Algebra 2R

a voyage into the unknown

koteczek

~

Pomoce dydaktyczne: playlista z losowymi wykladami

SYLABUS:

I. Podstawy teorii równań algebraicznych

1. Rozszerzenia ciał. Rozszerzenia o pierwiastek wielomianu nierozkładalnego. Ciało rozkładu wielomianu: istnieje, jedyność.

2. Ciało algebraicznie domknięte: definicja. Każde ciało zawiera się w ciele algebraicznie domkniętym (konstrukcja). Podciało proste: istnienie, jedyność. Ciała proste.

3. Pierwiastki z jedności, pierwiastki pierwotne. Grupa pierwiastków z jedności w ciele: każda jej skończona podgrupa jest cykliczna. Wielomiany podziału koła. Funkcja Frobeniusa. Ciała skończone: własności.

II. Teoria Galois

1. Rozszerzenia [elementy] algebraiczne, przestępne: definicja. Stopień rozszerzenia. Warunki równoważne algebraiczności. Wielomian minimalny elementu ciała nad podciałem, własności.

2. Algebraiczne domknięcie ciała: definicja, istnienie, jedyność, własności (jednorodność). Istnienie rzeczywistych liczb przestępnych, liczby Liouville'a.

3. Rozszerzenia normalne: definicja, własności. Rozszerzenia [elementy, wielomiany] rozdzielcze. Twierdzenie Abela o elemencie pierwotnym. Rozszerzenia czysto nierozdzielcze (radykalne): definicja, własności. Stopień rozdzielczy [radykalny] rozszerzenia: definicja, własności.

Spis rzeczy niezbyt mądrych

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. Układy równań

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

Fakt 1.1.1. $\bar{a} = (a_1, \dots, a_n) \subseteq S$, *gdzie* S *jest rozszerzeniem pierścienia* R, *jest* *rozwiązaniem układu równań* $U \iff g(\bar{a}) = 0$ *dla każdego wielomianu* $g \in (f_1, \dots, f_m) \lhd R[X]$.

Dowód:

$\Longleftarrow$ 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.

$\Longrightarrow$ 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 kombinacką wielomianów $f_1, \dots, f_m$, która na $\bar{a}$ przyjmują 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 $S = R[\overline{X}]/(f_1, \dots, f_m)$ i rozważmy

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

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

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

i dlatego

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

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

Niech

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

czyli jako potencjalne rozwiązanie rozważamy zbiór obrazów wielomianów stopnia 1 przez wcześniej zdefiniowaną funkcję $j : R[\overline{X}] \to S$. 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

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

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

Uwaga 1.1.2. *Skonstruowane powyżej rozwiązanie* $\bar{a}$ *układu* U *ma następującą własność uniwersalności:*

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

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

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

$$\begin{tikzcd}
R \arrow[r, "\subseteq"] \arrow[d, "\subseteq"'] & R[\bar{a}] \subseteq S \arrow[dl, "h"] \\
R[\bar{a}'] \subseteq S' &
\end{tikzcd}$$

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 $I \triangleleft R[\bar{X}]$, czyli

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

Z twierdzenia o faktoryzacji wielomianów w pierścieniu od razu dostajemy od razu

$$R[X]$$

1.2. Ciała

Dla $K \subseteq L$ ciał i $a_1, \dots, a_n = \bar{a} \in L$ definiujemy ideał $I(\bar{a}/L)$ w $K[X_1, \dots, X_n]$ 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

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

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* $K[\bar{X}]$ (czyli najmniejsze ciało, że pierścień może być w nim zanurzony).

Przykład:

Dla $K = \mathbb{Q}, L = \mathbb{R}$ zachodzi:

$$K[\sqrt{2}] = \mathbb{Q}[\sqrt{2}] = \{q + p\sqrt{2} \ : \ q, p \in \mathbb{Q}\}$$

$$K[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$

$$K(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$$

to ostatnie to usuwanie niewymierności z mianownika.

Twierdzenie: Niech $K \subseteq L_1, K \subseteq L_2$ będą ciałami. Wybieramy $\{a_1, \dots, a_n\} \in L_1$ i $\{b_1, \dots, b_n\} \in L_2$. Wtedy następujące warunki są równoważne:

- $\hookrightarrow$ istnieje izomorfizm $\phi : K[a_1, \dots, a_n] \to K[b_1, \dots, b_n]$ taki, że $\phi \restriction K = id_K$ oraz $\phi(a_i) = b_i$.
- $\hookrightarrow$ $I(\bar{a}/K) = I(\bar{b}/K)$.

