

Algebra 2R

a voyage into the unknown

koteczek

~

Spis rzeczy niezbyt mądrych

1	Teoria równań algebraicznych	3
1.1	Układy równań	3
1.2	Rozszerzenia ciał	5

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 \bar{X} , czyli $R[X_1, \dots, X_n] = R[\bar{X}]$. Pojawia się problem: *czy istnieje rozszerzenie pierścienia 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 1.1.1. $\bar{a} = (a_1, \dots, a_n) \subseteq S$, 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 1.1.2. 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

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

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 1.1.3. 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 1.1.4. 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. Zasadniczy temat: ciała

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 1.2.1. 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

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

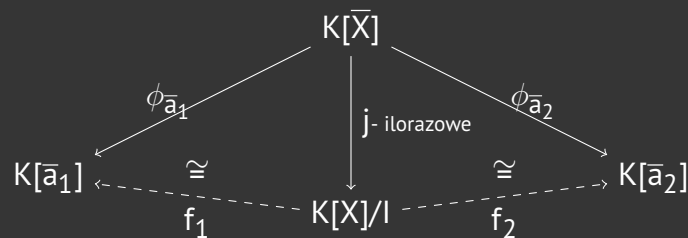
Mamy

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

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 1.2.2. 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: Wcześniejsze uwagi **KTÓRE KONKRETNIE?**

Twierdzenie 1.2.3. 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 1.2.4. 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 1.2.5.

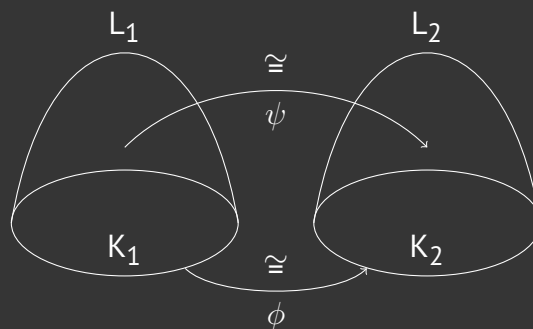
1. Załóżmy, że $f(X) \in K[X]$ jest nierozkładalny. Niech $L_1 = K(a_1)$, $L_2 = K(a_2)$ i $f(a_i) = 0$ w L_i . Wtedy $L_1 \cong_K L_2$.

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 1.2.1 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 $\phi : K_1[X] \xrightarrow[\cong]{K_2} K_2[X]$ 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

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

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

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 1.2.6. 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 1.2.4 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 $\phi : K_1 \rightarrow K_2$ jest izomorfizmem nad ciałem i $f_i \in K_i[X]$ jest wielomianem stopnia > 0 , $\phi(f_1) = f_2$, to wtedy istnieje $\psi : L_1 \rightarrow L_2$ izomorfizm nad ciałami rozkładu tych K_i .