Algebra 2R

a voyage into the unknown

koteczek

$\sim$

Spis treści

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

Fakt 1.1. $\overline{a} = (a_1, ..., a_n) \subseteq S$, *gdzie* S *jest rozszerzeniem pierścienia* R, *jest* *rozwiązaniem układu równań* $U \iff g(\overline{a}) = 0$ *dla każdego wielomianu* $g \in (f_1, ..., f_m) \triangleleft R[X]$.

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

$\Longrightarrow$ Rozważamy dwa przypadki:

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

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

2. 2. $(f_1, ..., f_m) \cap R = \{0\}$. (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 $S = R[\overline{X}]/(f_1, ..., f_m)$ i rozważmy

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

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

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

   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

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

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

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

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

Uwaga 1.2. *Skonstruowane powyżej rozwiązanie* $\overline{a}$ *układu* U *ma następującą własność uniwersalności:*

(☞) Jeżeli $S' \supseteq R$ *jest rozszerzeniem pierścienia z 1 i* $\overline{a}' = (a_1', ..., a_m') \subseteq S$ *jest rozwiązaniem* U *w* S'*, to istnieje jedyny homomorfizm*

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

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

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

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

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

Dowód. Niech $I = \{g \in R[\bar{X}] \ : \ g(\bar{a}') = 0\} \subseteq S'$. Oczywiście mamy, że $I \triangleleft R[\bar{X}]$, a więc

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

Z twierdzenia o faktoryzacji wie

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

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

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

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

Z twierdzenia o homomorfizmie pierścieni dostajemy jedyny homomorfizm

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

taki, że $h(\bar{a}) = \bar{a}'$. ☕

Uwaga 1.3. *Jeśli* $I = (f_1, ..., f_m)$, *to* $h : R[\bar{a}] \xrightarrow{\cong} R[\bar{a}']$.

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 $g(\bar{X}) \in K[\bar{X}]$ mamy $g(\bar{a}_1) = 0$ w $K[\bar{a}_1] \iff g(\phi(\bar{a}_1)) = 0$, a $\phi(\bar{a}_1) = \bar{a}_2$, czyli $g(\bar{a}_2) = 0$. Stąd $g \in I(\bar{a}_1/K) \iff g \in I(\bar{a}_2/K)$.

$1 \impliedby 2$

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 $\phi_{\bar a_i} \restriction K = \mathrm{id}_K$ (wielomiany mające tylko wyraz stały nie zmieniają wartości po podstawieniu x).

Z twierdzenia o izomorfizmie wiemy, że istnieją izomorfizmy

$$f_i : K[\bar X]/\ker(\phi_{\bar a_i}) = K[\bar X]/I(\bar a_i/K) = K[\bar X]/I \xrightarrow{\cong} \mathrm{Im}(\phi_{\bar a_i}) = K[\bar a_i]$$

$$\begin{tikzcd}
& K[\bar X] \arrow[dl, "\phi_{\bar a_1}"'] \arrow[d, "j\text{- ilorazowe}"] \arrow[dr, "\phi_{\bar a_2}"] & \\
K[\bar a_1] & K[X]/I \arrow[l, dashed, "\cong", "f_1"'] \arrow[r, dashed, "\cong", "f_2"'] & K[\bar a_2]
\end{tikzcd}$$

Niech $f = f_2 f_1^{-1} : K[\bar a_1] \to K[\bar a_2]$. Jako złożenie dwóch izomorfizmów f również jest izomorfizmem. Pozostaje sprawdzić, czy $f(\bar a_1) = \bar a_2$.

$f(\bar a_1) = f_2(f_1^{-1}(\bar a_1))$ i zauważmy, że $f_1^{-1}(\bar a_1) = w(\bar X) \in K[\bar X]/I$, gdzie $w(\bar X) = \bar X$. Idąc po kolei wynika to z tego, że $f_1 \circ j = \phi_{\bar a_1}$.

Gdy włożymy w lewą stronę $w(\bar X) = \bar X$ dostajemy $f_1 \circ j(w) = f_1(\bar X)$ (gdy oczywiście $\bar a_i \not\equiv 0$), a z kolei po włożeniu tego do prawej strony wychodzi $\phi_{\bar a_1}(w) = w(\bar a_1) = \bar a_1$ i mamy, że $f_1(w) = \bar a_1 \implies f_1^{-1}(\bar a_1) = w$.

$$f(\bar a_1) = f_2(f_1^{-1}(\bar a_1)) = f_2(w) = w(\bar a_2) = \bar a_2$$

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

Dowód. Uwaga 1.4.

Twierdzenie 1.6. *Niech* $I \triangleleft K[\bar X]$. *Wtedy istnieje ciało* $L \supseteq K$ *oraz* $\bar a = (a_1, ..., a_n) \subseteq L$ *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 $\bar a = (a_1, ..., a_n)$ 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. 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. 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.

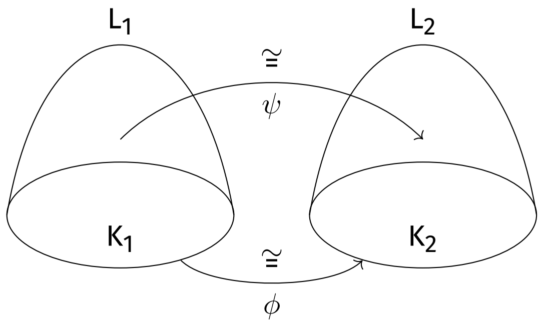
Założmy, że $K \subseteq L_1, K \subseteq L_2$ są rozszerzeniami ciała. Wtedy mówimy, że **L_1 jest izomorficzne z L_2 nad K** [$L_1 \cong_K L_2$] $\iff$ istnieje izomorfizm $f : L_1 \to L_2$ taki, że $f \restriction K = id_K$.

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. 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. 2. Zacznijmy od rozrysowania tej sytuacji:



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

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

jest ideałem maksymalnym. Mamy

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

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

$$\big\downarrow$$

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

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 $a_1, ..., a_n$, gdzie $a_1, ..., a_n$ 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 $L' = K'(a_1, ..., a_r)$ - ciało rozkładu wielomianu f_1 nad K'. Wtedy

   $$L = K(a_0, ..., a_r)$$

   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 $\phi \subseteq \psi_0$.

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

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:

- $\mathbb{C}$ jest algebraicznie domknięte.
- $\mathbb{R}$ nie jest algebraicznie domknięte, gdyż $x^2 + 1$ nie ma pierwiastka rzeczywistego.
- $\mathbb{Q}[i]$ 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

- $K \subseteq K_\alpha \subseteq K_\beta$ dla $\alpha < \beta < \kappa$
- 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 $K' = \bigcup_{\beta<\alpha} K_\beta$. Musimy pokazać, że K' jest ciałem.

1. 1. α to liczba graniczna. Definiujemy $K' = \bigcup_{\beta<\alpha} K_\beta$ 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. 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:

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

   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

- $L_0 = K$
- $L_{n+1} \supseteq L_n$, gdzie L_{n+1} dane jest przez lemat, to znaczy $(\forall\ f \in L_n[X])$ f ma pierwiastek w L_{n+1}.

Niech

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

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*

- $\mathrm{char}(K) = \mathrm{char}(L)$
- $0_K = 0_L$ *oraz* $1_K = 1_L$
- $K^* = K \setminus \{0\} < L^* = L \setminus \{0\}$ 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:

- $\mathbb{Q}$, gdzie $\mathrm{char}(\mathbb{Q}) = 0$ to ciało proste nieskończone.
- 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. $\mu(R) = \{a \in R : (\exists\, n)\ a^n = 1\} = \bigcup_{n>0} \mu_n(R)$ 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. $\mu_n(R) \lhd R^*$ *jest grupą jednostek pierścienia*
2. $\mu(R) \lhd R^*$
3. $\mu(R)$ *jest torsyjną grupą abelową (każdy element jest pierwiastkiem z 1).*

Przykłady

1. $\mu(\mathbb{C}) = \bigcup_{n>0} \mu_n(\mathbb{C}) \lneq (\{z \in \mathbb{C} : |z| = 1\}, \cdot) < \mathbb{C}^* = C \setminus \{0\}$ 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. 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. 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. 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. $1 \implies 2$

Wystarczy pokazać, że $K[a]$ jest ciałem. Rozważamy $I(a/K) \triangleleft K[X]$. Wiemy, że $K[X]$ jest PID, więc potrzebujemy, aby $I(a/K)$ było ideałem pierwszym.

$$f \cdot g \in I(a/K) \iff 0 = \widehat{f \cdot g}(a)$$

gdzie daszek oznacza homomorfizm ewaluacji, który jest również homomorfizmem w punkcie. Czyli

$$\widehat{f \cdot g}(a) = \widehat{f}(a)\widehat{g}(a) = 0 \iff \widehat{f}(a) = 0 \lor \widehat{g}(a) = 0.$$

Czyli $I(a/K)$ jest ideałem pierwszym w pierścieniu PID, więc jest ideałem maksymalnym. Mamy więc, że

$$K[a]/I(a/K)$$

jest ciałem, więc jest izomorficzne z K(a), bo K[a] to najmniejszy pierścień generowany przez $K \cup \{a\}$ (tutaj pierścień), a K(a) to najmniejsze ciało generowane przez $K \cup \{a\}$.

$2 \implies 3$

Załóżmy, że $a \neq 0$. Wtedy $a^{-1} \in K[a]$, czyli istnieje wielomian $f \in K[X]$

$$f(x) = \sum_{i=1}^{n} b_i x^i, \quad b_n \neq 0$$

taki, że $a^{-1} = f(a)$. Wobec tego mamy

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

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

stąd mamy, że

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

jest w domknięciu liniowym $(1, a, ..., a^n)$. Indukcyjnie pokazujemy, że

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

1. $m = 0, ..., n + 1$ bo one są już w $Lin_k(1, a, ..., a^n)$.
2. Zakładamy teraz, że dla m mamy

$$a^m = \sum_{i=0}^{n} c_i a^i$$

i pokazujemy dla $m + 1$.

$$a^{m+1} = a \cdot a^m = a \sum_{i=0}^{n} c_i a^i = \sum_{i=0}^{n} c_i a^{i+1} \in Lim_K(1, a, ..., a^n),$$

bo $a^{n+1} \in Lim_K(1, a, ..., a^m)$.

Czyli

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

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

$3 \implies 1$

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

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

jest zbiorem liniowo zależnym. Z liniowej zależności wiemy, że

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

Stąd dla $f \in K[X]$ zadanego wzorem

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

mamy $f(a) = 0$, zatem a jest algebraiczny nad K. ☕

Definicja 4.4. 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 (ang. monic)

- f jest nazywany wielomianem **minimalnym** a nad K (wyznaczony jednoznacznie)
- stopień a nad K jest definiowany jako deg(f).

Uwaga 4.5. *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.

1. Oczywiste. f jest wielomianem nieredukowalnym, stąd jeśli istniałby g taki, że $g(a) = 0$ oraz $\deg(g) < \deg(f)$, to wtedy f byłby podzielny przez g, co daje sprzeczność z nieredukowalnością f.
2. Niech $n = \deg(f)$,
$$f(x) = x^n + \sum_{k<n} b_k x^k$$
Z tego, że $f(a) = 0$ mamy, że
$$a^n = -\sum_{k<n} b_k x^k \in \mathrm{Lin}_K(1, a, ..., a^{n-1}) \subseteq L.$$
Czyli $K(a) = \mathrm{Lin}_K(1, a, ..., a^{n-1})$ i wystarczy zobaczyć, że $\{1, ..., a^{n-1}\}$ jest liniowo niezależny. W przeciwnym przypadku dla pewnego $0 < r < m$ $a^r \in \mathrm{Lim}_K(1, a, ..., a^{t-1})$, czyli istnieje wielomian taki, że a jest jego pierwiastkiem, a stopień jest nie większy niż $r < n$ i to daje sprzeczność.
Czyli $\mathrm{Lim}_K(1, a, ..., a^n)$ jest bazą $K(a)$ nad K i koniec.

☕

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.

Jeśli $K \subseteq L \ni a$ jest algebraiczny, to $\deg(a/K) = n$, to
$$K(a) = K[a] = \{\sum_{i=0}^{n-1} b_i a^i \ : \ b_i \in K\}$$

Fakt 4.6. *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 jest liniowo niezależny
2. X jest bazą M nad K
3. $|X| = |I| \cdot |J|$

Czyli X jest bazą M nad K (1.,2.) i ma odpowiednią moc (3.).

1. 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.

2. X generuje M nad K, bo dla $m \in M$ mam

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

3. 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

$$0 = e_i f_j - e_{i'} f_j = (e_i - e_{i'}) f_j \implies e_i - e_{i'} = 0 \implies i = i'$$

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

Wniosek 4.7. *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 **??** 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 4.8.

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

Przykłady:

1. $\mathbb{Q}_{alg}(\mathbb{C}) := \widehat{\mathbb{Q}} = \mathbb{Q}^{alg}$ jest to tak zwane ciało liczb algebraicznych . $\widehat{\mathbb{Q}}$ jest przeliczalne, bo $\mathbb{Q}[x]$ jest przeliczalne, więc jest mnóstwo liczb przestępnych (zespolonych, które nie są algebraiczne, ale nie potrafimy żadnej wskazać).
2. K jest algebraicznie domknięte w K(X)
3. $\frac{1}{\sqrt[3]{2}+\sqrt{3}} \in \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$, bo $\mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$ jest ciałem

$$L = \underbrace{\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}]}_{\subseteq \mathbb{C}} = \underbrace{\underbrace{\mathbb{Q}[\sqrt[3]{2}]}_{\text{ciało}}[\sqrt{3}]}_{\sqrt[3]{2}\text{alg.w}} \mathbb{Q} = \{a + b\sqrt[3]{2} + c\sqrt[3]{2} \ : \ a, b, c \in \mathbb{Q}(\sqrt{3})\}$$

$$\sqrt[3]{2} + \sqrt{3} \in L \implies \frac{1}{\sqrt[3]{2} + \sqrt{3}} \in L$$

Wykład 5: Wielomiany koła, domknięcia algebraiczne

Uwaga 5.1. *Niech* $K \subseteq L \subseteq M$ *będą rozszerzeniami ciał.* $K \subseteq M$ *jest algebraiczne* $\iff$ $K \subseteq L$ *i* $L \subseteq M$ *są algebraiczne*

Dowód.
$\implies$ OK

$\impliedby$

Weźmy dowolny $m \in M$. $L \subseteq M$ jest algebraiczny, co oznacza $f(m) = 0$, gdzie $f \in L[X]$

$$f = \sum_{i=0}^{n} a_n x^i, \quad a_n \not= 0$$

W takim razie m jest algebraiczne nad ciałek $K(a_0, ..., a_n)$. Ale teraz

$$[K(m) \; : \; K] \leq [K(a_0, ..., a_m, m) \; :; K] \overset{4.6}{=} [K(a_0, ..., a_n, m) : K(a_0, ..., a_n)][K(a_0, ..., a_n) : K] < \infty$$

bo m jest algebraiczny $K(\bar{a})$. Czyli

$$[K(m) : K] < \infty$$

więc m jest algebraiczny nad K (uwaga 4.3). ☕

Uwaga 5.2. $K_{alg}(L)$ *jest relatywnie algebraicznie domknięty w* L*. To znaczy* $(K_{alg}(L))_{alg}(L) = K_{alg}(L)$.

Dowód. Ćwiczenia. ☕

5.1 Wielomian rozkładu koła [cyclotomic polynomials]

Rozważamy wielomian

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

dla $m \in \mathbb{N}$. Wiemy, że

- pierwiastki w_m w $\mathbb{C}$ są jednokrotne
- $\mu_m(\mathbb{C})$ jest grupą cykliczną
- $a \in \mu_m(\mathbb{C})$ jest generatorem $\mu_m(\mathbb{C}) = \{a^i \; : \; 0 \leq i \leq m\} \cong (\mathbb{Z}_m, +)$
- a^k generuje $\mu_m(\mathbb{C}) \iff \mathrm{NWD}(k, m) = 1$

Funkcja Eulera:

$$\phi(m) = |\{k \in \mathbb{N} \; : \; 0 \leq k < m. \; \mathrm{NWD}(k, m) = 1\}|$$

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

Niech

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

i zdefiniujmy

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

F_m to m-*ty wielomian cyklotoniczny.*

Uwaga 5.3.

