

Algebra 2R

Na podstawie wykładów

Prof. Newelskiego

w semestrze letnim 2022/2023

~



as long as algebra is taught in school, there will be prayer in school

Spis treści

Teoria równań algebraicznych	4
1.1 Rozwiązanie układów równań	4
1.2 Rozszerzanie ciał	6
Ciała skończone i pierwiastki z jedności	10
2.1 Algebraiczne domknięcie ciała	11
Ciała proste, pierwiastki z jedności	13
3.1 Ciała proste	13
3.2 Pierwiastki z jedności	13
3.3 Ciała skończone	15
Rozszerzenia ciał	16
4.1 Wymiar przestrzeni liniowej	16
Wielomiany koła, domknięcia algebraiczne	21
5.1 Wielomian rozkładu koła [cyclotomic polynomials]	21
5.2 Domknięcia algebraiczne	24
Wstęp do teorii Galois	27
6.1 Grupy Galois	27
6.2 Rozszerzenia algebraiczne normalne	27
6.3 Rozszerzenia rozdzielcze	29
Rozszerzenia radykalne (czysty Bangladesz)	32
7.1 Stopień rozdzielczy, radykalny ciała	34
Przekształcenia liniowe	36
8.1 Norma, ślad	36
8.2 Rozszerzenia Galois	37
Rozszerzenia abelowe	41
9.1 Rozszerzenia abelowe	41
9.2 Rozwiązywalne rozszerzenia ciał i rozszerzenia przez pierwiastki	42
Rozszerzenia przestępne ciał	48
10.1 Własności	48
Moduły	50
10.1 Moduły wprowadzenie	50
10.2 Cel: zrozumieć moduły	52
11.3 Suma prosta modułów	53
11.4 Baza modułu	54
11.5 Moduły projektywne, cykliczne, torsyjne	57
11.6 Moduły skończenie generowane	58
Iloczyn tensorowy modułów	61
11.1 Funkcja dwuliniowa	61
12.2 Konstrukcja produktu tensorowego	61
Własności produktu tensorowego	64
13.1 Iloczyn tensorowych funkcji	66
13.2 Iloczyny zewnętrzne	67

Moduły nad pierścieniami PID	69
14.1 Moduły p-primarne	70
14.2 Moduły nierozkładalne	73
Przestrzeń liniowa jako $K[X]$-moduł	74
15.1 Klatki Jordana	74
15.2 R-algebry	75
15.3 Radykały	76

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

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

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

\Rightarrow Rozważamy dwa przypadki:

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

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

2. $(f_1, \dots, f_m) \cap R = \{0\}$. (nie ma wyrazów wolnych różnych od 0)

Teraz wiemy, że układ U jest niesprzeczny, a więc możemy skonstruować pierścień z 1 S będący rozszerzeniem R [$S \supseteq R$] oraz rozwiązanie $\bar{a} \subseteq S$ spełniające nasz układ równań.

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

$$j : R[\bar{X}] \rightarrow S = R[\bar{X}]/(f_1, \dots, f_m)$$

nazywane **przekształceniem ilorazowym**. Po pierwsze, zauważmy, że $j \upharpoonright R$ jest 1 – 1, bo

$$\ker(j \upharpoonright R) = \ker(j) \cap R = (f_1, \dots, f_m) \cap R = \{0\}$$

i dlatego

$$j \upharpoonright R : R \xrightarrow{\cong} j[R] \subseteq S.$$

Z uwagi na ten izomorfizm, będziemy utożsamiać $R, j[R]$. W takim razie, S jest rozszerzeniem pierścienia R . Czyli mamy rozszerzenie pierścienia R .

Niech

$$\bar{a} = (a_1, \dots, a_n) = (j(X_1), \dots, j(X_n)) \subseteq S,$$

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

$$\hat{f}_i(\bar{a}) = \hat{f}_i(j(X_1), \dots, j(X_n)) = j(\hat{f}_i(X_1, \dots, X_n)) = j(f_i) = 0.$$

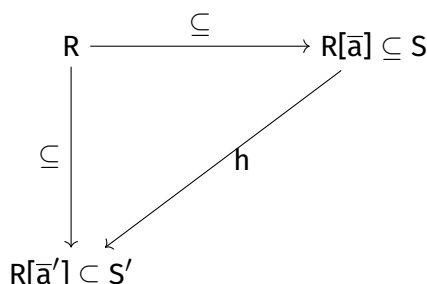


Uwaga 1.2. Skonstruowane powyżej rozwiązanie \bar{a} układu U ma następującą własność uniwersalności:

(🔗) Jeżeli $S' \supseteq R$ jest rozszerzeniem pierścienia R i $\bar{a}' = (a'_1, \dots, a'_m) \subseteq S'$ jest rozwiązaniem U w S' , to istnieje jedyny homomorfizm

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

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



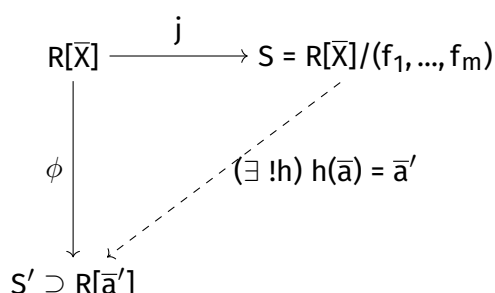
Tutaj $R[\bar{a}] \subseteq S$ jest **podpierścieniem generowanym przez $R \cup \{\bar{a}\}$** , czyli zbiór:

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

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

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

Z twierdzenia o faktoryzacji wie



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

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

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

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

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

Z twierdzenia o homomorfizmie pierścieni dostajemy jedyny homomorfizm

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

taki, że $h(\bar{a}) = \bar{a}'$. ☕

Uwaga 1.3. Jeśli $I = (f_1, \dots, f_m)$, 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, $\text{Im } \phi = \text{Im}(h \circ j)$, a ϕ jest epimorfizmem ("na"), więc również h musi być "na".

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


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

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

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

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

Uwaga 1.4. W sytuacji jak z definicji wyżej, gdy U jest układem niesprzecznym, wtedy \bar{a} jest rozwiązaniem ogólnym układu $U \iff$ zachodzi warunek (\S) .

Dowód. Ćwiczenia. 

1.2 Rozszerzanie ciał

Dla $K \subseteq L$ ciał i $\bar{a} \subseteq L$ definiujemy **ideał \bar{a} nad K** jako:

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

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

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

Tutaj $K(X_1, \dots, X_n)$ to **ciało ułamków pierścienia** $K[\bar{a}]$ w ciele L (czyli najmniejsze ciało, że pierścień może być w nim zanurzony). Czasami oznaczamy to przez $K[\bar{a}]_0$.

Uwaga 1.5. 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 $\phi : K[\bar{a}_1] \rightarrow K[\bar{a}_2]$ taki, że $\phi \upharpoonright K = \text{id}_K$ oraz $\phi(\bar{a}_1) = \bar{a}_2$.
2. $I(\bar{a}_1/K) = I(\bar{a}_2/K)$.

Dowód.

1 \implies 2

Implikacja jest jasna, bo dla $g(\bar{X}) \in K[\bar{X}]$ 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

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

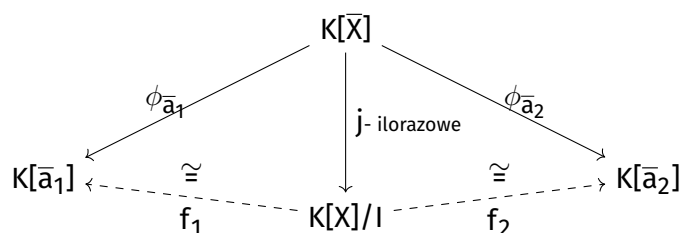
Tak samo dla \bar{a}_2 możemy określić analogicznie odwzorowanie ewaluacyjne $\phi_{\bar{a}_2} : K[\bar{X}] \rightarrow K[\bar{a}_2]$. Wtedy

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

ale ponieważ $I(\bar{a}_1/K) = I(\bar{a}_2/K)$, to $\ker(\phi_{\bar{a}_1}) = \ker(\phi_{\bar{a}_2})$. Oznaczmy $I = I(\bar{a}_1/K) = I(\bar{a}_2/K)$. Widzimy, że $\phi_{\bar{a}_i} \upharpoonright K = \text{id}_K$ (wielomiany mające tylko wyraz stały nie zmieniają wartości po podstawieniu x).

Z twierdzenia o izomorfizmie wiemy, że istnieją izomorfizmy

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



Niech $f = f_2 f_1^{-1} : K[\bar{a}_1] \rightarrow K[\bar{a}_2]$. 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 $\bar{a}_i \neq 0$), 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 $I = (f_1, \dots, f_m)$ dla pewnych $f_i \in K[\bar{X}]$. Wtedy istnieje rozszerzenie pierścienia $S \supseteq K$ oraz $\bar{a} \subseteq S$ - rozwiązanie ogólne układu $f_1(\bar{X}) = \dots = f_m(\bar{X}) = 0$ takie, że $I(\bar{a}/K) = I$.

Dowód. Uwaga 1.4.



Twierdzenie 1.6. Niech $I \triangleleft K[\bar{X}]$. Wtedy istnieje ciało $L \supseteq K$ oraz $\bar{a} = (a_1, \dots, a_n) \subseteq L$ takie, że $f(\bar{a}) = 0$ dla każdego $f \in I$.

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

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

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

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

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

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

Wtedy $g(\bar{a}) = 0$ dla każdego $g(\bar{X}) \in M \supseteq I$ (bo inaczej mielibyśmy wyrazy wolne).



Wniosek 1.7. Niech $f \in K[X]$ stopnia > 0 . Wtedy istnieje ciało $L \supseteq K$ rozszerzające ciało K takie, że f ma pierwiastek w ciele L .

Przykłady:

1. Rozpatrzmy ciało $K = \mathbb{Q}$ i $f(X) = X - 2$. Wtedy $I = (f) \triangleleft \mathbb{Q}[X]$ jest ideałem maksymalnym, bo jest on pierwszy (w tym wypadku nierozkładalny). Równanie $f = 0$ ma rozwiązanie ogólne w pierścieniu ilorazowym

$$\mathbb{Q}[X]/I \cong \mathbb{Q}.$$

Czyli nie zawsze musimy rozszerzać ciało do czegoś nowego.

2. $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i) = \mathbb{R}[z]$ dla każdego $z \in \mathbb{C} \setminus \mathbb{R}$, co jest na liście zadań.

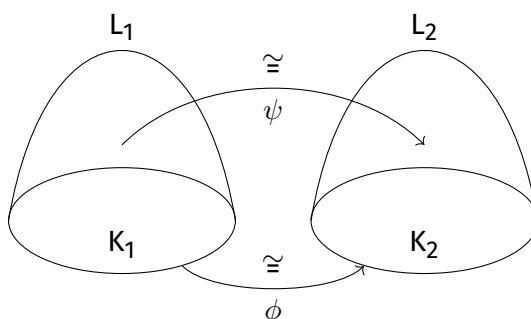
Założmy, że $K \subseteq L_1, K \subseteq L_2$ są rozszerzeniami ciała. Wtedy mówimy, że L_1 jest izomorficzne z L_2 nad K [$L_1 \cong_K L_2$] \iff istnieje izomorfizm $f : L_1 \rightarrow L_2$ taki, że $f \upharpoonright K = \text{id}_K$.

Fakt 1.8.

1. Założmy, 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: założmy, że $\phi : K_1 \rightarrow K_2$ jest izomorfizmem i $f_1 \in K_1[X], f_2 \in K_2[X], \phi(f_1) = f_2, f_i$ jest nierozkładalne. Dodatkowo założmy, że $L_1 = K_1(a_1)$ i $L_2 = K_2(a_2)$, gdzie $f_i(a_i) = 0$ w L_i . Wtedy istnieje izomorfizm $\psi : L_1 \rightarrow L_2$ taki, że $\psi(a_1) = a_2$.

Dowód.

1. $I(a_1/K) = (f) = I(a_2/K)$, stąd na mocy 1.5 mamy $K(a_1) \cong_K K(a_2)$. Po dowodzie przypadku 2. możemy uzasadniać, że jest to szczególny przypadek tego ogólniejszego stwierdzenia właśnie.
2. Zacznijmy od rozrysowania tej sytuacji:



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

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

jest ideałem maksymalnym. Mamy

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

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



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, \dots, a_n , gdzie a_1, \dots, a_n to wszystkie pierwiastki f w L .

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

Wniosek 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 izomorfizmu nad K .

Dowód.

1. Dowód przez indukcję względem stopnia f

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

Założmy teraz, że stopień wielomianu f jest > 1 i też zachodzi dla wszystkich wielomianów stopnia $< \deg(f)$ i wszystkich ciał K' . Teraz z 1.7 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_1 istnieje $L' = K'(a_1, \dots, a_r)$ - ciało rozkładu wielomianu f_1 nad K' . Wtedy

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

jest ciałem rozkładu f nad K .

2. Udowodnimy wersję ogólniejszą:

(👉) Jeśli $\phi : K_1 \xrightarrow{\cong} K_2$ 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 założmy, 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 $\phi \subseteq \psi_0$.

$$\begin{array}{ccc}
 K_1(a_1) & \xrightarrow[\exists \psi_0]{\cong} & K_2(a_2) \\
 \parallel & & \parallel \\
 K'_1 & & K'_2 \\
 \cap & & \cap \\
 L_1 & \xrightarrow[\exists \psi_1]{\cong} & L_2
 \end{array}$$

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. Skonstruujemy 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 $K_0 = K$.

Założmy, że $\alpha < \kappa$ i mamy $\{K_\beta : \beta < \alpha\}$ spełniając warunki powyżej. Niech $K' = \bigcup_{\beta < \alpha} K_\beta$. Musimy pokazać, że K' jest ciałem.

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. $\alpha = \beta + 1$ 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:

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

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

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

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 jednośc

3.1 Ciała proste

Uwaga 3.0. Załóżmy, że mamy ciała $K \subseteq L$. Wtedy

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

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

Przykład:

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

Uwaga 3.1.

