : R[\bar{a}] \xrightarrow[R]{\cong} [\bar{a}']$.

Wtedy mamy $\ker \phi = \ker j$, czyli $\ker(h \circ j) = \ker \phi = \ker j$, no a z tego wynika, że $\ker h$ jest trywialne, czyli h jest apimorfizmem (1-1). Z drugiej strony, $\text{Im } \phi = \text{Im}(h \circ j)$, a ϕ jest epimorfizmem ("na"), więc również h musi być "na".

Założmy, że $S \supseteq R$ jest rozszerzeniem pierścienia oraz $\bar{a} \in S^n$. Wtedy:

1. ideał \bar{a} nad R definiujemy jako

$$I(\bar{a}/R) = \{g \in R[\bar{X}] : g(\bar{a}) = 0\}$$

2. \bar{a} nazywamy **rozwiązaniem ogólnym** układu U , jeśli ideał

$$I(\bar{a}/R) = (f_1, \dots, f_m).$$

Uwaga 1.4. W sytuacji jak z definicji wyżej, gdy U jest układem niesprzecznym, wtedy \bar{a} jest rozwiązaniem ogólnym układu $U \iff$ zachodzi warunek (☕).

Dowód: Ćwiczenia.

1.2 Rozszerzanie ciał

Dla $K \subseteq L$ ciał i $\bar{a} \subseteq L$ definiujemy **ideał \bar{a} nad K** jako:

$$I(\bar{a}/L) := \{f(X_1, \dots, X_n) \in K[\bar{X}] : f(\bar{a}) = 0\},$$

to znaczy generujemy ideał w wielomianach nad K zawierający wszystkie wielomiany (niekoniecznie tylko jednej zmiennej) zerujące się w \bar{a} .

Przykład:

Dla $K = \mathbb{Q}, L = \mathbb{R}, n = 1, a_1 = \sqrt{2}$ mamy

$$I(\sqrt{2}/\mathbb{Q}) = \{f(x^2 - 2) : f \in \mathbb{Q}[X]\} = (x^2 - 2) \triangleleft \mathbb{Q}[X]$$

Dalej, definiujemy

$$K[\bar{a}] := \{f(\bar{a}) : f \in K[\bar{X}]\}$$

czyli **podpierścień L generowany przez $K \cup \{\bar{a}\}$** oraz $K(\bar{a})$, czyli **podciało L** generowane przez $K \cup \{\bar{a}\}$:

$$K(\bar{a}) := \{f(\bar{a}) : f \in K(X_1, \dots, X_n) \text{ i } f(\bar{a}) \text{ dobrze określone}\}.$$

Tutaj $K(X_1, \dots, X_n)$ to *ciało ułamków pierścienia* $K[\bar{a}]$ w ciele L (czyli najmniejsze ciało, że pierścień może być w nim zanurzony). Czasami oznaczamy to przez $K[\bar{a}]_0$.

Uwaga 1.5. Niech $K \subseteq L_1, K \subseteq L_2$ będą ciałami. Wybieramy $\bar{a}_1 \in L_1$ i $\bar{a}_2 \in L_2$, $|\bar{a}_1| = |\bar{a}_2| = n$. Wtedy następujące warunki są równoważne:

1. istnieje izomorfizm $\phi : K[\bar{a}_1] \rightarrow K[\bar{a}_2]$ taki, że $\phi \upharpoonright K = \text{id}_K$ oraz $\phi(\bar{a}_1) = \bar{a}_2$.
2. $I(\bar{a}_1/K) = I(\bar{a}_2/K)$.

Dowód:

1 \implies 2

Implikacja jest jasna, bo dla $g(\bar{X}) \in K[\bar{X}]$, bo $g(\bar{a}_1) = 0$ w $K[\bar{a}_1] \iff g(f(\bar{a}_1)) = 0$, a $f(\bar{a}_1) = \bar{a}_2$.

1 \Leftarrow 2

Zwróćmy uwagę na odwzorowanie ewaluacji \bar{a}_1

$$\phi_{\bar{a}_1} : K[\bar{X}] \xrightarrow{\text{"na"}} K[a_1]$$

zadane wzorem

$$\phi(w(\bar{X})) = w(\bar{a}_1).$$

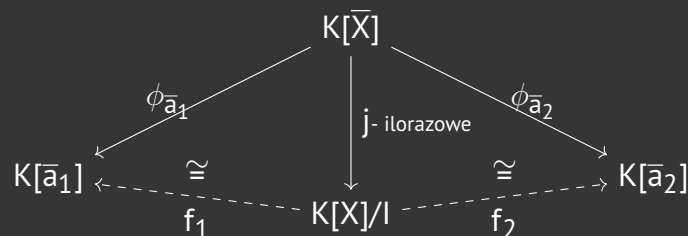
Mamy

$$\ker(\phi_{\bar{a}_1}) = I(\bar{a}_1/K).$$

Tak samo dla \bar{a}_2 możemy określić analogicznie odwzorowanie ewaluacyjne $\phi_{\bar{a}_2} : K[\bar{X}] \rightarrow K[\bar{a}_2]$. Wtedy

$$I(\bar{a}_2/K) = \ker(\phi_{\bar{a}_2}),$$

ale ponieważ $I(\bar{a}_1/K) = I(\bar{a}_2/K)$, to $\ker(\phi_{\bar{a}_1}) = \ker(\phi_{\bar{a}_2})$. Oznaczmy $I = I(\bar{a}_1/K) = I(\bar{a}_2/K)$. Widzimy, że $\phi_{\bar{a}_i} \upharpoonright K = \text{id}_K$.