1. $w_m(x) = x^m - 1 = F_m(x) \cdot v_m(x) = F_m(x) \cdot \prod_{\substack{d<m \\ d|m}} F_d(x)$

2. $F_m(x) \in \mathbb{Z}[X]$

Dowód:

1. Wiemy, że wielomian w_m ma m pierwiastków na płaszczyźnie Gaussa, więc jest iloczynem dwumianów $x - b$, $b \in \mu_m(\mathbb{C})$, czyli

$$\alpha \in \mu_m(\mathbb{C}) \implies \alpha^d - 1 \quad d = \mathrm{ord}(\alpha),\ d|m$$

Wtedy α jest pierwiastkiem pierwotnym z 1 stopnia d. Wobec tego

$$F_d(x) = \prod_{\substack{\alpha\in\mu_m(\mathbb{C}) \\ \mathrm{ord}(\alpha)=d}} (x-\alpha) \implies \text{(teza)}$$

2. Dowód przez indukcję względem m. Dla $m = 1$ mamy $F_m(x) = x - 1 \in \mathbb{Z}[X]$.

Teraz zakładamy, że dla wszystkich $0 < d < m$ 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 jest iloczynem $\prod_{\substack{\alpha\in\mu_m(\mathbb{C}) \\ \mathrm{ord}(\alpha)=d}} (x-\alpha)$

$w_m(x)$ w $\mathbb{Z}[X]$ jest podzielny przez v_m i dostajemy:

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

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

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

czyli $F_m = L \in \mathbb{Z}[X]$.

Uwaga 5.4. [Lemat Gaussa] $F_m(x)$ *jest wielomianem nierozkładalnym w* $\mathbb{Q}[X]$ *(równoważnie w* $\mathbb{Z}[X]$*).*

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 ε'-pierwiastek G_1 oraz liczba pierwsza p taka, że $p \nmid m$ i $G_1(b) = G_2(b^p) = 0$.

Dowód lematu:

Niech ε będzie jakimś pierwiastkiem G_1, a τ będzie jakimś pierwiastkiem G_2. W takim razie

$$\tau, \varepsilon \in \mu_m(\mathbb{C}) \implies \tau = \varepsilon^l$$

dla pewnego l takiego, że $NWD(l, m) = 1$.

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

$$\text{pierwiastem } G_1 = \varepsilon, \varepsilon^{p_1}, \varepsilon^{p_1p_2}, ..., \varepsilon^{p_1,...,p_s} = \tau \text{ pierwiastek } G_2$$

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

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

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

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

Wimy już, że $G_1(\varepsilon) = 0$ 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 $G_2(\varepsilon^p) = G_3(\varepsilon) = 0$, 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

$$f : \mathbb{Z} \to \mathbb{Z}_p \mathbb{Z}/p\mathbb{Z} =$$

i indukowany przez niego epimorfizm pierścieni

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

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

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

$$\bar{f}(F_m) | \bar{f}(w_m) = x^m - 1.$$

Zatem w pewnym rozszerzeniu $L \supseteq \mathbb{Z}_p$ w_m ma pierwiastek wielokrotny co daje sprzeczność.

Uwaga 5.5. *Jeżeli $\varepsilon \in \mathbb{C}$ jest pierwiastkiem pierwotnym z 1 stopnia m, to* $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \phi(m)$.

Dowód: $F_m(x) \in \mathbb{Q}[X]$ jest nierozkładalny, a ε jest jego pierwiastkiem. To znaczy, że $F_,(x)$ jest wielomianem minimalnym dla ε nad $\mathbb{Q}$. Mamy, że $[\mathbb{Q}(b) : \mathbb{Q}] = \deg F_m = \phi(m)$.

Lemat 5.6. [lemat Liouville'a o aproksymacji diofantycznej]: *Jeżeli* $a \in \mathbb{R}$ *jest liczbą algebraiczną stopnia* $N > 1$, *to istnieje* $c = c(a) \in \mathbb{R}_+$ *takie, że dla każdego* $r = \frac{p}{q} \in \mathbb{Q}$ *zachodzi*

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

Lemat Liouville'a mówi o cesze. Jeżeli liczba nie spełnia tego lematu, to jest liczbą przestępną .

Dowód. Niech $N > 1$ i $a \in \mathbb{Q}$. Niech $f \in \mathbb{Z}[X]$ taki, że $f(a) = 0$ i $\deg(f) = \deg(a/\mathbb{Q})$. Teraz zauważmy, że na f patrzymy jako na funkcję wielomianową. To znaczy, dla każdego $x \in \mathbb{R}$ patrząc na

$$\widehat{f}(x) = \widehat{f}(x) - \underbrace{\widehat{f}(a)}_{=0}$$

ale funkcje wielomianowe są różniczkowalne. Dlatego możemy skorzystać z theoremierdzenia o wartości średniej. To znaczy

$$\widehat{f}(x) - \widehat{f}(a) = \widehat{f}'(x - a)$$

My wiemy, że a jest pierwiastkiem jednokrotnym wielomianu f(x). Niech $\varepsilon > 0$ takie, że $a \in (a - \varepsilon, a + \varepsilon)$ jest jedynym pierwiastkiem f(x) w tym przedziale. Oczywiście,

$$\deg(\widehat{f}'(x)) < \deg(\widehat{f}(x)) \implies \widehat{f}'(a) \neq 0.$$

Bez straty ogólności $\widehat{f}'(a) > 0$. Niech i $d = \sup_{x \in I} \widehat{f}'(x)$.

$$c = c(a) = \min(\varepsilon, \frac{1}{d}).$$

Udowodnimy, że c jest dobrze określona. Niech $r = \frac{p}{q} \in \mathbb{Q}$ i $p, q \in \mathbb{Z}$, $q > 0$.

$$f(x) = \sum_{k=0}^{N} a_k x^k, \quad a_k \in \mathbb{Z}, a_N \neq 0$$

Rozważamy przypadki:

1. $f \notin I$. Wtedy $\left|a - \frac{p}{q}\right| \geq \varepsilon \geq \frac{\varepsilon}{q^N} \geq \frac{c}{q^n}$
2. $f \in I$. Wtedy $\left|a - \frac{p}{q}\right|$ i $\frac{p}{q}$ może być naszym x. Czyli

$$\left|a - \frac{p}{q}\right| = \frac{|f(\frac{p}{q})|}{|f(f'(t)|} \geq \frac{|f(\frac{p}{q})|}{d} \geq \frac{c}{q^N}$$

   bo $c \leq \frac{1}{d}$

$$0 \neq |f(\frac{p}{q})| = \left|\sum_{k=0}^{N} a_k \frac{p^k}{q^k}\right| = \frac{\left|\sum_{k=0}^{N} a_k p^k q^{N-k}\right|}{q^N} \geq \frac{1}{q^N}$$

☕

5.2 Domknięcia algebraiczne

Definicja 5.7. 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 $\widehat{K}, K^{alg}$.

Uwaga 5.8. *Dla każdego K istnieje algebraiczne domknięcie $\widehat{K}$.*

Dowód. Rozważmy $K_\infty \supseteq K$ - ciało algebraicznie domknięte (theoremierdzenie 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:

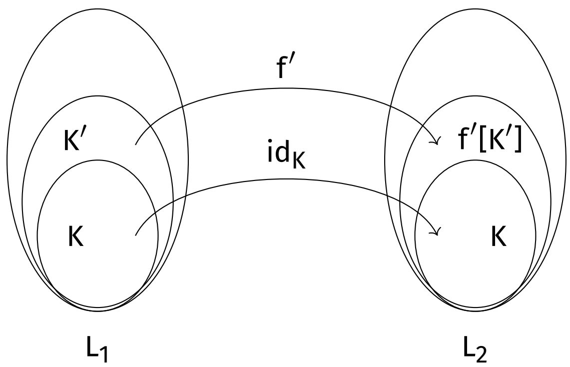
   $K \subseteq \widehat{K} = K_{alg}(K_\infty)$ z definicji jest rozszerzeniem algebraicznym.

Twierdzenie 5.9. *$\widehat{K}$ 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. Można użyć indukcji pozaskończonej, a można też użyć lematu Zorna. My zrobimy to drugie. Niech

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



Oczywiście, $\mathfrak{K} \neq \emptyset$, bo $(K, id_K) \in \mathfrak{K}$. 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 $L_1 = K_2$.

Zrobimy sprytnie wprost: $K_1 = L_1$, $K \subseteq K_2 \subseteq L_2$ i $K_1 \cong_K K_2$. K_1 jest aglebraicznie domknięte, więc K_2 też takie musi być. Czyli $K \subseteq K_2 \subseteq L_2$ jest algebraiczne, więc $K_2 = L_2$, bo założyliśmy, że $b \in L_2 \setminus K_2$ i wtedy wielomina minimalny $f_b(x) \in K_2[X]$ ma pierwiastek $c \in K_2$, czyli $(x - c)|f_n(x)$ a więc $x - c = f_b(x)$ jest nierozkładalny i $b = c$.

Wniosek 5.10. *Jeśli $K \cong L$, to $\widehat{K} \cong \widehat{L}$. Dokładniej, jeżeli $f_0 : LK \to L$ jest izomorfizmem ciał, to istnieje izomorfizm $f : \widehat{K} \to \widehat{L}$ taki, że $f \restriction K = f_0$.*

Dowód. Ćwiczenia ☕

Uwaga 5.11. *Jeśli* $K \subseteq L$ *jest algebraicznym rozszerzeniem ciał, to istnieje monomorfizm* $f : L \to \widehat{K}$ *taki, że* $f \restriction K = id_K$.

Dowód. Ćwiczenie ☕

Wykład 6: Wstęp do teorii Galois

6.1 Grupy Galois

Niech K będzie ciałem, $\widehat{K}$ jego algebraicznym domknięciem. Niech $K \subseteq L$ będzie rozszerzeniem algebraicznym ciał [BSO: $L \subseteq \widehat{K}$]. **Grupą Galois** rozszerzenia $K \subseteq L$ nazywamy

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

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
   - 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 $f \in \mathrm{Gal}(L/K)$.
   - 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. $\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{f_0, f_1\} \cong \mathbb{Z}$, bo $\sqrt{2}$ może przejść na siebie albo na $-\sqrt{2}$. Wtedy $f_0 = \mathrm{id}$, a $f_1(-\sqrt{2})$

Grupę Galois $\mathrm{Gal}(\widehat{K}/K)$ nazywamy **absolutną grupą Galois** ciała K.

Czy każda grupa skończona jest izomorficzna z $\mathrm{Gal}(L/\mathbb{Q})$ *dla pewnego* $\mathbb{Q} \subseteq L$*?* Jest to otwarty problem teorii Galois.

Uwaga 6.1. $a, b \in \widehat{K}$, *takie, że* $I(a/K) = I(b/K)$, *to wtedy istnieje* $f \in \mathrm{Gal}(\widehat{K}/K)$ *takie, że* $f(a) = b$.

Dowód.

$$\begin{tikzcd}
K[a] \arrow[r, "\cong", "f"'] \arrow[d, "\subseteq"] & K[b] \arrow[d, "\subseteq"] \\
K[a]^{alg} = \widehat{K} \arrow[r, "\exists f'", "\cong"'] & \widehat{K} = K[b]^{alg}
\end{tikzcd}$$

Co jest wnioskiem z wniosku 5.10. ☕

6.2 Rozszerzenia algebraiczne normalne

$\widehat{K}$ jest największym algebraicznym rozszerzeniem K tzn. $K \subseteq L$ oznacza, że istnieje $f : L \to \widehat{K}$ monomorfizm ciał taki, że $f \restriction K = \mathrm{id}_K$. (☕)

Mówmy, że rozszerzenie algebraiczne $K \subseteq L$ jest **normalne**, gdy w (☕) $f[L] \subseteq \widehat{K}$ dla wszystkich $f : L \to K$.

Przykład Rozszerzenie $K \subseteq \widehat{K}$ jest normalne.

Uwaga 6.2. *Załóżmy, że* $K \subseteq L \subseteq \widehat{K}$*. Wtedy rozszerzenie* $K \subseteq L$ *jest normalne* $\iff$ *dla każdego* $f \in \mathrm{Gal}(\widehat{K}/K)$ $f[L] = L$.

Dowód. $\implies$ z definicji, bo $\mathrm{id}_K[L] = L$.

$\impliedby$ z definicji.

☕

Czyli $K \subseteq L_1 \subseteq L$ i $K \subseteq L$ jest normalna, to $L_1 \subseteq L(\subseteq \widehat{K})$, więc $\mathrm{Gal}(\widehat{L_1}/L_1) \leq \mathrm{Gal}(\widehat{K}/K)$.

Twierdzenie 6.3. *Dla $K \subseteq L$ algebraicznego rozszerzenia jest normalne $\iff$ dla każdego $b \in L$ wielomian minimalny $f \in K[X]$ rozkłada się w $L[X]$ na iloczyn czynników liniowych.*

Dowód. Bez straty ogólności rozważamy $L \subseteq \widehat{K}$.

$\Longrightarrow$

Dowód nie wprost, to znaczy załóżmy, że istnieje $b \in L$ takie, że $w_b(x)$ ma pierwiastek $a \in \widehat{K} \setminus L$. Ale wtedy z Uwagi 6.1. na jednorodność $\widehat{K}$ istnieje $f \in \mathrm{Gal}(\widehat{K}/K)$ takie, że $f(b) = a$, więc $f[L] = L$ co jest sprzeczne z 6.2.

$\Longleftarrow$

Założmy nie wprost, że na mocy 6.2. istnieje $f \in \mathrm{Gal}(\widehat{K}/K)$ takie, że $f[L] \neq L$. Ale L i f[L] są wzajemnie sprzężone, więc wybierzmy $a \in L \setminus f[L]$. Symetrycznie, $a' \in f[L] \setminus L$, $f' : f[L] \xrightarrow{\cong} L$ spełnia warunek (☕).
Niech $w_a(x)$ jest wielomianem minimalnym a nad K. Wtedy $w_a(X) = f(w_a(x))$, bo $f \restriction K = \mathrm{id}_K$. Czyli w_a jest wielomianem minimalnym dla $b = f(a)/K$. Czyli $L \overset{f}{\cong}_K f[L]$. Z (☕) wiemy, że $w_a(x)$ rozkłada się nad L na czynniki liniowe. Czyli $w_a(x)$....f[L]..., co daje nam sprzeczność, bo a jest pierwiastkiem $w_a(X)$, ale $a \notin f[L]$. ☕

Rozszerzenie ciał $K \subseteq L$ jest **skończone**, jeśli $[L : K] < \infty$.

Twierdzenie 6.4. *Niech $K \subseteq L$ będą rozszerzeniami ciał. Wtedy następujące warunki są równoważne:*

1. *rozszerzenie $K \subseteq L$ jest skończone i normalne*
2. *L jest ciałem rozkładu pewnego wielomianu*

Dowód. Bez straty ogólności załóżmy, że $K \subseteq L \subseteq \widehat{K}$.

(2) $\Longrightarrow$ (1)

Załóżmy, że L jest ciałem rozkłądu pewnego wielomianu. Wtedy $L = K(a_1, ..., a_n)$, gdzie $a_1, ..., a_n$ to wszystkie pierwiastki wielomianu w(x) w $\widehat{K}$.

Niech $f \in \mathrm{Gal}(\widehat{K}/K)$, wtedy $f(a_1, ..., f(a_n)$ to też wszystkie pierwiastki wielomianu w(x). Stąd

$$f[L] = K(f(a_1), ..., f(a_n)) = K(a_1, ..., a_n) = L,$$

zatem rozszerzenie $K \subseteq L$ jest normalne i skończone.

