Algebra 2R

a voyage into the unknown

koteczek

$\sim$

Spis rzeczy niezbyt mądrych

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* $g \in (f_1, \ldots, f_m) \triangleleft R[X]$.

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) $\widehat{f_i} \in (f_1, \ldots, f_m)$ mamy

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

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 $\bar{a}' = (a'_1, \dots, a'_m) \subseteq S$ 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 $I \lhd R[\bar{X}]$, a więc

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

Z twierdzenia o faktoryzacji wie

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

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

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

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

Z twierdzenia o homomorfizmie pierścieni dostajemy jedyny homomorfizm

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

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, $\mathrm{Im}\phi = \mathrm{Im}(h \circ j)$, 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 1.4. *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:
$$I(\bar{a}/L) := \{f(X_1, \ldots, X_n) \in K[\overline{X}] : f(\bar{a}) = 0\},$$
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 1.5. *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* $\phi \restriction K = \mathrm{id}_K$ *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 $\bar{a}_1$

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

zadane wzorem

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

Mamy

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

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

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

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

Dowód: Uwaga 1.4.

Twierdzenie 1.6. *Niech* $I \lhd K[\overline{X}]$. *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 $I \subseteq M \lhd K[\overline{X}]$ 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 $j \restriction K : K \to L$ 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 $g(\overline{X}) \in M \supseteq I$ (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.

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 1.8.

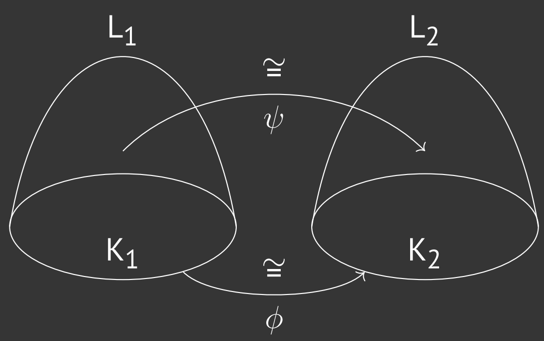
1. Załóżmy, że $f(X) \in K[X]$ *jest nierozkładalny. Niech* $L_1 = K(a_1)$, $L_2 = K(a_2)$ *i* $f(a_i) = 0$ *w* L_i. *Wtedy* $L_1 \cong_K L_2$.

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

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

jest ideałem maksymalnym. Mamy

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

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

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 $\phi \subseteq \psi_0$.

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

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_α ma pierwiastek w $K_{\alpha+1}$.

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

Załóżmy, że $\alpha < \kappa$ i mamy $\{K_\beta : \beta < \alpha\}$ spełniają warunki powyżej. Niech $K' = \bigcup\limits^{\uparrow}_{\beta<\alpha} K_\beta$. Musimy pokazać, że K' jest ciałem.

1. α to liczba graniczna. Definiujemy $K' = \bigcup\limits^{\uparrow}_{\beta<\alpha} K_\beta$ 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 1.7 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:

$$L = \bigcup^{\uparrow}_{\alpha<\kappa} K_\alpha$$

i to ciało spełnia nasz lemat.

Wracamy teraz do dowodu twierdzenia 2.3 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 w L_{n+1}.

Niech

$$L_\infty = \bigcup^{\uparrow}_{n<\omega} L_n \supseteq K.$$

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*

- $\hookrightarrow$ $\mathrm{char}(K) = \mathrm{char}(L)$
- $\hookrightarrow$ $0_K = 0_L$ *oraz* $1_K = 1_L$
- $\hookrightarrow$ $K^* = K \setminus \{0\} < L^* = L \setminus \{0\}$ oraz dla $x \in K$ $-x$ w K jest równe $-x$ w L.

