Algebra 2R

a voyage into the unknown

koteczek

$\sim$

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

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

Dowód:

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

$\Longrightarrow$ Rozważamy dwa przypadki:

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

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

2. $(f_1, \ldots, f_m) \cap R = \{0\}$. (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 $\overline{a} \subseteq S$ spełniające nasz układ równań.

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

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

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

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

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

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

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

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

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* $\bar{a}' = (a_1', \ldots, a_m') \subseteq S$ *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 $I \lhd R[\bar{X}]$, a więc

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

Z twierdzenia o faktoryzacji wie

$$\begin{tikzcd}
R[\bar{X}] \arrow[r, "j"] \arrow[d, "\phi"'] & S = R[\bar{X}]/(f_1, \ldots, f_m) \arrow[dl, dashed, "(\exists\,!h)\ h(\bar{a}) = \bar{a}'"] \\
S' \supseteq R[\bar{a}'] &
\end{tikzcd}$$

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

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

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

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

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

Z twierdzenia o homomorfizmie pierścieni dostajemy jedyny homomorfizm

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

taki, że $h(\bar{a}) = \bar{a}'$.

Uwaga 1.1.3. *Jeśli* $I = (f_1, \ldots, f_m)$*, 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, $\mathrm{Im}\phi = \mathrm{Im}(h \circ j)$, a ϕ jest epimorfizmem ("na"), więc również h musi być "na".

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

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

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

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

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

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:

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

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

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

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 $K \cup \{\bar{a}\}$:

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

Tutaj $K(X_1, \ldots, X_n)$ 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* $\phi : K[\bar{a}_1] \to K[\bar{a}_2]$ *taki, że* $\phi \restriction K = id_K$ *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 $g(\overline{X}) \in K[\overline{X}]$, bo $g(\bar{a}_1) = 0$ w $K[\bar{a}_1] \iff g(f(\bar{a}_1)) = 0$, a $f(\bar{a}_1) = \bar{a}_2$.

$1 \Longleftarrow 2$

Zwróćmy uwagę na odwzorowanie ewaluacji $\overline{a}_1$

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

zadane wzorem

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

Mamy

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

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

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

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

$$\begin{tikzcd}
& K[\overline{X}] \arrow[dl, "\phi_{\overline{a}_1}"'] \arrow[d, "j\text{- ilorazowe}"] \arrow[dr, "\phi_{\overline{a}_2}"] & \\
K[\overline{a}_1] & K[X]/I \arrow[l, dashed, "\cong", "f_1"'] \arrow[r, dashed, "\cong"', "f_2"] & K[\overline{a}_2]
\end{tikzcd}$$

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

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

Uwaga 1.2.2. *Niech* $I \triangleleft K[\overline{X}]$ *noetherowskiego pierścienia* $K[\overline{X}]$. *Niech* $I = (f_1, \dots, f_m)$ *dla pewnych* $f_i \in K[\overline{X}]$. *Wtedy istnieje rozszerzenie pierścienia* $S \supseteq K$ *oraz* $\overline{a} \subseteq S$ *- rozwiązanie ogólne układu* $f_1(\overline{X}) = \dots = f_m(\overline{X}) = 0$ *takie, że* $I(\overline{a}/K) = I$.

Dowód: Wcześniejsze uwagi KTÓRE KONKRETNIE?

Twierdzenie 1.2.3. *Niech* $I \triangleleft K[\overline{X}]$. *Wtedy istnieje ciało* $L \supseteq K$ *oraz* $\overline{a} = (a_1, \dots, a_n) \subseteq L$ *takie, że* $f(\overline{a}) = 0$ *dla każdego* $f \in I$.

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

$$j : K[\overline{X}]/M \to L = K[\overline{X}]/M.$$

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

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

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

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

Wtedy $g(\overline{a}) = 0$ dla każdego $g(\overline{X}) \in M \supseteq I$ (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 $I = (f) \lhd \mathbb{Q}[X]$ 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.

Załóżmy, 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 $f : L_1 \to L_2$ taki, że $f \restriction K = id_K$.

Fakt 1.2.5.

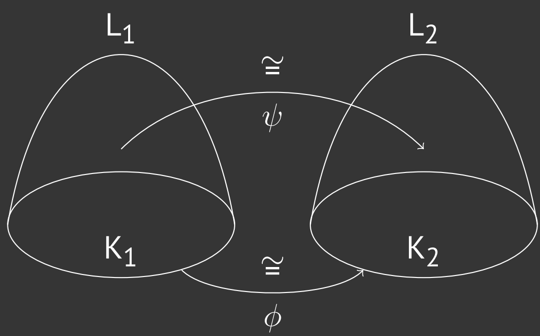
1. Załóżmy, że $f(X) \in K[X]$ *jest nierozkładalny. Niech* $L_1 = K(a_1)$, $L_2 = K(a_2)$ *i* $f(a_i) = 0$ *w* L_i. *Wtedy* $L_1 \cong_K L_2$.

2. Ogólniej: załóżmy, że $\phi : K_1 \to K_2$ *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* $\phi \in \psi : L_1 \to L_2$ *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. Zacznijmy od rozrysowania tej sytuacji:



Izomorfizm $\phi : K_1[X] \xrightarrow[K\ 2]{\cong} [X]$ 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

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

jest ideałem maksymalnym. Mamy

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

$$
\begin{tikzcd}
K_1[X] \arrow[rr, "\cong", "\phi"'] & {} \arrow[d] & K_2[X] \\
K_1[X]/(f_1) \arrow[rr, "\cong", "\phi"'] \arrow[d, "\cong"', "h_1"] & {} & K_2[X]/(f_2) \arrow[d, "\cong"', "h_2"] \\
L_1 = K_1(a_1) \arrow[rr, "\cong", "\psi"'] & & L_2 = K_2(a_2) \\
K_1 \arrow[u, phantom, "\cup|"] \arrow[rr, "\phi"'] & & K_2 \arrow[u, phantom, "\cup|"]
\end{tikzcd}
$$

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 $a_1, \ldots, a_n$, gdzie $a_1, \ldots, a_n$ 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 izomorfizmy nad K.*

Dowód:

1. Dowód przez indukcje względem stopnia f

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

Załóżmy teraz, że stopień wielomianu f jest > 1 i tez 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 $L' = K'(a_1, \ldots, a_r)$ - ciało rozkładu wielomianu f_1 nad K'. Wtedy

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

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 załóżmy, 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 1.2.5:(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 $\phi \subseteq \psi_0$.

$$\begin{tikzcd}
K_1(a_1) \arrow[r, "\cong", "\exists\, \psi_0"'] \arrow[d, equal] & K_2(a_2) \arrow[d, equal] \\
K_1' \arrow[d, phantom, sloped, "\subseteq"] & K_2' \arrow[d, phantom, sloped, "\subseteq"] \\
L_1 \arrow[r, "\cong", "\exists\, \psi_1"'] & L_2
\end{tikzcd}$$

Mamy, 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 1.2.7. *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 .