(1) $\Longrightarrow$ (2)

Niech $K \subseteq L$ będzie skończone i normalne. Wtedy $L = K(a_1, ..., a_n)$ dla pewnych $a_1, ..., a_n \in L$ i $\{a_1, ..., a_n\}$ będzie bazą L nad K. Wtedy istnieje $w \in K[X] \setminus \{0\}$ takie, że $w(a_1) = ... = w(a_n) = 0$, zatem

$$L \supseteq \{\text{ pierwiastki } w\} \supseteq \{a_1, ..., a_n\}.$$

COŚ TUTAJ JEST NIE TAK ☕

Przykłady:

1. Niech $K \subseteq L$ będą ciałami skończonymi, wtedy $K \subseteq L$ jest ciałem normalnym, bo $|L| = p^n$, $w_{p^n-1}(x) = x^{p^n-1} - 1$ i L jest ciałem rozkładu w nad K.
2. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ to rozszerzenie skończone, ale nie normalne. Jest tak, bo
   - $x^3 - 2$ jest nierozkładalny nad $\mathbb{Q}$ (kryterium Eisteina)
   - W ciele $\mathbb{C}$ $x^3 - 2$ ma 3 pierwiastki, z których tylko jeden jest w $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$a

Uwaga 6.5. *Niech* $K \subseteq L \subseteq \widehat{K}$ *i niech* L_1 *będzie ciałem generowanym przez* $\bigcup\{f[L] : f \in Gal(\widehat{K}/K)\}$. *Wtedy* L_1 *to* ***normalne domknięcie ciała*** L ***w*** $\widehat{K}$. *Wtedy*

1. *Rozszerzenie* $K \subseteq L_1$ *jest normalne*
2. *Jeśli* $K \subseteq L_2$ *i* $L \subseteq L_2$ *są normalne, to istnieje monomorfizm* $L_1 \to L_2$ *taki, że* $f \restriction K = id$.

Dowód. (1) Z 6.2

(2)

Bez straty ogólności załóżmy, że $K \subseteq L \subseteq L_2 \subseteq \widehat{K}$ i $K \subseteq L \subseteq L_2 \subseteq \widehat{K}$. Niech $f \in Gal(\widehat{K}/K), f[L] \subseteq L_2$. W takim razkie $\bigcup\{f[L] : f \in Gal(\widehat{K}/K)\} \subseteq L_2$, z czego wynika, że $L_1 \subseteq L_2$. ☕

6.3 Rozszerzenia rozdzielcze

- Niech K będzie ciałem i $a \in \widehat{K}$. Mówimy, że a jest **rozdzielczy nad** K, gdy wielomian minimalny a, $w_a(x) \in K[X]$ ma tylko pierwiastki jednokrotne w $\widehat{K}$.
- Algebraiczne rozszerzenie $K \subseteq L$ jest **rozszerzeniem rozdzielczym**, gdy dla każdego $a \in L$ a jest rozdzielcze nad K.
- Wielomian $w(x) \in K[X]$ jest **rozdzielczy**, gdy w ma tylko pierwiastki jednokrotne w $\widehat{K}$.

Uwaga 6.6. *Załóżmy, że* $w(x) \in K[X]$ *jest wielomianem nierozkładalnym stopnia* > 0. *Wtedy*

1. $w(x)$ *jest rozdzielczy* $\iff$ $w(x)$ *i* $w'(x)$ *są względnie pierwsze*
2. *Jeśli* $char(K) = 0$, *to* w *jest rozdzielczy*
3. *Jeśli* $char(K) = p > 0$, *to* w *jest nierozdzielczy* $\iff$ $w(x) \in K[X^p]$, *to znaczy* $w(x) = v(x^p$ *dla pewnego* $v(x) \in K[X]$*).*

Dowód. Dowód zadanie z listy 4 ☕

Przykłady:

1. Niech $K \subseteq L$ będzie rozdzielcze i $K \subseteq L_1 \subseteq L$. Wtedy $L_1 \subseteq L$ też jest rozdzielcze [ćwiczenia]
2. Jeśli $char(K) = 0$, to każde rozszerzenie algebraiczne ciała K jest rozdzielcze.
3. Niech $K \subseteq L$ będą ciałami skończonymi. Wtedy $K \subseteq L$ jest rozdzielcze.

   Ciał L rozkładu wielomianu $x^{p^n} - x$ o pierwiastkach jednokrotnych.
4. Rozszerzeni nierozdzielnicze: niech $K = F_p(X) \subseteq L = K(\sqrt[p]{x})$. Niech $w_a(T) = T^p - x \in K[T]$ będzie wielomianem minimalnym $a = \sqrt[p]{x}$. Wtedy $w_a' = 0$, czyli w ciele L istnieje p-krotny pierwiastek w_a: $w_a(T) = (t-a)^p$.a

Lemat 6.7.

1. *Jeśli* $a \in \widehat{K}$, *to* $|\{f(a) : f \in Gal(\widehat{K}/K)\}| \leq$ *stopień* a *nad* K
2. a *jest rozdzielczy nad* K $\iff$ *w podpunkcie (1) jest równość.*

Dowód.

$$\{f(a) : f \in Gal(\widehat{K}/K)\} \overset{??}{=} \{\text{pierwiastki wielomianu minimalnego } w_a \in K[X] \text{ nad } K\}$$

czyli $deg(a/K) = deg(w_a)$. ☕

Element $a \in L$ nazywamy **elementem pierwotnym** rozszerzenia $K \subseteq L$, gdy $L = K(a)$.

Twierdzenie 6.8. *Niech $K \subseteq L$ będzie rozszerzeniem skończonym, $L = K(a_1, \ldots, a_n)$ i $a_1, \ldots, a_n$ rozdzielcze nad K. Wtedy istnieje $a^* \in L$ rozdzielczy nad K taki, że $L = K(a^*)$.*

Dowód. Bez starty ogólności załóżmy, że $K \subseteq L \subseteq \widehat{K}$. Rozważmy dwa przypadki:

1. K jest skończone. Wtedy L także jest skończone, a L^* jest cykliczna. Niech więc $a^* \in L^*$ będzie generatorem L^*. Wtedy $L = K(a^*)$.

2. K jest nieskończone.

   Dowód przez indukcję względem n. Dla $n = 1$ jest oczywiste. Robimy więc krok indukcyjny $(n-1) \implies n$:
$$K(a_1, \ldots, a_{n-1}) = K(b)$$
$$K(a_1, \ldots, a_{n-1}, a_n) = K(b, a_n)$$
   Niech teraz k będzie stopniem b nad K, a m - stopniem a_n nad $K(b)$. Z lematu 6.7 wiemy, że istnieją $f_1, \ldots, f_k \in \mathrm{Gal}(\widehat{K}/K)$ takie, że $f_1(b), \ldots, v_k(b)$ są parami różne. Niech więc $f_{1,1}, \ldots, f_{1,m} \in G(\widehat{K}/K(b))$ takie, że $f_{1,1}(a), \ldots, f_{1,m}(a)$ są parami różne.

   Dla $i = 1, \ldots, k, j = 1, \ldots, m$ niech $f_{i,j} = f_i \circ f_{1,j} \in \mathrm{Gal}(\widehat{K}/K)$.

$$\begin{tikzcd}
K(b)(a) \arrow[r, "f_{i,j}"] & K(b, f_{1,j}(a)) \arrow[r, "f_i"] & K(f_i(b), f_i(f_{1,j}(a))) \\
K(b) \arrow[u, "\subseteq"] \arrow[ur, "\subseteq"] \arrow[r] & K(f_i(b)) \arrow[ur, "\subseteq"] & \\
K \arrow[u, "\subseteq"] & K \arrow[u, "\subseteq"] &
\end{tikzcd}$$

   Zauważmy, że
$$\langle i, j\rangle \neq \langle i', j'\rangle \implies \langle f_{i,j}(a), f_{i,j}(b)\rangle \neq \langle f_{i',j'}(a), f_{i',j'}(b)\rangle,$$
   bo są dwie możliwości:

   - $i \neq i'$, wtedy $f_{i,j} = f_i(b) \neq f_{i'}(b) = f_{i',j'}(b)$
   - $i = i' \ \wedge\ j \neq j'$, wtedy $f_{ij}(a) = f_i(f_{1,j}(a)) \neq f_{i'}(f_{1,j}(a)) = f_{i'j'}(a)$, bo $f'_{1,j}(a) \neq f'_{1,j'}(a)$.

   Skoro K było nieskończone, to istnieje $c \in K$ takie, że dla $\langle i, j\rangle \neq \langle i', j'\rangle$ mamy
$$f_{i,j}(b) + f_{i,j}(a) \cdot c \neq f_{i',j'}(b) + f_{i',j'}(a) \cdot c,$$
   bo
$$F(x) = \prod_{\langle i,j\rangle \neq \langle i',j'\rangle} [f_{i,j}(b) + f_{ij}(a)x - (f_{i'j'}(b) + f_{i'j'}(a)x)]$$
   i c po prostu nie jest pierwiastkiem F.

   Postulujemy, że $K(b, a_n) = K(a^*)$, gdzie $a^* = b + a_n c$ jest elementem pierwotnym.

   $\supseteq$ jest jasne

   $\subseteq$ $f_{ij}(a^*)$, $1 \leq i \leq k$, $1 \leq j \leq m$ parami różne.

   Wiemy, że $\deg(a^*/K) \geq k \cdot m$, z drugiej strony
$$k \cdot m \leq [K(a^*) : K] \leq [K(a_b, b) : K] = [K(b) : K][K(a_n, b) : K(b)] = km$$
   czyli wszędzie wyżej są równości i mamy $K(a^*) = K(a_n, b)$.

Wniosek 6.9.

1. *Jeśli* $L = K(a_1, ..., a_n)$ *i* a_i *są rozdzielcze nad* K*, to* $L \supseteq K$ *też jest rozdzielcze.*
2. $K \subseteq L$ *jest rozdzielcze i* $L \subseteq M$ *jest rozdzielcze, to* $K \subseteq M$ *też jest rozdzielcze.*

Dowód. 1. Niech $L = K(a)$ i a jest rozdzielczy nad K. Załóżmy, że $b \in L$ nie jest rozdzielczy nad K. Wtedy $L = K(b, a)$.

$$\begin{array}{ccccc} n \cdot m & & n & & m \\ \shortparallel & & \shortparallel & & \shortparallel \\ \deg(a/K) & = & \deg(b/K) & \cdot & \deg(a/K(b)) \\ \shortparallel & & \shortparallel & & \shortparallel \\ [K(a) : K] & = & [K(b) : K] & \cdot & [K(a,b) : K(b)] \end{array}$$

Wybierzmy teraz $g \in K[X]$ takie, że $g(a) = b$. Wtedy

$$n \cdot m = |\{f(a) \; : \; f \in \mathrm{Gal}(\widehat{K}/K)\}| = (\star),$$

bo a jest rozdzielczy nad K. Dalej,

$$(\star) = |\{(f(b), f(a)) \; : \; f \in \mathrm{Gal}(\widehat{K}/K)\}| = (\star\star),$$

bo $f(b)$ ma $k < n$ możliwości, gdyż b nie jest rozdzielczy nad K i korzystamy z 6.7. Przy ustalonym $f(b)$ skakać po $f(a)$ możemy na co najwyżej m sposobów, bo $\deg(a/K(b)) = m = \deg(f(a)/K(f(b))$. Czyli koniec końców

$$(\star\star) \leq k \cdot m < n \cdot m,$$

co daje sprzeczność.

2. Podobny dowód zostawiony studentowi do pokiwania głową, że rozumie a w duszy płacz bo co się dzieje?

Wykład 7: Rozszerzenia radykalne (czysty Bangladesz)

Niech $K \subseteq L \subseteq \widehat{K}$ jak zwykle. Wtedy

- $a \in L$ jest **czysto nierozdzielczy** nad K, czyli **radykalny**, gdy wielomian minimalny a nad K, $w_a(x) \in K[X]$, ma tylko jeden pierwiastek w $\widehat{K}$.
- $K \subseteq L$ jest **rozszerzeniem radykalnym** (czysto nierozdzielczym), gdy dla każdego $a \in L$ a jest radykalne nad K.

Uwaga 7.1.

1. *Jeśli* $\mathrm{char}(K) = 0$, *to* a *nad* K *jest czysto nierozdzielczy* $\iff$ $a \in K$.
2. a *jest radykalne nad* K $\iff$ *dla każdego* $f \in \mathrm{Gal}(\widehat{K}/K)$ $f(a) = a$
3. *Jeśli* $\mathrm{char}(K) = p$, *to* a *jest radykalne nad* K $\iff$ *istnieje* $n \geq 0$ $a^{p^n} \in K$.

Dowód.

1. $w_a(x)$ ma tylko pierwiastki jednokrotne, gdy $\mathrm{char}(K) = 0$
2. Oczywiste $\star$
3. $\Longleftarrow$ oczywiste: $w_a(x) \in K[X]$ dzieli $x^{p^n} - a^{p^n} = (x-a)^{p^n} \in K[X]$

   $\Longrightarrow$ Dowodzimy indukcją po $n = \deg(a/K)$. Niech $w_a(x) = (x-a)^n \in K[X]$i $w_a'(x) = n(x-a)^{n-1} \in K[X]$ i $w_a' \in I(a/K)$ gdy $n > 1$, czyli $w_a'(x) = 0$, więc $p|n$. Niech więc $n = p \cdot n_1$ i wtedy $w_a(x) = (x^p - a^p)^{n_1}$ i a^p jest radykalny nad K, bo $\deg(a^p/K) \leq n_1 < n$. Z założenia indukcyjnego istnieje $k \geq 0$ takie, że $(a^p)^{p^k} = a^{p^{k+1}} \in K$ i to jest to, czego szukaliśmy.

☕

Niech $K \subseteq L$ będzie rozszerzeniem algebraicznym. Definiujemy

1. rozdzielcze domknięcie K w L: $\mathrm{sep}_L(K) = \{a \in L \ : \ a \text{ radykalne nad } K\}$
2. radykalne domknięcie (czysto nierozdzielcze) K w L: $\mathrm{rad}_L(K) = \{a \in L \ : \ a \text{ radykalny nad } K\}$

Wniosek 7.2. $K \subseteq \mathrm{sep}_L(K)$ *i* $\mathrm{rad}_L(K) \subseteq L \subseteq \widehat{K}$ *to ciała takie, że* $\mathrm{sep}_L(K) \cap \mathrm{rad}_L(K) = K$.

Dowód. Fakt, że $\mathrm{sep}_L(K)$ jest ciałem wynika z 6.9. Natomiast to, że $\mathrm{rad}_L(K)$ jest ciałem wynika z tego, że

$$\mathrm{rad}_L(K) = L \cap \bigcap_{f \in \mathrm{Gal}(\widehat{K}/K)} \mathrm{Fix}(f) = \{a \in \widehat{K} \ : \ f(a) = a\}$$

Dalej, dla $a \in \mathrm{sep}_L(K) \cap \mathrm{rad}_L(K)$ mamy $w_a(x) = x - a$ jest wielomianem minimalnym a nad K. ☕

- $\widehat{K}^s = \mathrm{sep}_{\widehat{K}}(K)$ jest rozdzielczym domknięciem K
- $\widehat{K}^r = \mathrm{rad}_{\widehat{K}}(K)$ jest radykalnym domknięciem K.

Uwaga 7.3.