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

Przykład:

- $\hookrightarrow$ $\mathbb{Q}$, gdzie $\mathrm{char}(\mathbb{Q}) = 0$ to ciało proste nieskończone.
- $\hookrightarrow$ Ciałem prostym skończonym jest na przykład $\mathbb{Z}_p$ dla liczby pierwszej p, wtedy $\mathrm{char}(\mathbb{Z}_p) = p$.

Uwaga 3.1.

1. *Każde ciało zawiera jedyne podciało proste*
2. *Z dokładnościa 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. $a \in R$ 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. $\mu(R) = \{a \in R \ : \ (\exists\, n)\ a^n = 1\} = \bigcup\limits_{n>0} \mu_n(R)$ jest **grupą pierwiastków z 1**
4. a jest **pierwiastkiem pierwotnym** [primitive root] stopnia n z 1 $\iff$ $a \in \mu_n(R)$ oraz dla każdego $k < n$ $a \notin \mu_k(R)$.

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. $\mu(\mathbb{C}) = \bigcup\limits_{n>0} \mu_n(\mathbb{C}) \lneq (\{z \in \mathbb{C} \ : \ |z| = 1\}, \cdot) < \mathbb{C}^* = C \setminus \{0\}$ jest nieskończona.
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. $\mu_n(K) = \{$zera wielomianu $x^n - 1\}$. Ten wielomian będziemy oznaczali $w_n(x) = x^n - 1$.

Uwaga 3.3.

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

2. *Jeśli* $\mathrm{char}(K) = p > 0$ *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 $\mathrm{char}(K) = 0$ 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 $\mathrm{char}(K) = p$. Niech $n = p^l n_1$. Rozważmy wielomian

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

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* $\mathrm{char}(K) = p > 0$*, 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 $\mathrm{ord}(x) = n$.

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

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

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

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

Gdyby tak nie było, to istniałby $y \in G$, $\mathrm{ord}(y) \nmid k$. 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 $\mathrm{ord}(y') = p^\alpha$, a dla $x_0' = x_0^{p^\beta}$ mamy $\mathrm{ord}(x') = k'$. Wobec tego $\mathrm{ord}(x_0'y') = p^\alpha \cdot k'$, 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 3.3, 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. $\mathrm{char}(K) = p \implies |K| = p^n$ *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 $\mathrm{char}(K) = p$, 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 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
$$(a^{p^n-1} = 1 \ \vee\ a = 0) \iff a \in K.$$
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. Bes 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 2.1.(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* $a \in L \setminus K$.

- *Jeżeli a jest algebraiczny nad K, to istnieje* $f \in K[X]$ *stopnia* > 0 *i* $f(a) = 0$
- a *jest przestępny nad* K *[transcendental]* $\iff$ 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* $\mathbb{Q}$.

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 $f \in K[X]$ rózny od 0. I załóżmy, że $0 = \widehat{f}(X)$ to funkcja wielomianowa.

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

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 $I \lhd R$ jest ideałem maksymalnym pierścienia R, to R/I jest ciałem. Czyli

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

jest ciałem.

$2 \implies 3$

Załóżmy, 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

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

$$0 = f(a)a - 1 = b_n a^{n+1} + b_a a^2 + \ldots + b_0 a - 1,$$

stąd mamy, że

$$a^{n+1} = -\frac{1}{b_n}(b_{n-1}a^n + \ldots + b_0 a - 1) \in Lin_K(1, a, \ldots, a^n)$$

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

$$(\forall\ m \geq 0)\ a^m \in Lin_K(1, a, \ldots, a^n),$$

czyli

$$K[a] = K(a) = Lin_K(1, a, \ldots, a^n),$$

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

$3 \implies 1$

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

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

jest zbiorem liniowo zależnym. Z liniowej zależności wiemy, że

$$(\exists\ n \in \mathbb{N})(\exists\ b_{n-1}, \ldots, b_0)\ a^n = b_{n-1}a^{n-1} + \ldots + b_1 a + b_0.$$

Stąd dla $f \in K[X]$ zadanego wzorem

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

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* $I(a/K) = (f)$ *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

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

Czyli $K(a) = \mathrm{Lin}_K(1, a, \dots, a^{n-1})$ 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 zbiorków 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 $\sum_i k_i j e_i = l_j$ 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

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

Z tego wynika, że $[M : K] = |X| = |I||J| = [L : K][M : L]$.