1. Każde ciało zawiera jedyne podciało proste
2. Z dokładnością 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 jednośc

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. $\mu_n(R) \triangleleft R^*$ jest grupą jednostek pierścienia
2. $\mu(R) \triangleleft R^*$
3. $\mu(R)$ jest **torsyjną grupą abelową** (każdy element jest pierwiastkiem z 1).

Przykłady

1. $\mu(\mathbb{C}) = \bigcup_{n>0} \mu_n(\mathbb{C}) \subsetneq (\{z \in \mathbb{C} : |z| = 1\}, \cdot) \subset \mathbb{C}^* = \mathbb{C} \setminus \{0\}$ 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. $\mu_n(K) = \{\text{zera wielomianu } x^n - 1\}$. Ten wielomian będziemy oznaczali $w_n(x) = x^n - 1$.

Uwaga 3.3.

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

2. Jeśli $\text{char}(K) = p > 0$ i $n = p^l n_1$ takie, że $p \nmid n_1$, to wszystkie pierwiastki $w_n(x) = x^n - 1$ mają krotność p^l w K .

Dowód:

1. Niech $a \in K$ takie, że $w_n(a) = 0$. Z twierdzenia Bezouta mamy, że

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

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

Z tego, że $\text{char}(K) = 0$ 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 $\text{char}(K) = p$. Niech $n = p^l n_1$. Rozważmy wielomian

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

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

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

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

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

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


Gdyby tak nie było, to istniałby $y \in G$, $\text{ord}(y) \nmid k$. 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 $\text{ord}(y') = p^\alpha$, a dla $x'_0 = x_0^{p^\beta}$ mamy $\text{ord}(x'_0) = k'$. Wobec tego $\text{ord}(x'_0 y') = p^\alpha \cdot k'$, 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 Ciąta skończone

Twierdzenie 3.6. Niech K będzie ciałem skończonym. Wtedy

1. $\text{char}(K) = p \implies |K| = p^n$ dla pewnego $n \in \mathbb{N}$
2. Dla każdego $n > 0$ istnieje dokładnie jedno ciało K takie, że $|K| = p^n$ z dokładnością do izomorfizmu.

Ciało mocy p^n będziemy oznaczać $F(p^n)$.

Dowód. 1. Skoro $\text{char}(K) = p$, to $\mathbb{Z}_p \subseteq K$ jest najmniejszym podciałem 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 przestrzeń liniowa 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 $K = \{0\} \cup \{\text{pierwiastki } w_{p^{n-1}}\}$. 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 $f^n = f \circ \dots \circ f$, $f^n(x) = x^{p^n}$. 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 .

Założmy nie wprost, że K' to inne ciało mocy p^n . Bez 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 $f \in K[X]$ różny 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 $\widehat{}$ oznacza homomorfizm ewaluacji, który jest również homomorfizmem w punkcie. Czyli

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

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

Założmy, 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

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

$$0 = f(a)a - 1 = b_n a^{n+1} + b_{n-1} a^n + \dots + b_0 a - 1,$$

stąd mamy, że

$$a^{n+1} = -\frac{1}{b_n}(b_{n-1}a^n + \dots + b_0 a - 1) \in \text{Lin}_K(1, a, \dots, a^n)$$

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

$$(\forall m \geq 0) a^m \in \text{Lin}_K(1, a, \dots, a^n).$$

1. $m = 0, \dots, n+1$ bo one są już w $\text{Lin}_K(1, a, \dots, a^n)$.

2. Zakładamy teraz, że dla m mamy

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

i pokazujemy dla $m+1$.

$$a^{m+1} = a \cdot a^m = a \sum_{i=0}^n c_i a^i = \sum_{i=0}^n c_i a^{i+1} \in \text{Lin}_K(1, a, \dots, a^n),$$

bo $a^{n+1} \in \text{Lin}_K(1, a, \dots, a^n)$.

Czyli

$$K[a] = K(a) = \text{Lin}_K(1, a, \dots, a^n),$$

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

3 \implies 1

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

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

jest zbiorem liniowo zależnym. Z liniowej zależności wiemy, że

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

Stąd dla $f \in K[X]$ zadanego wzorem

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

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. Oczywiście. 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

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

Czyli $K(a) = \text{Lin}_K(1, a, \dots, a^{n-1})$ i wystarczy zobaczyć, że $\{1, \dots, a^{n-1}\}$ jest liniowo niezależny. W przeciwnym przypadku dla pewnego $0 < r < n$ $a^r \in \text{Lin}_K(1, a, \dots, a^{r-1})$, czyli istnieje wielomian taki, że a jest jego pierwiastkiem, a stopień jest nie większy niż $r < n$ i to daje sprzeczność.

Czyli $\text{Lin}_K(1, a, \dots, a^n)$ 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

$$K(a) = K[a] = \left\{ \sum_{i=0}^{n-1} b_i a^i : b_i \in K \right\}$$

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 zbiorów 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 l.n.z., czyli istnieją $k_{ij} \in K$ takie, że

$$\sum_{j \in J} \sum_{i \in I} k_{ij} e_i f_j = 0,$$

ale $\sum_i k_{ij} e_i = l_j$ 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 $j \neq j'$ $e_i f_j = e_{i'} f_{j'}$. 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

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

Okazuje się, że K_{alg} jest podciałem.

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

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

Z faktu 4.6 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. $K_{\text{alg}}(L)$ nazywamy **algebraicznym domknięciem** K w L .
2. K jest **relatywnie algebraicznie domknięte** w $L \iff K_{\text{alg}}(L) = K$.

Przykłady:

1. $\mathbb{Q}_{\text{alg}}(\mathbb{C}) := \hat{\mathbb{Q}} = \mathbb{Q}^{\text{alg}}$ jest to tak zwane **ciało liczb algebraicznych**. $\hat{\mathbb{Q}}$ jest przeliczalne, bo $\mathbb{Q}[x]$ jest przeliczalne, więc jest mnóstwo liczb **przestępnych** (zespólonych, 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

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

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

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 $f \in L[X]$

$$f = \sum_{i=0}^n a_n x^i, \quad a_n \neq 0$$

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

$$[K(m) : K] \leq [K(a_0, \dots, a_n, m) : K] \stackrel{4.6}{=} [K(a_0, \dots, a_n, m) : K(a_0, \dots, a_n)] [K(a_0, \dots, a_n) : K] < \infty$$

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

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

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

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

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 $\mu_m(\mathbb{C}) \iff \text{NWD}(k, m) = 1$

Funkcja Eulera:

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

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

Niech

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

i zdefiniujmy

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

F_m to m -ty wielomian cyklotomiczny.

Uwaga 5.3.

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

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

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

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

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

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

$w_m(x)$ 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 $\mathbb{Z}[X]$.

Założmy 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 $\text{NWD}(l, m) = 1$.

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

$$\text{pierwiastek } G_1 = \varepsilon, \varepsilon^{p_1}, \varepsilon^{p_1 p_2}, \dots, \varepsilon^{p_1 \dots p_s} = \tau \text{ pierwiastek } G_2$$

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

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

i indukowany przez niego epimorfizm pierścieni

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

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

Stąd wiemy, że

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

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

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 $d = \sup_{x \in I} \widehat{f}'(x)$.

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

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

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

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

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



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 $\widehat{K}, K^{\text{alg}}$.

Uwaga 5.8. Dla każdego K istnieje algebraiczne domknięcie \hat{K} .

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

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

1. \hat{K} jest algebraicznie domknięte:

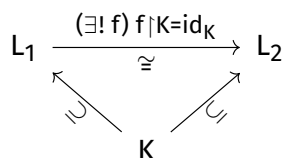
Jeżeli $f \in \hat{K}[X]$, to f ma pierwiastek w K , ale $\hat{K} \subseteq K_\infty$, to znaczy, że $a \in \hat{K}$ jest algebraiczne nad K .

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

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



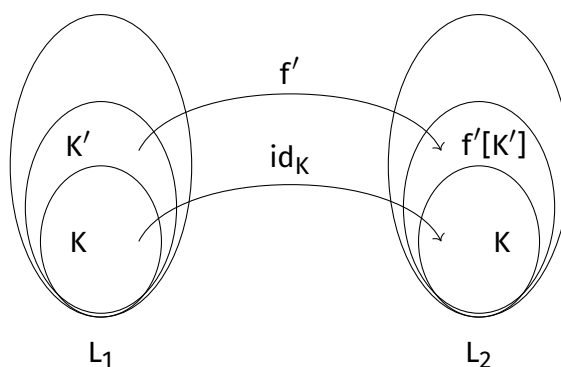
Twierdzenie 5.9. \hat{K} jest jedyne z dokładnością do izomorfizmu nad K .



Dowód. Można użyć indukcji pozaskończonej, a można też użyć lematu Zorna. My zrobimy to drugie.

Niech

$$\mathfrak{K} = \{(k', f') : K \subseteq K' \subseteq L_1, f' : K' \xrightarrow{1-1} L_2, f' \upharpoonright K = \text{id}_K\}$$



Oczywiście, $\mathfrak{K} \neq \emptyset$, bo $(K, \text{id}_K) \in \mathfrak{K}$. W \mathfrak{K} definiujemy relację porządku w naturalny sposób, to znaczy

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

Wtedy (\mathfrak{K}, \leq) jest zbiorem częściowo uporządkowanym i niepustym (bo jest $(K, \text{id}_K) \in \mathfrak{K}$). 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 $K_1 = L_1$.

Założmy 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

$$K_2 = f_1[K_1]$$

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

$v(x)$ 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 $(K_1, f_1) \preceq (K_1(a), f_2)$, 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 algebraicznie 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 $(x - c) | f_b(x)$ 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 $f_0 : LK \rightarrow L$ jest izomorfizmem ciał, to istnieje izomorfizm $f : \widehat{K} \rightarrow \widehat{L}$ taki, że $f \upharpoonright K = f_0$.

Dowód. Ćwiczenia



Uwaga 5.11. Jeśli $K \subseteq L$ jest algebraicznym rozszerzeniem ciał, to istnieje monomorfizm $f : L \rightarrow \widehat{K}$ taki, że $f \upharpoonright K = \text{id}_K$.

Dowód. Ćwiczenie



Wykład 6: Wstęp do teorii Galois

6.1 Grupy Galois

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

$$G(L/K) = \text{Gal}(L/K) = \{f \in \text{Aut}(L) : f|_K = \text{id}_K\} = \text{Aut}(L/K)$$

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

Przykład:

- Niech K będzie ciałem prostym ($\cong \mathbb{Q}$ lub \mathbb{Z}_p). Wtedy $\text{Gal}(L/K) = \text{Aut}(L)$, bo
 - Niech $\text{char}(K) = \text{char}(L) = p > 0$ i niech $f \in \text{Aut}(L)$. Wtedy $f(1) = 1$, $f(\underbrace{1 + \dots + 1}_k) = \underbrace{1 + \dots + 1}_k$, a ponieważ $K = \{\underbrace{1 + \dots + 1}_k : k \in \{1, \dots, p\}\}$, zatem $f|_K = \text{id}_K$, czyli $f \in \text{Gal}(L/K)$.
 - Niech $\text{char}(K) = \text{char}(L) = 0$, wtedy $K \cong \mathbb{Q}$. Niech $f \in \text{Aut}(L)$. Wtedy $f(0) = 0$, $f(1) = 1$, a dla dowolnego $k \in \mathbb{N}$ $f(\underbrace{1 + \dots + 1}_k) = \underbrace{1 + \dots + 1}_k$, 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 $f|_K = \text{id}_K$.
- $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \text{Aut}(\mathbb{Q}(\sqrt{2})) = \{f_0, f_1\} \cong \mathbb{Z}$, bo $\sqrt{2}$ może przejść na siebie albo na $-\sqrt{2}$. Wtedy $f_0 = \text{id}$, a $f_1(-\sqrt{2})$

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

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

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

Dowód.

$$\begin{array}{ccc} K[a] & \xrightarrow[\cong]{f} & K[b] \\ \downarrow \subseteq & & \downarrow \subseteq \\ K[a]^{\text{alg}} = \hat{K} & \xrightarrow[\cong]{\exists f'} & \hat{K} = K[b]^{\text{alg}} \end{array}$$

Co jest wnioskiem z wniosku 5.10.



6.2 Rozszerzenia algebraiczne normalne

\hat{K} jest największym algebraicznym rozszerzeniem K tzn. $K \subseteq L$ oznacza, że istnieje $f : L \rightarrow \hat{K}$ monomorfizm ciał taki, że $f|_K = \text{id}_K$. ☕

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

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

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

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

\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 $\text{Gal}(\widehat{L}_1/L_1) \leq \text{Gal}(\widehat{K}/K)$.

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 $L \subseteq \widehat{K}$.

\implies

Dowód nie wprost, to znaczy założymy, 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 $f \in \text{Gal}(\widehat{K}/K)$ takie, że $f(b) = a$, więc $f[L] = L$ co jest sprzeczne z 6.2.

\impliedby

Założmy nie wprost, że na mocy 6.2. istnieje $f \in \text{Gal}(\widehat{K}/K)$ 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 $f|_K = \text{id}_K$. Czyli w_a jest wielomianem minimalnym dla $b = f(a)/K$. Czyli $L \stackrel{f}{\cong} f[L]$. Z (☝) wiemy, że $w_a(x)$ rozkłada się nad L na czynniki liniowe. Czyli $w_a(x) \dots f[L] \dots$, 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 założymy, że $K \subseteq L \subseteq \widehat{K}$.

(2) \implies (1)

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

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

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

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

(1) \implies (2)

Niech $K \subseteq L$ będzie skończone i normalne. Wtedy $L = K(a_1, \dots, a_n)$ dla pewnych $a_1, \dots, a_n \in L$ i $\{a_1, \dots, a_n\}$ będzie bazą L nad K . Wtedy wiemy, że dla każdego i istnieje $w_i \in K[X] \setminus \{0\}$ taki, że $w_i(a_i) = 0$ i w_i rozkłada się na czynniki liniowe (bo $K \subseteq L$ normalne). Niech więc $w(x) = \prod w_i(x)$. Zachodzi $w(a_i) = 0$ dla każdego i i w rozkłada się na czynniki liniowe w L , bo każdy w_i się rozkładał. Zatem

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

i L jest ciałem rozkładu $w \in K[X]$.