1. *Gdy* $K \subseteq L \subseteq \widehat{K}$, *to* $\mathrm{sep}_L(K) = \widehat{K}^s \cap L$, $\mathrm{rad}_L(K = \widehat{K}^r \cap L$
2. *Załóżmy, że* $K \subseteq L \subseteq M \subseteq \widehat{K}$, *wtedy* $K \underset{rad}{\subseteq} L \underset{rad}{\subseteq} M \iff K \underset{rad}{\subseteq} M$

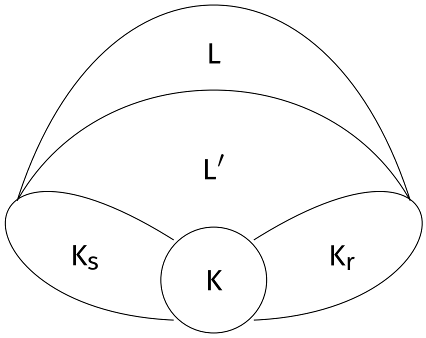
3. *Jeśli* $\mathrm{char}(K) = 0$, *to* $\mathrm{sep}_L(K) = K^{alg}(L)$ *i* $\mathrm{rad}_L(K) = K$, *oraz* $\widehat{K}^s = \widehat{K}$, $\widehat{K}^r = K$.

Fakt 7.4. *Załóżmy, że* $K \subseteq L \subseteq \widehat{K}$, $K_s = \mathrm{sep}_L(K)$, $K_r = \mathrm{rad}_L(K)$, $L' = K_s \cdot K_r$ *i niech* $L' = K_s \cdot K_r$ *będzie złożeniem ciał* K_s *i* K_r *w* L *(tzn. ciało generowane w* L *przez* $K_s \cup K_r$: $L' = K_s(K_r) = K_r(K_s)$*). Wtedy:*

1. $[L' : K] = [K_s : K] \cdot [K_r : K]$
2. *Gdy* $K \subseteq L$ *jest rozszerzeniem normalnym, to* $K_s \cdot K_r = L$
3. $K_s \subseteq L$ *jest radykalne, a* $K_r \subseteq L'$ *rozdzielcze*

Dowód. Jeśli $\mathrm{chark}(K) = 0$, to problem jest trywialny, bo $K_r = K$, $K_s = L$ i $L' = L$.

Załóżmy więc, że $\mathrm{char}(K) = p > 0$.



1. $L' = K_r(K_s) \supseteq K_r \supseteq K$, więc:

$$[L' : K] = [K_r(K_s) : K_r][K_r : K]$$

Wystarczy pokazać, że $[K_s : K] = [K_r(K_s) : K_r]$.

Zadanie z listy 4: Załóżmy, że $K \subseteq L, M \subseteq \widehat{K}$ są rozszerzeniami ciała takie, że $L \cap M = K$. Jeśli dla wszystkich L_0, M_0 takich, że $K \subseteq L_0 \subseteq L$ i $K \subseteq M_0 \subseteq M$ są skończone i $[L_0(M_0) : L_0] = [M_0 : K]$, to $[L(M) : L] = [M : K]$.

W takim razie wystarczy, że pokażemy

$$[K_r(K_s) : K] = [K_s : K]$$

korzystając z zadania 4 (wyżej). Niech $K \subseteq K_r^0 \subseteq K_r$ i $K \subseteq K_s^0 \subseteq K_s$, pierwsze rozszerzenia są skończone. Na mocy twierdzenia Abela możemy wybrać $a \in K_s^0$ takie, że $K_s^0 = K(a)$. Wtedy również

$$K_r^0(K_s^0) = K_r^0(a)$$

i $[K_s^0 : K]$ = stopień a nad K, $[K_r^0(a) : K_r^0]$ = stopień a nad K_r^0. Wystarczy pokazać, że oba te stopnie się zgadzają.

Niech $n = [K(a) : K]$ = stopień a nad K. Wtedy

$$1, a, ..., a^{n-1}$$

to baza liniowa $K(a)$ nad K. Przez to, że a jest rozdzielczy nad K i $p = \mathrm{char}(K)$, to $K(a) = K(a^p)$ [zad. 7 lista 4], czyli dla każdego $l > 0$

$$1, a^{p^l}, ..., a^{(n-1)p^l}$$

też jest bazą $K(a)$ nad K.

Pokażemy, że $1, a, ..., a^{n-1}$ jest bazą liniową $K_r^0(a)$ nad K_r^0:

- liniowa niezależność:

$$\sum k_i a^i = 0,\ k_i \in K_r^0$$

Niech l będzie takie, że $k_i^{p^l} \in K$ dla wszystkich i, wtedy

$$\sum k_i^{p^l} a^{ip^l} = 0 \implies (\forall\, i)\ k_i = 0$$

Czyli $[K_r^0(a) : K_r^0] \leq [K(a) : K] = n$ i $1, a, \dots, a^{n-1}$ jest bazą $K_r^0(a)/K_r^0$.

2. Bez straty ogólności załóżmy, że $[L : K] < \infty$, bo

$$L = \bigcup \{L_0 : K \underset{\text{skon,norm}}{\subseteq} L_0 \subseteq L\}$$

   (a) Niech $a \in L \supseteq K_r$, postulujemy, że a jest rozdzielczy nad K_r. Niech $a = a_1, a_2, \dots, a_n$ będą wszystkimi pierwiastkami wielomianu $w_a(X) \in K[X]$ i niech

$$v(x) = \prod_{i=1}^{n} (x - a_i).$$

   Wtedy dla $f \in \mathrm{Gal}(\widehat{K}/K)$ mamy $f[L] = L$, więc f permutuje $\{a_1, \dots, a_n\}$. Stąd $f(v(x)) = v(x)$, czyli f zachowuje współczynniki $v(x)$. To onzacza, że $v(x) \in K_r[X]$ i mamy, że a jest rozdzielczy nad K_r.

   (b) $L \supseteq K_s$ jest radykalne: z uwagi 6.6(3) wiemy, że jeśli $a \in L$ to dla pewnego l mamy a^{p^l} jest rozdzielcze nad K. Czyli $a^{p^l} \in K_s$, więc a jest radykalny nad K_s.

   Z podpunktów wyżej wiemy, że $L \subseteq K_r \cdot K_s$ jest rozszerzeniem rozdzielczym i radykalnym, więc $L = K_r \cdot K_s$.

3. $L \supseteq K_s$ jest radykalne w sposób analogiczny do rozumowania wyżej. $L' \supseteq K_r$ jest rozdzielcze, bo $L' = K_r[K_s]$.

7.1 Stopień rozdzielczy, radykalny ciała

$K \subseteq L \subseteq \widehat{K}$

Definiujemy $[L : K]_s = [\mathrm{sep}_L(K) : K]$ jako **stopień rozdzielczy** ciała L nad K oraz $[L : K]_r = [L : \mathrm{sep}_L(K)]$ jako **stopień radykalny** L nad K.

Z wyników wyżej dostajemy

$$[L : K] = [L : K]_s \cdot [L : K]_r,$$

bo $K \subseteq \mathrm{sep}_L(K)$ jest rozdzielcze, a $\mathrm{sep}_L(K) \subseteq L$ jest radykalne.

Uwaga 7.5. $K \subseteq L \subseteq \widehat{K}$

1. *Jeśli* $K \subseteq L$ *jest rozdzielcze, to* $[L : K] = |\{f \restriction L \ :\ f \in \mathrm{Gal}(\widehat{K}/K)\}| = |\{f : L \to \widehat{K} \ :\ f \restriction K = \mathrm{id}\}|$
2. *Ogólnie,* $[L : K]_s = |\{f \restriction L \ :\ f \in \mathrm{Gal}(\widehat{K}/K)\}|$ *(jak wyżej)*

Dowód. Rozważamy $[L : K] < \infty$. Przypadek ogólny $[L : K]$ można zredukować do przypadku skończonego, co jest ćwiczeniem na liście [wskazówka: *rozważyć odpowiednią bazę liniową* L *nad* K]

1. Z twierdzenia Abela $L = K(a)$ i dla $f \in \mathrm{Gal}(\widehat{K}/K)$, $f \restriction L$ jest wyznaczone jednoznacznie przez $f(a)$. Wiemy, że $f(a) \in \{\text{pierwiastki } w_a(x)\}$, których jest $n = [L : K]$.
2. $l \supseteq K_s$ to rozszerzenie radykalne, więc $f \restriction L$ jest wyznaczone przez $f \restriction K_s$. Dlatego:

$$|\{f \restriction L \ :\ f \in \mathrm{Gal}(\widehat{K}/K)\}| = |\{f \restriction K_s \ :\ f \in \mathrm{Gal}(\widehat{K}/K)\}| = [K_s : K] = [L : \underset{\mathrm{sep}_L(K)}{\underset{\shortparallel}{K_s}}]$$

Uwaga. *Jeśli* $\mathrm{char}(K) = p$ *i* $[L:K]_r < \infty$*, to* $[L:K]_r$ *jest potęgą* p.

Dowód. Indukcja względem $[L:K]_r = [L:K_s]$. Bez starty ogólności załóżmy, że $K = K_s$. Niech $a \in L \setminus K$, wtedy a jest radykalne nad K, czyli istnieje minimalne l takie, że $a^{p^l} \in K$.

Niech $a' = a^{p^{l-1}}$, wtedy $a' \in L \setminus K$ i $(a')^p \in K$, dlatego $w_{a'}(x) = x^p - (a')^p$ i $K \subseteq K(a') \subseteq L$, pierwsze rozszerzenie ma stopień p, a drugie jest radykalne.

Mamy $[L:K(a')] < [L:K]$, więc z założenia indukcyjnego $[L:K(a')] = p^r \implies [L:K] = p^{r+1}$ ☕

Wykład 8: Przekształcenia liniowe

Od teraz $K \subseteq L$ to będzie skończone rozszerzenie ciała, L będzie przestrzenią liniową nad K o wymiarze $\dim_K L = [L : K]$. Dla $a \in L$ będziemy opisywać homomorfizm

$$f_a : L \to L$$

$$f_a(z) = a \cdot z$$

będący K-liniowym przekształceniem.

8.1 Norma, ślad

- $N_{L/K}(a) = \det(f_a)$ jest normą homomorfizmu f_a
- $Tr_{L/K}(a) = Tr(f_a)$ jest śladem f_a.

Fakt 8.1. *Niech* $\{f_1, ..., f_j\} = \{f : L \to \widehat{K} \ : \ f \restriction K = id\}$, $k = [L : K]_s$ *i* $a \in L$. *Wtedy*

1. $N_{L/K}(a) = \left[\prod_{i=1}^{k} f_i(a)\right]^{[L:K]_r}$
2. $Tr_{L/K}(a) = [L : K]_r \cdot \sum_{i=1}^{k} f_i(a)$.

Rozważmy najpierw przypadek, gdy $L_K(a)$ i a jest rozdzielczy nad K. Niech $w_a(x) = x^k + a_{k-1}x^{k-1} + ... + a_1 x + a_0 \in K[X]$ będzie wielomianem minimalnym dla a nad K.Niech $b_1 = a, ..., b_n \in \widehat{K}$ będą pierwiastkami w_a i możemy założyć bez straty ogólności, że $b_i = f_i(a)$. W takim razie, jeśli popatrzymy na w_a w $\widehat{K}$, to mamy

$$w_a = \prod (x - b_i)$$

$$a_{k-1} = -\sum b_i$$

$$a_0 = (-1)^k \prod b_i$$

Na mocy zadania 4 z listy 5 dostajemy więc

$$N_{L/K}(a) = (-a)^k a_0 = \prod f_i(a)$$
$$Tr_{L/K}(a) = -a_{k-1} = \sum f_i(a)$$

Dowód. 1. Niech $a \in L$. WtedyO JEZU JA NIE MYŚLĘĘĘ

2. Jeśli $[L : K]_r \neq 1$, to $[L : K]_r = p^l$ dla $l \geq 1$ i $T_r(a) = 0$

   (a) $a \in K_s$, to $tr_{L/K}(a) = [L : K_s] \cdot Tr_{K_s/K}(a) \underset{char(K)=p}{=} 0$

   (b) $a \notin K_s$, wtedy $w_a(x) \in K[X]$ nie jest rozdzielczy na mocy 6.6(4). Czyli $K[X^p] \ni w_a(x) = x^{tp} + a_{(t-1)p}x^{(t-1)p} + ...$ Stąd $a_{tp-1} = 0 = Tr_{L/K}(a) = [L : K(a)] \underbrace{Tr_{K(a)/K}(a)}_{=0}$

3. Jeśli $[L : K]_r = 1$, to $L = K$ i $K \subseteq L$ jest rozdzielcze. Patrzymy na ciąg

$$K \subseteq K(a) \subseteq L$$

mamy

$$Tr_{L/K}(a) = [L : K(a)] \cdot Tr_{K(a)/K}(a)$$

Możemy wziąc b takie, że $K(a, b) = L$. Teraz liczymy homomorfizmy $L \underset{K}{\to} \widehat{K}$

8.2 Rozszerzenia Galois

$K \subseteq L \subseteq \widehat{K}$

- Mówimy, że rozszerzenie algebraiczne jest **Galois**, gdy dla każdego $a \in L \setminus K$ istnieje $f \in Gal(L/K)$ takie, że $f(a) \neq a$.
- Niech $G \leq Aut(L)$. Wtedy **ciałem punktów stałych** grupy G nazywamy

$$L^G = \{a \in L \ : \ (\forall f \in G) \ f(a) = a\} = \bigcap_{f \in G} Fix(f)$$

Uwaga: Jeśli $K \subseteq L$ jest algebraiczne, to $K \subseteq L$ jest Galois $\iff K = L^{G(L/K)}$ [ćwiczenia].

Przykłady:

1. $L = K(a)$ i a jest algebraiczne nad K. w_a jest wielomianem minimalnym dla a i $a = a_1, ..., a_k$ są wszystkie pierwiastki w_a w L. Wtedy $G(L/K) \ni F$ jest wyznaczone przez $f(a) \in \{a_1, ..., a_k\}$. Stąd też $|Gal(L/K)| \leq k \leq [L : K]$.
2. $L = K(a_1, ..., a_k) \supseteq K$ jest ciałem rozkładu wielomianu $w(x) \in K[X]$ ($a_1, ..., a_k$ to wszystkie pierwiastki w w L). $Gal(L/K) \ni f$ jest wyznaczone przez $f \restriction \{a_1, ..., a_n\} \in Sum(\{a_1, ..., a_n\})$ i istnieje monomorfizm $G(L/K) \to Sum(\{a_1, ..., a_n\})$ taki, że $f \mapsto f \restriction \{a_1, ..., a_n\}$.
3. $\zeta_a \in \mathbb{C}$ jest pierwiastkiem pierwotnym z 1 sotpnia m. Wtedy $[\mathbb{Q}[\eta_1] : \mathbb{Q}] = \phi(m)$ i $\eta_1 \in \{\zeta_1, ..., \zeta_{\phi(m)} \subseteq \mathbb{C}$ to wszystkie pierwiastki pierwotne stopnia m z 1 w $\mathbb{C}$. Dowolny $Gal(\mathbb{Q}[\zeta_1]/\mathbb{Q}) \ni f$ jest wyznaczony przez $f(\zeta_1)$ (może być dowolny ζ_i, $1 \leq i \leq m$), bo $Gal(\mathbb{Q}[\zeta_1]/\mathbb{Q}) = \mathbb{Q}(\zeta_i)$. Czyli $f(\zeta_1) = \zeta_1^{l_f}$ dla pewnego $0 < l_f <$ takiego, że $gcd(m, l_f) = 1$. Czyli $Gal(\mathbb{Q}(\zeta_1)/\mathbb{Q}) \cong \mathbb{Z}_m^k$ takie, że $f \mapsto l_f$.

Twierdzenie 8.2. *Niech $K \subseteq L$ będzie algebraiczne. Wtedy $K \subseteq L$ jest Galois $\iff K \subseteq L$ jest rozdzielcze i normalne.*

Dowód. Bez starty ogólności niech $L \subseteq \widehat{K}$

$\Longrightarrow$ Niech $a \in L \setminus K$ i niech $a = a_1, ..., a_n \in L$, wszystkie parami różne, będą pierwiastkami $w_a(x) \in K[X]$ w L.

Niech $v(x) = (x - a_1)(x - a_2)...(x - a_n) \in L[X]$, wtedy $v(x)|w_a(x)$ i $v(x)$ jest niezmienniczy względem $Gal(L/K)$ [f permutuje $a_1, ..., a_n$]. Czyli $v(x) \in L^{Gal(L/K)}[X] = K[X]$, bo $K \subseteq L$ jest Galois. Stąd $w_a|v$, więc $v = w$ jest rozdzielczy i rozkłada się nad L na czynniki liniowe. Stąd wynika, że $K \subseteq L$ jest rozdzielcze i normalne.

