Algebra 2R

a voyage into the unknown

koteczek

$\sim$

Spis rzeczy niezbyt mądrych

1. 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 $f_1, \ldots, f_m \in R[X_1, \ldots, X_n]$. 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. $\overline{a} = (a_1, \ldots, a_n) \subseteq S$, *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

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

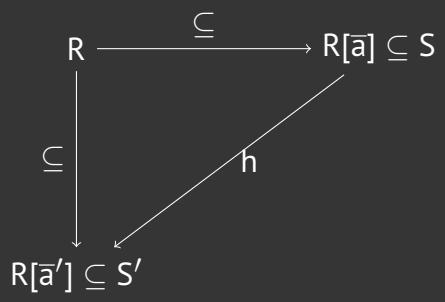
TUTAJ TRZEBA POUZASADNIAĆ KILKA RÓWNOŚCI, ALE MOŻE NIE BĘDĘ TEGO ROBIŁA NA AISD

Uwaga 1.2. *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.*



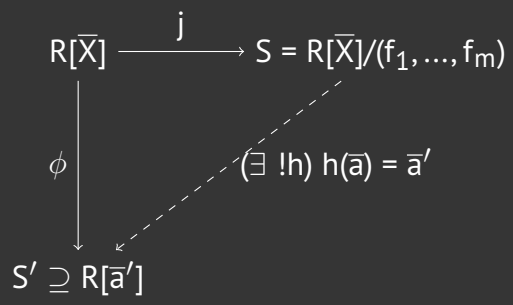
Tutaj $R[\bar{a}] \subseteq S$ **jest podpierścieniem generowanym przez** $R \cup \{\bar{a}\}$, czyli zbiór:

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

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



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 1.3. *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

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

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

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

Uwaga 1.4. *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:

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

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

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

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 1.5. *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* $\phi : K[\bar{a}_1] \to K[\bar{a}_2]$ *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 $g(\bar{X}) \in K[\bar{X}]$, bo $g(\bar{a}_1) = 0$ w $K[\bar{a}_1] \iff g(f(\bar{a}_1)) = 0$, a $f(\bar{a}_1) = \bar{a}_2$.

$1 \Longleftarrow 2$

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

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

zadane wzorem

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

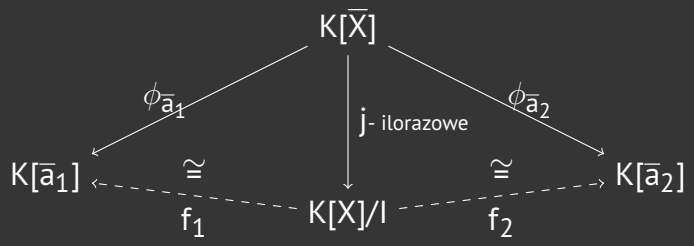
Mamy

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

Tak samo dla $\bar{a}_2$ możemy określić analogicznie odwzorowanie ewaluacyjne $\phi_{\bar{a}_2} : K[\bar{X}] \to K[\bar{a}_2]$. 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 $\phi_{\bar{a}_i} \restriction K = id_k$.



Niech $f = f_2 f_1^{-1} : K[\bar{a}_1] \to K[\bar{a}_2]$ 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* $I = (f_1, \ldots, f_m)$ *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: Wcześniejsze uwagi KTÓRE KONKRETNIE?

Twierdzenie 1.6. *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 $I \subseteq M \triangleleft K[\bar{X}]$ będzie ideałem maksymalnym. Niech $L = K[\bar{X}]/M$ i określmy przekształcenie ilorazowe

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

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

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

Możemy utożsamić K z j[K], czyli $K \subseteq L$. Niech $\bar{a} = (a_1, \ldots, a_n)$ 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 $I = (f) \lhd \mathbb{Q}[X]$ 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 $f \restriction K = \mathrm{id}_K$.

Fakt 1.8.

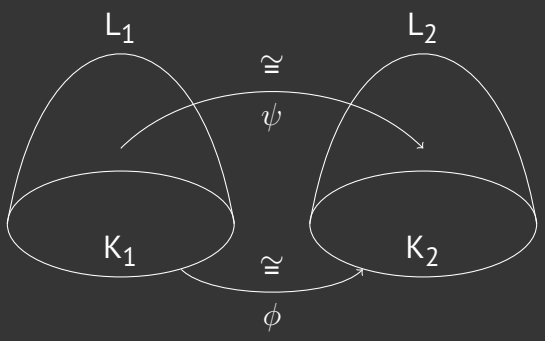
1. Załóżmy, że $f(X) \in K[X]$ *jest nierozkładalny. Niech* $L_1 = K(a_1)$, $L_2 = K(a_2)$ *i* $f(a_i) = 0$ *w* L_i. *Wtedy* $L_1 \cong_K L_2$.