Niech $f = f_2 f_1^{-1} : K[\bar{a}_1] \rightarrow K[\bar{a}_2]$ jest funkcją spełniającą warunki punktu 1.

MOŻE TUTAJ ŁADNIE SPRAWDZIĆ ŻE NAPRAWDĘ JEST TO DOBRZE SPEŁNIAJĄCA WARUNKI FUNKCJA?

Uwaga. Niech $I \triangleleft K[\bar{X}]$ *noetherowskiego* pierścienia $K[\bar{X}]$. Niech $I = (f_1, \dots, f_m)$ dla pewnych $f_i \in K[\bar{X}]$. Wtedy istnieje rozszerzenie pierścienia $S \supseteq K$ oraz $\bar{a} \subseteq S$ - rozwiązanie ogólne układu $f_1(\bar{X}) = \dots = f_m(\bar{X}) = 0$ takie, że $I(\bar{a}/K) = I$.

Dowód: Uwaga ??.

Twierdzenie 1.6. Niech $I \triangleleft K[\bar{X}]$. Wtedy istnieje ciało $L \supseteq K$ oraz $\bar{a} = (a_1, \dots, a_n) \subseteq L$ takie, że $f(\bar{a}) = 0$ dla każdego $f \in I$.

Dowód: Niech $I \subseteq M \triangleleft K[\bar{X}]$ będzie ideałem maksymalnym. Niech $L = K[\bar{X}]/M$ i określmy przekształcenie ilorazowe

$$j : K[\bar{X}]/M \rightarrow L = K[\bar{X}]/M.$$

Ponieważ $M \cap K = \{0\}$ (bo inaczej w ideale byłby wielomian odwracalny), to $j \upharpoonright K : K \rightarrow L$ jest funkcją $1 \mapsto 1$, czyli

$$j \upharpoonright K : K \xrightarrow{1 \mapsto 1} j[K] \subseteq L.$$

Możemy utożsamić K z $j[K]$, czyli $K \subseteq L$. Niech $\bar{a} = (a_1, \dots, a_n)$ takie, że dla każdego $i \in [n]$

$$a_i = j(X_i) \in L.$$

Wtedy $g(\bar{a}) = 0$ dla każdego $g(\bar{X}) \in M \supseteq I$ (bo inaczej mielibyśmy wyrazy wolne).

Wniosek 1.7. Niech $f \in K[X]$ stopnia > 0 . Wtedy istnieje ciało $L \supseteq K$ rozszerzające ciało K takie, że f ma pierwiastek w ciele L .

Przykłady:

1. Rozpatrzmy ciało $K = \mathbb{Q}$ i $f(X) = X - 2$. Wtedy $I = (f) \triangleleft \mathbb{Q}[X]$ jest ideałem maksymalnym, bo jest on pierwszy (w tym wypadku nierozkładalny). Równanie $f = 0$ ma rozwiązanie ogólne w pierścieniu ilorazowym

$$\mathbb{Q}[X]/I \cong \mathbb{Q}.$$

Czyli nie zawsze musimy rozszerzać ciało do czegoś nowego.

2. $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i) = \mathbb{R}[z]$ dla każdego $z \in \mathbb{C} \setminus \mathbb{R}$, co jest na liście zadań.

Założmy, że $K \subseteq L_1, K \subseteq L_2$ są rozszerzeniami ciała. Wtedy mówimy, że **L_1 jest izomorficzne z L_2 nad K** [$L_1 \cong_K L_2$] \iff istnieje izomorfizm $f : L_1 \rightarrow L_2$ taki, że $f \upharpoonright K = \text{id}_K$.

Fakt 1.8.

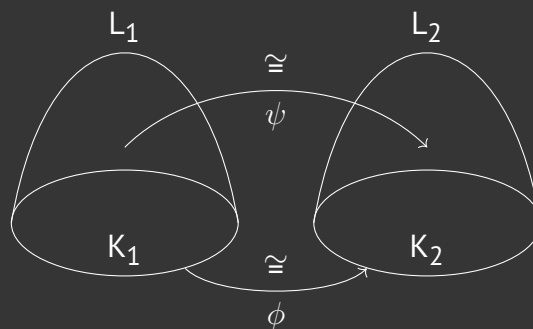
1. Załóżmy, że $f(X) \in K[X]$ jest nierozkładalny. Niech $L_1 = K(a_1)$, $L_2 = K(a_2)$ i $f(a_i) = 0$ w L_i . Wtedy $L_1 \cong_K L_2$.

2. Ogólniej: załóżmy, że $\phi : K_1 \rightarrow K_2$ jest izomorfizmem i $f_1 \in K_1[X], f_2 \in K_2[X], \phi(f_1) = f_2, f_i$ jest nierozkładalne. Dodatkowo załóżmy, że $L_1 = K_1(a_1)$ i $L_2 = K_2(a_2)$, gdzie $f_i(a_i) = 0$ w L_i . Wtedy istnieje izomorfizm $\psi \in \psi : L_1 \rightarrow L_2$ taki, że $\psi(a_1) = a_2$.