$\Longleftarrow$

Weźmy $a \in L \setminus K$ i niech $w_a(x)$ będzie wielomianem minimalnym [rozdzielczym]. Istnieje $a \neq a' \in L$ będące innym pierwiastkiem w_a w L (bo L normalne). Istnieje $f \in Gal(\widehat{K}/K)$ takie, że $f(a) = a'$. Ponieważ $K \subseteq L$ było normalne, to $f[L] = L$ i mamy $f \restriction L \in Gal(L/K)$, $f \restriction L(a) \neq a$, czyli z uwagi wcześniej $K \subseteq L$ jest Galois.

Wniosek 8.3. *Załóżmy, że mamy $K \subseteq L \subseteq M \subseteq K$. $K \subseteq M$ jest rozszerzeniem Galois $\iff L \subseteq M$ jest Galois.*

Twierdzenie 8.4. *Twierdzenie Artina: niech $G \leq Aut(L)$, wtedy $L^G \subseteq L$ jest rozszerzeniem Galois i $[L : L^G] = |G|$.*

Dowód. Niech $G \leq Gal(L/L^G)$, wtedy:

- dla każdego $x \in L \setminus L^G$ istnieje $f \in Gal(L/L^G)$ takie, że $f(x) = x$
- $L^G \subseteq L$ jest algebraiczne:

  Niech $a \in L \setminus L^G$, $\{a = a_0, ..., a_l\} = G(a)$ będzie orbitą a w L. Niech $w(x) = (x - a_0)(x - a_1)...(x - a_n) \in L[X]$. Wtedy dla każdego $g \in G$ mamy $g(w(x)) = w(x)$ i $w \in L^G[X] \implies$ a jest algebraiczny nad L^g.

Ponieważ $\deg(w) \leq |G|$, to $[L^G(a) : L^g] \leq |G|$. L^g jest rozdzielczym rozszerzeniem L, co razem z twierdzeniem Abela daje nam $[L : L^G] \leq |G|$ i $L = L^G(a)$ dla pewnego a. Czyli $w_a(x) \in L^G[X]$ jest wielomianem minimalnym a nad L^G, więc $\deg(w_a) \leq |G|$.

$L^g \subseteq L$ jest rozdzielcze i normalne. Czyli $|Gal(L^G/L)| = \deg(w_a) = [L : L^G] \leq |G|$. Ponieważ $G \leq Gal(L/L^G)$, to $G = Gal(L/L^G)$ i $[L : L^g] = |G|$

☕

Wniosek 8.5. *Niech $K \subseteq L$ będzie skończonym rozszerzeniem Galois. Wtedy $[L : K] = |Gal(L/K)|$*

Dowód. Niech $G = Gal(L/K)$, wtedy $K = L^G$ i G jest skończona i z twierdzenia Artina $[L : K] = [L : L^G] = |G|$ ☕

$K \subseteq L \subseteq \widehat{K}$. Definiujemy

$$\mathscr{L} = \{L' : K \subseteq L' \subseteq L\}$$

$$\mathscr{G} = \{H : H \leq Gal(L/K)\}$$

Od razu pojawiają nam się naturalne homomorfizmy:

$$\Gamma : \mathscr{L} \to \mathscr{G}$$

$$L' \mapsto Gal(L/L') \leq Gal(L/K)$$

$$\Lambda : \mathscr{G} \to \mathscr{L}$$

$$G \mapsto [K \subseteq] L^G \subseteq L$$

Twierdzenie 8.6. *Załóżmy, że $K \subseteq L$ jest skończonym rozszerzeniem Galois Wtedy Γ jest bijekcją i $\Lambda = \Gamma^{-1}$.*

Dowód.

$$\mathscr{L} \ni L' \overset{\Gamma}{\mapsto} Gal(L/L') \overset{\Lambda}{\mapsto} L^{Gal(L/L')} = L',$$

bo $L' \subseteq L$ jest Galois i używamy 8.3.

Czyli $\Lambda \circ \Gamma = od_{\mathscr{L}}$. Tak samo w drugą stronę:

$$\mathscr{G} \ni H \overset{\Lambda}{\mapsto} L^H \subseteq K \overset{\Gamma}{\mapsto} Gal(L/L^H) = H$$

☕

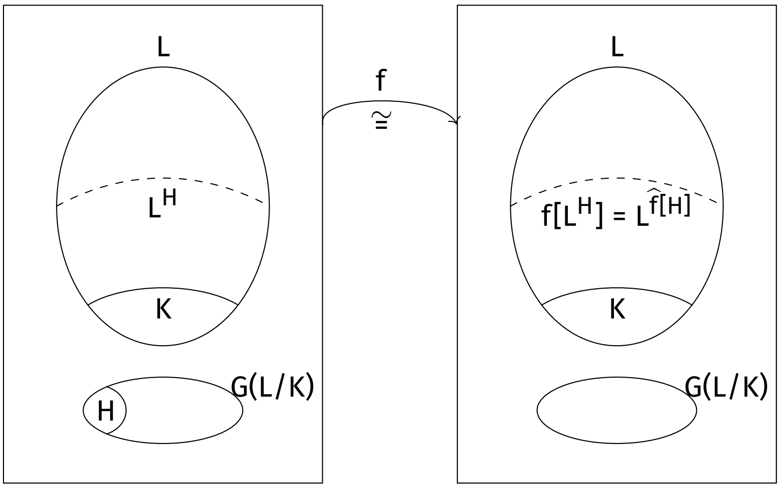
Wniosek 8.9. *Załóżmy, że $K \subseteq L$ jest skończone i Galois. Dla $H \leq Gal(L/K)$ mamy $H \triangleleft Gal(L/K) \iff K \subseteq L^H (= \Lambda(H))$ jest normalne (tzn. tutaj Galois).*

Ponadto wtedy $Gal(L^H/K) \cong Gal(L/K)/H$

Przed dowodem ćwiczenie, które pojawi się na liście zadań:

Niech $K \subseteq L' \subseteq L \subseteq \widehat{K}$ takie, że $K \subseteq L$ jest normalne (może być też skończone). Wtedy $K \subseteq L'$ jest normalne $\iff$ dla każdej $f \in Gal(L/K)$ $f[L'] = L'$ [ćwiczenia].

Dowód. Weźmy sobie $f \in Gal(L/K)$ RYSUNEK



NIE ROZUMIEM

Wykład 9: Rozszerzenia abelowe

9.1 Rozszerzenia abelowe

Załóżmy, że $K \subsetneq L$ jest skończonym rozszerzeniem Galois. Wtedy rozszerzenie $K \subsetneq L$ jest abelowe (cykliczne) gdy $\mathrm{Gal}(L/K)$ jest abelowe (cykliczne).

Twierdzenie 9.3. *Załóżmy, że $K \subseteq L_1 \subseteq L$ to rozszerzenia ciał. Jeśli $K \subseteq L$ jest abelowe (cykliczne), to $K \subseteq L_1$ i $L_1 \subseteq L$ też takie są.*

Dowód. Z tego, że $\mathrm{Gal}(L/L_1) \triangleleft \mathrm{Gal}(L/K)$ wynika, że $K \subseteq L_1$ i $L_1 \subseteq L$ jest rozszerzeniem Galois i $\mathrm{Gal}(L_1/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/L_1)$. Dlatego mamy $\mathrm{Gal}(L/L_1)$ i $\mathrm{Gal}(L_1/K)$ są abelowe (cykliczne).

Przykłady:

1. Niech $K \subseteq \widehat{K}$ i $\zeta \in \widehat{K}$ będzie pierwiastkiem pierwotnym stopnia n z 1.

$$\begin{array}{ccc} \mathrm{Gal}(K(\zeta)/K) & \hookrightarrow & \mathbb{Z}_n^* \\ \Psi & & \Psi \\ f & \longmapsto & l_f \end{array}$$

   l_f wybieramy tak, żeby $f(\zeta) = \zeta^{l_f}$ $0 < l_f < n$. Gdy $\mathrm{char}(K) = 0$, to homomorfizm wyżej jest izomofrizmem, wpp nie musi być to prawdą. Natomiast mamy pewność, że $K(\zeta) \supseteq K$ jest rozszerzeniem abelowym.

2. Niech $\mathrm{char}(K) = p$ i $p \nmid n$. Wybierzmy $a \in K$ takie, że $\sqrt[n]{a} \notin K$. Załóżmy, że $\zeta \in K$ jest pierwiastkiem pierwotnym z 1 stopnia n.

   W takim przypadku, $L = K(\sqrt[n]{a}) \supseteq K$ jest rozszerzeniem Galois i niech $w(x) = x^n - a$ (niekoniecznie nierozkładalny). Pierwiastki $w(a)$ w L mają postać $\zeta^i \sqrt[n]{a}$ dla $i = 0, \ldots, n-1$.

   Niech $f \in \mathrm{Gal}(L/K)$ będzie wyznaczony przez $f(\sqrt[n]{a}) = \zeta^{l_f} \sqrt[n]{a}$ dla $0 \leq l_f < n$. Wtedy funkcja jak wyżej, tzn.

$$\mathrm{Fal}(L/K) \ni f \mapsto l_f \in \mathbb{Z}_n^*$$

   jest monomorfizmem, ponieważ

$$\mathrm{Gal}(L/K) \ni f \mapsto l_f$$

$$\mathrm{Fal}(L/K) \ni g \mapsto l_g$$

$$(g \circ f)(\sqrt[n]{a}) = g(\zeta^{l_f} \sqrt[n]{a}) = \zeta^{l_f} g(\sqrt[n]{a}) = \zeta^{l_f} \zeta^{l_g} \sqrt[n]{a} = \zeta^{l_f + l_g} \sqrt[n]{a},$$

   więc $l_{g \circ f} = l_g +_n l_f$. Z tego powodu, $\mathrm{Gal}(L/K)$ jest grupą cykliczną.

Twierdzenie 9.4. *Załóżmy, że $K \subsetneq L$ jest rozszerzeniem cykliczny takim, że $[L : K] = n$. Niech $\zeta \in K$ będzie pierwiastkiem pierwotnym z 1 stopnia n (czyli $p \nmid n$ gdy $\mathrm{char}(K) = p$). Wtedy $(\exists\, a \in K)\ L = K(\sqrt[n]{a})$.*

Dowód. Niech $\gamma \in \mathrm{Gal}(L/K)$ będzie generatorem rozszerzenia L rzędu n. Dla $b \in L$ niech

$$c(b) = b + \zeta\gamma(b) + \ldots + \zeta^{n-1}\gamma^{n-1}(b)$$

$$\gamma(c(b)) = \gamma(b) + \zeta\gamma^2(b) + \ldots + \zeta^{n-1}\underbrace{\gamma^n(b)}_{=b} = \zeta^{-1}c(b)$$

$$\gamma^i(c(b)) = \zeta^{-a}c(b), \ \ i = 0, 1, 2, \ldots$$

Jeżeli $c(b) \neq 0$ [założenie ad hoc], to

$$\{\gamma^0(c(b)), \gamma(c(b)), \ldots, \gamma^{n-1}(c(b))\}$$

jest n-elementowym zbiorem pierwiastków wielomianu $w_{c(b)}(x) \in K[X]$, czyli

$$[K(c(b) : K] \geq n \implies K(c(b)) = L,$$

bo $K(c(b)) \subseteq L$.

Mamy $c(b)^n \in K$, bo

$$\gamma^i(c(b)^n) = \left[\gamma^i(c(b))\right]^n = [\zeta^{-i}c(b)]^n = \zeta^{-in}c(b)^n = c(b)^n$$

dla wszystkich $i = 0, 1, ..., n-1$. Dlatego $c(b) = \sqrt[n]{a}$ dla $a = c(b)^n \in K$ i $L = K(\sqrt[n]{a})$.

Wszystko to zachodzi pod warunkiem, że $c(b) \neq 0$, ale wiemy, że istnieje $b \in L$ takie, że $c(b) \neq 0$, bo: ☕

Twierdzenie 9.5. *Załóżmy, że* $\alpha_1, ..., \alpha_n \in \mathrm{Aut}(L)$, $a_1, ..., a_n \in L$ *i każdy jest* $\neq 0$. *Wtedy*

$$(\exists\, c \in L)\ (\sum a_i\alpha_i)(c) \neq 0$$

Innymi słowy: $\alpha_1, ..., \alpha_n$ *są liniowo niezależne w przestrzeni* L^L *nad* L.

Dowód. Indukcja względem n. Dla $n = 1$ jest to oczywiste. $c = 1 : a_1\alpha_1(1) = a_1 \neq 0$.

Krok indukcyjny:

Załóżmy nie prosty, że $(\forall\, x \in L)\ \sum^{n+1} a_i\alpha_i(x) = 0$. Niech $a \in L$ dowolne różne od zera. Wtedy

$$\begin{aligned}
(\forall\, x \in L)\ &\sum^{n+1} a_i\alpha_i(ax) = 0\\
&\sum^{n+1}(a_i\alpha_i(a))\alpha_i(x) = 0\\
&\sum^{n+1} a_i\alpha_i(a)[\alpha_{n+1}(a)]^{-1}\alpha_i(x) = 0\\
&\underbrace{\sum^{n+1} a_i\alpha_i(x)}_{=0} - \sum^{n+1} a_i\alpha_i(a)\alpha_{n+1}(a)^{-1}\alpha_i(x) = 0\\
&\sum^{n+1} \underbrace{\left[a_i - a_i\alpha_i(a)\alpha_{n+1}(a)^{-1}\right]}_{=0 \text{ gdy } i=n+1} \cdot\alpha_i(x) = 0\\
&\sum^{n} \left[a_i - a_i\alpha_i(a)\alpha_{n+1}(a)^{-1}\right] \alpha_i(x) = 0\\
(1 - \alpha_{n+1}(a)^{-1}) &\sum^{n} a_i\alpha_i(a) = 0
\end{aligned}$$

Z założenia indukcyjnego wiemy, że cała ta suma nie jest zerem, więc zerem musi być $1 - \alpha_{n+1}$, czyli każdy poziom sumy po wymnożeniu jest zerem i:

$$a_i - a_i\alpha_i(a)\alpha_{n+1}(a)^{-1} = 0,$$

czyli $\alpha_i(a) = \alpha_{n+1}(a)$ gdy $a_i \neq 0$. Z tego wynika, że dla każdego $a \in L$ jest $\alpha_i(a) = \alpha_{n+1}(a)$ i w takim razie $\alpha_i = \alpha_n$, co daje sprzeczność, bo α_i były parami różne. ☕

9.2 Rozwiązywalne rozszerzenia ciał i rozszerzenia przez pierwiastki

Załóżmy, że $K \subseteq L$ jest skończonym rozszerzeniem ciał.

1. $K \subseteq L$ jest **rozszerzeniem rozwiązywalnym**, gdy $K \subseteq L$ jest Galois i $\mathrm{Gal}(L/K)$ jest grupą rozwiązywalną.
2. $K \subseteq L$ jest **rozszerzeniem ciała przez pierwiastki** [radicals], gdy istnieje k oraz

$$L \subseteq L_0 \supseteq L_1 \supseteq ... \supseteq L_k = K$$

takie, że dla każdego $i < k$ L_i jest ciałem rozkładu wielomianu

- $x^{n_i} - b_i$, $b_i \in L_{i+1}$ nad L_{i+1} ($p \nmid n_i$ jeśli $\mathrm{char}(K) = p$
- lub $x^p - x - b_i$ dla L_{i+1} nad L_{i+1}

Twierdzenie 9.6. *Załóżmy, że $K \subseteq L$ jest rozszerzeniem skończonym ciał. Wtedy $K \subseteq L$ jest rozszerzeniem przez pierwiastki $\iff$ istnieje $L' \supseteq L$ takie, że $K \subseteq L'$ jest rozwiązalne.*

Dowód. $\implies$

Możemy założyć, że $K \subseteq L_0$ jest rozszerzeniem Galois (przez rozszerzenie ciąg), wtedy mamy ciąg normalny grup [ćwiczenie].

$$\mathrm{Gal}(L_0/L_k) \triangleright \mathrm{Gal}(L_0/L_{k-1} \triangleright \mathrm{Gal}(L_0/L_{k-1}) \triangleright \ldots \triangleright \mathrm{Gal}(L_0/L_1) \triangleright \{e\}$$

faktorami tego ciągu są $\mathrm{Gal}(L_i/L_{i+1})$. Wystarczy pokazać, że $L_i \supseteq L_{i+1}$ jest rozwiązywalna [wtedy można rozdrobić ciąg wyżej tak, by miał faktory abelowe].