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 $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$

Uwaga 6.5. Niech $K \subseteq L \subseteq \hat{K}$ i niech L_1 będzie ciałem generowanym przez $\bigcup \{f[L] : f \in \text{Gal}(\hat{K}/K)\}$. Wtedy L_1 to **normalne domknięcie ciała L w \hat{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 $L_1 \rightarrow L_2$ taki, że $f|_K = \text{id}$.

Dowód. (1) Z 6.2

(2)

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

6.3 Rozszerzenia rozdzielcze

- Niech K będzie ciałem i $a \in \hat{K}$. Mówimy, że a jest **rozdzielczy nad K** , gdy wielomian minimalny a , $w_a(x) \in K[X]$ ma tylko pierwiastki jednokrotne w \hat{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 \hat{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 $\text{char}(K) = 0$, to w jest rozdzielczy
3. Jeśli $\text{char}(K) = p > 0$, 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 $\text{char}(K) = 0$, 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 $K = \mathbb{F}_p(X) \subseteq L = K(\sqrt[p]{X})$. 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 : $w_a(T) = (t - a)^p \cdot a$

Lemat 6.7.

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

Dowód.

$$\{f(a) : f \in \text{Gal}(\widehat{K}/K)\} \stackrel{6.1}{=} \{\text{pierwiastki wielomianu minimalnego } w_a \in K[X] \text{ nad } K\}$$

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, $L = K(a_1, \dots, a_n)$ i a_1, \dots, a_n rozdzielnicy nad K . Wtedy istnieje $a^* \in L$ rozdzielnicy nad K taki, że $L = K(a^*)$.

Dowód. Bez starty ogólności założmy, 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 $(n-1) \implies n$:

$$K(a_1, \dots, a_{n-1}) = K(b)$$

$$K(a_1, \dots, a_{n-1}, a_n) = K(b, a_n)$$

Niech teraz k będzie stopniem b nad K , a m - stopniem a_n nad $K(b)$. Z lematu 6.7 wiemy, że istnieją $f_1, \dots, f_k \in \text{Gal}(\widehat{K}/K)$ takie, że $f_1(b), \dots, f_k(b)$ są parami różne. Niech więc $f_{1,1}, \dots, f_{1,m} \in \text{Gal}(\widehat{K}/K(b))$ takie, że $f_{1,1}(a), \dots, f_{1,m}(a)$ są parami różne.

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

$$\begin{array}{ccccc} K(b)(a) & \xrightarrow{f_{i,j}} & K(b, f_{1,j}(a)) & \xrightarrow{f_i} & K(f_i(b), f_i(f_{1,j}(a))) \\ \subseteq \uparrow & \searrow \subseteq & & \searrow \subseteq & \\ K(b) & \xrightarrow{\quad} & K(f_i(b)) & & \\ \subseteq \uparrow & & \subseteq \uparrow & & \\ K & & K & & \end{array}$$

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 $f_{i,j}(a) = f_i(f_{1,j}(a)) \neq f_i(f_{1,j'}(a)) = f_{i',j'}(a)$, 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

$$F(x) = \prod_{\langle i,j \rangle \neq \langle i',j' \rangle} [f_{i,j}(b) + f_{i,j}(a)x - (f_{i',j'}(b) + f_{i',j'}(a)x)]$$

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 $L = K(a_1, \dots, a_n)$ 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 $L = K(b, a)$.

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

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

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

bo a jest rozdzielczy nad K . Dalej,

$$(*) = |\{(f(b), f(a)) : f \in \text{Gal}(\widehat{K}/K)\}| = (**),$$

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

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

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.

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

Dowód.

- $w_a(x)$ ma tylko pierwiastki jednokrotne, gdy $\text{char}(K) = 0$
- Oczywiste \star
- \Leftarrow oczywiste: $w_a(x) \in K[X]$ dzieli $x^{p^n} - a^{p^n} = (x - a)^{p^n} \in K[X]$
 \Rightarrow Dowodzimy indukcyjnie 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

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

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

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

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

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



✿ $\widehat{K}^s = \text{sep}_{\widehat{K}}(K)$ jest rozdzielczym domknięciem K

✿ $\widehat{K}^r = \text{rad}_{\widehat{K}}(K)$ jest radykalnym domknięciem K .

Uwaga 7.3.

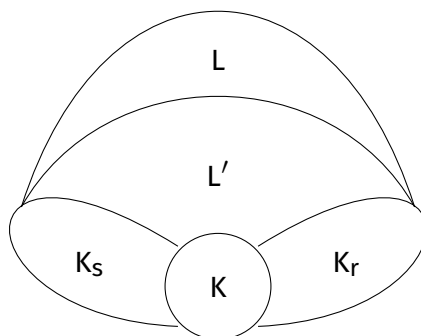
1. Gdy $K \subseteq L \subseteq \widehat{K}$, to $\text{sep}_L(K) = \widehat{K}^S \cap L$, $\text{rad}_L(K) = \widehat{K}^r \cap L$
2. Załóżmy, że $K \subseteq L \subseteq M \subseteq \widehat{K}$, wtedy $K \underset{\text{rad}}{\subseteq} L \underset{\text{rad}}{\subseteq} M \iff K \underset{\text{rad}}{\subseteq} M$
3. Jeśli $\text{char}(K) = 0$, to $\text{sep}_L(K) = K^{\text{alg}}(L)$ i $\text{rad}_L(K) = K$, oraz $\widehat{K}^S = \widehat{K}$, $\widehat{K}^r = K$.

Fakt 7.4. Załóżmy, że $K \subseteq L \subseteq \widehat{K}$, $K_S = \text{sep}_L(K)$, $K_r = \text{rad}_L(K)$, $L' = K_S \cdot K_r$ 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 $\text{char}(K) = 0$, to problem jest trywialny, bo $K_r = K$, $K_S = L$ i $L' = L$.

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



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 $[K_S^0 : K] = \text{stopień } a \text{ nad } K$, $[K_r^0(a) : K_r^0] = \text{stopień } a \text{ nad } K_r^0$. Wystarczy pokazać, że oba te stopnie się zgadzają.

Niech $n = [K(a) : K] = \text{stopień } a \text{ nad } K$. Wtedy

$$1, a, \dots, a^{n-1}$$

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

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

też jest bazą $K(a)$ nad K .

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

- liniowa niezależność:

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

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 założmy, że $[L : K] < \infty$, bo

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

- (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 $f \in \text{Gal}(\widehat{K}/K)$ 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 oznacza, 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 rozdzielczy nad K . Czyli $a^{p^l} \in K_s$, więc a jest radykalny nad K_s .

Z punktów 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 rozdzielczy, bo $L' = K_r[K_s]$.



7.1 Stopień rozdzielczy, radykalny ciała

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

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

Z wyników wyżej dostajemy

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

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

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

1. Jeśli $K \subseteq L$ jest rozdzielcze, to $[L : K] = |\{f \upharpoonright L : f \in \text{Gal}(\widehat{K}/K)\}| = |\{f : L \rightarrow \widehat{K} : f \upharpoonright K = \text{id}\}|$
2. Ogólnie, $[L : K]_S = |\{f \upharpoonright L : f \in \text{Gal}(\widehat{K}/K)\}|$ (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 $f \in \text{Gal}(\widehat{K}/K)$, $f \upharpoonright L$ 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 $f \upharpoonright L$ jest wyznaczone przez $f \upharpoonright K_S$. Dlatego:

$$|\{f \upharpoonright L : f \in \text{Gal}(\widehat{K}/K)\}| = |\{f \upharpoonright K_S : f \in \text{Gal}(\widehat{K}/K)\}| = [K_S : K] = [L : K_S] \stackrel{\text{sep}_L(K)}{=} [L : K]$$



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

Dowód. Indukcja względem $[L : K]_r = [L : K_S]$. Bez starty ogólności założmy, 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

$$f_a : L \rightarrow L$$

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

będący K -liniowym przekształceniem.

8.1 Norma, ślad

$\Rightarrow N_{L/K}(a) = \det(f_a)$ jest normą homomorfizmu f_a

$\Rightarrow \text{Tr}_{L/K}(a) = \text{Tr}(f_a)$ jest śladem f_a .

Fakt 8.1. Niech $\{f_1, \dots, f_k\} = \{f : L \rightarrow \hat{K} : f|_K = \text{id}\}$, $k = [L : K]_S$ i $a \in L$. Wtedy

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

$$2. \text{Tr}_{L/K}(a) = [L : K]_r \cdot \sum_{i=1}^k f_i(a).$$

Rozważmy najpierw przypadek, gdy $L_K(a)$ i a jest rozdzielczy nad K . Niech $w_a(x) = x^k + a_{k-1}x^{k-1} + \dots + a_1x + a_0 \in K[X]$ będzie wielomianem minimalnym dla a nad K . Niech $b_1 = a, \dots, b_n \in \hat{K}$ 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 \hat{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

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

$$\text{Tr}_{L/K}(a) = -a_{k-1} = \sum f_i(a)$$

Dowód.

1. Niech $a \in L$. Wtedy

$$[L : K_S] = [L : \text{sep}_L(K)] = [L : K]_r = p^l \xrightarrow{\text{zad}} a^{p^l} \in K_S.$$

Mamy więc

$$[N_{L/K}(a)]^{p^l} = N_{L/K}(a^{p^l}) \stackrel{\text{zad}}{=} [N_{K_S/K}(a^{p^l})]^{[L:K_S]} = [N_{K_S/K}(a^{p^l})]^{p^l}.$$

Niech $b = a^{p^l}$, wtedy

$$N_{K_S/K}(b) \stackrel{\text{zad}}{=} [N_{K(b)/K}(b)]^{[K_S:K(b)]} \stackrel{\text{zad}}{=} \prod_{i=1}^k f_i(b)$$

Tutaj $f_1, \dots, f_k : L \rightarrow \hat{K}$ są parami różne, więc $f_1|_{K_S}, \dots, f_k|_{K_S} : K_S \rightarrow \hat{K}$ również są parami różne.

Dlatego zachodzi

$$N_{L/K}(a) = N_{K_S/K}(b) = \prod_{i \leq k} f_i(a^{p^l}) = \left[\prod_{i \leq k} f_i(a) \right]^{p^l}$$

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

(a) $a \in K_S$, to $\text{tr}_{L/K}(a) = [L : K_S] \cdot \text{Tr}_{K_S/K}(a) \underset{\text{char}(K)=p}{=} 0$

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

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

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

mamy

$$\text{Tr}_{L/K}(a) = [L : K(a)] \cdot \text{Tr}_{K(a)/K}(a)$$

Możemy wziąć b takie, że $K(a, b) = L$. Teraz liczymy homomorfizmy $L \xrightarrow{\hat{K}} \hat{K}$ i dostajemy:

$$[L : K(a)] \cdot \text{Tr}_{K(a)/K}(a) = \sum_{i \leq k} f_i(a)$$



8.2 Rozszerzenia Galois

$$K \subseteq L \subseteq \hat{K}$$

➡ Mówimy, że rozszerzenie algebraiczne jest **Galois**, gdy dla każdego $a \in L \setminus K$ istnieje $f \in \text{Gal}(L/K)$ takie, że $f(a) \neq a$.

➡ Niech $G \leq \text{Aut}(L)$. Wtedy **ciałem punktów stałych** grupy G nazywamy

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

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

Przykłady:

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

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

Niech $v(x) = (x - a_1)(x - a_2) \dots (x - a_n) \in L[X]$, wtedy $v(x) | w_a(x)$ i $v(x)$ jest niezmienniczy względem $\text{Gal}(L/K)$ [f permutuje a_1, \dots, a_n]. Czyli $v(x) \in L^{\text{Gal}(L/K)}[X] = K[X]$, 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.

\Leftarrow

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 $f \in \text{Gal}(\hat{K}/K)$ takie, że $f(a) = a'$. Ponieważ $K \subseteq L$ było normalne, to $f[L] = L$ i mamy $f \upharpoonright L \in \text{Gal}(L/K)$, $f \upharpoonright L(a) \neq a$, czyli z uwagi wcześniej $K \subseteq L$ jest Galois. ☕

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

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

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

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

Niech $a \in L \setminus L^G$, $\{a = a_0, \dots, a_l\} = G(a)$ będzie orbitą a w L . Niech $w(x) = (x - a_0)(x - a_1) \dots (x - a_n) \in L[X]$. 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 $|\text{Gal}(L^G/L)| = \deg(w_a) = [L : L^G] \leq |G|$. Ponieważ $G \leq \text{Gal}(L/L^G)$, to $G = \text{Gal}(L/L^G)$ i $[L : L^G] = |G|$ ☕

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

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

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

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

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

Od razu pojawiają nam się naturalne homomorfizmy:

$$\Gamma : \mathcal{L} \rightarrow \mathcal{G}$$

$$L' \mapsto \text{Gal}(L/L') \leq \text{Gal}(L/K)$$

$$\Lambda : \mathcal{G} \rightarrow \mathcal{L}$$

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

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

Dowód.

$$\mathcal{L} \ni L' \xrightarrow{\Gamma} \text{Gal}(L/L') \xrightarrow{\Lambda} L^{\text{Gal}(L/L')} = L',$$

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

Czyli $\Lambda \circ \Gamma = \text{id}_{\mathcal{L}}$. Tak samo w drugą stronę:

$$\mathcal{G} \ni H \xrightarrow{\Lambda} L^H \subseteq K \xrightarrow{\Gamma} \text{Gal}(L/L^H) = H$$



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

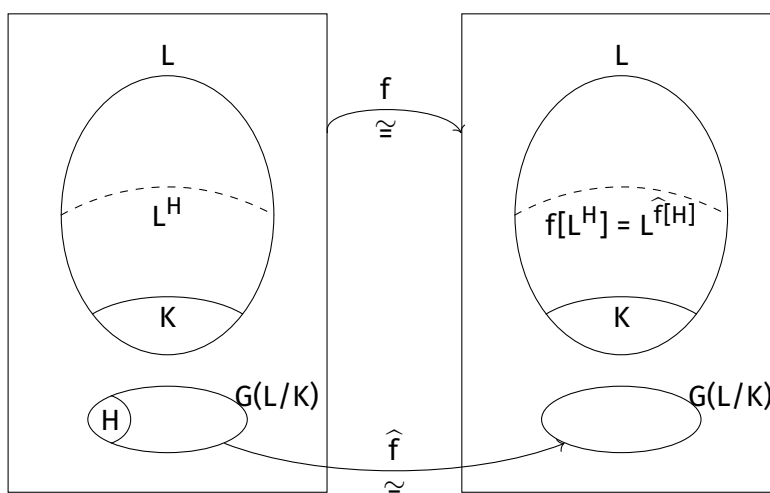
Ponadto wtedy $\text{Gal}(L^H/K) \cong \text{Gal}(L/K)/H$

Przed dowodem ćwiczenie, które pojawi się na liście zadań:

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

Dowód. Mocno rysunkowy (teoria modeli). Niestety, twórca notatek nie miał nigdy wcześniej styczności z teorią modeli.