Dowód:

1. $I(a_1/K) = (f) = I(a_2/K)$, stąd na mocy ?? mamy $K(a_1) \cong_K K(a_2)$. Po dowodzie przypadku 2. możemy uzasadniać, że jest to szczególny przypadek tego ogólniejszego stwierdzenia właśnie.

2. Zaczniemy od rozrysowania tej sytuacji:



Izomorfizm $\phi : K_1[X] \xrightarrow[\cong]{K_2} [X]$ indukuje nam przekształcenie

$$K_1[X]/(f_1) \xrightarrow[\phi]{\cong} K_2[X]/(f_2),$$

bo $\phi(f_1) = f_2$. Wiemy, że f_i jest nierozkładalne, czyli

$$I(a_i/K_i) = (f_i) \triangleleft K_i[X]$$

jest ideałem maksymalnym. Mamy

$$L_i = K_i(a_i) = K_i[a_i] \cong K[X]/I(a_i/K_i).$$

$$\begin{array}{ccc}
 K_1[X] & \xrightarrow[\phi]{\cong} & K_2[X] \\
 & \downarrow & \\
 K_1[X]/(f_1) & \xrightarrow[\phi]{\cong} & K_2[X]/(f_2) \\
 \downarrow h_1 & & \downarrow h_2 \\
 L_1 = K_1(a_1) & \xrightarrow[\psi]{\cong} & L_2 = K_2(a_2) \\
 \cup & & \cup \\
 K_1 & \xrightarrow[\phi]{} & K_2
 \end{array}$$

Wykład: 2: Ciała skończone i pierwiastki z jedności

Ciało $L \supseteq K$ nazywamy **ciałem rozkładu nad K** wielomianu $f \in K[X]$, gdy spełnione są warunki:

1. f rozkłada się w pierścieniu $L[X]$ na czynniki liniowe (stopnia 1)
2. Ciało L jest rozszerzeniem ciała K o elementy a_1, \dots, a_n , gdzie a_1, \dots, a_n to wszystkie pierwiastki f w L .

Przykład: Jeżeli $\deg(f) = 0$, to nie istnieje ciało rozkładu f .

Wniosek 2.1. Załóżmy, że $f \in K[X]$ jest wielomianem stopnia > 0 . Wtedy

1. istnieje L : ciało rozkładu f nad K ,
2. to ciało jest jedyne z dokładnością do izomorfizmu nad K .

Dowód:

1. Dowód przez indukcję względem stopnia f

Jako przypadek bazowy rozważmy f takie, że $\deg(f) = 1$. Wtedy $L = K$ i wszystko wniosek jest spełniony.

Założmy teraz, że stopień wielomianu f jest > 1 i też zachodzi dla wszystkich wielomianów stopnia $< \deg(f)$ i wszystkich ciał K' . Teraz z ?? wiemy, że istnieje rozszerzenie ciała $L \supseteq K$ takie, że f ma pierwiastek w L . Nazwijmy ten pierwiastek a_0 i niech

$$K' = K(a_0).$$

Ponieważ $K'[X]$ wielomian f ma pierwiastek a_0 , to możemy zapisać

$$f = (x - a_0)f_1$$

dla pewnego $f_1 \in K'[X]$ i $\deg(f_1) < \deg(f)$. Z założenia indukcyjnego dla f_a istnieje $L' = K'(a_1, \dots, a_r)$ - ciało rozkładu wielomianu f_1 nad K' . Wtedy

$$L = K(a_0, \dots, a_r)$$

jest ciałem rozkładu f nad K .

2. Udowodnimy wersję ogólniejszą:

(🐞) Jeśli $\phi : K_1 \xrightarrow{\cong} K_2$ jest izomorfizmem nad ciałem i $f_i \in K_i[X]$ jest wielomianem stopnia > 0 , $\phi(f_1) = f_2$, to wtedy istnieje $\psi : L_1 \xrightarrow{\cong} L_2$ izomorfizm nad ciałami rozkładu f_i w K_i rozszerzający izomorfizm ϕ (to znaczy $\phi \subseteq \psi$).

Wykorzystamy indukcję po $\deg(f)$. W przypadku bazowym mamy $\deg(f) = 1$, czyli $L_1 = K_1, L_2 = K_2$ i $\phi = \psi$.

Teraz niech $\deg(f) > 1$ i założmy, że dla wszystkich ciał K' oraz wielomianów stopnia $< \deg(f)$ jest to prawdą. Niech

$$f_i = f'_i \cdot g_i,$$

gdzie $f'_i, g_i \in K_i[X]$ i g_i jest wielomianem nierozkładalnym w K . Wiemy już, że istnieje $a_i \in L_i$ będące pierwiastkiem wielomianu g_i .

Z faktu ??(2), wiemy, że istnieje wtedy izomorfizm

$$\psi_0 : K_1(a_1) \xrightarrow{\cong} K_2(a_2)$$

taki, że $\psi_0(a_1) = a_2$ i $\phi \subseteq \psi_0$.

$$\begin{array}{ccc} K_1(a_1) & \xrightarrow[\exists \psi_0]{\cong} & K_2(a_2) \\ \parallel & & \parallel \\ K'_1 & & K'_2 \\ \cap & & \cap \\ L_1 & \xrightarrow[\exists \psi_1]{\cong} & L_2 \end{array}$$

Z założenia wiemy, że L_i to ciało rozkładu f'_i nad K_i . W takim razie z założenia indukcyjnego istnieje izomorfizm

$$\psi_1 : L_1 \xrightarrow{\cong} L_2$$

taki, że $\psi \subseteq \psi_0$ i to już jest koniec.