Alternatywnie: $H \triangleleft G$, jeśli H jest rozwiązywalna i G/H jest rozwiązywalna, to G jest rozwiązywalna [ćwiczenie].

Rozważamy przypadki wielomianów z definicji wyżej:

- $x^{n_i} - b_i$

  Niech $a_i = \sqrt[n_i]{b_i} \in L_i$. Wtedy $L_i = L_{i+1}(\zeta_{n_i}, a_i)$, ζ_{n_i} jest pierwiastkiem pierwotnym z 1 stopnia n_i.

  $$L_i = L_{i+1}(\zeta_{n_i}, a_i) \overset{(\text{☢})}{\supseteq} L_{i+1}(\zeta_{n_i}) \supseteq L_{i+1}$$

  Ponieważ $L_{i+1} \quad \supseteq \quad L_i$ jest rozszerzeniem Galois, to takie jest również rozszerzenie (☢) i

  $\mathrm{Gal}(L_{i+1}\overbrace{(\zeta_{n_i}, a_i)}^{L_i}/L_{i+1}(\zeta_{n_i})) \cong \mathbb{Z}^*_{n_i}$ jest cykliczna i abelowa.

  Również rozszerzenie $L_{i+1} \subseteq L_{i+1}(\zeta_{n_i})$ jest Galois i grupa $\mathrm{Gal}(L_{i+1}(\zeta_{n_i})/L_{i+1})$ jest abelowa.

  Stąd

  $$\mathrm{Gal}(L_i/L_{i+1}) \overset{(\text{☽})}{\triangleright} \mathrm{Gal}(L_i/L_{i+1}(\zeta_{n_i}) \triangleright \{e\}$$

  i faktor w (☽) jest izomorficzny do abelowej grupy $\mathrm{Gal}(L_i(\zeta_{n_i})/L_{i+1})$. Czy $\mathrm{Gal}(L_i/L_{i+1})$ jest rozwiązywalna stopnia ≤ 2.

- $x^p - x - b_i$

  Niech $a \in L_i$ będzie peirwiastkiem wielomianu wyżej. Wtedy $a + 1$ jest również pierwiastkiem, bo

  $$(a+1)^p - (a+1) - b_i = a^p + 1^p - a - 1 - b_i = a^p - a - b_i = 0$$

  Dlatego $a, a+1, \ldots, a_(p-1) \in L_i$ i wszystkie są pierwiastkami wielomianu wyżej. Stąd $L_i = L_{i+1}(a)$.

  Niech $f \in \mathrm{Gal}(L_i/L_{i+1})$ będzie wielomianem wyznaczanym przez $f(a) = a + l_f$. Przekształtcanie

  $$\mathrm{Fal}(L_i/L_{i+1}) \ni f \mapsto l_f \in \mathbb{Z}^*_p$$

  daje $\mathrm{Gal}(L_i/L_{i+1}) \hookrightarrow \mathbb{Z}^*_p$ (w istocie jest tutaj $\cong$). Więc $l_i \supseteq L_{i+1}$ jest rozszerzeniem cyklicznym, czyli rozwiązywalny,

$\impliedby$

Niech $K \quad \subseteq \quad L$ będzie rozszerzeniem rozwiązywalnym. Pokażemy, że jest też rozszerzeniem pierwiastkowym.

Niech

$$\mathrm{Gal}(L/K) \triangleright G_{k-1} \triangleright G_{k-2} \triangleright \ldots \triangleright G_0 = \{e\}$$

będzie ciągiem normalnym podgrup o faktorach abelowych i bez straty ogólności cyklicznych, prostych, tzn. $\cong \mathbb{Z}_q$, q - liczba pierwsza. Wtedy

$$\begin{array}{ccccccccc} L & = & L^{G_0} & \supseteq & L^{G_1} & \supseteq & \dots & \supseteq & K \\ & & \parallel & & \parallel & & & & \parallel \\ & & L_0 & \supseteq & L_1 & \supseteq & \dots & \supseteq & L_k \end{array}$$

jest ciągiem rozszerzeń cyklicznych, prostych.

Claim: Wystarczy teraz pokazać, że jeśli $K \subseteq L$ jest cykliczne, $L \subseteq \widehat{K}$ i $Gal(L/K)$ jest prosta, to $K \subseteq L$ jest pierwiastkowe.

Dowód na boczku: Niech $[L : K] = n$, $Gal(L/K) \cong \mathbb{Z}_n^*$, a n jest liczbą pierwszą. Rozważamy przypadki charakterystyk ciał:

- $carh(K) = p \not| n$ lub $char(K) = 0$

  Niech $\zeta \in \widehat{K}$ będzie pierwiastkiem pierwotnym z 1 stopnia n. Mamy, że $K \subseteq K(\zeta)$ i $K(\zeta) \subseteq L(\zeta)$ jest rozszerzeniem Galois. Dalej, $[L(\zeta) : K(\zeta)] | [L : K]$, bo $Gal(L(\zeta)/K(\zeta)) \hookrightarrow Gal(L/K) \cong \mathbb{Z}_n^*$. Niech $m = [L(\zeta) : K(\zeta_]$, czyli $m = 1$ lub $m = n$. Z twierdzenia 9.4 dostajemy

  $$L(\zeta) = K(\zeta)(\sqrt[n]{a}), \ a \in K(\zeta)$$

  gdy $m = n$. Gdy $m = 1$ jest trywialne.

- $char(K) = p = n$

  Niech $\gamma \in Gal(L/K)$ będzie generatorem. Z twierdzenia Dedekinda (9.5) wiemy, że istneiej $b \in L$ takie, że

  $$K \in Tr_{L/K}(b) = \sum_{i=0}^{p-1} \gamma^i(b) \neq 0$$

  Dla $b' = \frac{1}{t} b$ mamy $Tr_{L/K}(b') = 1$.

  Niech $a = \gamma(b') + 2\gamma^2(b') + \dots + (p-1)\gamma^{p-1}(b')$. Wtedy

  $$\gamma(a) = \gamma^2(b') + 2\gamma^3(b') + \dots + \underbrace{(p-1)\gamma^p(b')}_{=b'} = a - Tr_{L/K}(b') = a - 1,$$

  ale

  $$\gamma(a^p - a) = \gamma(a)^p - \gamma(a) = (a-1)^p - (a-1) = a^p - a$$

  więc $a^p - a \in Fix(\gamma) = K$. Niech $c = a^p - a$. Stąd a jest pierwiastkiem $x^p - x - v$ oraz L to ciało rozkładu $x^p - x - c$ nad K, więc $K \subseteq L$ jest pierwiastkowe.

☕

Przykłady:

1. Niech $S_n := Sym(\{x_1, \dots, x_n\})$ będzie grupą funkcji symetrycznych o n zmiennych, $L = K(x_1, \dots, x_n)$ i $M = K(x_1, \dots, x_n)^{S_n}$. Wiemy, że $S_n < Aut(L)$. Z twierdzenia Artina wiemy, że $K \subseteq L$ jest rozszerzeniem Galois oraz $S_n = Gal(L/M)$.

   W przypadku, gdy $n \geq 5$ S_n nie jest rozwiązalna, więc $M \subseteq L$ też takie nie jest. L jest ciałem rozkładu wielomianu

   $$\begin{aligned} M[T] \ni w(T) =& (T - x_1)(T - x_2)\dots(T - x_n) = \\ &= T^n - \sigma_1(\overline{x})T^{n-1} + \sigma_2(\overline{x})T^{n-2} + \dots + (-1)^{n-1}\sigma_{n-1}(\overline{x})T + (-1)^n\sigma_n(\overline{x}) \end{aligned}$$

   gdzie $\sigma_i(\overline{x}) = \sum_{1 \leq j_1 < \dots < j_i \leq n} x_{j_1} x_{j_2} \dots x_{j_n}$ to bazowe funkcje symetryczne (wzory Viete'a). Mamy $\sigma_i(\overline{x}) \in M = L^{S_n}$.

2. Gdy $K \subseteq L$ jest rozszerzeniem ciał oraz L jest ciałem rozkładu nad K wielomianu $w(x)$ stopnia co najwyżej 4, to $Gal(L/K)$ wkłada się w S_4, a S_4 jest grupą rozwiązywalną. Podgrupa grupy rozwiązywalnej jest nadal rozwiązywalna, więc równanie
$$w(x) = 0$$
jest rozwiązywalne przez pierwiastki.

   Niech $M = L^{Gal(L/K)}$. Wtedy z twierdzenia Artina wiemy, że $K \subseteq M$ jest radykalne, a $M \subseteq L$ jest Galois (fakt 7.4.). $Gal(L/M) = Gal(L/K) \implies M \subseteq L$ jest rozszerzeniem pierwiastkowym, tzn:
$$L \subseteq L_0 \supseteq L_1 \supseteq \ldots \supseteq L_k = M,$$
   wszystkie rozszerzenia $L_i \supseteq L_{i+1}$ są rozszerzeniami o pierwiastki, więc wszystkie pierwiastki $w(x)$ dają się wyrazić nad K poprzez stosowanie działań ciała (włączając dzielenie, odejmowanie) oraz "pierwiastkowanie" tj. branie rozwiązań wielomianów $x^n - a$ lub $x^p - x - a$.

   Gdy z kolei wielomian $w(x)$ jest stopnia 5 to nie musi być to prawdą [ćwiczenie: czy dla 6, 7 powyższe zachodzi?]

Fakt $K(\sigma_1, \ldots, \sigma_n) = K(x_1, \ldots, x_n)^{S_n}$

Dowód. $\subseteq$ jasne

$\supseteq$

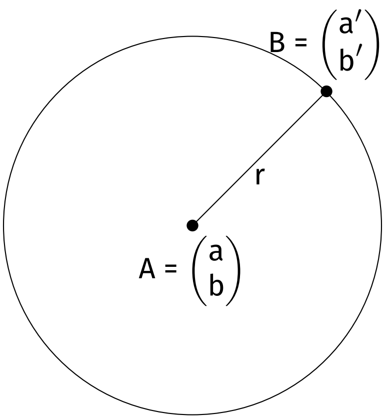
$$K(\vec{\sigma}) \subseteq K(\overline{x})^{S_n} \subseteq K(\overline{x})$$
$$n! = [K(\overline{x}) : K(\overline{x})^{S_n}] \leq [K(\overline{x}) : K(\vec{\sigma})] \leq n!,$$
z czego ostatnia nierówność zachodzi, bo $K(\overline{x})$ jest ciałem rozkładu wielomianu
$$w(T) = (T - x_1)\ldots(T - x_n)$$
nad $K(\sigma)$. Czyli mamy
$$[K(\overline{x}) : K(\overline{x})^{S_n}] = [K(\overline{x}) : K(\vec{\sigma})]]$$
i zawieranie $K(\vec{\sigma}) \subseteq K(\overline{x})^{S_n}$ jest tak naprawdę równością. ☕

Można też pokazać, że $K[\sigma_1, \ldots, \sigma_n] = K[x_1, \ldots, x_n]^{S_n}$, co jest **podstawowym twierdzeniem o wielomianach symetrycznych**.

Zastosowania: czyli konstrukcje przy pomocy cyrkla i linijki. Dane są punkty $A \neq B \in \mathbb{R}^2$.

- **cyrkiel**

  Mamy okrąg $\{\begin{pmatrix} x \\ y \end{pmatrix} : (x-a)^2 + (y-b)^2 = r^2\}$:

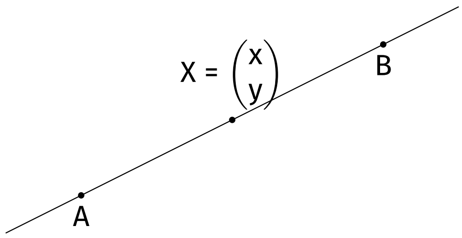


  czyli $r = \sqrt{(a'-a)^2 + (b'-b)^2}$

- **linijka**

  Rozważamy prostą L przechodzącą przez punkty A i B, czyli o równaniu

$$\begin{vmatrix} x - a & a' - a \\ y - b & b' - b \end{vmatrix} = 0$$



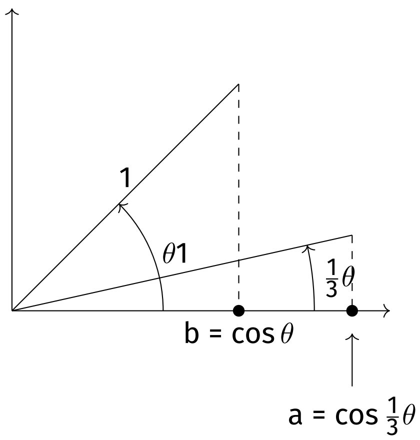
Niech $(a_1, b_1), \ldots, (a_n, b_n) \in \mathbb{R}^2$. *Punkt* $(a, b) \in \mathbb{R}^2$ *jest konstruowany przy pomocy cyrkla i linijki na płaszczyźnie* $\mathbb{R}^2$ *z punktów* $(a_1, b_1), \ldots, (a_n, b_n)$ *i punktów* $(0, 1), (1, 0)$ $\iff$ *rozszerzenie ciał* $K \subseteq K(a, b)$ *jest rozszerzeniem przez pierwiastki stopnia* ≤ 2. Tutaj oczywiście $K = \mathbb{Q}(a_1, b_1, \ldots, a_n, b_n)$.

- Kwadratura koła:

  Dane jest koło o promieniu 1 i punkt $(0, 1)$. Szukamy kwadratu o polu π. Równoważnie problem można wyrazić jako szukanie punktu $(0, \sqrt{\pi})$. Ale π jest liczbą przestępną, więc $\sqrt{\pi}$ też takie jest i rozwiązanie jest niemożliwe.

- Trysekcja kąta:

  Dany jest kąt $0 < \theta < \pi$ i naszym celem jest skonstruować kąt $\frac{1}{3}\theta$.



  a jest algebraiczne nad b, bo

$$4a^3 - 3a - b = 0.$$

  Cel jest niemożliwy, gdyż $[\mathbb{Q}(a, b) : \mathbb{Q}(b)] = 3$.

- Podwojenie sześcianu o krawędzi jednostkowej, równoważnie skonstruowanie $(0, a)$, gdzie $s^3 = 2$. Również jest to niemożliwe.

Wykład 10: Rozszerzenia przestępne ciał

$K \subseteq L$ to rozszerzenie ciał.

- $K \subseteq L$ jest **przestępne**, gdy istnieje $a \in L$ takie, że a jest przestępne nad K (tzn. $I(a/K) = 0$).
- $K \subseteq L$ jest **czysto przestępne**, gdy każde $a \in L$ jest przestępne nad K.

Uwaga 10.1. a *jest przestępne nad* $K \iff K(a) \cong K(x)$.

Dowód. Ćwiczenia

Niech $U = \widehat{U}$ będzie (dużym) ciałem oraz $K \subseteq U$ będzie podciałem. Niech $F \subseteq K$ będzie podciałem prostym.

- $acl_K : P(U) \to P(U)$ to operator algebraicznego domknięcia nad K taki, że dla $A \subseteq A$ $acl_K(A) = K(A)^{alg} \subseteq U$.
- $A \subseteq U$ jest algebraicznie domknięte nad K, gdy $A = cl_K(A)$.