Weźmy $f \in \text{Gal}(L/K)$



Mamy strukturę 2-sortową:

$$(L, \text{Gal}(L/K), \star),$$

gdzie L to struktura ciała, $\text{Gal}(L/K)$ daje strukturę grupy, a \star jest działaniem $\text{Gal}(L/K)$ na L .

Przekształcenie $f : L \xrightarrow{\cong} L$ indukuje izomorfizm

$$\hat{f} : \text{Aut}(L) \xrightarrow{\cong} \text{Aut}(L)$$

$$\hat{f}(\phi) = f \circ \phi \circ f^{-1},$$

to znaczy $\hat{f} = j_f \in \text{Inn}(\text{Aut}(L))$, gdzie $\text{Inn}(G)$ to automorfizmy powstałe przez sprzężanie f z ϕ .

Ponieważ $f \upharpoonright K = \text{id}_K$, to f indukuje również $\hat{f} : \text{Gal}(L/K) \rightarrow \text{Gal}(L/K)$, czyli

$$\hat{f} = j_f \in \text{Inn}(\text{Gal}(L/K))$$

Mamy więc izomorfizm

$$f \cup \hat{f} : (L, \text{Gal}(L/K), \star) \xrightarrow{\cong} (L, \text{Gal}(L/K), \star).$$

Czyli

$$L^H = \bigcap_{g \in H} \text{Fix}(g) \implies f[L^H] = \bigcap_{g \in \hat{f}[H]} \text{Fix}(g) = L^H = L^{\hat{f}[H]}$$



Dowód. Wersja bardziej zrozumiała dla zwykłych śmiertelników.

Pierwszą obserwację jest:

$$H \triangleleft \text{Gal}(L/K) \iff (\forall f \in \text{Gal}(L/K)) \hat{f}[H] = fHf^{-1} = H \xLeftrightarrow{\Gamma} L^{\hat{f}[H]} = L^{fHf^{-1}} = L^H$$

$$\begin{aligned} L^{\hat{f}[H]} &= L^{fHf^{-1}} = \{a \in L : (\forall g \in H) f(g(f^{-1}(a))) = a\} = \\ &= f[\{f^{-1}(a) : (\forall g \in H) g(f^{-1}(a)) = f^{-1}(a)\}] = f[L^H] \end{aligned}$$

Czyli mamy $f[L^H] = L^{\hat{f}[L]} = L^H$, co jest możliwe $\iff K \subseteq L^H$ jest rozszerzeniem normalnym.

Założmy, że $H \triangleleft \text{Gal}(L/K)$, tzn. $K \subseteq L^H$ jest rozszerzeniem Galois z poprzedniej części dowodu. Mamy wtedy

$$\phi : \text{Gal}(L/K) \twoheadrightarrow \text{Gal}(L^H/K)$$

czyli obcięcie identyczności do L^H . Jądro tego przekształcenia to:

$$\ker(\phi) = \{f \in \text{Gal}(L/K) : f \upharpoonright L^H = \text{id}_{L^H}\} = \text{Gal}(L/L^H) = H$$

tak jak w twierdzeniu Artina 8.4. Dlatego, na mocy twierdzenia o izomorfizmie grup, istnieje izomorfizm

$$\text{Gal}(L^H/K) \cong \text{Gal}(L/K)/H$$



Wykład 9: Rozszerzenia abelowe

9.1 Rozszerzenia abelowe

Założmy, że $K \subseteq L$ jest skończonym rozszerzeniem Galois. Wtedy rozszerzenie $K \subseteq L$ jest abelowe (cykliczne) gdy $\text{Gal}(L/K)$ 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 $\text{Gal}(L/L_1) \triangleleft \text{Gal}(L/K)$ wynika, że $K \subseteq L_1$ i $L_1 \subseteq L$ jest rozszerzeniem Galois i $\text{Gal}(L_1/K) \cong \text{Gal}(L/K)/\text{Gal}(L/L_1)$. Dlatego mamy $\text{Gal}(L/L_1)$ i $\text{Gal}(L_1/K)$ są abelowe (cykliczne). ☕

Przykłady:

- Niech $K \subseteq \hat{K}$ i $\zeta \in \hat{K}$ będzie pierwiastkiem pierwotnym stopnia $n \geq 1$.

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

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

- Niech $\text{char}(K) = p$ 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 $i = 0, \dots, n-1$.

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

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

jest monomorfizmem, ponieważ

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

$$\text{Gal}(L/K) \ni g \mapsto l_g$$

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

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

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

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

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

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

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

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

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

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

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

dla wszystkich $i = 0, 1, \dots, n-1$. 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 $\alpha_1, \dots, \alpha_n \in \text{Aut}(L)$, $a_1, \dots, a_n \in L$ i każdy jest $\neq 0$. Wtedy

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

Innymi słowy: $\alpha_1, \dots, \alpha_n$ 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:

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

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

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

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

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

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

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 $\text{char}(K) = p$)
- lub $x^p - x - b_i$ dla L_{i+1} nad L_{i+1}

Twierdzenie 9.6. Założmy, 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 rozwiązywalne.

Dowód. \implies

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

$$\text{Gal}(L_0/L_k) \triangleright \text{Gal}(L_0/L_{k-1}) \triangleright \text{Gal}(L_0/L_{k-2}) \triangleright \dots \triangleright \text{Gal}(L_0/L_1) \triangleright \{e\}$$

faktorami tego ciągu są $\text{Gal}(L_i/L_{i+1})$. 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 .

$$L_i = L_{i+1}(\zeta_{n_i}, a_i) \stackrel{(\clubsuit)}{\supseteq} L_{i+1}(\zeta_{n_i}) \supseteq L_{i+1}$$

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

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

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

Stąd

$$\text{Gal}(L_i/L_{i+1}) \stackrel{(\heartsuit)}{\triangleright} \text{Gal}(L_i/L_{i+1}(\zeta_{n_i})) \triangleright \{e\}$$

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

- $x^p - x - b_i$

Niech $a \in L_i$ będzie pierwiastkiem 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 $a, a + 1, \dots, a(p - 1) \in L_i$ i wszystkie są pierwiastkami wielomianu wyżej. Stąd $L_i = L_{i+1}(a)$.

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

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

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

\Leftarrow

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

Niech

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

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

$$\begin{array}{ccccccc} L & = & L^{G_0} & \supseteq & L^{G_1} & \supseteq & \dots \supseteq K \\ & & \text{"} & & \text{"} & & \text{"} \\ & & L_0 & \supseteq & L_1 & \supseteq & \dots \supseteq L_k \end{array}$$

jest ciągiem rozszerzeń cyklicznych, prostych.

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

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

- $\text{carh}(K) = p \neq n$ lub $\text{char}(K) = 0$

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, $[L(\zeta) : K(\zeta)] \mid [L : K]$, bo $\text{Gal}(L(\zeta)/K(\zeta)) \hookrightarrow \text{Gal}(L/K) \cong \mathbb{Z}_n^*$. 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.

- $\text{char}(K) = p = n$

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

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

Dla $b' = \frac{1}{K}b$ mamy $\text{Tr}_{L/K}(b') = 1$.

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

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

ale

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

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



Przykłady:

1. Niech $S_n := \text{Sym}(\{x_1, \dots, x_n\})$ 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 $S_n < \text{Aut}(L)$. Z twierdzenia Artina wiemy, że $K \subseteq L$ jest rozszerzeniem Galois oraz $S_n = \text{Gal}(L/M)$.

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

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

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

2. Gdy $K \subseteq L$ jest rozszerzeniem ciał oraz L jest ciałem rozkładu nad K wielomianu $w(x)$ stopnia co najwyżej 4, to $\text{Gal}(L/K)$ 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 $M = L^{\text{Gal}(L/K)}$. Wtedy z twierdzenia Artina wiemy, że $K \subseteq M$ jest radykalne, a $M \subseteq L$ jest Galois (fakt 7.4.). $\text{Gal}(L/M) = \text{Gal}(L/K) \implies M \subseteq L$ jest rozszerzeniem pierwiastkowym, tzn:

$$L \subseteq L_0 \supseteq L_1 \supseteq \dots \supseteq L_k = M,$$

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

Dowód. \subseteq jasne

\supseteq

$$\begin{aligned} K(\bar{\sigma}) &\subseteq K(\bar{x})^{S_n} \subseteq K(\bar{x}) \\ n! &= [K(\bar{x}) : K(\bar{x})^{S_n}] \leq [K(\bar{x}) : K(\bar{\sigma})] \leq n!, \end{aligned}$$

z czego ostatnia nierówność zachodzi, bo $K(\bar{x})$ jest ciałem rozkładu wielomianu

$$w(T) = (T - x_1) \dots (T - x_n)$$

nad $K(\bar{\sigma})$. Czyli mamy

$$[K(\bar{x}) : K(\bar{x})^{S_n}] = [K(\bar{x}) : K(\bar{\sigma})]$$

i zawieranie $K(\bar{\sigma}) \subseteq K(\bar{x})^{S_n}$ jest tak naprawdę równością.

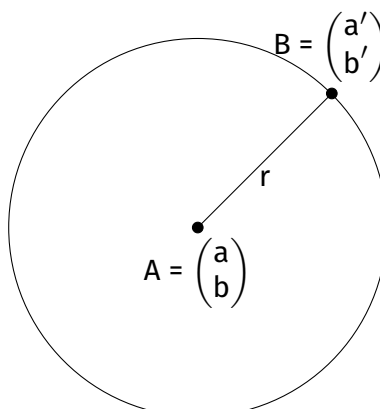


Można też pokazać, że $K[\sigma_1, \dots, \sigma_n] = K[x_1, \dots, x_n]^{S_n}$, co jest **podstawowym twierdzeniem o wielomianach symetrycznych**.

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

- **cyrkiel**

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

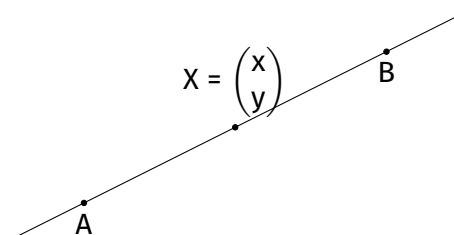


czyli $r = \sqrt{(a' - a)^2 + (b' - b)^2}$

- **linijka**

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

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



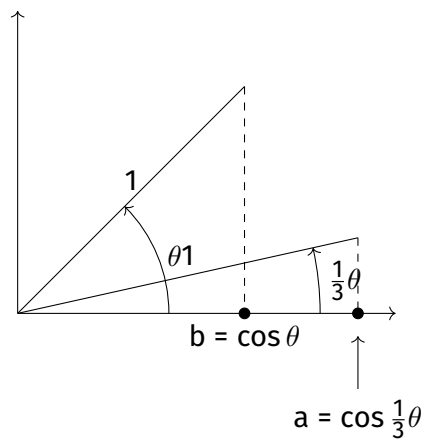
Niech $(a_1, b_1), \dots, (a_n, b_n) \in \mathbb{R}^2$. Punkt $(a, b) \in \mathbb{R}^2$ jest konstruowany przy pomocy cyrkla i linijki na płaszczyźnie \mathbb{R}^2 z punktów $(a_1, b_1), \dots, (a_n, b_n)$ i punktów $(0, 1), (1, 0) \iff$ rozszerzenie ciał $K \subseteq K(a, b)$ jest rozszerzeniem przez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

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

➡ $\text{acl}_K : P(U) \rightarrow P(U)$ to operator algebraicznego domknięcia nad K taki, że dla $A \subseteq A$ $\text{acl}_K(A) = K(A)^{\text{alg}} \subseteq U$.

➡ $A \subseteq U$ jest algebraicznie domknięte nad K , gdy $A = \text{cl}_K(A)$.

10.1 Własności

- $\text{acl}_K(\emptyset) = \hat{K}$
- (a) $A \subseteq B \implies \text{cl}_K(A) \subseteq (B)$ *monotoniczność*
(b) $A \subseteq \text{acl}_K(A)$
(c) $\text{acl}_K(\text{acl}_K(A)) = \text{acl}_K(A)$ *idempotentność*, tzn: acl_K jest operatorem domknięcia.
- $\text{acl}_K(A) = \bigcup_{A_0 \subseteq A, \text{ sk.}} \text{acl}_K(A_0)$ *skończony charakter*
- własność wymiany*
$$a \in \text{acl}_K(A \cup \{b\}) \setminus \text{acl}_K(A) \implies b \in \text{acl}_K(A \cup \{a\})$$

Dowód.

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

\subseteq

Weźmy $b \in K(A)^{\text{alg}}$. Wtedy istnieje $w(x) \in K(A)[X]$ takie, że $w(b) = 0$ i $w \neq 0$. w ma współczynniki w $K(A_0)$ dla pewnego skończonego $A_0 \subseteq A$, więc $b \in K(A_0)^{\text{alg}}$.

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

Niech teraz $a \in K(A, b)^{\text{alg}}$ i dla wygody oznaczmy $L = K(A)^{\text{alg}}$. Wtedy $K(A, b)^{\text{alg}} = L(b)^{\text{alg}}$. 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 $L[b]$).

$$w(x) = \underbrace{c_n}_{\neq 0} x^n + \dots + c_1 x + c_0$$

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

$$v(y) = v_n(y) \cdot a^n + \dots + v_1(y) \cdot a + v_0(y).$$

$\in L[a][y]$

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



➤ $A \subseteq U$ jest **algebraicznie niezależny** nad K , gdy dla każdego $a \in A$ $a \notin \text{acl}_K(A \setminus \{a\})$.