Wniosek 2.2. Jeśli $f_1 \in K_1[X]$ i $f_2 \in K_2[X]$ są nierozkładalnymi wielomianami, $\phi : K_1 \xrightarrow{\cong} K_2$ izomorfizmem i $\phi(f_1) = f_2$, a L_1, L_2 to ciała rozkładu f_1, f_2 odpowiednio nad K_1 i K_2 , $a_i \in L_i$ to pierwiastek f_i , to wtedy istnieje $\psi : L_1 \xrightarrow{\cong} L_2$ takie, że $\psi(a_1) = a_2$.

Dowód: Wynika z dowodu stwierdzenia .

2.1 Algebraiczne domknięcie ciała

Ciało L jest **algebraicznie domknięte** \iff dla każdego $f \in L[X]$ o stopniu > 0 istnieje pierwiastek f w L . To znaczy każdy wielomian rozkłada się na czynniki liniowe nad L .

Przykład:

- $\hookrightarrow \mathbb{C}$ jest algebraicznie domknięte.
- $\hookrightarrow \mathbb{R}$ nie jest algebraicznie domknięte, gdyż $x^2 + 1$ nie ma pierwiastka rzeczywistego.
- $\hookrightarrow \mathbb{Q}[i]$ nie jest algebraicznie domknięte, bo $x^2 - 2$ nie ma pierwiastka.

Twierdzenie 2.3. Każde ciało K zawiera się w pewnym ciele algebraicznie domkniętym.

Dowód:

Jak mamy wielomian nad ciałem, to istnieje rozszerzenie ciała do tego wielomianu. I dalej leci kombinatoryka.

Lemat: Dla każdego ciała K istnieje $L \supseteq K$ takie, że $(\forall f \in K[X])$ stopnia > 0 , f ma pierwiastek w L .

Rozważmy dobry porządek na zbiorze wielomianów z $K[X]$ stopnia > 0

$$\{f \in K[X] : \deg(f) > 0\} = \{f_\alpha : \alpha < \kappa\}.$$

Tutaj α, κ to liczby porządkowe, niekoniecznie skończone. Skonstruujmy rosnący ciąg rozszerzeń ciał $\{K_\alpha : \alpha < \kappa\}$ taki, że

- $\hookrightarrow K \subseteq K_\alpha \subseteq K_\beta$ dla $\alpha < \beta < \kappa$
- $\hookrightarrow f_\alpha$ ma pierwiastek w $K_{\alpha+1}$.

Dowód przez indukcję pozaskończoną. Dla $K_0 = K$.

Założmy, że $\alpha < \kappa$ i mamy $\{K_\beta : \beta < \alpha\}$ spełniając warunki powyżej. Niech $K' = \bigcup_{\beta < \alpha} K_\beta$. Musimy pokazać, że K' jest ciałem.

1. α to liczba graniczna. Definiujemy $K' = \bigcup_{\beta < \alpha} K_\beta$ jako zbiór.

Musimy określić działania w K' . Niech $x, y \in K'$, wtedy istnieje $\beta < \alpha$ takie, że $x, y \in K_\beta$. Czyli $x + y \in K_\beta \subseteq K'$ i $xy \in K_\beta \subseteq K'$. W takim razie K' jest rozszerzeniem ciała K_β .

Teraz definiujemy $K_\alpha = K'$ i otrzymujemy pożądane rozszerzenie ciała.

2. $\alpha = \beta + 1$ to następnik, wtedy $K' = K_\beta$.

Wielomian f_α jest wielomianem nad $K \subseteq K'$. Z wniosku ?? wiemy, że istnieje rozszerzenie $K_\alpha \supseteq K$ takie, że f_α ma pierwiastek w K_α .

L definiujemy jako sumę po wyżej udowodnionej konstrukcji:

$$L = \bigcup_{\alpha < \kappa} K_\alpha$$

i to ciało spełnia nasz lemat.

Wracamy teraz do dowodu twierdzenia ?? i niech $(L_n, n < \omega)$ będzie rosnącym ciągiem ciał takim, że

$$\hookrightarrow L_0 = K$$

$$\hookrightarrow L_{n+1} \supseteq L_n, \text{ gdzie } L_{n+1} \text{ dane jest przez lemat, to znaczy } (\forall f \in L_n[X]) f \text{ ma pierwiastek w } L_{n+1}.$$

Niech

$$L_\infty = \bigcup_{n < \omega} L_n \supseteq K.$$

Jest to ciało, ponieważ suma rosnącego ciągu ciał jest ciałem. Dalej mamy, że jest to ciało algebraicznie domknięte, gdy dowolny $f \in L_\infty[X]$ ma stopień skończony > 0 , czyli istnieje n takie, że $f \in L_n[X]$. A więc f ma wszystkie pierwiastki w $L_{n+1} \subseteq L_\infty$.