Wniosek 4.6. *Niech $K \subseteq L$ będzie rozszerzeniem skończonego ciała. Niech*

$$K^{alg}(L) = \{a \in L \ : \ a \textit{ jest algebraiczny nad } K\}.$$

Okazuje się, że K^{alg} jest podciałem.

Dowód:

Weźmy $a, b \in K^{alg}$. Wiemy, że $[K(a) : K]$ i $[K(b) : K]$ są skończone. Mamy, że

$$K \subseteq K(a) \subseteq K(a, b)$$

Z faktu 4.5 wiemy, że

$$[K(a, b) : K] = [K(a, b) : K(a)] \cdot [K(a) : K]$$

czyli również $K(a, b)$ jest skończone. Zatem dla $x \in K(a, b)$ mamy

$$[K(x) : K] \leq [K(a, b) : K]$$

też jest skończone, zatem x jest algebraiczny nad K.

Dla $x \in K(a, b)$ mamy $[K(x) : K] \leq [K(a) : K]$, czyli również jest skończone. W takim razie, x jest algebraiczny nad K i należy do K^{alg}.

Definicja 4.7.

1. $K^{alg}(L)$ *nazywamy* ***algebraicznym domknięciem*** K *w* L.
2. K *jest* ***relatywnie algebraicznie domknięte*** *w* L $\iff$ $K^{alg}(L) = K$.

Wniosek 4.8.

- *Niech* $K \subseteq L \subseteq M$ *będą rozszerzeniami ciał.* $K \subseteq M$ *jest algebraiczne* $\iff$ $K \subseteq L$ *i* $L \subseteq M$ *są algebraiczne*
- $K^{alg}(L)$ *jest relatywnie algebraicznie domknięte w* L, *tzn.* $K^{alg}(L) = [K^{alg}(L)]^{alg}(L)$

4.2 Wielomian rozkładu koła

Rozważamy wielomian

$$w_m(x) = x^m - 1$$

dla $m \in \mathbb{N}$. Wiemy, że

$\hookrightarrow$ pierwiastki w_m w $\mathbb{C}$ są jednokrotne

$\hookrightarrow$ $\mu_m(\mathbb{C})$ jest grupą cykliczną

$\hookrightarrow$ $a \in \mu_m(\mathbb{C})$ jest generatorem $\mu_m(\mathbb{C}) = \{a^i \ : \ 0 \leq i \leq m\} \cong (\mathbb{Z}_m, +)$

$\hookrightarrow$ a^k generuje $\mu_m(\mathbb{C}) \iff NWD(k, m) = 1$

Zatem $\mu_m(\mathbb{C})$ ma $\phi(m)$ generatorów.?????

Niech

$$\{k \in \mathbb{N} \ : \ 0 < k < m, NWD(k, m) = 1\} = \{m_1, \ldots, m_{\phi(n)}\}$$

i zdefiniujmy

$$F_m(x) := (x - a^{m_1})\ldots(x - a^{m_{\phi(n)}}) \in \mathbb{C}[X]$$

Uwaga 4.9.