10.1 Własności

1. $acl_K(\emptyset) = \widehat{K}$
2. (a) $A \subseteq B \implies cl_K(A) \subseteq (B)$ *monotoniczność*
   (b) $A \subseteq acl_K(A)$
   (c) $acl_K(acl_K(A)) = acl_K(A)$ *idempotetność*, tzn: acl_K jest operatorem domknięcia.
3. $acl_K(A) = \bigcup_{\substack{A_0 \subseteq A \\ \text{sk.}}} acl_K(A_0)$ *skończony charakter*
4. *własność wymiany*
$$a \in acl_K(A \cup \{b\} \setminus acl_K(A) \implies b \in acl_K(A \cup \{a\})$$

Dowód.

3. $[acl_K(A) =]K(A)^{alg} = \bigcup_{\substack{A_0 \subseteq A \\ \text{sk}}} K(A_0)^{alg}$

   $\subseteq$

   Weźmy $b \in K(A)^{alg}$. Wtedy istnieje $w(x) \in K(A)[X]$ takie, że $w(b) = 0$ i $w \not\equiv 0$. w ma współczynniki w $K(A_0$ dla pewnego skończonego $A_0 \subseteq A$, więc $b \in K(A_0)^{alg}$.

4. Jeśli $a \notin \underbrace{(K(A)^{alg})}_{=L}$, to wtedy $b \notin K(A)^{alg}$, tzn. b jest przestępny nad L i $L(b) \cong L[Y]$. Jest tak, bo

   $b \in K(A)^{alg} \implies a \in K(A, b)^{alg} = K(A)^{alg}$

   Niech teraz $a \in K(A, b)^{alg}$ i dla wygody oznaczmy $L = K(A)^{alg}$. Wtedy $K(A, b)^{alg} = L(b)^{alg}$. Wtedy istnieje $w(x) \in L[X], w(a) = 0$ i stopień w jest niezerowy.

   Bez straty ogólności: $w(x) \in L[b][X]$ (bo $L(b)$ jest ciałem ułamków pierścienia $L[b]$).

$$w(x) = \underset{\neq 0}{c_n} x^n + \ldots + c_1 x + c_0$$

   $c_i \in L[b]$, tzn. $c_i = v_i(b)$ i $v_i \in L[Y]$. Niech

$$\underset{\in L[a][y]}{v(y)} = v_n(y) \cdot a^n + \ldots + v_1(y) \cdot a + v_0(y).$$

$$\left.\begin{array}{l} v(b) = 0 \\ v \neq 0[\text{ćwiczenia}] \end{array}\right\} \implies b \in acl_K(A \cup \{a\}) = L(a)^{alg}$$

☕

- ✎ $A \subseteq U$ jest **algebraicznie niezależny** nad K, gdy dla każdego $a \in A$ $a \notin acl_K(A \setminus \{a\})$.

  Równoważnie: dla każdego n i dla wszystkich $a_1, ..., a_n \in A$ parami różnych, dla każdego $w(x_1, ..., x_n) \in K[\overline{X}]$ $w(\overline{a}) \neq 0$.
- ✎ A jest **bazą przestępną zbioru** $B \subseteq U$ nad K, gdy A jest algebraicznie niezależny nad K i $A \subseteq B \subseteq acl_K(A)$.
- ✎ **wymiar przestępny** B nad K $trdeg_K(B)$ to moc jakiejkolwiek bazy przestępnej zbioru B nad K.
- ✎ Gdy $K = F$ jest ciałem prostym, to pomijamy je w $acl_K, trdeg_K$. Jest to uzasadnione przez następujące twierdzenie.

Twierdzenie 10.2.

1. *Jeśli* $A \subseteq B \subseteq U$ *i* A *jest algebraicznie niezależny nad* K*, to istnieje* A', $A \subseteq A' \subseteq B$*, czyli baza przestępna* B *nad* K.
2. *Każde dwie bazy przestępne zbioru* B *nad* K *są równoliczne.*

Dowód. Ćwiczenia (patrz: dowód dla operatora Lin w przestrzeni liniowej) ☕

Przykład

1. Niech K będzie ciałem, $x_i, i \in I$ zmiennymi oraz $U = K(x_i : i \in I)^{alg}$. Wtedy $\{x_i : i \in I\} \subseteq U$ jest algebraicznie niezależne nad K i $trdeg_K(U) = |I|$.
2. Jeśli $K \subseteq L \subseteq U$ oraz $\{a_i : i \in I\}$ jest bazą przestępną L nad K, to

   $$K(a_i : i \in I\} \cong_K K(x_i : i \in I)$$

   $$K \subseteq K(a_i : i \in I) \subseteq L$$

   z czego pierwsze rozszerzenie jest czysto przestepne, a drugie - algebraiczne.

Wykład 11: Moduły

10.1 Moduły wprowadzenie

Przestrzenie liniowe nad pierścieniami

Definicja 10.3. Niech R będzie pierścieniem z 1, niekoniecznie przemienny. $(M, +, r)_r \in R$ jest modułem nad R, gdy spełnia aksjomaty przestrzeni liniowej nad R.

Moduł może być:

- lewostronny, wtedy $M \ni x \mapsto rx$ dla każdego r, x jest w M
- prawostronny (analogicznie, $xr \in M$).

Łączność mnożenia w modułach:

lewostronna	prawostronna	mieszana
$r_1(r_2m) = (r_1r_2)m$	$(mr_1)r_2 = m(r_1r_2)$	jeśli jesteśmy w lewostronnym module: $(mr_2)r_1 = m(r_2r_1)$ i nie to samo co przy prawostronnym

Przykłady:

1. $R = K$ to ciała, K-moduł to przestrzeń liniowa nad K
2. G jest grupą abelową, wtedy G jest $\mathbb{Z}$-modułem
3. G jest grupą abelową, wtedy End(G) są pierścieniem z jednością (id_G) i działaniami zdefiniowanymi dla $f, g \in End(G)$:
$$(f + g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(g(x)).$$
Grupa G może być traktowana jako moduł nad End(G) z działaniem zadanym przez $f \cdot x = f(x)$ dla $f \in End(G)$ i $x \in G$.
4. Załóżmy, że $j : R \to End(G)$ jest homomorfizmem pierścieni z 1. Wtedy j wyznacza na G strukturę R-modułu poprzez działanie: $r \cdot x = j(r) \cdot x$ dla $r \in R$ i $x \in G$.
5. Gdy $R_1 \subseteq R$ jest podpierścieniem z 1, to R jest modułem nad R_1.
6. Gdy $j : R_1 \to R$ jest homomorfizmem pierścieni z jednością i $M = (M, +, r)_{r \in R}$ jest R-modułem, to M jest R_1-modułem z dzialaniem indukowanym przez j. To znaczy, dla $r_1 \in R_1$ oraz $x \in M$ mamy $r_1 \cdot x := j(r_1) \cdot x$.
7. R jest pierścieniem z jednością i $I \subseteq R$ jest ideałem lewostronnym. Wtedy I jest R-modułem.

Definicja 10.4. Załóżmy, że M jest R-modułem oraz $N \subseteq M$. Wtedy N jest R-podmodułem M, gdy N jest modułem względem działam z M, to znaczy:

- $(N, +) \leq (M, +)$
- N jest zamknięty względem mnożenia przez skalary $r \in R$ w M.

Uwaga 10.5. *Niech M będzie R-modułem, wtedy*

1. $0 \cdot m = 0 \in M$

2. $r \cdot 0 = 0$

3. $(-1)m = -m$

Dowód.

1. $0 \cdot m = (0 + 0) \cdot m = 0m + 0m \implies 0m = 0$

2. $r \cdot 0 = r(0+0) = r0 + r0 \implies r0 = 0$

3. $(-1)m + 1m = (-1+1)m = 0m = 0 \implies (-1)m = -m$

☕

Uwaga 10.6. *Przekrój dowolnej niepustej rodziny podmodułów M jest podmodułem M.*

Przykład:

$\{0\} \subseteq M$ jest podmodułem zerowym.

Wniosek 10.6. *Niech $A \subseteq M$. Wtedy istnieje najmniejszy podmoduł (ze względu na zawieranie) $N \subseteq M$ taki, że $A \subseteq M$. Jest to* ***podmoduł generowany przez*** A

$$N = \{\sum r_i a_i \;:\; r_i \in R,\; a_i \in A\} \cup \{0\}$$

1. Jeśli $N_1, N_2 \subseteq M$ są podmodułami, to $N_1 + N_2$ też jest podmodułem. To samo, jeśli weźmiemy n takich podmodułów.

2. Produkt R-modułów M, N, czyli $M \times N$, też jest R-modułem

3. $M = N_1 \oplus \ldots \oplus N_k$ jest modułem dla $N_1, \ldots, N_k$ podmodułów M. Dodatkowo, dla każdego $m \in M$ istnieją jedyne $n_1, \ldots, n_k$ takie, że $m = n_1 + \ldots + n_k$.

Homomorfizm modułów $h : M \to N$ działa tak samo jak zwykle. Nazwy izo-, endo-, auto-, mono- nadal są applicable.

Niech $h : M \to N$ będzie homomorfizmem R-modułów. Dla $N' \subseteq N$ podmodułu $h^{-1}[N']$ jest podmodułem M. Dla $M' \subseteq M$ podmodułem jest $h[M'] \subseteq N$.

O odwzorowaniu $F : M_1 \times \ldots \times M_n \to M$ mówimy, że jest n-liniowym odwzorowaniem R-modułów, gdy jest liniowe na każdej współrzędnej.

Dla $M' \subseteq M$ podmodułu definiujemy **moduł ilorazowy** jako $M/M' = \{m + M' \;:\; m \in M\}$. Warstwy działają tutaj tak samo jak w grupach czy pierścieniach ilorazowych.

Twierdzenie 10.7. *Zasadnicze twierdzenie o homomorfizmie R-modułów. Niech M, N będą modułami. Wtedy dla każdego $f : M \to N$ istnieje dokładnie jeden $\bar{f}$ taki, że*

$$\begin{tikzcd} M \arrow[r, "\forall f"] \arrow[d, "\text{iloraz}"'] & N \\ M/\ker(F) \arrow[ur, dashed, "\exists!\,\bar{f}"'] & \end{tikzcd}$$

Twierdzenie 10.8. *Niech $f : M \to N$ i $g : M \to U$ będą homomorfizmami R-modułów. Wtedy $h : U \to N$ istnieje $\iff \ker(g) \subseteq \ker(g)$.*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "g"] & N \\ U \arrow[ur, dashed, "\exists\, h \iff \ker(f) \supseteq \ker(g)"'] & \end{tikzcd}$$

Zbiór wszystkich homomorfizmów między modułem M i N oznaczamy

$$\mathrm{Hom}_R(M, N) = \{h : M \to N \;:\; h \text{ jest homomorfizmem R-modułów}\}.$$

Tak jak w przypadku homomorfizmów między grupami czy pierścieniami, mamy $h : M \to N$ jest różnowartościowe $\iff \ker(h) = \{0\}$.

Dla R będącego przemiennym pierścieniem $\mathrm{Hom}_R(M, N)$ można traktować jako R-moduł definiując działania dla $m \in M$ przez:

$$\begin{array}{ll} (h_1 + h_2)(m) = h_1(m) + h_2(m) & h_1, h_2 \in \mathrm{Hom}_R(M, N) \\ (rh)(m) = r \cdot h(m) & r \in R \end{array}$$

10.2 Cel: zrozumieć moduły

Dany jest R-moduł M. Gdy $M = \bigoplus_i M_i$, gdzie $M_i \subseteq M$ jest małymi podmodułami o zrozumiałej strukturze, to struktura M też jest zrozumiała.

Definicja 10.9. Mówimy, że R-moduł M jest **prosty**, gdy $M \neq 0$ i dla każdego $N \subsetneq M$ podmodułu, $N = 0$.

Pierścień enodmorfizmów R-modułu M definiujemy jako

$$\mathrm{End}_R(M) = \{h : M \to M \ : \ h \text{ - homomorfizm modułów}\}.$$

Jest to podpierścień pierścienia $\mathrm{End}(M, +)$, który traktuje M jako grupę względem dodawania.

Lemat 10.10. *Lemat Schura: jeśli M jest R-modułem prostym, to $\mathrm{End}_R(M)$ jest pierścieniem z dzieleniem (prawie ciało, poza tym, że nie musi być przemienny).*

Dowód. Niech $0 \neq f \in \mathrm{End}_R(M)$. Wtedy $\mathrm{Im}(f) = M$, bo jest to niezerowy podmoduł M, a M przecież było modułem prostym. Stąd właśnie Im jest całością. $\ker(f) = \{0\}$, czyli f jest $1-1$ i "na".

Załóżmy, że M jest R-modułem oraz $K = \mathrm{End}_R(M)$ jest pierścieniem z dzieleniem ("ciało nieprzemienne"). Uwaga! nie zakładamy prostości M (ale możliwe że to wyniknie z K-pierścień z dzieleniem). Wtedy o M możemy myśleć jako o K-module. Załóżmy, że $n = \dim_K(M) < \infty$. Wtedy $\mathrm{End}_K(M) \cong M_{n\times n}(K)$.

Wybierzmy $r \in R$ i niech $\phi_r : M \to M$ takie, że $\phi_r(m) = r \cdot m$. Wtedy $\phi_r \in \mathrm{End}_K(M)$ (? gdy R-przemienny ? - zadanie)

$$r \longmapsto m(\phi_r) \in M_{n\times n}(K)$$

$$\cup$$

$$R \xrightarrow{\text{homomorfizm pierścieni z 1}} M_{n\times n}(K)$$

Powyższe jest rozwinięte jako teoria reprezentacji pierścieni

Niech R będzie pierścieniem z $1 \neq 0$ i M będzie R-modułem.

- Układ $\{m_i\} \subseteq M$ jest **liniowo niezależny**, gdy

$$(\forall \{r_i\} \subseteq R) \sum r_i m_i = 0 \implies (\forall i)\ r_i = 0$$

- Liniowa zależność jest zaprzeczeniem
- $S \subseteq M$ jest liniowo niezależny, gdy układ $\{m_i\} = S$ (bez powtórzeń)
- $B \subseteq M$ jest bazą, gdy:
  - jest liniowo niezależny
  - generuje M jako R-moduł
  - $\mathrm{Lin}_R(B) = M$.

Przykład:

1. $\{0\} \subseteq M$ jest liniowo niezależny, natomiast układ (m_0, m_0) jest liniowo zależny, bo $1 \cdot m_0 + (-1) \cdot m_0 = 0$.
2. $\mathbb{Q}$ jako $\mathbb{Z}$-moduł (a, b) jest liniowo zależny dla wszystkich $a, b \in \mathbb{Q}$.

   Bez straty ogólności $a, b \neq 0$ i $a \neq b$. $a = \frac{m}{n}$, $b = \frac{p}{q}$, czyli

   $$(np) \cdot a - (qm) \cdot b = pm - mp = 0$$

   W takim razie, $\mathbb{Q}$ nie ma bazy jako $\mathbb{Z}$-moduł.

11.3 Suma prosta modułów

(Abstrakcyjna) suma prosta rodziny modułów (koprodukt) to

$$\bigsqcup M_i = \bigoplus M_i = \{f \in \prod M_i \ : \ \{i \in I \ : \ f(i) \neq 0\} \text{ jest skończony}\}$$

Innymi słowy, elementy sumy prostej to krotki $(m_1, ..., m_n, ...)$ takie, że tylko dla skończenie wielu i mamy $m_i \neq 0$. Dla każdego j istnieje naturalne włożenie $f_j : M_j \to \bigsqcup M_i$ zdefiniowane przez $f_j(m) = (0, ..., 0, m, 0, ...)$, gdzie m występuje na j-tej pozycji.