Dowodzik:

$K[\bar{a}] \cong K[\bar{b}] \implies I(\bar{a}/K) = I(\bar{b}/K)$

Niech $\omega \in K[\overline{X}]$. Wtedy $\omega \in I(\bar{a}/K)$ wtedy i tylko wtedy, gdy $\omega(\bar{a}) = 0$, to mamy z definicji $I(\bar{a}/K)$. Wiemy też, że $\phi(a) \in K[\overline{X}]$ wtedy, gdy $\omega(\phi(\bar{a})) = 0$, a ponieważ $\phi(\bar{a}) = \bar{b}$, to również $\omega(\bar{b}) = 0$ i mamy, że $\omega \in I(\bar{b}/K)$. Czyli izomorfizm między $K[\bar{a}] = K[\bar{b}]$ implikuje, że $I(\bar{a}/K) = I(\bar{b}/K)$.

$K[\bar{a}] \cong K[\bar{b}] \impliedby I(\bar{a}/K) = I(\bar{b}/K)$

Spróbujmy zdefiniować izomorfizm ϕ tak, że dla $\omega \in K[\overline{X}]$ mamy $\phi(\omega(\bar{a})) = \omega(\bar{b})$

1. ϕ jest homomorfizmem:

$$\phi(\omega(\bar{a}) \cdot v(\bar{a})) = f((\omega \cdot v)(\bar{a})) = (\omega \cdot v)(\bar{b}) = \omega(\bar{b}) \cdot v(\bar{b}) = \phi(\omega(\bar{a})) \cdot \phi(v(\bar{a}))$$

2. ϕ jest różnowartościowe:

$$\phi(\omega(\bar{a})) = \phi(v(\bar{a})) \iff \omega(\bar{b}) = v(\bar{b}) \iff (\omega - v)(\bar{b}) = 0 \iff \omega - v \in I(\bar{b}/K) = I(\bar{a}/K) \iff (\omega - v)(\bar{a}) = 0 \iff \omega(\bar{a})$$

3. ϕ jest dobrze zdefiniowane (czyli przyjmuje tylko jedną wartość dla jednego argumentu):

$$\omega(\bar{a}) - v(\bar{a}) = 0 \iff (\omega - v)(\bar{a}) = 0 \iff \omega - v \in I(\bar{a}/K) \iff \omega - v \in I(\bar{b}/K) \iff (\omega - v)(\bar{b}) = 0 \iff \omega(\bar{b}) - v(\bar{b}) = 0$$

Możemy teraz zapytać, czy każdy ideał w pierścieniu wielomianów $K[X]$ jest postaci $I(\bar{a}/K)$ dla pewnego $\bar{a} \in L \supset K$? Albo ogólniej, czy dla pierścienia przemiennego R z $1_R \neq 0_R$ oraz ideału $I = (f_1, \dots, f_m) = I(\bar{a}/R) \triangleleft R[X]$, czy istnieje nadpierścień S taki, że $1_S = 1_R$ i $0_S = 0_R$ oraz układ

$$f_1(\overline{x}) = \dots = f_m(\overline{m}) = 0$$

ma rozwiązanie w S? Takie rozwiązanie spełniałoby $\bar{a} \in S \iff (\forall\ g \in (f_1, \dots, f_m))\ g(\bar{a}) = 0$.

2. Równania w pierścieniach

2.1. Układy równań

Notacja: przez R, S oznaczamy pierścienie przemienne z $1 \neq 0$. Przez K, L oznaczamy ciała.

Niech $f_1, \dots, f_n \in R[X_1, \dots, X_n] = R[\overline{X}]$.

Problem: Czy istnieje rozszerzenie pierścieni z jednością $R \subseteq S$ takie, że układ $U : f_1(\overline{X}) = \dots = f_m(\overline{X}) = 0$ ma rozwiązanie w pierścieniu S?

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

Dowód: Rozważmy przypadki:

1. $(f_1, \dots, f_m) \ni b \neq 0$ i $b \in R$. Wtedy układ U jest sprzeczny i nie ma rozwiązania w żadnym pierścieniu rozszerzającym R, więc możemy ten przypadek odrzucić.

2. $(f_1, \dots, f_m) \cap R = \{0\}$, czyli negacja pierwszego przypadku. Teraz układ U jest niesprzeczny i skonstruujemy pierścień $S \supseteq R$ z jednością (czyli rozszerzenie pierścienia S) i rozwiązanie $\overline{a} \subseteq S$.