Wykład: 3: Ciała proste, pierwiastki z jedności

3.1 Ciała proste

Uwaga 3.0. Załóżmy, że mamy ciała $K \subseteq L$. Wtedy

$$\hookrightarrow \text{char}(K) = \text{char}(L)$$

$$\hookrightarrow 0_K = 0_L \text{ oraz } 1_K = 1_L$$

$$\hookrightarrow K^* = K \setminus \{0\} \subseteq L^* = L \setminus \{0\} \text{ oraz dla } x \in K \text{ } -x \text{ w } K \text{ jest równe } -x \text{ w } L.$$

K jest **ciałem prostym** wtedy i tylko wtedy, gdy K nie zawiera żadnego właściwego podciała.

Przykład:

$$\hookrightarrow \mathbb{Q}, \text{ gdzie } \text{char}(\mathbb{Q}) = 0 \text{ to ciało proste nieskończone.}$$

$$\hookrightarrow \text{Ciałem prostym skończonym jest na przykład } \mathbb{Z}_p \text{ dla liczby pierwszej } p, \text{ wtedy } \text{char}(\mathbb{Z}_p) = p.$$

Uwaga 3.1.

1. Każde ciało zawiera jedyne podciało proste
2. Z dokładnością do $\cong \mathbb{Q}, \mathbb{Z}_p$ to wszystkie ciała proste.

Przykład: Załóżmy, że K jest skończone. Wtedy K^* też jest skończone rzędu $|K^*| = n < \infty$. Później dowiemy się, że $|K| = p^k$, a więc $|K^*| = p^k - 1$. Wiemy, że dla każdego $x \in K^*$ zachodzi $x^n = 1$.

3.2 Pierwiastki z jedności

Niech R będzie pierścieniem przemiennym z $1 \neq 0$. Mamy następujące definicje:

$$1. a \in R \text{ jest } \textbf{pierwiastkiem z 1} \text{ stopnia } n > 0 \iff a^n = 1$$

$$2. \mu_n(R) = \{a \in R : a^n = 1\} \text{ jest } \textbf{grupą pierwiastków z 1} \text{ stopnia } n$$

$$3. \mu(R) = \{a \in R : (\exists n) a^n = 1\} = \bigcup_{n>0} \mu_n(R) \text{ jest } \textbf{grupą pierwiastków z 1}$$

$$4. a \text{ jest } \textbf{pierwiastkiem pierwotnym} \text{ [primitive root] stopnia } n \text{ z } 1 \iff a \in \mu_n(R) \text{ oraz dla każdego } k < n \text{ } a \notin \mu_k(R).$$

Uwaga 3.2.

1. $\mu_n(R) \triangleleft R^*$ jest grupą jednostek pierścienia
2. $\mu(R) \triangleleft R^*$
3. $\mu(R)$ jest **torsyjną grupą abelową** (każdy element jest pierwiastkiem z 1).

Przykłady

$$1. \mu(\mathbb{C}) = \bigcup_{n>0} \mu_n(\mathbb{C}) \leq (\{z \in \mathbb{C} : |z| = 1\}, \cdot) \triangleleft \mathbb{C}^* = \mathbb{C} \setminus \{0\} \text{ jest nieskończona.}$$

$$2. \mu(\mathbb{C}) \cong (\mathbb{Q}, +) / (\mathbb{Z}, +), \text{ bo } f : \mathbb{Q} \xrightarrow[\text{homo}]{\text{"na"}} \mu(\mathbb{C}) \text{ taki, że } f(w) = \cos(w2\pi) + i \sin(w2\pi) \text{ ma jądro } \ker(f) = \mathbb{Z}.$$

$$3. \mu(\mathbb{R}) = \{\pm 1\}$$

$$4. \mu_n(K) = \{\text{zera wielomianu } x^n - 1\}. \text{ Ten wielomian będziemy oznaczali } w_n(x) = x^n - 1.$$

Uwaga 3.3.

1. Jeśli $\text{char}(K) = 0$, to $w_n(x) = x^n - 1$ ma tylko pierwiastki jednokrotne w K [simple roots]
2. Jeśli $\text{char}(K) = p > 0$ i $n = p^l n_1$ takie, że $p \nmid n_1$, to wszystkie pierwiastki $w_n(x) = x^n - 1$ mają krotność p^l w K .

Dowód:

1. Niech $a \in K$ takie, że $w_n(a) = 0$. Z twierdzenia Bezouta mamy, że

$$w_n(x) = x^n - 1 = x^n - a^n = (x - a)(x^{n-1} + ax^{n-2} + \dots + a^{n-2}x + a^{n-1}) = (x - a)v_n(x),$$

gdzie $v_n(x) = x^{n-1} + ax^{n-2} + \dots + a^{n-2}x + a^{n-1}$.

Z tego, że $\text{char}(K) = 0$ wynika, że $v_n(a) = na^{n-1} \neq 0$, skąd wynika, że a jest jednokrotnym pierwiastkiem $w_n(x)$.

2. Jesteśmy w ciele K o $\text{char}(K) = p$. Niech $n = p^l n_1$. Rozważmy wielomian

$$w_n(X) = X^n - 1 = (X^{n_1})^{p^l} - 1^{p^l} = (X^{n_1} - 1)^{p^l} = w_{n_1}(X)^{p^l}.$$

Czyli $\mu_n(K) = \mu_{n_1}(K)$. Załóżmy, że $a \in K$ to pierwiastek wielomianu $w_n(X)$. Wtedy a jest też pierwiastkiem wielomianu w_{n_1} w ciele K . Wtedy

$$w_{n_1}(X) = (X - a)v_{n_1}(X),$$

v_{n_1} jak w przypadku wyżej. Wówczas

$$v_{n_1}(a) = n_1 a^{n_1-1} \neq 0,$$

bo $p \nmid n_1$. Jeśli a jest 1-krotnym pierwiastkiem $w_{n_1}(X)$, to jest on p^l -krotnym pierwiastkiem $w_n(X)$.