1. $w_m(x) = x^m - 1 = F_m(x) \cdot \prod_{\substack{d<m \\ d|m}} F_d(x)$
2. $F_m(x) \in \mathbb{Z}[X]$

Dowód:

1. Wiemy, że wielomian jest iloczynem dwumianów $x-$*pierwiastek*, te dla $w_m(x)$ są schowane w $\mu_m(\mathbb{C})$, czyli

$$w_m(x) = \prod_{b \in \mu_m(\mathbb{C})} (x - b) = \prod_{d|m} \prod_{\substack{b \in \mu_m(\mathbb{C}) \\ ord(b)=d}} (x - b) = \prod_{d|m} F_d(x) = F_m(x) \prod_{\substack{d<m \\ d|m}} F_d(m)$$

2. Dowód przez indukcję względem m. Dla $m = 1$ mamy $F_m(x) = x - 1 \in \mathbb{Z}[X]$. Teraz zakładamy, że dla $d < m$ jest $F_d(x) \in \mathbb{Z}[X]$. Z punktu (1) wiemy, że

$$x^m - 1 = w_m(x) = F_m(x)v_m(x)$$

z założenia indukcyjnego $v_m(x) \ \in \ \mathbb{Z}[X]$, bo każdy z nich ma stopień mniejszy niż m i $v_m(x)$ jest unormowany.

$w_m(x)$ dzielimy z resztą w $\mathbb{Z}[X]$ i dostajemy:

$$w_m(x) = v_m(x) \cdot L(x) + R(x)$$

ale w $\mathbb{C}[X] \supseteq \mathbb{Z}[X]$ było

$$w_m(x) = v_m(x) \cdot F_m(x),$$

czyli

$$F_m(x)v_m(x) = v_m(x)L(x) + R(x)$$
$$R(x) = v_m(x)[F_m(x) - L(x)]$$

ale $\deg(R) < \deg(v)$, czyli $R = 0$ i $F_m = L \in \mathbb{Z}[X]$.

Uwaga 4.10. $F_m(x)$ *jest wielomianem nierozkładalnym w* $\mathbb{Q}[X]$.

Dowód:

Po pierwsze zauważmy, że F_m jest nierozkładalny w $\mathbb{Q}[X] \iff$ nierozkładalny w $\mathbb{Z}[X]$.

Załóżmy nie wprost, że

$$F_m(x) = G_1(x) \cdot G_2(x)$$

dla $G_1, G_2 \in \mathbb{Z}[X]$. Możemy założyć, że $G_1(x)$ jest dalej nierozkładalny w $\mathbb{Z}[X]$ oraz $0 < \deg(G_1) < \deg(F_m) = \phi(m)$

Lemat: Istnieje b-pierwiastek pierwotny stopnia n oraz liczba pierwsza p taka, że $p \nmid m$ i $G_1(b) = G_2(b^p) = 0$.

Dowód lematu:

Z tego, że $0 < \deg(G_1)$ i $G_1 | F_m$, $0 < \deg(G_2)$ i $G_2 | F_m$ mamy, że istnieje pierwiastek pierwotny b stopnia m taki, że $G_1(b) = 0$ oraz pierwiastek pierwotny b' stopnia m taki, że $G_2(b') = 0$. Zatem istnieje $k \in \mathbb{N}$, $NWD(k, m) = 1$ takie, że $b' = b^k$, bo grupa $\mu_m(\mathbb{C})$ jest cykliczna i b jest jej generatorem.

Niech $k = p_1 \cdot \ldots p_s$ będzie rozkładem na liczby pierwsze. Wtedy mamy ciąg różnych liczb

$$b, b^{p_1}, b^{p_1 p_2}, \ldots, b^{p_1, \ldots, p_s} = b^k$$

które są pierwiastkami pierwotnymi stopnia m. Z tego wynika, że każda z tych liczb jest pierwiastkiem G_1 lub G_2, czyli istnieje taka pozycja i, że

$$G_1(b^{p_1 \cdots p_i}) = 0,$$

$$G_2(b^{p_1 \cdots p_{i+1}}) = 0$$

wtedy $b := b^{p_1 \cdots p_i}$ oraz $p = p_{i+1}$ i lemat jest spełniony.