2. Ogólniej: załóżmy, że $\phi : K_1 \to K_2$ *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 1.5 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

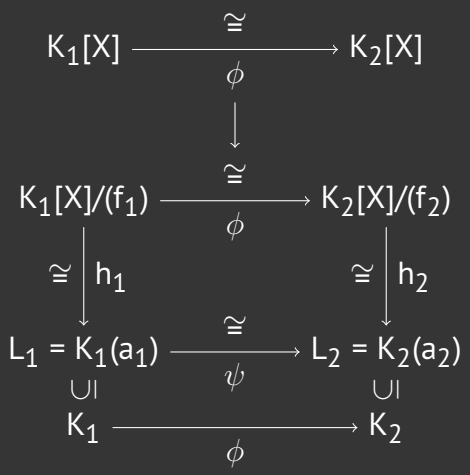
$$K_1[X]/(f_1) \xrightarrow[\phi]{\cong} K_2[X]/(f_2),$$

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

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


$K_1[X]$
$\cong$
$K_2[X]$
ϕ
$K_1[X]/(f_1)$
$\cong$
$K_2[X]/(f_2)$
ϕ
$\cong$
h_1
$\cong$
h_2
$L_1 = K_1(a_1)$
$\cong$
$L_2 = K_2(a_2)$
ψ
$\cup$
$\cup$
K_1
K_2
ϕ

2. 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 $a_1, \ldots, a_n$, gdzie $a_1, \ldots, a_n$ to wszystkie pierwiastki f w L.

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

Wniosek 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 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 1.7 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 1.8:(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 $\phi \subseteq \psi_0$.

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

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 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 zawiera się w pewnym ciele algebraicznie domkniętym.*

Dowód:

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

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

$$\{f \in K[X] \ : \ \deg(f) > 0\} = \{f_\alpha \ : \ \alpha \subset x\}$$

Skonstruujmy rosnący ciąg ciał $\{K_\alpha \ : \ \alpha \subset x\}$ taki, że

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

Załóżmy, że $\alpha < x$ i mamy $\{K_\beta \ : \ \beta < \alpha\}$.

1. α to liczba graniczna, wtedy $K_\alpha = \bigcup\limits_{\beta<\alpha}^{\uparrow} K_\beta$

2. $\alpha = \beta + 1$ to następnik, wtedy $K_\alpha = K_\beta(a)$, gdzie a to pierwiastek wielomianu f_β.

Czyli lemat jest prawdziwy.

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

$\hookrightarrow L_0 = K$

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

Niech

$$\hat{K} = L_\infty = \bigcup_{n<\omega}^{\uparrow} L_n.$$

Jest to ciało, ponieważ suma rosnącego ciągu ciał jest ciałem. Dalej mamy, że również

$$L[X] = \bigcup_{n<\omega}^{\uparrow} L_n[X]$$

i L[X] jest algebraicznie domknięte.

Uwaga 2.4. *Załóżmy, że mamy ciała* $K \subseteq L$. *Wtedy*

$\hookrightarrow char(K) = char(L)$

$\hookrightarrow 0_K = 0_L$ *oraz* $1_K = 1_L$

$\hookrightarrow K^* = K \setminus \{0\} < L^* = L \setminus \{0\}$

2.2. Pierwiastki z jedności

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

Przykład:

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

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

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

1. $a \in R$ jest **pierwiastkiem z** 1 stopnia $n > 0 \iff a^n = 1$
2. $\mu_n(R) = \{a \in R\ :\ a^n = 1\}$ jest **grupą pierwiastków z** 1 stopnia n
3. $\mu(R) = \bigcup_{n>0} \mu_n(R)$ jest **grupą pierwiastków z** 1
4. a jest **pierwiastkiem pierwotnym** stopnia n z $1 \iff a \in \mu_n(R)$ oraz $(\forall\ k < n) a \notin \mu_k(R)$.

Uwaga 2.5.

1. $\mu_n(R) \triangleleft R^X$ *jest grupą jednostek pierścienia*

2.$\mu(R) \triangleleft R^X$

3. $\mu(R)$ *jest torsyjną grupą abelową (każdy element jest pierwiastkiem z* 1*).*

Przykłady

1. $\mu(\mathbb{C}) = \bigcup_{n>0} \mu_n(\mathbb{C}) \lneq (\{z \in \mathbb{C}\ :\ |z| = 1\}, \cdot) < \mathbb{C}^x = C \setminus \{0\}$
2. $\mu(\mathbb{C}) \cong (\mathbb{Q}, +)/(\mathbb{Z}, +)$, bo $f : \mathbb{Q} \xrightarrow[\text{homo}]{\text{"na"}} \mu(\mathbb{C})$ taki, że $f(w) = \cos(w2\pi) + i\sin(w2\pi)$ ma jądro $\ker(f) = \mathbb{Z}$.