Twierdzenie 3.4. Niech $G < \mu(K)$ i G jest podgrupą skończoną o $|G| = n$. Wtedy

1. $G = \mu_n(K)$
2. G jest cykliczna
3. Jeśli $\text{char}(K) = p > 0$, to $p \nmid n$.

Dowód

1. Jeśli $|G| = n$, to dla każdego $x \in G$ mamy $x^n = 1$. Z tego wynika, że $G \subseteq \mu_n(K)$, ale $|\mu_n(K)| \leq n$, czyli $G = \mu_n(K)$.

2. Chcemy pokazać, że dla wielomianu $w_n(X)$ mamy n różnych pierwiastków. Wystarczy pokazać, że istnieje $x \in G$ taki, że $\text{ord}(x) = n$.

Założmy nie wprost, że dla każdego $x \in G$ $\text{ord}(x) < n$. Niech

$$k = \max\{\text{ord}(x) : x \in G\}.$$

Niech $x_0 \in G$ takie, że $\text{ord}(x_0) = k$. Wtedy

$$(\forall y \in G) \text{ord}(y) \mid k.$$

Gdyby tak nie było, to istniałby $y \in G$, $\text{ord}(y) \nmid k$. Czyli istnieje liczba pierwsza p taka, że l jest podzielne przez wyższą potęgę p niż k . To oznacza, że $l = p^\alpha l'$ i $k = p^\beta k'$, gdzie $p \nmid l'$ i $\alpha > \beta$.

Rozważmy $y' = y^l$. Skoro y ma rząd l , to $\text{ord}(y') = p^\alpha$, a dla $x'_0 = x_0^{p^\beta}$ mamy $\text{ord}(x') = k'$. Wobec tego $\text{ord}(x'_0 y') = p^\alpha \cdot k'$, ale to jest większe od k i dostajemy sprzeczność.

3. Wiemy, że wszystkie pierwiastki $w_n = x^n - 1$ są jednokrotne, bo jest ich w tym przypadku dokładnie n (z poprzedniego punktu). Z uwagi ??, że jeśli $n = p^l n_1$, to pierwiastki wielomianu $w_n(x)$ mają krotność p^l . Ale w tym przypadku pierwiastki mają krotność jeden, czyli $p^l = 1$ i $n = 1 \cdot n_1$, gdzie $p \nmid n_1$.

Wniosek 3.5. Jeśli $a \in \mu_n(K)$ jest pierwiastkiem pierwotnym z 1 stopnia $n > 1$, to a generuje $\mu_n(K)$.

Dowód:

$\mu_n(K) \supseteq \langle a \rangle = \mu_k(K)$ dla pewnego $k \in \mathbb{N}$. Ale ponieważ a było pierwiastkiem pierwotnym z 1, to musimy mieć $n = k$.

3.3 Ciała skończone

Twierdzenie 3.6. Niech K będzie ciałem skończonym. Wtedy

1. $\text{char}(K) = p \implies |K| = p^n$ dla pewnego $n \in \mathbb{N}$
2. Dla każdego $n > 0$ istnieje dokładnie jedno ciało K takie, że $|K| = p^n$ z dokładnością do izomorfizmu.

Ciało mocy p^n będziemy oznaczać $F(p^n)$.

Dowód:

1. Skoro $\text{char}(K) = p$, to $\mathbb{Z}_p \subseteq K$ jest najmniejszym podciałem prostym ciała K . W takim razie, K jest skończoną przestrzenią liniową nad \mathbb{Z}_p . Jeśli $n = \dim_{\mathbb{Z}_p}(K)$, to K jest izomorficzne z \mathbb{Z}_p^n , jako przestrzeń liniowa nad \mathbb{Z}_p . W takim razie $|K| = p^n$.

2.

Istnienie:

Niech $n > 0$. Rozważmy

$$w_{p^n-1}(x) = x^{p^n-1} \in \mathbb{Z}_p[X].$$

Niech $L \supseteq \mathbb{Z}_p$ będzie ciałem rozkładu wielomianu w_{p^n-1} , a $K = \{0\} \cup \{\text{pierwiastki } w_{p^n-1}\}$. Wtedy

$$|K| = 1 + p^n - 1 = p^n,$$

czyli mamy potencjalne ciało rzędu p^n . Wystarczy więc pokazać, że K jest ciałem.

Niech $f : L \xrightarrow{1-1} L$ będzie funkcją Frobeniusa $x \mapsto x^p$. Teraz niech $f^n = f \circ \dots \circ f$, $f^n(x) = x^{p^n}$. Jest to monomorfizm, bo składamy ze sobą n takich samych funkcji 1-1. Dla $a \in L$ mamy

$$(a^{p^n-1} = 1 \vee a = 0) \iff a \in K.$$

Co więcej, $a^{p^n-1} = 1 \iff a^{p^n} = a \iff f^n(a) = a$, czyli $K = \{a \in L : f^n(a) = a\}$ jest zbiorem punktów stałych morfizmu f^n , czyli jest ciałem, czego dowód jest pozostawiony na ćwiczenia.