Niech $S = R[\overline{X}]/(f_1, \dots, f_m)$ i rozważmy $jR[\overline{X}] \to S$ ilorazowe. Po pierwsze zauważmy, że $j \restriction R$ jest $1-1$, bo

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

i dlatego

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

Z uwagi na ten izomorfizm utożsamiamy R z $j[R]$ i S jest więc rozszerzeniem pierścienia R.

Niech $\overline{a} = (a_1, \dots, a_m) = (j(X_1), \dots, j(X_m))$, czyli zbiór obrazów wielomianów stopnia 1 z peirścienia S. Wtedy $\overline{a}$ jest rozwiązaniem układu U w pierścieniu S. Oznaczmy funkcję wielomianową przez

$$\hat{f}_i(\overline{a}) = \hat{f}_i(j(X_1), \dots, j(X_m)) = j(\hat{f}_i(X_1, \dots, X_m)) = j(f_i) = 0$$

powyższe równości należy sprawdzić w ramach ćwiczenia.

Uwaga: Skonstruowane powyżej rozwiązanie $\overline{a}$ układu U ma następującą własność uniwersalności. Jeśli $S' \supseteq R$ jest rozszerzeniem pierścieni z 1 i $\overline{a}' = (a_1', \dots, a_n') \subseteq S$ jest rozwiązaniem U w S', to istnieje jedyny homomorfizm $h : R[\overline{a}] \to R[\overline{a}']$ taki, że $h \restriction R$ jest identycznością na R i $h(\overline{a}) = \overline{a}'$. Wszystkie rozwiązania układów sa homomorficzne.

$R[\overline{a}] \subseteq S$ to podpierścień generowany przez $R \cup \{\overline{a}\}$, czyli

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

Dowód: Niech $I = \{g \in R\overline{X} \ : \ g(\overline{a}') = 0\}$ w S'. Oczywiście $I \triangleleft R[\overline{X}]$. Znaczy to, że

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

z twierdzenia o faktoryzacji wielomianów w pierściueniu (????) dostajemy od razu

$$R[X] \xrightarrow{j} S = R[\overline{X}]/(f_1, \dots, f_m)$$

i $R[\overline{a}'] \subseteq S'$. Widzimy, że $I = \ker\phi \subseteq \ker j = (f_1, \dots, f_m)$. Z twierdzenia o homomorfizmie peirścieni dostajemy jedyne $h : R[X]/(f_1, \dots, f_m) \to R[\overline{a}']$ taki, że $h(\overline{a}) = \overline{a}'$.

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

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

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

II. $\bar{a}$: rozwiązanie ogólne układu U gdy ideał $I(\bar{a}/R) = (f_1, \ldots, f_m)$.

Uwaga: W sytuacji z definicji powyżej, gdy U jest niesprzeczne, wtedy $\bar{a}$ jest rozwiązaniem ogólnym układu U $\iff$ zachodzi warunek z gwizdką.

Dowód: ćwiczenia.

2.2. Ciała

$K \subseteq L$ i $\bar{a} \subseteq L$. Definiujemy ideał $\bar{a}$ nad K jako

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

Wtedy $K[\bar{a}]$ = podpierścień ciała L generowany przez $K \cup \{a_1, \ldots, a_m\} = \{g(\bar{a}) \ : \ g \in K[\bar{X}]$.

$K(\bar{a})$ to podciało ciała L generowane przez $K \cup \{a_1, \ldots, a_m\}$. Czyli jest to ciało ułamków pierścienia $K[\bar{a}]$ w ciele L. Inaczej piszemy $K[\bar{a}]_0$

$$K(\bar{a}) = \{g(\bar{a} \ : \ g \in K(\bar{X}) \text{ i } g(\bar{a}) \text{ jest dobrze określone})\}$$

Uwaga: Załóżmy, że $K \subseteq L_1, K \subseteq L_2$ są to rozszerzenia ciał i $\bar{a}_1 \subseteq L_1$, $\bar{a}_2 \in L_2$ i $|\bar{a}_1| = |\bar{a}_2| = n$. Wtedy następujące warunki są równoważne:

1. $(\exists\ f : K[\bar{a}_1] \xrightarrow{\cong} K[\bar{a}_2])\ f(\bar{a}_1) = \bar{a}_2$ i $f \restriction K = id_K$
2. $I(\bar{a}_1/K) = I(\bar{A}_2/K)$

Dowód:

$1 \implies 2$ jest jasne, bo dla $g(\bar{x}) \in K[\bar{x}]$ takie, że $g(\bar{a}_1) = 0$ w $K[\bar{a}_1] \iff g(f(\bar{a}_1)) = 0$ dla w $K[\bar{a}_2]$.