Równoważnie: dla każdego n i dla wszystkich $a_1, \dots, a_n \in A$ parami różnych, dla każdego $w(x_1, \dots, x_n) \in K[\bar{X}]$ $w(\bar{a}) \neq 0$.

➤ A jest **bazą przestępną zbioru** $B \subseteq U$ nad K , gdy A jest algebraicznie niezależny nad K i $A \subseteq B \subseteq \text{acl}_K(A)$.

➤ **wymiar przestępny** B nad K $\text{trdeg}_K(B)$ to moc jakiejkolwiek bazy przestępnej zbioru B nad K .

➤ Gdy $K = F$ jest ciałem prostym, to pomijamy je w $\text{acl}_K, \text{trdeg}_K$. 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 $U = K(x_i : i \in I)^{\text{alg}}$. Wtedy $\{x_i : i \in I\} \subseteq U$ jest algebraicznie niezależne nad K i $\text{trdeg}_K(U) = |I|$.
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 przestępne, 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
 $r_1(r_2m) = (r_1r_2)m$

prawostronna
 $(mr_1)r_2 = m(r_1r_2)$

mieszana
jeśli jesteśmy w lewostron-
nym module:
 $(mr_2)r_1 = m(r_2r_1)$
i nie to samo co przy pra-
wostronnym

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 $\text{End}(G)$ są pierścieniem z jednością (id_G) i działaniami zdefiniowanymi dla $f, g \in \text{End}(G)$:

$$(f + g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(g(x)).$$

Grupa G może być traktowana jako moduł nad $\text{End}(G)$ z działaniem zadany przez $f \cdot x = f(x)$ dla $f \in \text{End}(G)$ i $x \in G$.

4. Załóżmy, że $j : R \rightarrow \text{End}(G)$ 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 $j : R_1 \rightarrow R$ jest homomorfizmem pierścieni z jednością i $M = (M, +, r)_{r \in R}$ jest R -modułem, to M jest R_1 -modułem z działaniem 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 działań 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 $A \subseteq N$. Jest to **podmoduł generowany przez A**

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

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

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

Niech $h : M \rightarrow N$ 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 $F : M_1 \times \dots \times M_n \rightarrow M$ 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 $f : M \rightarrow N$ istnieje dokładnie jeden \bar{f} taki, że

$$\begin{array}{ccc} M & \xrightarrow{\forall f} & N \\ \text{iloraz} \downarrow & \nearrow \exists! \bar{f} & \\ M/\ker(f) & & \end{array}$$

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

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ \downarrow g & \nearrow \exists h & \\ U & & \end{array} \iff \ker(f) \supseteq \ker(g)$$

Zbiór wszystkich homomorfizmów między modułem M i N oznaczamy

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

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

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

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

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 $N \subseteq M$ podmodułu, $N = 0$.

Pierścień endomorfizmów R -modułu M definiujemy jako

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

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

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

Dowód. Niech $0 \neq f \in \text{End}_R(M)$. Wtedy $\text{Im}(f) = M$, 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". ☕

Założmy, że M jest R -modułem oraz $K = \text{End}_R(M)$ 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. Założmy, że $n = \dim_K(M) < \infty$. Wtedy $\text{End}_K(M) \cong M_{n \times n}(K)$.

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

$$\begin{aligned} r &\longmapsto m(\phi_r) \in M_{n \times n}(K) \\ &\downarrow \psi \\ R &\xrightarrow{\text{homomorfizm pierścieni z 1}} M_{n \times n}(K) \end{aligned}$$

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
- $\text{Lin}_R(B) = M$.

Przykład:

- $\{0\} \subseteq M$ jest liniowo niezależny, natomiast układ (m_0, m_0) jest liniowo zależny, bo $1 \cdot m_0 + (-1) \cdot m_0 = 0$.
- \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, \dots, m_n, \dots) takie, że tylko dla skończonej liczby i mamy $m_i \neq 0$. Dla każdego j istnieje naturalne włożenie $f_j : M_j \rightarrow \bigsqcup M_i$ zdefiniowane przez $f_j(m) = (0, \dots, 0, m, 0, \dots)$, gdzie m występuje na j -tej pozycji.

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

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

Przyjęto się uznawać za naturalne przekształcenie $h : \bigoplus M_i \rightarrow M$ zadane przez

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

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

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

$$\begin{array}{ccc} M_{i_0} & \xrightarrow{g_{i_0}} & M \\ \downarrow f_{i_0} & \nearrow \exists! h & \\ \bigsqcup M_i & & \end{array}$$

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

$$g_i = \text{id}_{M_i} : M_i \rightarrow M$$

oraz h jak z uwagi 11.1

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

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 $\sqcup M_i$ jest wolnym R -modułem.

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

$$f_{i_0} : M_{i_0} \xrightarrow{\cong} f_{i_0}[M_{i_0}] \subseteq \sqcup M_i \\ \bigcup f_i[B_i]$$

jest bazą $\sqcup M_i$.



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 $g : A \rightarrow N$ istnieje jedyna funkcja $g' : M \rightarrow N$ 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

$$\begin{array}{ccc} M & \xrightarrow{j} & M/M' \\ & \searrow 0 & \nearrow \\ & M & \end{array}$$

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

$$\begin{array}{ccc}
 A & \xrightarrow{g=0} & M/M' \\
 \downarrow \cap & \nearrow \exists! g' & \\
 M & &
 \end{array}$$

- A jest liniowo niezależne:

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

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

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

- Jeśli $A = \{a_i\}_{i \in I}$ jest bazą M to wtedy
 - Ra_i jest podmodułem M
 - $M = \bigoplus Ra_i$
- 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. Założmy, że R jest przemienny. Wtedy każde dwie bazy R -modułu M są równoliczne.

Dowód. Problem redukuje 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

$$j : M \rightarrow M/M'$$

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

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

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

to $B_1 \sim j[B_1]$ oraz $B_2 \sim j[B_2]$. Ale R/I jest ciałem, więc M/M' jest przestrzenią liniową 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 .

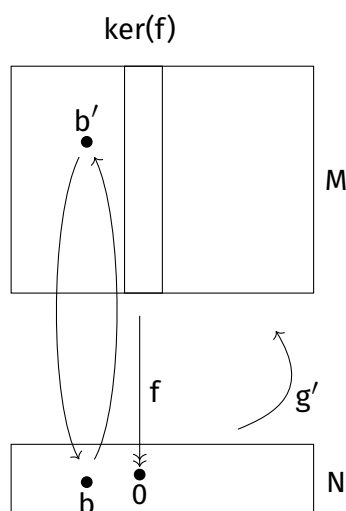
$$\begin{array}{ccc} \text{id} : M & & \\ \downarrow \text{I} \cap & \searrow \text{na} & \\ (\exists! f) : N & \xrightarrow{\text{R-liniowe}} & M \end{array}$$

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



Fakt 11.8. Załóżmy, że M, N są R -modułami, N jest wolny i $f : M \rightarrow N$ 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 $g : B \rightarrow M$ takie, że $g(b) = b'$. Z uwagi 11.4(3) wiemy, że istnieje jedyne $g' : N \rightarrow M$ R liniowe takie, że g' rozszerza g .

Wtedy $f \circ g' : N \rightarrow N$ i $(f \circ g') \upharpoonright B = \text{id}_B$, czyli z uwagi 11.4 $f \circ g' = \text{id}_N$. 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 $f : M \rightarrow N$ mamy $M = \ker(f) \oplus M'$ dla pewnych podmodułów $M' \subseteq M$.

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

$$\begin{array}{ccc} & M & \\ \exists g \nearrow & \downarrow \forall f & \\ N & \xrightarrow{\text{id}} & N \end{array}$$

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 $N = \text{Im}(g) \oplus N'$. To znaczy, obraz g jest **składnikiem prostym** N .

Przykłady:

1. Moduł wolny jest projektywny

2. W przypadku, gdy R jest ciałem, to każdy R -moduł jest projektywny i iniektywny.

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

\Rightarrow

$M = aR$, wtedy $f : R \rightarrow M, r \mapsto ra$, 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)

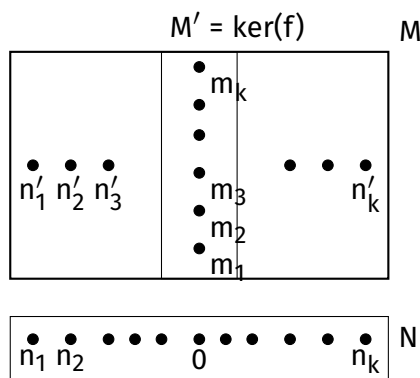
11.6 Moduły skończenie generowane

Twierdzenie 11.14. R jest pierścieniem przemiennym z $1 \neq 0$. Niech M, N będą R -modułami oraz $f : M \rightarrow N$ 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 $\{n_1, \dots, n_k\} \subseteq N$ i $\{m_1, \dots, m_l\} \subseteq M'$ będą zbiorami generatorów. Weźmy $n'_1, \dots, n'_k \in M$ takie, że $f(n'_i) = n_i$.



W takim razie, $\{n'_1, \dots, n'_k, m_1, \dots, m_l\}$ generują M , bo dla dowolnego $x \in M$ mamy $f(x) \in N$, więc $f(x) = \sum r_i n_i$ dla $r_i \in R$. 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 .



Wniosek 11.15. Załóżmy, że R jest pierścieniem przemiennym. Wtedy następujące warunki są równoważne:

1. R jest pierścieniem noetherowskim
2. Jeśli M jest skończenie generowanym R -modułem i $N \subseteq M$ jest jego podmodułem, to N też jest skończenie generowany.

Dowód.

- (2) \implies (1) Niech $I \triangleleft R$. Zauważmy, że $R = R \cdot 1$ jest skończenie generowanym R -modułem cyklicznym. Z tego względu, $I \subseteq R$ również jest skończenie generowanym R -modułem. W takim razie, każdy ideał $I \triangleleft R$ jest skończenie generowany i R jest pierścieniem noetherowskim.
- (1) \implies (2) Weźmy R -moduł M generowany przez $\{m_1, \dots, m_l\}$. Niech $W = Rm_1 \oplus \dots \oplus Rm_l$ będzie R -modułem wolnym o bazie $\{m_1, \dots, m_l\}$.

Rozważmy epimorfizm $\phi : W \rightarrow M$ zadany przez $\phi(m_i) = m_i$ oraz podmoduł $N \subseteq M$:

$$\begin{array}{ccc} W & \xrightarrow{\phi} & M \\ \cup I & & \cup I \\ N' = \phi^{-1}[N] & & N \end{array}$$

Wystarczy pokazać, że N' jest skończenie generowanym podmodułem W (bo baza N będzie \leq niż baza N' przez fakt, że ϕ jest surjekcją).

Indukcja względem ilości elementów bazy M :

$l = 1$ Wtedy $W \cong R$. Niech $\psi : W \xrightarrow{\cong} R$ oraz $N'' = \psi[N']$ będzie podmodułem R . Podmoduły pierścienia to jego ideały. Z noetherowskości R mamy, że $N'' = \psi[N']$ jest skończenie generowanym ideałem. W takim razie N' również jest skończenie generowany, gdyż ψ byłoby izomorfizmem.

$l > 1$ Załóżmy, że teza zachodzi dla wszystkich $l' < l$. Niech $\pi : W \rightarrow R$ będzie rzutem na l -tą współrzędną (czyli ostatnią).

$$\begin{array}{ccc} W & \xrightarrow{\pi} & R \\ \cup & & \cup \\ N' & \xrightarrow{\phi|_{N'}} & \pi[N'] \end{array}$$

$\pi[N']$ jest podmodułem pierścienia R , więc działa jak ideał. Ideały w pierścieniu noetherowskim są skończenie generowane, czyli $\pi[N']$ jest skończenie generowany.

Sprawdźmy teraz $\ker(\phi|_{N'}) \subseteq \underbrace{R \times \dots \times R}_{l-1} \times \{0\} \cong \underbrace{R \times \dots \times R}_{l-1}$ jest podmodułem mod-

ułu o bazie z $(l - 1)$ elementami, czyli na mocy założenia indukcyjnego $\ker(\phi|_{N'})$ jest skończenie generowane. Na mocy twierdzenia 11.14(1) N' jest więc skończenie generowany ($\pi|_{N'} : N' \rightarrow \pi[N']$ jest homomorfizmem, $\ker(\pi|_{N'})$ jest skończenie generowany i $\pi[N'] \cong N' / \ker(\pi|_{N'})$ również jest skończenie generowany).



Wykład 12: Iloczyn tensorowy modułów

11.1 Funkcja dwuliniowa

Definicja 11.16. Niech R będzie pierścieniem przemiennym z 1, a M_1, M_2, N będą R -modułami. Mówimy wówczas, że $f : M_1 \times M_2 \rightarrow N$ jest **R-dwuliniowe**, gdy f jest R -liniowe na każdej współrzędnej, to znaczy

$$f(m_1 + m'_1, m_2) = f(m_1, m_2) + f(m'_1, m_2)$$

$$f(m_1, m_2 + m'_2) = f(m_1, m_2) + f(m_1, m'_2)$$

$$f(rm_1, m_2) = rf(m_1, m_2) = f(m_1, rm_2)$$

Uwaga 11.17. Zazwyczaj f jak w definicji wyżej nie jest R -liniowe.

$$\begin{aligned} f(m_1 + m'_1, m_2 + m'_2) &= f(m_1, m_2 + m'_2) + f(m'_1, m_2 + m'_2) = \\ &= f(m_1, m_2) + f(m_1, m'_2) + f(m'_1, m_2) + f(m'_1, m'_2) \neq f(m_1, m_2) + f(m'_1, m'_2) \end{aligned}$$

Zazwyczaj również $\text{Im}(f) = f[M_1 \times M_2] \subseteq N$ nie jest podmodułem, ale generuje podmoduł $[\text{Im}(f)] \subseteq N$.

Chcemy znaleźć funkcję $f : M_1 \times M_2 \rightarrow \text{coś}$ dwuliniową taką, że to "coś" jest R -modułem generowanym przez $\text{Im}(f)$ i to "coś" jest tak duże jak to tylko możliwe.