Wimy już, że $G_1(b) = 0$ i $G_1 \in \mathbb{Z}[X]$ jest wielomianem nierozkładalnym. Niech p będzie liczbą pierwszą z lematu. Rozważmy

$$G_3(x) = G_2(x^p).$$

Wtedy $G_2(b^p) = G_3(b) = 0$, ale stąd wynika, że $G_1(x)$ dzieli $G_3(x)$. Niech więc

$$G_3(x) = G_1(x)H(x) \in \mathbb{Z}[X].$$

Rozważmy homomorfizm

$$f : \mathbb{Z} \to \mathbb{Z}_p$$

i indukowany przez niego

$$\bar{f} : \mathbb{Z}[X] \to \mathbb{Z}_p[X].$$

Z założenia $F_m = G_1 G_2$ mamy, że

$$\bar{f}(F_m) = \bar{f}(G_1)\bar{f}(G_2)$$

a z rozumowania powyżej ($G_3 = G_1 H$)

$$\bar{f}(G_3) = \bar{f}(G_1)\bar{f}(H)$$

ale

$$\bar{f}(G_3(x)) = \bar{f}(G_2(x^p)) = \bar{f}(G_2(x))^p,$$

bo współczynniki $f(G_2(x^p))$ są w $\mathbb{Z}_p$, a $(\sum c_i x^i)^p = \sum c_i x^{pi}$, bo $c_i^{kp} = c_i^k$ dla $c_i \in \mathbb{Z}_p$.

Stąd wiemy, że

$$f(G_2(x))^p = \bar{f}(G_1)\bar{f}(H).$$

Pierścień $\mathbb{Z}_p[X]$ jest UFD, więc $\bar{f}(G_1)$ i $\bar{f}(G_2)$ mają wspólny dzielnik w $\mathbb{Z}_p[X]$, stopnia co najmniej 1. Zatem z

$$\bar{f}(F_m) = \bar{f}(G_1)\bar{f}(G_2)$$

ma co najmniej pierwiastek wielokrotny. Jest to sprzeczność, bo nie mogą istnieć pierwiastki wielokrotne: $\bar{f}(F_m) | x^m - 1 = w_m$, a $x^m - 1$ ma pierwiastki jednokrotne w $\mathbb{Q}$.

Wniosek 4.11. *Jeżeli* $b \in \mathbb{C}$ *jest pierwiastkiem pierwotnym z* 1 *stopnia* m, *to* $[\mathbb{Q}(b) : \mathbb{Q}] = \phi(m)$.

Dowód: $F_m(x)$ jest wielomianem minimalnym dla b nad $\mathbb{Q}$. Mamy, że $[\mathbb{Q}(b) : \mathbb{Q}] = \deg F_m = \phi(m)$.

Lemat 4.12. [twierdzenie Liouville'a o aproksymacji diofantycznej]: *Jeżeli* $a \in \mathbb{R}$ *jest liczbą algebraiczną stopnia* $N > 1$, *to istnieje* $c \in \mathbb{R}_+$ *takie, że dla każdego* $r = \frac{p}{q} \in \mathbb{Q}$ *zachodzi*

$$\left|a - \frac{p}{q}\right| \geq \frac{c}{q^N}$$

Definicja 4.13. *Ciało* $L \supseteq K$ *jest* ***algebraicznym domknięciem*** K *wtedy i tylko wtedy, gdy:*

1. L *jest algebraicznie domknięte*
2. $L \supseteq K$ *jest rozszerzeniem algebraicznym, to znaczy dla każdego* $a \in L$ a *jest pierwiastkiem algebraicznym nad* K

Takie L *oznaczamy przez* $\widehat{K}$.

Wniosek 4.14. *Dla każdego* K *istnieje algebraiczne domknięcie* $\widehat{K}$.