$\impliedby$ Zwróćmy uwagę na odwzorowanie ewaluacji $\bar{a}_1$

$$\phi_{\bar{a}_1} : K[\bar{X}] \xrightarrow{\text{epi}} K[\bar{a}_1]$$

mamy $\phi_{\bar{a}_1}(w(\bar{x})) = w(\bar{a}_1)$, czyli do wielomianu ϕ podstawia $\bar{a}_1$. Oczywiście,

$$\ker(\phi_{\bar{a}_1}) = I(\bar{a}_1/K) = I(\bar{a}_2/K) = \ker\phi_{\bar{a}_2}$$

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

Dowód: Patrz na poprzednie uwagi, których było już dość dużo.

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

Dowód: Niech $I \subseteq M \triangleleft K[X]$ będzie ideałem maksymalnym. Niech $L = K[\bar{X}]/M$, $j : K[\bar{X}] \to L$ ilorazowe, $M \cap K = \{0\}$, więc $j \restriction K : K \to L$ jest $1-1$, a więc

$$j \restriction K : K \xrightarrow{1-1} j[K] \subseteq L.$$

Utożsamiamy K z $j[K]$, to znaczy $K \subseteq L$. Niech $\bar{a} = (a_1, \ldots, a_n)$, $a_i = j(X_i) \in L$. $g(\bar{a}) = 0$ dla każdego $g(\bar{X}) \in M \subseteq I$.

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

Przykład:

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

2. $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i) = \mathbb{R}[z]$ dla każdej $z \in \mathbb{C} \setminus \mathbb{R}$.

Załóżmy, że $k \subseteq L_1$, $K \subseteq L_2$ to rozszerzenia ciała. Wtedy mówimy, że L_1 jest izomorficzne z L_2 nad K $[L_1 \cong_K L_2] \iff$ gdy istnieje izomorfizm $f : L_1 \to L_2$ taki, że $f \restriction K = id_K$.

Fakt:

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

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

Podpunkt pierwszy jest szczególnym przypadkiem podpunktu 2, gdy $\phi = id$.

Dowód:

1. $T(a_1/K) = (f) = I(a_2/K)$, stąd na mocy faktu 1.5 mamy $K(a_1) \cong_K K(a_2)$.

2. Popatrzmy najpierw na izomomfizm $K_1[X]]$xrightarrow[ϕ]$\cong K_2[X]$ Wtedy ten ϕ indukuje $K_1[X]/(f_1 \xrightarrow[\phi]{\cong} K_2[X]/(f_2)$, bo $\phi(f_1) = f_2$. Zatem

$$I(\bar{a}_i/K_i) = (f_i) \triangleleft K_i[X]$$

$$L_i = K_i(a_i) = K_i[a_i] \cong K_i[\overline{X}]/I(a_j/K_j)$$

Ciało $L \supseteq K$ jest **ciałem rozkładu** [decomposition field] 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.

Nie są warunkami równoważnymi, bo 1 może być spełnione przez coś większego niż 2, a my chcemy najmniejsze takie ciało.

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

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

1. istnieje L: ciało rozkładu f nad K,

2. ciało to jest jedyne z dokładnością do izomorfizmu nad K.

Dowód:

1. Dowód przez indukcję względem stopnia f.

$\deg(f) = 1 \implies L = K$ i jest OK

Załóżmy, że stopień $f > 1$ i teza zachodzi dla wszystkich wielomianów stopnia $< \deg(f)$ i wszystkich ciał K'. Teraz z wniosku 1.7. wiemy, że istnieje rozszerzenie ciała K, w którym wielomian f ma pierwiastek, powiedzmy a_0 to ten pierwastek:

$$K' = K(a_0)$$

w $K'[X]$ ma pierwastek a_0, więc dzieli się przez $(x - a_0)$, więc

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

gdzie $f_1 \in K'[X]$, $0 < \deg(f_1) < \deg(f)$. Z założenia indukcyjnego dla f_1 istnieje $L' = K'(a_1, \ldots, a_r)$ - ciało rozkładu wielomianu f_1 nad K'. Wtedy $L = K(a_0, \ldots, a_r)$ jest ciałek rozkładu f nad K.

2. Udowodnimy wersję ogólniejszą: Jeśli $\phi : K_1 \to K_2$ jest izomorfizmem nad ciałem i $f_i \in K_i[X]$ jest wielomianem stopnia > 0, $\phi(f_1) = f_2$, to wtedy istnieje $\psi : L_1 \to L_2$ izoorfizm nad ciałami rozkładu tych K_i.