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

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

Uwaga 2.6.

1. Jeśli $\text{char}(K) = 0$*, to* $w_n(x) = x^n - 1$ *ma tylko pierwiastki jednokrotne w* K

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

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

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

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

Fakt 2.7. *Załóżmy, że* $\text{char}(K) = p > 0$*. Wtedy funkcja* $f : K \to K$ *taka, że* $f(x) = x^p$ *jest homomorfizmem ciał oraz monomorfizmem zwanym* ***funkcją Frobeniusa****.*

Uwaga 2.8. $x \mapsto x^p$ *nie musi być funkcją "na" (automorfizmem). Na przykład* $K = \mathbb{Z}_p(f)$*, wtedy* $x \mapsto x^p$ *nie jest "na".*

2. Mając powyższy fakt i uwagę z tyłu, przechodzimy do dowodu 2.

Niech $f : K[X] \to K[X]$, $f(h(x)) = w(x)^p$ i

$$f(\sum a_k x^k) = \sum a_k^p x^{n \cdot p}$$

Z faktu wyżej mamy, że f jest $1 - 1$. Ponieważ $n = p^l n_1$, to mamy

$$w_n(x) = x^n - 1 = x^n - 1^n = (x^{n_1})^{p^l} - (1^{n_1})^{p^l} = \ldots l \text{ razy} \ldots = (x^{n_1} - 1)^{p^l} = \underbrace{w_{n_1} \cdot \ldots \cdot w_{n_1}}_{p^l},$$

zatem każdy pierwiastek $w_n(x)$ ma krotność co najmniej p^l. Wystarczy więc pokazać, że każdy pierwiastek $w_{n_1}(x)$ jest jednokrotny.

Niech $a \in K$ takie, że $w_{n_1}(a) = 0$. Wtedy

$$w_{n_1}(x) = x^{n_1} - a^{n_1} = (x - 1)(x^{n_1 - 1} + \ldots + a^{n_1 - 1}) = (x - a)v_{n_1}(x),$$

gdzie v_{n_1} jest analogiczne jak w dowodzie 1. Ale przecież $v_{n_1}(a) = n_1 \cdot a^{n_1 - 1} \neq 0$, bo $p \nmid n_1$.

Twierdzenie 2.9. *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. Wystarczy pokazać, że istnieje $x \in G$ taki, że $\text{rank}(x) = n$.

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

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

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

$$(\forall\ y \in G)\ \text{rank}(y) | k.$$

Czyli

$$(\forall\ y \in G)\ y^k = 1,$$

co pociąga $G \subseteq \mu_k(K)$ i $|G| \leq k < n$. 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 2.6, 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 2.10. *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 $n = k$.

Twierdzenie 2.11. *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 K. W takim razie, K jest przestrzenią liniową nad $\mathbb{Z}_p$. Jeśli $n = \dim_{\mathbb{Z}_p}(K)$, to K jest izomorficzne z $\mathbb{Z}_p^n$, jako przestrzenie liniowe 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 $K = \{0\} \cup \{$ 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 $f^n = f \circ \ldots \circ f$, $f^n(x) = x^{p^n}$. Jest to monomorfizm, bo składamy ze sobą n takich samych funkcji 1 – 1. Dla $a \in L$ mamy

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

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.

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. Niech $x \in K' \setminus \{0\}$. wiemy, że $x^{p^n-1} = 1$, czyli w_{p^n-1} rozkłada się nad K' na czynniki liniowe. Zatem K' jest również ciałem rozkładu w_{p^n-1} nad $\mathbb{Z}_p$, stąd $K \cong K'$ nad $\mathbb{Z}_p$ i mamy sprzeczność.

2.3. Rozszerzenia ciał

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

- ↪ Jeżeli a jest algebraiczny nad K, to istnieje $f \in K[X]$ stopnia > 0 i $f(a) = 0$
- ↪ a jest przestępny nad K $\iff$ a nie jest algebraiczny.
- ↪ **Rozszerzenie** $L \supseteq K$ jest **algebraiczne** $\iff$ dla każdego $a \in L$ a jest algebraiczny nad K.
- ↪ **Rozszerzenie jest przestępne** $\iff$ nie jest algebraiczne.
- ↪ Niech $a \in \mathbb{C}$. Wtedy a jest algebraiczna, gdy a jest algebraiczna nad $\mathbb{Q}$.

Uwaga 2.12. *Niech* a *jak wyżej. Wtedy* a *jest algebraiczny nad* K $\iff I(a/K) \neq \{0\}$.

Niech $K \subseteq L$ będzie rozszerzeniem ciała K. Wtedy L jest **przestrzenią liniową nad** K. Definiujemy

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

jako wymiar przestrzeni liniowej.

Uwaga 2.13. *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:

$1 \implies 2$