Dowód: Rozważmy $K_\infty \supseteq K$ - ciało algebraicznie domknięte (twierdzenie z początku wykładu). Pokażemy, że

$$\widehat{K} = K^{alg}(K_\infty) = \{a \in K_\infty \ : \ a \text{ algebraiczny nad } K\}$$

1. $\widehat{K}$ jest algebraicznie domknięte:

Jeżeli $f \in \widehat{K}[X]$, to f ma pierwiastek w K, ale $\widehat{K} \subseteq K_\infty$, to znaczy, że $a \in \widehat{K}$ jest algebraiczne nad K.

2. $K \subseteq \widehat{K}$ jest rozszerzeniem algebraicznym:

$K \subseteq \widehat{K} = K^{alg}(K_\infty)$ z definicji jest rozszerzeniem algebraicznym.

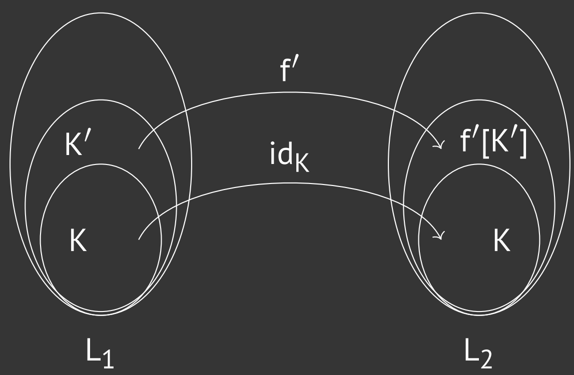
Twierdzenie 4.15. $\widehat{K}$ *jest jedyne z dokładnością do izomorfizmu nad* K.

$$\begin{tikzcd} L_1 \arrow[rr, "(\exists!\, f)\ f\restriction K = id_K", "\cong"'] & & L_2 \\ & K \arrow[ul, "\subseteq"] \arrow[ur, "\subseteq"'] & \end{tikzcd}$$

Dowód:

Niech

$$\mathfrak{K} = \{(k', f') \ : \ K \subseteq K' \subseteq L_1, f' : K' \xrightarrow{1-1} L_2, \ f' \restriction K = id_k\}$$



W $\mathfrak{K}$ definiujemy relację porządku w naturalny sposób, to znaczy

$$(K', f') \leq (K'', f'') \iff K' \subseteq K'' \ \wedge \ f'' \restriction K' = f''.$$

Wtedy $(\mathfrak{K}, \leq)$ jest zbiorem częściowo uporządkowanym i niepustym (bo jest $(K, id_K) \in \mathfrak{K}$). Ponadto każdy wstępujący łańcuch $(\mathfrak{K}, \leq)$ ma ograniczenie górne. Na mocy lematu Kuratowskiego-Zorna w tej rodzinie istnieje element maksymalny, nazwijmy go (K_1, f_1). Pokażemy, że $K_1 = L_1$.

Załóżmy nie wprost, że istnieje $a \in L_1 \setminus K_1$. Niech $w(x) \in K_1[X]$ będzie wielomianem minimalnym elementu a nad K_1. Niech

$$K_2 = f_1[K_1]$$
$$v(x) = f_1(a_0) + f_1(a_1)x + \ldots + f_1(a_n)x^n \in K_2[X].$$

$v(x)$ też jest nierozkładalny nad K_2, bo $w(x)$ był nierozkładalny nad K_1. Niech $b \in L_2$ będzie pierwiastkiem wielomianu v.

Zauważmy, że $K_1(a) = K_1[a]$, bo $w(x)$ jest nierozkładalny nad K_1, ale

$$K_1[a] \simeq K_1[X]/(w) \simeq K_2[X]/(v) \simeq K_2[b] \simeq K_2(b).$$

Czyli $K_1(a) \simeq K_2(b)$ i $f_2 : K_1(a) \xrightarrow{\cong} K_2(b)$ jest izomorfizmem rozszerzającym f_1. Wtedy mamy $(K_1, f_1) \lneq (K_1(a), f_2)$, co daje sprzeczność z maksymalnością (K_1, f_1). Zatem $L_1 = K_2$.