Jedyność K:

Ciało K stworzone jak wyżej jest ciałem rozkładu $w_{p^n-1}(x)$ nad \mathbb{Z}_p .

Załóżmy nie wprost, że K' to inne ciało mocy p^n . Bez straty ogólności $\mathbb{Z}_p \subseteq K'$. Niech $x \in K'$. wiemy, że $x = 0$ lub $x^{p^n-1} = 1$. W takim razie w_{p^n-1} rozkłada się nad K' na czynniki liniowe. Zatem K' jest również ciałem rozkładu w_{p^n-1} nad \mathbb{Z}_p .

Z wniosku ??(2) mamy, że dwa ciała rozkładu nad jednym wielomianem są izomorficzne i $K \cong K'$ nad \mathbb{Z}_p i mamy sprzeczność.

Wykład: 4: Rozszerzenia ciał

Definicja 4.1. Niech $K \subseteq L$ będą ciałami i $a \in L \setminus K$.

\hookrightarrow Jeżeli a jest algebraiczny nad K , to istnieje $f \in K[X]$ stopnia > 0 i $f(a) = 0$

$\hookrightarrow a$ jest przestępny nad K [transcendental] $\iff a$ nie jest algebraiczny.

\hookrightarrow Rozszerzenie $L \supseteq K$ jest algebraiczne \iff dla każdego $a \in L$ a jest algebraiczny nad K .

\hookrightarrow Rozszerzenie jest przestępne \iff nie jest algebraiczne.

\hookrightarrow Niech $a \in \mathbb{C}$. Wtedy a jest algebraiczna, gdy a jest algebraiczna nad \mathbb{Q} .

Przykłady:

1. W \mathbb{C} na i jest pierwiastkiem algebraicznym wielomianu $x^2 + 1$, a $\sqrt[n]{d}$ jest pierwiastkiem $x^n - d$.
2. Ciało $F(p^n)$ ma charakterystykę p i $F(p) \subseteq F(p^n)$ jest rozszerzeniem ciał, które jest algebraiczne. Dla dowolnego $a \in F(p^n)$ to jest ono pierwiastkiem wielomianu $X^{p^n} - X$, czyli a jest algebraiczne nad $F(p)$.
3. Pierwiastki przestępne to na przykład e, π, E^π , aczkolwiek nie jesteśmy pewni tego ostatniego [doczytać w S. Lang, Algebra].
4. Rozważamy $K \subseteq L = K(X)$, czyli pierścień ułamków. Weźmy $x \in K(X)$ - przestępny nad K . Załóżmy, że istnieje wielomian $f \in K[X]$ różny od 0. I założmy, że $0 = \hat{f}(X)$ to funkcja wielomianowa.

$$0 = \hat{f}(X) = f \neq 0$$

i jest to sprzeczność.

Uwaga 4.2. Niech a jak wyżej. Wtedy a jest algebraiczny nad $K \iff I(a/K) \neq \{0\}$ jako ideał $K[X]$.

4.1 Wymiar przestrzeni liniowej

Niech $K \subseteq L$ będzie rozszerzeniem ciała K . Wtedy L jest przestrzenią liniową nad K . Definiujemy stopień rozszerzenia [coś innego jak indeks przy grupach]

$$[L : K] := \dim_K(L)$$

jako wymiar przestrzeni liniowej nad K .

Uwaga 4.3. Niech $a \in L \setminus K$. Następujące warunki są równoważne:

1. a jest algebraiczny nad K
2. $K[a] = K(a)$, to znaczy $K[a]$ jest ciałem (usuwanie niewymierności z mianownika)
3. $[K(a) : K] = \dim_K(a) < \infty$

Dowód:

$$1 \implies 2$$

Wiemy, że $K[X]$ jest euklidesowy (bo K to ciało), więc $K[X]$ jest też PID.

Skoro a jest algebraiczny nad K , to istnieje $f \in K[X]$ takie, że $f(a) = 0$, a więc

$$0 \neq I(\bar{a}/K) \triangleleft K[X]$$

czyli $I(a/K)$ jest maksymalnym ideałem głównym. Teraz, jeśli $I \triangleleft R$ jest ideałem maksymalnym pierścienia R , to R/I jest ciałem. Czyli

$$K[a] \cong K[X]/I(a/K)$$

jest ciałem.

2 \implies 3

Założmy, że $a \neq 0$. Wtedy $a^{-1} \in K[a]$, czyli istnieje wielomian $f \in K[X]$ taki, że

$$f(x) = \sum_{i=1}^n b_i x^i, \quad b_n \neq 0$$

i $a^{-1} = f(a)$. Wobec tego mamy

$$1 = f(a) \cdot a$$

$$0 = f(a)a - 1 = b_n a^{n+1} + b_{n-1} a^n + \dots + b_0 a - 1,$$

stąd mamy, że

$$a^{n+1} = -\frac{1}{b_n}(b_{n-1}a^n + \dots + b_0a - 1) \in \text{Lin}_K(1, a, \dots, a^n)$$

jest w domknięciu liniowym $(1, a, \dots, a^n)$. Indukcyjnie można pokazać, że

$$(\forall m \geq 0) a^m \in \text{Lin}_K(1, a, \dots, a^n),$$

czyli

$$K[a] = K(a) = \text{Lin}_K(1, a, \dots, a^n),$$

co daje, że $[K(a) : K] \leq n < \infty$.