Niech X będzie R -modułem wolnym o bazie $\{\langle m_1, m_2 \rangle : m_1 \in M_1, m_2 \in M_2\}$

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{f_0} & X \\ & \searrow f=j \circ f_0 & \swarrow j \\ & X/L & \end{array}$$

Niech $f_0 : M_1 \times M_2 \rightarrow X$ będzie funkcją zadaną przez

$$f_0(m_1, m_2) = \langle m_1, m_2 \rangle.$$

Taka funkcja nie jest 2-liniowa, czyli musimy utożsamić w X pewne elementy tak, aby f_0 stało się 2-liniowe. Innymi słowy, chcemy znaleźć najmniejszy podmoduł $L \subseteq X$ taki, że

$$f = j \circ f_0$$

jest R -dwuliniowe, gdzie $j : X \rightarrow X/L$ jest odwzorowaniem ilorazowym.

12.2 Konstrukcja produktu tensorowego

Fakt 12.1. Odwzorowanie $f : M_1 \times M_2 \rightarrow X/L$ jest R -dwuliniowe \iff dla wszystkich $m_1, m'_1 \in M_1$ i $m_2, m'_2 \in M_2$ oraz $r \in R$ mamy:

- $\langle m_1 + m'_1, m_2 \rangle - [\langle m_1, m_2 \rangle + \langle m'_1, m_2 \rangle] \in L$
- $r\langle m_1, m_2 \rangle - \langle rm_1, m_2 \rangle \in L$
- $\langle m_1, m_2 + m'_2 \rangle - [\langle m_1, m_2 \rangle + \langle m_1, m'_2 \rangle] \in L$
- $r\langle m_1, m_2 \rangle - \langle m_1, rm_2 \rangle \in L$

Dowód. Łatwy [można przeczytać w "Commutative Algebra" ~ M. Atiyah].



Definicja 12.2. Produkt tensorowy modułów M_1 i M_2 to funkcja

$$f : M_1 \times M_2 \rightarrow X/L,$$

gdzie X/L jak wyżej zwykle oznaczamy przez $M_1 \otimes M_2$. Element produktu tensorowego, czyli $f(m_1, m_2)$, oznaczamy przez $m_1 \otimes m_2$.

Analogicznie, dla M_1, \dots, M_k R -modułów, odwzorowanie R - k -liniowe $f(m_1, \dots, m_k) := m_1 \otimes \dots \otimes m_k$ też jest produktem tensorowym.

Tensory proste $m_1 \otimes m_2$ ($m_1 \otimes \dots \otimes m_k$) generują $M_1 \otimes M_2$ ($M_1 \otimes \dots \otimes M_k$). Pozostałe elementy to **tensor złożony** i są to R -liniowe kombinacje tensorów prostych.

Uwaga 12.3. Niech $f : M_1 \times M_2 \rightarrow M_1 \otimes M_2$ zdefiniowane jako $f(m_1, m_2) = m_1 \otimes m_2$. Jest to odwzorowanie R -dwuliniowe, często oznaczane po prostu przez \otimes . Wtedy dla każdego $g : M_1 \times M_2 \rightarrow N$ R -dwuliniowego istnieje dokładnie jedno $h : M_1 \otimes M_2 \rightarrow N$ R -liniowe takie, że diagram

$$\begin{array}{ccc} M_1 \times M_2 & \xrightarrow{\otimes=f} & M_1 \otimes M_2 \\ & \searrow g & \swarrow h \\ & N & \end{array}$$

komutuje. Warunek wyżej jest nazywany **warunkiem uniwersalności**

Dowód. Przyjrzyjmy się diagramowi:

$$\begin{array}{ccccc} & & M_1 \otimes M_2 = X/L & & \\ & \nearrow f & & \nwarrow j: \text{ilorazowe} & \\ M_1 \times M_2 & & & & X \leftarrow R\text{-moduł wolny o bazie } M_1 \times M_2 \\ & \searrow g & \swarrow h & \nearrow f_0 = \text{id} & \\ & & N & & \end{array}$$

l: R -homomorfizm
 $l(\langle m_1, m_2 \rangle) = g(m_1, m_2)$

Warunek na funkcję l wyznacza ją jednoznacznie, gdyż X jest modułem wolnym, a my wyznaczyliśmy na co przechodzą elementy jego bazy.

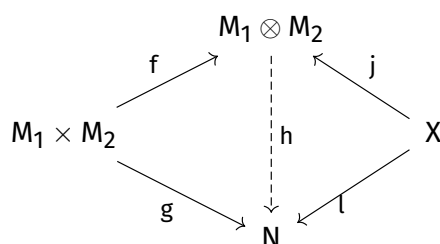
Jeśli funkcja $g = f \circ f_0$ jest dwuliniowa, to $\ker(l) \supseteq L$, bo:

$$\begin{aligned} g(m_1 + m'_1, m_2) &= g(m_1, m_2) + g(m'_1, m_2) \implies \\ l(\langle m_1 + m'_1, m_2 \rangle) &= l(\langle m_1, m_2 \rangle) + l(\langle m'_1, m_2 \rangle) \implies \\ 0 &= l(\langle m_1 + m'_1, m_2 \rangle) - [l(\langle m_1, m_2 \rangle) + l(\langle m'_1, m_2 \rangle)] = \\ &= \underbrace{l(\langle m_1 + m'_1, m_2 \rangle - [\langle m_1, m_2 \rangle + \langle m'_1, m_2 \rangle])}_{\in L} = 0 \end{aligned}$$

Analogicznie dla pozostałych generatorów L . W takim razie,

$$\{\text{generatory } L\} \subseteq \ker(l) \implies \underbrace{L}_{\ker(j)} \subseteq \ker(l).$$

Z twierdzenia o faktoryzacji R-homomorfizmów istnieje dokładnie jedno $h : M_1 \otimes M_2 \rightarrow N$ takie, że diagram

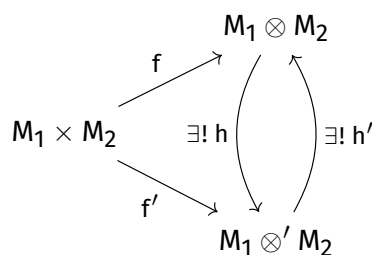


komutuje. Udowodnienie jedności h zostawiamy jako ćwiczenie. ☕

Uwaga 12.4. Warunek z uwagi 12.3 wyznacza $M_1 \otimes M_2$ z dokładnością do \cong .

Dowód. Przy użyciu teorii kategorii.

Założmy, że $M_1 \times M_2 \xrightarrow{f'} M_1 \otimes' M_2$ jest R-dwuliniowe i spełnia warunek .



gdzie istnienie h i h' wynika z warunku .


Założmy, że $h' \circ h = \text{id}_{M_1 \otimes M_2}$, wtedy h jest izomorfizmem R-modułów. Wiemy, że diagram wyżej komutuje, więc $h' \circ h = h'$, więc $\text{id}_{M_1 \otimes M_2} = h'$, czyli $\text{id} = h'$, gdyż h' było jedyne. W takim razie $M_1 \otimes' M_2 \cong M_1 \otimes M_2$. ☕

Z tego powodu $M_1 \otimes M_2$, jak i bardziej ogólnie $M_1 \otimes \dots \otimes M_k$ możemy definiować "abstrakcyjnie" przez kategorijski warunek uniwersalności.

Wykład 13: Własności produktu tensorowego

Przykład: po pierwsze zauważmy, że $R[X]$ i $R[Y]$ to R -moduły. Możemy powiedzieć, że $R[X] \otimes R[Y] \cong R[X, Y]$ w tym sensie, że

$$R[X] \times R[Y] \xrightarrow{\otimes} R[X, Y]$$

dane przez $W(X) \otimes V(Y) = W(X) \cdot V(Y)$. Odwzorowanie to spełnia warunek :

$$\begin{array}{ccc} R[X] \times R[Y] & \xrightarrow{\otimes} & R[X, Y] \\ & \searrow \text{g 2-liniowe} & \swarrow \exists! h \text{ R-liniowe?} \\ & N & \end{array}$$

a więc homomorfizm h musi spełniać warunek

$$h(W(X) \cdot V(Y)) = g(W(X), V(Y))$$

dla wszystkich $W(X) \in R[X]$ oraz $V(Y) \in R[Y]$. Ten warunek wraz z R -liniowością g wyznacza h na całym $R[X, Y]$ w sposób jednoznaczny na diagramie wyżej. Nie trudno też sprawdzić, że $h \circ \otimes = g$, co daje komutowanie diagramu.

Dlaczego jednak h istnieje? Rozpocznijmy od jednomianów $\{X^n Y^m\}_{n,m \geq 0}$ jako bazy $R[X, Y]$. Mamy

$$h(X^n Y^m) = g(X^n, Y^m)$$

jest dobrze zdefiniowane. Dla wielomianu $W(X, Y) \in R[X, Y]$ takiego, że

$$W(X, Y) = \sum_{n,m} r_{n,m} X^n Y^m$$

a więc


$$h(W) = h\left(\sum_{n,m} r_{n,m} X^n Y^m\right) = \sum_{n,m} r_{n,m} h(X^n Y^m) = \sum_{n,m} r_{n,m} g(X^n, Y^m).$$

Czyli funkcja h działa na wszystkich wielomianach z $R[X, Y]$.

Wniosek. W takim razie, jeśli M_n jest wolnym R -modułem wymiaru n o bazie $\{b_1, \dots, b_n\}$ a M_m jest wolnym R -modułem wymiaru m o bazie $\{c_1, \dots, c_m\}$, to $M_n \otimes M_m$ jest R -modułem o bazie $\{b_i \otimes c_j\}_{\substack{i \leq n \\ j \leq m}}$ i wymiarze $n \cdot m$.

Dowód. $M_n \cong R_{<n}[X]$, gdzie $R_{<n}[X]$ jest modułem wielomianów stopnia $< n$. Wtedy

$$M_n \otimes M_m \cong R_{<n}[X] \otimes R_{<m}[Y] \cong R_{<n \cdot m}[X, Y]$$

gdzie $R_{<n \cdot m}[X, Y]$ to moduł wielomianów $W(X, Y)$ takich, że $\deg_X(W) < n$ oraz $\deg_Y(W) < m$. Dalszy ciąg dowodu podąża za rozumowaniem z przykładu wyżej. 

Własności iloczynu tensorowego:

1. $M_1 \otimes M_2 \cong M_2 \otimes M_1$
2. $(M_1 \otimes M_2) \otimes M_3 \cong M_1 \otimes (M_2 \otimes M_3) \cong M_1 \otimes M_2 \otimes M_3$
3. $R \otimes M \cong M$


Dowód.

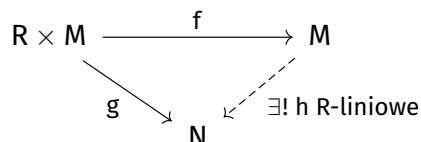
1. Ćwiczenie

2. Ćwiczenie

3. Niech $f : R \times M \rightarrow M$ będzie R -dwuliniowym odwzorowaniem zadany przez

$$f(r, m) = r \cdot m.$$

Wystarczy teraz pokazać, że f spełnia warunek :



Funkcja h zdefiniowana przez

$$h(m) = h(f(1, m)) = g(1, m)$$

jest jedyna ze względu na jedyność g . Jest też R -homomorfizmem, bo g jest R -liniowe na drugiej współrzędnej.

Diagram komutuje, bo g jest R -liniowe na obu współrzędnych, a więc

$$(h \circ f)(r, m) = h(rm) = g(1, rm) = r \cdot g(1, m) = g(r, m)$$



Uwaga 13.1.

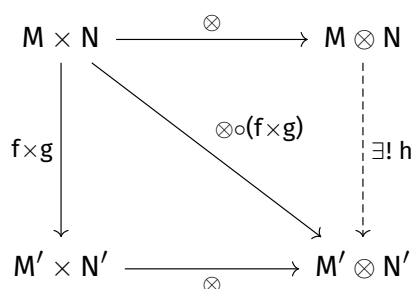
1. Jeśli $A \subseteq M$ i $B \subseteq N$ są zbiorami generującymi te moduły, to $A \otimes B = \{a \otimes b : a \in A, b \in B\}$ jest generatorem $M \otimes N$.
2. Załóżmy, że $f : M \rightarrow M'$ i $g : N \rightarrow N'$ są R -liniowe. Wtedy istnieje dokładnie jedno R -liniowe

$$h : M \otimes N \rightarrow M' \otimes N'$$

zdefiniowane przez

$$h(m \otimes n) = f(m) \otimes g(n)$$


Dowód.



Gdzie $h(m \otimes n) = f(m) \otimes g(n)$.

Funkcja $\otimes \circ (f \times g)$ jest dwuliniowa, bo

$$\begin{aligned} \otimes \circ (f \times g)(x + y, n) &= \otimes(f(x) + f(y), g(n)) = (f(x) + f(y)) \otimes g(n) = \\ &= f(x) \otimes g(n) + f(y) \otimes g(n) = \\ &= \otimes \circ (f \times g)(x, n) + \otimes \circ (f \times g)(y, n) \end{aligned}$$

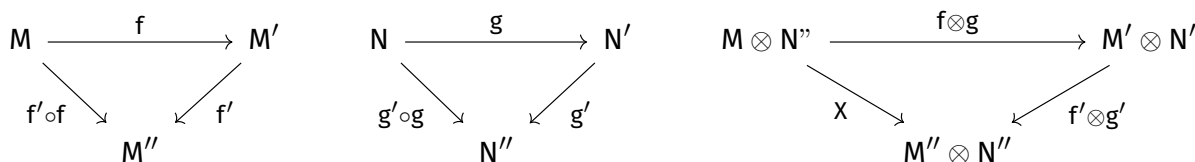
R -liniowość h , jego jedyność oraz komutowanie diagramu wyżej pokazujemy tak jak w dowodach wcześniejszych uwag. 

13.1 Iloczyn tensorowych funkcji

Definicja 13.2. $f \otimes g = h$ jak z uwagi 13.1 nazywamy **iloczynem tensorowym** f i g

Uwaga 13.3.

1.