Niech $K_2 = f[K_1] = f[L_1]$. Pokażemy nie wprost, że $K_2 = L_2$. Załóżmy, że istnieje $a \in L_2 \setminus K_2$. Niech $w(x) \in K_2[X]$ wielomian minimalny dla a nad K_2. Wtedy $w(x)$ nie ma pierwiastka w K_2, ale $K_2 = f_1[L_1]$ jest algebraicznie domknięte, bo L_1 jest algebraicznie domknięte, co daje sprzeczność.

Wniosek 4.16. *Jeśli* $K \cong L$, *to* $\widehat{K} \cong \widehat{L}$. *Dokładniej, jeżeli* $f_0 L K \to L$ *jest izomorfizmem ciał, to istnieje izomorfizm* $f : \widehat{K} \to \widehat{L}$ *taki, że* $f \restriction K = f_0$.

Wniosek 4.17. *Jeśli* $K \subseteq L$ *jest algebraicznym rozszerzeniem ciał, to istnieje monomorfizm* $f : L \to \widehat{K}$ *taki, że* $f \restriction K = id_K$.

Dowód: Mamy dane $K \subseteq L \subseteq \widehat{L}$ rozszerzenia algebraiczne, zatem rozszerzenie $K \subseteq \widehat{L}$ jest algebraiczne. Stąd $\widehat{L}$ jest algebraicznym domknięciem K. Z twierdzenia 4.15 istnieje izomorfizm $g : \widehat{L} \to \widehat{K}$ taki, że $g \restriction K = id_K$. Wtedy $f = g \restriction L$ jest szukanym monomorfizmem.

Wykład 5: Teoria Galois

Definicja 5.1. *Niech* K *będzie ciałem,* $\widehat{K}$ *jego algebraicznym domknięciem. Niech* $K \subseteq L$ *będzie rozszerzeniem algebraicznym ciał.* ***Grupą Galois*** *rozszerzenia* $K \subseteq L$ *nazywamy*

$$\mathrm{Gal}(L/K) = \{f \in \mathrm{Aut}(L) \ : \ f \restriction K = \mathrm{id}_K\} = \mathrm{Aut}(L/K)$$

ze składaniem jako działaniem. Jest to jednocześnie podgrupa wszystkich automorfizmów.

Przykład:

1. Niech K będzie ciałem prostym ($\cong$ z $\mathbb{Q}$ lub z $\mathbb{Z}_p$). Wtedy $\mathrm{Gal}(L/K) = \mathrm{Aut}(L)$, bo
   - $\hookrightarrow$ Niech $\mathrm{char}(K) = \mathrm{char}(L) = p > 0$ i niech $f \in \mathrm{Aut}(L)$. Wtedy $f(1) = 1$, $f(\underbrace{1 + ... + 1}_{k}) = \underbrace{1 + ... + 1}_{k}$, a ponieważ $K = \{\underbrace{1 + ... + 1}_{k} \ : \ k \in \{1, ..., p\}\}$, zatem $f \restriction K = \mathrm{id}_K$, czyli $f \in \mathrm{Gal}(L/K)$.
   - $\hookrightarrow$ Niech $\mathrm{char}(K) = \mathrm{char}(L) = 0$, wtedy $K \cong \mathbb{Q}$. Niech $f \in \mathrm{Aut}(L)$. Wtedy $f(0) = 0, f(1) = 1$, a dla dowolnego $k \in \mathbb{N}$ $f\,\underbrace{1 + ... + 1}_{k} = \underbrace{1 + ... + 1}_{k}$, stąd dostajemy, że $f(n) = n$ dla $n \in \mathbb{Z}$, a z własności $\mathbb{Q}$ dostajemy, że $f(\frac{m}{n}) = \frac{m}{n}$, zatem $f \restriction K = \mathrm{id}_K$.
2. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$.

Skorowidz twierdzonek