3 \implies 1

$[K(a) : K] < \infty$, z czego wynika, że

$$\{1, a, \dots, a^n, \dots\} = \{a^t : t \in \mathbb{N}\} \subseteq K(a)$$

jest zbiorem liniowo zależnym. Z liniowej zależności wiemy, że

$$(\exists n \in \mathbb{N})(\exists b_{n-1}, \dots, b_0) a^n = b_{n-1}a^{n-1} + \dots + b_1a + b_0.$$

Stąd dla $f \in K[X]$ zadanego wzorem

$$f(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0$$

mamy $f(a) = 0$, zatem a jest algebraiczny nad K .

Niech $a \in L \supseteq K$ będzie algebraicznym pierwiastkiem nad K , $I(a/K) = \{w \in K[X] : w(a) = 0\} = (f)$, $f \neq 0$, $f \in K[X]$, f unormowany (czyli współczynnik przy wyrazie wiodącym jest 1?)

$\hookrightarrow f$ jest nazywany wielomianem **minimalnym** a nad K (wyznaczony jednoznacznie)

\hookrightarrow **stopień** a nad K jest definiowany jako $\deg(f)$.

Przykład:

1. $\sqrt{2} \in \mathbb{R} \supseteq \mathbb{Q}$, wtedy $f(x) = x^2 - 2$ jest wielomianem minimalnym $\sqrt{2}$ nad \mathbb{Q} i stopień $\sqrt{2}$ nad \mathbb{Q} jest równy 2.

2. $\pi \in \mathbb{R}$ nie ma stopnia, bo π nie jest liczbą algebraiczną nad \mathbb{Q}

3. $\sqrt[7]{7 + \sqrt[3]{3}} - \sqrt[6]{6} \in \mathbb{R}$, czy jest to algebraiczne nad \mathbb{Q} ? Tak i ma stopień 126.

Uwaga 4.4. Załóżmy, że $l(a/K) = (f)$ i f jest unormowany. Wówczas:

1. f jest unormowanym wielomianem minimalnego stopnia takim, że $f(a) = 0$
2. $\deg(f) = [K(a) : K]$, czyli stopień tego wielomianu jest równy stopniu przestrzeni liniowej $K(a)$ nad K .

Dowód:

Niech $n = \deg(f)$,

$$f(x) = x^n + \sum_{k < n} b_k x^k$$

Z tego, że $f(a) = 0$ mamy, że

$$a^n = - \sum_{k < n} b_k a^k \in \text{Lin}_K(1, a, \dots, a^{n-1}) \subseteq L.$$

Czyli $K(a) = \text{Lin}_K(1, a, \dots, a^{n-1})$ i wystarczy zobaczyć, że $\{1, \dots, a^{n-1}\}$ jest liniowo niezależny nad K , to znaczy jest bazą $K(a)$ nad K . Jest, bo f jest minimalnego stopnia.

Fakt 4.5. Niech $K \subseteq L \subseteq M$ będą rozszerzeniami ciał. Wtedy

$$[M : K] = [M : L] \cdot [L : K]$$

Dowód:

Niech $\{e_i : i \in I\}$ będzie bazą L nad K , a $\{f_j : j \in J\}$ będzie bazą M nad L . Stąd $|I| = [L : K]$ i $|J| = [M : L]$.

Chcemy za pomocą tych dwóch zbiorów zrobić bazę M nad K . Rozważmy zbiór

$$X = \{e_i \cdot f_j : i \in I, j \in J\}.$$

Musimy pokazać, że

1. $|X| = |I| \cdot |J|$
2. X jest liniowo niezależny
3. X jest bazą M nad K

Te dwa ostatnie mówią, że X jest bazą.

1. Załóżmy, nie wprost, że dla $i \neq i'$ i $j \neq j'$ i $e_i f_j = e_{i'} f_{j'}$. Czyli

$$e_i f_j - e_{i'} f_{j'} = 0,$$

czyli $f_j, f_{j'}$ są liniowo zależne nad L , czyli mamy, że $f_j = f_{j'}$ i

$$0 = e_i f_j - e_{i'} f_j = (e_i - e_{i'}) f_j \implies e_i - e_{i'} = 0 \implies i = i'$$

2. Załóżmy nie wprost, że X nie jest lnz, czyli istnieją $k_{ij} \in K$ takie, że

$$\sum_{j \in J} \sum_{i \in I} k_{ij} e_i f_j = 0,$$

ale $\sum_i k_{ij} e_i = l_j$ są elementami L , czyli

$$\sum_{j \in J} l_j f_j = 0$$

więc f_j są liniowo zależne, a przecież były bazowe, w takim razie

$$0 = l_j = \sum_{i \in I} k_{ij} e_i,$$

$e_i \neq 0$, czyli $k_{ij} = 0$ i koniec.

3. X generuje M nad K , bo dla $m \in M$ mam

$$m = \sum l_j f_j = \sum \left(\sum a_{ij} e_i \right) f_j = \sum \sum a_{ij} e_i f_j = \sum \sum k_{ij} e_i f_j$$