[dowód: wystarczy sprawdzić $X = (f' \otimes g') \circ (f \otimes g) = (f' \circ f) \otimes (g' \circ g)$]

2. $\text{id}_M \otimes \text{id}_N = \text{id}_{M \otimes N}$

3. $\phi : \text{Hom}(M, M') \times \text{Hom}(N, N') \rightarrow \text{Hom}(M \otimes N, M' \otimes N')$ zadane przez $\phi(f, g) = f \otimes g$ jest R -dwuliniowe.

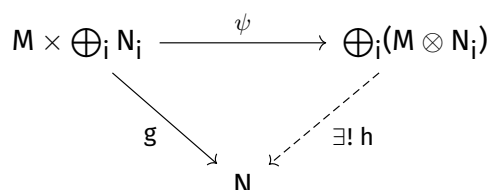
Uwaga 13.4. Dla R -modułu M oraz R -modułów $\{N_i\}_{i \in I}$ istnieje izomorfizm

$$\psi : M \otimes \left(\bigoplus_{i \in I} N_i \right) \xrightarrow{\cong} \bigoplus_{i \in I} (M \otimes N_i)$$

zadany przez

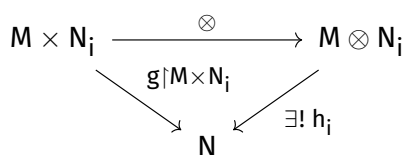
$$\psi(m \otimes \sum n_i) = \sum m \otimes n_i$$

Dowód. Rozważmy diagram



Musimy pokazać istnienie i jedność h oraz komutowanie diagramu (ostatnie jest trywialne).

istnienie h pokażemy najpierw dla dowolnego i , a następnie korzystając z własności uniwersalności \bigoplus_i przeniesiemy na całą sumę prostą.

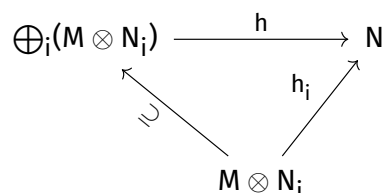


h_i definiujemy wtedy jako

$$h_i(m \otimes n_i) = g(m, n_i)$$

a jego istnienie oraz jedność udowadniamy tak jak wcześniej.

Ponieważ dla każdego i istnieje dokładnie jedna funkcja h_i , to z własności uniwersalności \bigoplus możemy stwierdzić, że dla każdego i istnieje $\exists! h : \bigoplus (M \otimes N_i) \rightarrow N$ takie, że



to znaczy

$$h(m \otimes n_i) = h_i(m \otimes n_i) = g(m, n_i),$$

czyli

$$h\left(\sum_i m \otimes n_i\right) = \sum_i h_i(m \otimes n_i) = \sum_i g(m, n_i) = g(m, \sum_i n_i).$$

Dla $N = M \otimes (\bigoplus N_i)$ dostajemy h -izomorfizm oraz $h(\sum m \otimes n_i) = m \otimes \sum n_i$.

jedyność h sprawdzamy dla elementów $\sum m \otimes n_i$, gdyż generują one $\bigoplus (M \otimes N_i)$:

$$(h \circ \psi)(m \otimes \sum_i n_i) = h\left(\sum_i m \otimes n_i\right) = g(m, \sum_i n_i)$$

i od razu widać, że diagram jak wyżej komutuje.



13.2 Iloczyny zewnętrzne

Niech $R = K$ będzie ciałem, a V będzie przestrzenią liniową nad K . Zdefiniujemy

$$V^{\otimes n} = \underbrace{V \otimes \dots \otimes V}_n.$$

Zdefiniujemy działanie $\sigma \in S_n$ działa na $V \otimes \dots \otimes V$ przez permutowanie współrzędnych w tensorach prostych, tzn.

$$\sigma(v_1 \otimes \dots \otimes v_n) = v_{\sigma(1)} \otimes \dots \otimes v_{\sigma(n)}$$

Definicja 13.5. Niech $x \in V^{\otimes n}$. Mówimy, że

- x jest **symetryczny**, jeśli dla każdego $\sigma \in S_n$ mamy $\sigma(x) = x$
- x jest **antysymetryczny**, jeśli dla każdego $\sigma \in S_n$ $\sigma(x) = \text{sgn}(\sigma) \cdot x$.

Dalej, definiujemy zbiory

$$\Lambda^n V = \{x \in V^{\otimes n} : x \text{ antisymetryczny}\}$$

$$S^n V = \{x \in V^{\otimes n} : x \text{ symetryczny}\}$$

Jeśli $\text{char}(K) = 0$, to wówczas $\Lambda^n V, S^n V \leq V^{\otimes n}$.

Gdy $n = 2$, to mamy $V \otimes V = \Lambda^2 V \oplus S^2 V$ rozumiane jako

$$V \otimes V \ni x = \frac{1}{2}(x + \sigma(x)) + \frac{1}{2}(x - \sigma(x)) \in \Lambda^2 V \oplus S^2 V,$$

gdzie $\sigma = (1, 2) \in S_2$ (bo drugi element S_2 to identyczność). Widzimy, że $S^2 V \cap \Lambda^2 V = \{0\}$.

O n -liniowej funkcji $f : \underbrace{V \times \dots \times V}_n \rightarrow W$ mówimy, że jest

- **symetryczna**, gdy dla każdego $\sigma \in S_n$ mamy $f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = f(v_1, \dots, v_n)$
- **antysymetryczna**, gdy dla każdego $\sigma \in S_n$ mamy $f(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = \text{sgn}(\sigma) \cdot f(v_1, \dots, v_n)$

Przykład: funkcja $\det : K^n \times \dots \times K^n \rightarrow K$ jest antisymetryczna.

Dla $x \in V^{\otimes n}$ definiujemy

- $x_s = \frac{1}{n!} \sum_{\sigma \in S_n} \sigma(x) \in S^n V \leq V^{\otimes n}$
- $x_a = \frac{1}{n!} \sum_{\sigma \in S_n} \text{sgn}(\sigma) \cdot \sigma(x) \in \Lambda^n V \leq V^{\otimes n}$.

Wtedy funkcja f zadana przez

$$f(v_1, \dots, v_n) = v_1 \wedge \dots \wedge v_n = (v_1 \otimes \dots \otimes v_n)_a$$

jest n -liniowa antysymetryczna, a diagram

$$\begin{array}{ccc} V_1 \times \dots \times V_n & \xrightarrow{f} & \Lambda^n V \\ & \searrow g & \swarrow \exists! h \\ & W & \end{array}$$

g: n -liniowe antysymetryczne

komutuje.

Uwaga 13.6. Niech K będzie ciałem takim, że $\text{char}(K) \neq 2$ i niech $\{e_1, \dots, e_n\} \subseteq V$ będzie bazą V nad K . Wtedy

$$\{e_{i_1} \wedge \dots \wedge e_{i_n} : 1 \leq i_1 < i_2 < \dots < i_n \leq k\}$$

jest bazą $\Lambda^n V$.

Stąd też gdy $n < k$

$$\dim(\Lambda^n V) = \binom{k}{n}$$

$$\dim(\Lambda^k V) = 1$$

i dla $n > k$ $\dim(\Lambda^n V) = 0$.

Przykłady:

1. Mamy $v \wedge v = -v \wedge v = 0$, gdyż $\{v, v\}$ i $\{v, -v\}$ nie są zbiorami liniowo niezależnymi.
2. Dla $v_1, v_2 \in V$ liniowo niezależnych nad K mamy

$$v_1 \wedge v_2 = r \cdot w_1 \wedge w_2$$

dla $r \neq 0$ wtedy i tylko wtedy, gdy

$$\text{Lin}(v_1, v_2) = \text{Lin}(w_1, w_2)$$

3. Poprzedni przykład możemy uogólnić dla $v_1, \dots, v_n \in V$ liniowo niezależnych. Wtedy dla $w_1, \dots, w_n \in V$ mamy

$$(\exists r \neq 0) v_1 \wedge \dots \wedge v_n = r \cdot w_1 \wedge \dots \wedge w_n \iff \text{Lin}(v_1, \dots, v_n) = \text{Lin}(w_1, \dots, w_n)$$

4. $(V \otimes W)^* \cong V^* \otimes W^*$ i $\Lambda^n V^* \cong (\Lambda^n V)^*$
5. więcej przykładów w analizie wielowymiarowej, geometrii różniczkowej, formach różniczkowych etc.

Wykład 14: Moduły nad pierścieniami PID

Od teraz R niech będzie dziedziną ideałów głównych (PID) z $1 \neq 0$, a M niech będzie R -modułem wolnym (tzn. $\dim_R(M)$ jest dobrze określone).

Twierdzenie 14.1. *Podmoduł R -modułu wolnego F jest wolny i wymiaru co najwyżej $\dim_R(F)$.*

Dowód. Niech F będzie modułem wolnym o bazie $\{b_1, \dots, b_n\}$, $M \subseteq F$ jego podmodułem. Dla $0 < l \leq n$ rozważmy

$$M_l = M \cap \bigoplus_{i \leq l} Rb_i$$

natomiast gdy $l = 0$, niech $M_l = \{0\}$.

Uwaga: Zauważmy, że dla każdego $l \leq n$ M_l ma wymiar $\dim(M_l) \leq l$.

Dowód. Dla $l = 1$ mamy $M_1 \subseteq Rb_1 \cong R$ [bso. $M_1 \neq \{0\}$], więc po utożsamieniu Rb_1 z R $M_1 \triangleleft R$ jest ideałem, stąd $M_1 = Ra$ jest ideałem głównym o bazie $\{a\}$ (generowanie $M_1 = Ra$ przez taką bazę jest jasne, a liniowa niezależność wynika z R - dziedzina).

Gdy założymy, że dla dowolnego l stwierdzenie wyżej działa, możemy je pokazać dla $(l + 1)$. Rozważmy rzut na $(l + 1)$ -współrzedną

$$\pi_{l+1} : M_{l+1} \rightarrow Rb_{l+1} \cong R$$

gdzie

$$M_{l+1} \subseteq \bigoplus_{i \leq l+1} Rb_i \cong R^{l+1}.$$

Zauważmy, że $\pi_{l+1}[M] \triangleleft R$ możemy traktować jako podmoduł, więc:

1. $\pi_{l+1} = 0 \implies M_{l+1} = \ker(\pi_{l+1}) = M_l$ więc z założenia indukcyjnego $\dim(M_{l+1}) = \dim(M_l) \leq l < l + 1$
2. $\pi_{l+1} \neq 0 \implies \text{Im}(\pi_{l+1}) = Ra_{l+1}$ jest wolny i jest ideałem w R . W takim razie

$$\pi_{l+1} : M_{l+1} \twoheadrightarrow Ra_{l+1}$$

jest surjekcją i M_{l+1} jest projektywny z faktu 11.8. Mamy więc

$$M_{l+1} = \ker(\pi_{l+1}) \oplus N$$

gdzie $N \cong Ra_{l+1}$ i $M_l = \ker(\pi_{l+1})$ są modułami wolnymi. W takim razie również M_{l+1} jest modułem wolnym i z założenia indukcyjnego M_l jest rangi co najwyżej l , a Ra_{l+1} jest rangi jeden. Czyli M_{l+1} jest rangi co najwyżej $l + 1$.



W przypadku ogólnym, tzn. gdy $\dim(F)$ jest nieskończony, możemy udowodnić twierdzenie korzystając z indukcji pozaskończonej (na tej samej zasadzie co w skończonym przypadku).



Uwaga 14.2. *Podmoduł N modułu skończenie generowanego M jest skończenie generowany. Jeśli M ma zbiór generatorów mocy n , to N ma zbiór generatorów mocy $\leq n$.*

Dowód. Załóżmy, że M jest generowany przez a_1, \dots, a_n i niech

$$\begin{array}{ccc} f : R^n & \longrightarrow & M \\ \cup & & \cup \\ f[f^{-1}[N]] & = & N \end{array}$$

f będzie epimorfizmem takim, że

$$f(r_1, \dots, r_n) = ra_1 + \dots + ra_n.$$

R^n będziemy traktować jako moduł wolny o standardowej bazie (e_1, \dots, e_n) . Ponieważ $f^{-1}[N]$ jest modułem wolnym rangi $\leq n$, to N jest generowany przez co najwyżej n elementów. ☕

Twierdzenie 14.3. Załóżmy, że M jest modułem skończenie generowanym. Wtedy

1. Jeśli M jest beztorsyjny, to M jest modułem wolnym
2. $M = M_t \oplus F$, gdzie M_t to część torsyjna M , a $F \subseteq M$ jest pewnym modułem wolnym M .

Dowód. 1. Niech $\{x_1, \dots, x_n\} \subseteq M$ będzie zbiorem generatorów, a $\{b_1, \dots, b_k\}$ będzie jego maksymalnym podzbiorem liniowo niezależnym.

Rozważmy x_i dla $i = 1, \dots, n$. Układ $\langle x_i, b_1, \dots, b_k \rangle$ jest liniowo zależny ze względu na maksymalność $\{b_1, \dots, b_k\}$, więc

$$a_i x_i + r_1 b_1 + \dots + r_k b_k = 0$$

dla pewnym $a_i, r_1, \dots, r_k \in R$ i część jest $\neq 0$. Ponieważ b_1, \dots, b_k były liniowo niezależne, to na pewno nie może być $a_i = 0$, więc $a_i x_i \in N$, gdzie $N = Rb_1 + \dots + Rb_k$ jest modułem wolnym.

Weźmy $a = a_1 \cdot \dots \cdot a_n \neq 0$, bo R jest dziedziną. Stąd $ax_i \in N$ dla $i = 1, \dots, n$. Czyli dla każdego $x \in M$ mamy $ax \in N$, bo $x = \sum r_i x_i$, czyli $ax = \sum r_i \underbrace{ax_i}_{\in N} \in N$.

Rozważmy teraz $f : M \rightarrow N$ zadane przez $f(x) = ax$. Zauważmy, że f jest 1-1, bo M jest beztorsyjny. W takim razie $M \cong f[M] \subseteq N$ jest podmodułem modułu wolnego, czyli $f[M]$ jest modułem wolny. Przez izomorfizm M również jest modułem wolnym.