Najprostszy przypadek sumy prostej to suma dwóch modułów: $M \oplus N$. Działania w tym module definiujemy przez:

$$\begin{aligned} &(m_1 \oplus n_1) + (m_2 \oplus n_2) = (m_1 + m_2) \oplus (n_1 + n_2) && m_i \in M,\ n_i \in N \\ &r(m \oplus n) = (rm) \oplus (rn) && r \in R,\ m \in M,\ n \in N. \end{aligned}$$

Przyjęło się uznawać za naturalne przekształcenie $h : \bigoplus M_i \to M$ zadane przez

$$h(m_1, ..., m_n, ...) = \sum m_i \in M.$$

Stąd elementu $\bigoplus M_i$ czasem oznacza się przez $\sum m_i$.

Uwaga 11.1. *Jeśli dla każdego $i \in I$ istnieje $M_i \to M$ to istnieje dokładnie jeden $h : \bigsqcup M_i \to M$ taki, że dla każdego i_0*

$$\begin{tikzcd} M_{i_0} \arrow[r, "g_{i_0}"] \arrow[d, "f_{i_0}"] & M \\ \bigsqcup M_i \arrow[ur, dashed, "\exists!\, h"'] & \end{tikzcd}$$

Jest to nazywane własnością uniwersalności.

Dowód. Ćwiczenia ☕

Uwaga 11.2. $M = M_1 \oplus M_2$ *dla podmodułów* $M_1, M_2 \subseteq M$. *Wtedy dla*

$$g_i = id_{M_i} : M_i \to M$$

oraz h *jak z uwagi 11.1*

$$h : M_1 \sqcup M_2 \to M$$

jest izomorfizm modułów.

Dowód. Ćwiczenie, łatwy. ☕

11.4 Baza modułu

Definicja 11.3. M jest **wolnym R-modułem**, gdy M ma bazę.

Przykłady:

1. R jest wolnym R-modułem z bazą {1}.
2. $\mathbb{Q}$ nie jest wolnym $\mathbb{Z}$-modułem
3. $\{M_i\}$ są rodziną wolnych R-modułów, wtedy $\bigsqcup M_i$ jest wolnym R-modułem.

   Dowód. Niech $B_i \subseteq M_i$ będą bazami. Wtedy

$$f_{i_0} : M_{i_0} \xrightarrow{\cong} f_{i_0}[M_{i_0}] \subseteq \bigsqcup M_i$$

$$\bigcup f_i[B_i]$$

jest bazą $\bigsqcup M_i$. ☕

Uwaga 11.4. *Niech R będzie pierścieniem z jednością, a M R-modułem. Niech $A = \{a_i : i \in i\} \subseteq M$ będzie podzbiorem bez powtórzeń. Następujące warunki są równoważne:*

1. *A jest bazą*
2. *dla każdego $m \in M$ istnieją jedyne $r_i \in R$ takie, że $m = \sum r_i a_i$ i jest ich skończenie wiele*
3. *dla każdego N R-modułu dla każdej funkcji $g : A \to N$ istnieje jedyna funkcja $g' : M \to N$ indukowana przez g.*

Dowód. (1) $\iff$ (2) jak w algebrze liniowej.

(2) $\implies$ (3)

Weźmy dowolny $m \in M$, wtedy

$$g'(m) = \sum r_i g(a_i)$$

jest jedyną dobrą definicją.

(3) $\implies$ (1)

- A generuje M:

  Niech $M' = \langle A \rangle \subseteq M$. Rozważmy

$$\begin{tikzcd} M \arrow[r, "j"] & M/M' \\ M \arrow[ur, "0"] & \end{tikzcd}$$

  $g = j \restriction A = 0 \restriction A = 0$, więc na mocy (3)

$$\begin{tikzcd} A \arrow[r, "g=0"] \arrow[d, phantom, "\cap" rotate] & M/M' \\ M \arrow[ur, "\exists! g'"'] & \end{tikzcd}$$

- A jest liniowo niezależne:

  Załóżmy, że istnieje $\sum r_{i_k} a_{i_k} = 0$, $r_{i_k} \neq 0$. Niech $g : A \to R$ takie, że

$$g(a_0) = \begin{cases} 0 & i \neq i_0 \\ 1 & i = i_0 \end{cases}.$$

  Na mocy (3) wiemy, że istnieje dokładnie jedno $g' : M \to R$ takie, że

$$0 = g'(0) = g'(\sum r_i a_i) = \sum r_i g(a_i) = r_{i_0} \cdot 1 = r_{i_0} \neq 0$$

  co daje sprzeczność.

☕

Uwaga 11.5.

1. *Jeśli $A = \{a_i\}_{i \in I}$ jest bazą M to wtedy*
   (a) Ra_i *jest podmodułem* M
   (b) $M = \oplus Ra_i$

2. *Jeśli* A *jest dowolnym zbiorem, to istnieje* R*-moduł* M *o bazie* A*. Wtedy*

$$M = \sqcup_{a\in A} Ra$$

i wtedy $Ra \cong R$

Przykład: $\mathbb{Z}$ jest modułem wolnym (wolna grupa abelowa).

Twierdzenie 11.6. *Załóżmy, że* R *jest przemienny. Wtedy każde dwie bazy* R*-modułu* M *są równoliczne.*

Dowód. Problem redukujemy do algebry liniowej. Niech $I \triangleleft R$ będzie maksymalnym ideałem i niech $M' = IM \subseteq M$ będzie podmodułem generowanym przez

$$\{im \ : \ i \in I, m \in M\}.$$

Wtedy, jeśli popatrzymy na M/M', to ma on naturalną strukturę modułu nad R/I. Dla $(m + M')$ i $(r + I)$ definiujemy

$$(r + I)(m + M') = (rm + M')$$

oraz dodawanie jak w grupie ilorazowej.

Niech $B_1, B_2 \subseteq M$ będą bazami M. Ustalmy ilorazowe homomorfizmy

$$j : M \to M/M'$$

$$l : R \to R/I.$$

Chcemy pokazać, że $j[B_1], j[B_2]$ są bazami M/M' jako R/I-modułu.

- generowanie:

$$M \ni m = \sum r_i b_i \implies j(m) = \sum j(r_i b_i) = \sum [r_i b_i + M'] = \sum (r_i + I)(m_i + M') = \sum l(r_i) j(b_i)$$

- liniowa niezależność:

  Naszym celem jest pokazać, że jeśli

$$\sum l(r_i) j(b_i) = 0 \implies l(r_i) = 0$$

  to wtedy

$$j(\sum r_i b_i) = 0.$$

  Wiemy, że $\sum r_i b_i \in IM = M'$. Dalej:

$$\sum r_i b_i = \sum r_j' m_j'$$

  dla $r_j' \in I$ oraz $m_j' \in M$. Niech więc $m_j' = \sum s_{ij} b_i$ dla $s_{ij} \in R$ oraz $b_i \in B_1$. Wtedy

$$\sum r_j' m_j' = \sum_{i,j} r_j' s_{ij} b_i = \sum_i \left[\sum_j r_j' s_{ij} \right] b_i = \sum_i r_i b_i$$

  Sokoro dla każdego i mamy $r_i = \sum_j r_j' s_{ij} \in I$, to dla każdego i $l(r_i) = 0$ w R/I. Więc $j[B_1]$ jest liniowo niezależny w M/M' jako układ. Ponieważ możemy ustalić

$$j : B_1 \xrightarrow[\text{na}]{1-1} j[B_1]$$

  to $B_1 \sim j[B_1]$ oraz $B_2 \sum j[B_2]$. Ale R/I jest ciałem, więc M/M' jest przestrzenią liniowa nad R/I, więc ponieważ $j[B_i]$ są bazami tej przestrzeni liniowej, to

$$j[B_1] \sim j[B_2]$$

$$B_1 \sim B_2$$

Uwaga 11.7. *Każdy R-moduł M jest homomorficznym obrazem R-modułu wolnego.*

Dowód. Taki sam jak dla:

- grupy wolnej
- wolnej grupy abelowej
- algebry wolnej w rozmaitości algebraicznej

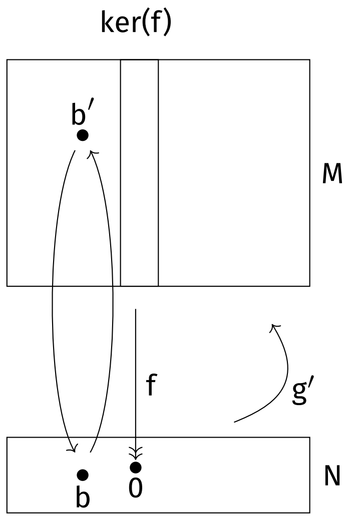
Niech $N = \bigsqcup_{m \in M} Rm$ będzie R-modułem wolnym o bazie M. Równie dobrze możemy wziąć $N = \bigsqcup_{a \in A} Ra$, gdzie A generuje M.

$$\begin{tikzcd} \mathrm{id} : M \arrow[dr, "\text{na}"] \arrow[d, phantom, sloped, "\subseteq"] & \\ (\exists!\, f) : N \arrow[r, "R\text{–liniowe}"'] & M \end{tikzcd}$$

Z uwagi 11.4(3) f istnieje i jest epimorfizmem.

Fakt 11.8. *Załóżmy, że M, N są R-modułami, N jest wolny i $f : M \to N$ jest epimorfizmem. Wtedy $M \cong \ker(f) \oplus N$. Więcej: istnieje $N' \cong N$ taki, że $M = \ker(f) \oplus N'$.*

Dowód. Niech $B \subseteq N$ będzie bazą modułu N.



Dla $b \in B$ ustalamy $b' \in M$ takie, że $f(b') = b$. Niech $g : B \to M$ takie, że $g(b) = b'$. Z uwagi 11.4(3) wiemy, że istnieje jedyne $g' : N \to M$ R-liniowe takie, że g' rozszerza g.

Wtedy $f \circ g' : N \to N$ i $(f \circ g') \restriction B = \mathrm{id}_B$, czyli z uwagi 11.4 $f \circ g' = \mathrm{id}_N$. Stąd g' jest $1-1$. Czyli $N \cong g'[N] \subseteq M$.

Pokażemy teraz, że $M = \ker(f) \oplus g'[N]$. Weźmy dowolny $m \in M$. Wtedy

$$m = \underbrace{(m - (g'f)(m))}_{\ker(f)} + \underbrace{(g'f)(m)}_{g'[N]}$$

bo

$$f(m - (g'f)(m)) = f(m) - (fg')f(m) - f(m) = 0.$$

Pozostaje nam pokazać, że $\ker(f) \cap g'[N] = 0$. Niech $m \in \ker(f) \cap g'[N]$. Wtedy $m = g'(n)$. Ale wtedy $0 = f(m) = (fg')(n) = n$. Wobec tego $n = 0$, więc $m = g'(n) = g'(0) = 0$.

11.5 Moduły projektywne, cykliczne, torsyjne

Definicja 11.9.

- R-moduł N jest **projektywny**, jeśli dla każdego M i każdego epimorfizmu $f : M \to N$ mamy $M = \ker(f) \oplus M'$ dla pewnych podmodułów $M' \subseteq M$.

  Jest to równoważne [ćwiczenia] istnieniu $g : N \to M$ takiego, że $f \circ g = \mathrm{id}_N$.

$$\begin{tikzcd} & M \arrow[d, "\forall f"] \\ N \arrow[ur, "\exists g"] \arrow[r, "id"'] & N \end{tikzcd}$$

  to znaczy, że f rozszczepia się.

- R-moduł M jest **injektywny** wtedy, gdy dla każdego N i każdego monomorfizmu $g : M \hookrightarrow N$ istnieje $N' \subseteq N$ taki, że $N = \mathrm{Im}(g) \oplus N'$. To znaczy, obraz g jest *składnikiem prostym* N.

Przykłady:

1. Moduł wolny jest projektywny
2. W przypadku, gdy R jest ciałem, to każdy R-modul jest projektywny i injektywny.

Definicja 11.10. Załóżmy, że R jest pierścieniem przemiennym z jednością. Mówimy, że M jest **R-modułem cyklicznym**, gdy jest generowany przez pojedynczy element. To znaczy, że istnieje $a \in M$ takie, że

$$M = Ra.$$

Przykłady:

1. $R = R1$ jest modułem cyklicznym
2. M jest R-modułem. i $a \in M$, to wtedy $Ra \subseteq M$ jest podmodułem cyklicznym.

Uwaga 11.11. *M jest modułem cyklicznym $\iff$ $M \cong R/I$ jako R-moduły dla pewnego $I \triangleright R$.*

Dowód. $\Longleftarrow$ R/I jest generowany przez $1 + I$ i to jest koniec.

$\Longrightarrow$

$M = aR$, wtedy $f : R \to M$, $r \mapsto ra$, jest epimorfizmem R-modułów. Czyli jeśli $I = \ker(f)$, to $R/I \cong M$.

Definicja 11.12.

- Dla $a \in M$ $I_a = \{r \in R \ : \ ra = 0\} \triangleright R$ jest **torsją** elementu a.
- a jest **torsyjny**, gdy $I_a \neq 0$. W przeciwnym przypadku mówimy, że a jest *beztorsyjny* .
- Mówimy, że M jest **modułem torsyjnym**, gdy każdy jego element jest torsyjny. M jest **beztorsyjny** , gdy każdy niezerowy element jest beztorsyjny.
- $M_t = \{a \in M \ : \ a \text{ jest torsyjny}\}$ nazywamy **częścią torsyjną** modułu M

Uwaga 11.13.

1. *M_t jest podmodułem M*
2. *M/M_t jest beztorsyjny.*

Dowód.

1. ćwiczenie
2. Załóżmy, że $m + M_t$ jest torsyjny. Czyli $r(m + M_t) = 0 + M_t$ dla pewnego $r \neq 0$. Ale to oznacza, że $rm \in M_t$. To znaczy, że $r'(rm) = 0$ dla pewnego $r' \neq 0$. Ale wtedy $(r'r)m = 0$ i $r'r \neq 0$, bo R jest dziedziną. Czyli m jest torsyjny i $m \in M_t$. W takim razie $m + M_t = 0$

Przykłady: grupy abelowe torsyjne/beztorsyjne (jako $\mathbb{Z}$-moduły)

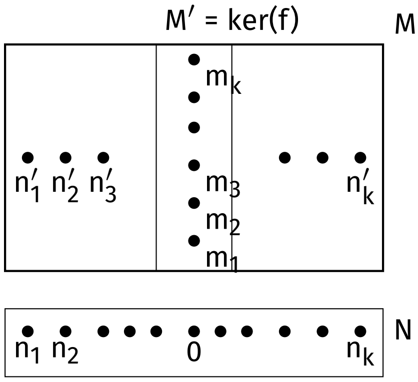
11.6 Moduły skończenie generowane

Twierdzenie 11.14. R *jest pierścieniem przemiennym z* $1 \neq 0$. *Niech* M, N *będą* R*-modułami oraz* $f : M \to N$ *jest epimorfizmem. Niech* $M' = \ker(f)$, $N \cong M/M'$.

1. N, M' *są skończenie generowane, to* M *też jest skończenie generowane*
2. M *jest skończenie generowany, to wtedy* N *też taki jest*

Dowód.

1. Niech $\{n_1, ..., n_k\} \subseteq N$ i $\{m_1, ..., m_l\} \subseteq M$ będą zbiorami generatorów. Weźmy $n'_1, ..., n'_k \in M$ takie, że $f(n'_i) = n_i$.



   W takim razie, $\{n'_1, ..., n'_k, m_1, ..., m_l\}$ generują M, bo dla dowolnego $x \in M$ mamy $f(x) \in N$, więc $f(x) = \sum r_i n_i$ dla $f_i \in R$. Niech więc $M \ni x' = \sum r_i n'_i$. Wtedy $f(x') = \sum r_i n_i$, czyli $f(x - x') = 0$ i mamy $x - x' \in M' = \ker(f)$. Więc $M' \ni x - x'$, z czego dostajemy $x - x' = \sum r'_j m_j$ dla $r'_j \in R$ i $x = x' + (x - x') = \sum r_i n'_i + \sum r'_j m_j$.

2. Ćwiczenie, łatwe. $A \subseteq M \implies f[A]$ generuje N, gdzie A jest zbiorem generatorów M.

Spis twierdzeń