2. Niech $j : M \rightarrow M/M_t$ będzie przekształceniem ilorazowym.

Zauważmy, że M/M_t jest skończenie generowanym modułem beztorsyjnym, więc na mocy (1) jest on wolny. Z 11.8 mamy więc, że M jest modułem projektywnym. Stąd $M = M_t \oplus F$, gdzie $M_t = \ker(j)$, a $F \cong M/M_t$. ☕

14.1 Moduły p-prymarne

Definicja 14.4. Niech $p \in R$ będzie elementem nierozkładalnym (czyli pierwszym bo jesteśmy w pierścieniu PID) i niech M będzie R -modułem. Mówimy, że

- $m \in M$ jest **p-torsyjny** $\iff I_m = \{r \in R : rm = 0\} = (p^k)$ dla pewnego $k > 0$. p^k można traktować jako "rzęd" m
- $M_p = \{m \in M : m \text{ p-torsyjny} \vee m = 0\}$ nazywamy **p-prymarną składową** M i jest to **podmoduł** M
- M jest **p-prymarny**, gdy $M = M_p$, tzn. dla każdego $m \in M$ istnieje k takie, że $p^k m = 0$.

Twierdzenie 14.5. Niech M będzie R -modułem, gdzie R jest pierścieniem PID.

1. $M_p \subseteq M_t$ jest podmodułem i nazywa się go **p-prymarną składową** M
2. $M_t = \bigoplus M_{p_i}$, gdzie p_i to wszystkie elementy pierwsze R (z dokładnością do stowarzyszenia).

Dowód. Patrz: dowód analogicznego stwierdzenia dla grup abelowych ☕

czyli $r_i \leq l$. Stąd otrzymujemy

$$p^{r_i} e_i = a m_n = p^l a_1 m_n = p^{r_i} (p^{l-r_i} a_1) m_n = p^{r_i} a' m_n$$

czyli

$$p^{r_i} (e_i - a' m_n) = 0$$

i $e_i - a' m_n$ jest w tej samej warstwie $R m_n$ co e_i , ale jest jednak różne od oryginalnego e_i .

Niech $M' \subseteq M$ będzie generowany przez $\{e_1, \dots, e_l\}$ i niech

$$j' : M' \rightarrow M/Rm_n$$

będzie przekształceniem ilorazowym i w dodatku "na", bo $\{\bar{e}_1, \dots, \bar{e}_l\}$ generuje M/Rm_n . Mamy $\ker(j') \cap M' = 0$, bo wpp.

$$j'(a_1 e_1 + \dots + a_l e_l) = 0 \implies a_1 \bar{e}_1 + \dots + a_l \bar{e}_l = 0$$

a ponieważ

$$M/Rm_n = \bigoplus_{i \leq l} R \bar{e}_i$$

to każdy z tych elementów musi być równy zero:

$$a_1 \bar{e}_1 = \dots = a_l \bar{e}_l = 0$$

a ponieważ p^{r_i} jest "rzędem" \bar{e}_i , to $p^{r_i} | a_i$. Ponieważ $p^{r_i} e_i = 0$, to również $a_i e_i = 0$, czyli j' jest różnowartościowe.

W takim razie, j' jest izomorfizmem $M' \cong M/Rm_n$, a więc $M' = \bigoplus \{\text{cykliczne}\}$. Przez izomorfizm $M' \cong M/Rm_n$ mamy $M = M' \oplus Rm_n$, gdzie Rm_n jest cykliczne, czyli $M = \bigoplus \{\text{cykliczne}\}$.



Uwaga 14.7. Załóżmy, że M jest skończenie generowanym R -modułem p -prymarnym. Wtedy

$$M \cong R/(p^{k_1}) \oplus R/(p^{k_2}) \oplus \dots \oplus R/(p^{k_l})$$

dla pewnych $1 \leq k_1 \leq \dots \leq k_l$. Ponadto ciąg k_1, \dots, k_l jest wyznaczony jednoznacznie.

Dowód. Z poprzedniego wniosku wiemy, że

$$M = M_1 \oplus \dots \oplus M_l$$

gdzie dla każdego i M_i jest p -prymarny, czyli $M_i \cong R/(p^{k_i})$. Bez straty ogólności przyjmijmy, że $1 \geq k_1 \geq \dots \geq k_l$.

Lemat 1: Jeśli N jest R -modułem, to N/pN jest $R/(p)$ -modułem (czyli przestrzenią liniową nad ciałem $R/(p)$.)

Lemat 2:

$$p^i(R/(p^k))/p^{i+1}(R/(p^k)) = \begin{cases} 0 & i \geq k \\ p^i R/(p^{i+1}) & i < k \end{cases}$$

gdzie $p^i R/(p^{i+1})$ jest przestrzenią liniową nad $R/(p)$ o wymiarze 1.

Założmy, że $k_i < k_{i+1}$. Wtedy

$$p^{k_i} M = p^{k_i} (M_{i+1} \oplus \dots \oplus M_l)$$

$$p^{k_i-1}M = p^{k_i-1}(M_{j+1} \oplus \dots \oplus M_i \oplus M_{i+1} \oplus \dots \oplus M_l),$$

gdzie $k_j < k_{j+1} = k_i < k_{i+1}$.

Wtedy na mocy **Lematu 1** $p^{k_i-1}M/p^{k_i}M$ jest przestrzenią liniową nad $R/(p)$ o wymiarze $(l - j)$. W dodatku mamy

$$p^{k_i-1}M/p^{k_i}M = p^{k_i-1}M_{j+1}/p^{k_i}M_{j+1} \oplus p^{k_i-1}M_{j+2}/p^{k_i}M_{j+2} \oplus \dots \oplus p^{k_i-1}M_l/p^{k_i}M_l.$$

Z **Lematu 2** wiemy, że

$$\dim_{R/(p)}(p^{k_i-1}M_{j+1}/p^{k_i}M_{j+1}) = \dots = \dim_{R/(p)}(p^{k_i-1}M_l/p^{k_i}M_l) = 1.$$

Wymiary $\dim_{R/(p)}(p^{k-1}M/p^kM)$ dla $k = 1, \dots, k_l$ pozwalają jednoznacznie odczytać $k_1 \leq k_2 \leq \dots \leq k_l$. ☕

14.2 Moduły nierozkładalne

Definicja 14.8. R-moduł M jest **nierozkładalny** $\iff M = M_1 \oplus M_2$ oznacza, że $M_1 = 0$ lub $M_2 = 0$.

Uwaga. Moduł cykliczny M jest nierozkładalny $\iff M$ jest beztorsyjny (wolny) lub p -prymarny.

Dowód. Ćwiczenie ☕

Twierdzenie 14.9. Jeśli M jest R-modułem skończenie generowanym, to

$$M = \bigoplus_{i \in I} M_i,$$

gdzie M_i są nierozkładalne.

Dodatkowo, jeśli I jest skończony, to M_i są cykliczne i wyznaczone jednoznacznie z dokładnością do izomorfizmu i permutacji I .

Dowód. Z poprzednich twierdzeń z tego rozdziału możemy założyć, że

$$M = F \oplus M_t$$

gdzie F jest wolny, a $M_t = \bigoplus_{p \text{ pierwsze}} M_p$, gdzie $M_p \cong R/(p^{k_1}) \oplus \dots \oplus R/(p^{k_l})$, jest podmodułem torsyjnym M . Z tego (i faktu, że $F = R \oplus \dots \oplus R$) widać, że M jest sumą prostą modułów nierozkładalnych.

Załóżmy teraz, że I jest skończony. Wtedy z poprzedniego punktu wiemy, że

$$M = \underbrace{M_1 \oplus \dots \oplus M_r}_{\substack{\text{beztorsyjne} \\ \cong R \oplus \dots \oplus R}} \oplus \underbrace{M_{r+1} \oplus \dots \oplus M_{r+s}}_{\text{torsyjne} \cong M_t}.$$

W takim razie $\bigoplus_{i \leq r} M_i \cong M/M_t \cong F$ jest modułem wolnym o wymiarze r .

Z twierdzeń 14.5 i 14.6 wiemy, że skoro M_{r+1} są wszystkie modułami torsyjnymi, to $M_{r+1} = \bigoplus \{\text{moduły } p\text{-prymarne cykliczne}\}$. W takim razie

$$(M_t)_p = \bigoplus \{M_{r+i} : M_{r+i} \text{ } p\text{-prymarny}\}$$

a więc

$$(M_t)_p = M_p \cong R/(p^{k_1}) \oplus \dots \oplus R/(p^{k_l})$$

gdzie jednoznaczność z dokładnością do izomorfizmu dostajemy z uwagi po twierdzeniu 14.5. ☕

Wykład 15: Przestrzeń liniowa jako $K[X]$ -moduł

Niech V będzie przestrzenią liniową nad ciałem K o wymiarze $\dim(V) = n < \infty$. Weźmy $\psi \in \text{End}_K(V)$. Wtedy dla $f = a_0 + a_1x + \dots + a_lx^l \in K[X]$ możemy zdefiniować:

$$f(\psi) = a_0 \text{id}_V + a_1 \psi^1 + \dots + a_l \psi^l \in \text{End}_K(V).$$

Takie odwzorowanie $K[X] \ni f \mapsto f(\psi) \in \text{End}_K(V)$ jest homomorfizmem pierścieni, więc V jest $K[X]$ -modułem z działaniem $f \cdot v = f(\psi)(v)$ dla $v \in V$ i f, ψ jak wyżej.

Uwaga 15.1. Przestrzeń liniowa V jest skończenie generowana i torsyjna jako $K[X]$ -moduł.

Dowód. generowanie: Niech $\{e_1, \dots, e_n\} \subseteq V$ będzie bazą K -liniową. W takim razie $\{e_1, \dots, e_n\}$ generuje V jako $K[X]$ -moduł, bo dla $k \in K \subseteq K[X]$ mamy $k \cdot v = kv$ w sensie przestrzeni liniowej V .

torsyjność: Dla $v \in V$ mamy

$$v, \psi(v), \psi^2(v), \dots, \psi^n(v)$$

są liniowo zależne w V , bo $\dim(V) = n$. W takim razie

$$a_0 v + a_1 \psi(v) + \dots + a_n \psi^n(v) = 0$$

dla pewnych $a_i \in K$. Możemy teraz wziąć $K[X] \ni f(x) = \sum a_i x^i$, wtedy $f \cdot v = 0$.



Uwaga: Jeśli $K[X]$ jest PID, to

$$V = \bigoplus_{\substack{p_i \in K[X] \\ \text{pierwsze}}} V_{p_i}.$$

Bycie pierwszym przez $p_i \in K[X]$ oznacza, że $p_i(x)$ jest wielomianem nierozkładalnym.

Możemy utożsamić

$$V_{p_i} \cong K[X]/(p_i^{k_1}) \oplus \dots \oplus K[X]/(p_i^{k_l})$$

gdzie $1 \leq k_1 \leq \dots \leq k_l$.

Jeśli K jest ciałem algebraicznie domkniętym, to $f_i(x) \in K[X]$ jest nierozkładalny $\iff \deg(f_i) = 1 \iff f_i = (x - a_i)$ (z dokładnością do stowarzyszenia).

15.1 Klatki Jordana

Strukturę $K[X]/(f^{k_s}) = K[X]/(x - a_i)^{k_s}$ jako K -modułu definiujemy przez przekształcenie ilorazowe

$$j : K[X] \rightarrow K[X]/(x - a_i)^{k_s}.$$

Wtedy bazą $K[X]/(x - a_i)^{k_s}$ jako K -modułu jest

$$B_{i,s} = \{j(1), j(x - a_i), \dots, j(x - a_i)^{k_s-1}\}.$$

Dowód tego stwierdzenia wykorzystuje fakt, że $K[X]/(x - a_i) \cong K[X]/x^s$ zadany przez $w(x) \mapsto w(x + a_i)$.

Dla $0 \leq u \leq k_s$ zachodzi

$$x \cdot (x - a_i)^u = (x - a_i)^{u+1} + a_i(x - a_i)^u,$$

czyli

$$\psi(j(x - a_i)^u) = \begin{cases} a_i j(x - a_i)^u & u = k_s - 1 \\ a_i j(x - a_i)^u + j(x - a_i)^{u+1} & 0 \leq u < k_s - 1, \end{cases}$$

więc

$$m_{B_{i,s}}(\psi \upharpoonright K[X]/(x - a_i)^{k_s}) = \begin{bmatrix} a_i & 0 & 0 & \dots & 0 \\ 1 & a_i & 0 & \dots & 0 \\ 0 & 1 & a_i & \dots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \dots & a_i \end{bmatrix}$$

jest klatką Jordana. Niech $B = \bigcup_{i,s} B_{i,s}$ będzie bazą Jordana V dla endomorfizmu ψ . Wtedy $m_B(\psi)$ jest macierzą z klatkami Jordana jak wyżej na przekątnej.

Uwaga 15.2. [Twierdzenie Jordana] *Jeśli K jest algebraicznie domknięte i V jest przestrzenią liniową nad V wymiaru $\dim(V) < \infty$, a $\psi : V \rightarrow V$ jest liniowe, to istnieje baza Jordana $B \subseteq V$ dla której $m_B(\psi)$ ma postać Jordana.*

Dodatkowo, rozmiary klatek J w $m_B(\psi)$ są wyznaczone jednoznacznie (nie zależą od wymiaru B).

15.2 R-algebry

Definicja 15.3. Niech R będzie pierścieniem przemiennym z $1 \neq 0$. Wtedy definiujemy **R-algebrę** (przemienną) jako R -moduł $S = (S, +, r)_{r \in R}$ z dodatkowym mnożeniem \cdot takim, że $(S, +, \cdot)$ jest pierścieniem przemiennym i dla każdego $r \in R$ oraz dowolnych $s, s' \in S$

$$r(s \cdot s') = rs \cdot s' = s \cdot (rs').$$

R-algebry oznaczamy

$$S = (S, +, \cdot, r)_{r \in R}$$

Przykłady:

1. Jeśli R jest pierścieniem, to R jest \mathbb{Z} -algebrą.
2. Dla pierścienia R , $R[X]$, $R[X, Y]$ są R-algebrami.
3. Jeśli $R \subseteq S$ jest podpierścieniem z $1_R = 1_S$, to S jest R-algebrą.

Uwaga 15.4.

1. Jeśli S jest R-algebrą z jednostką 1 , to

$$\eta : R \rightarrow S$$

zadana przez $\eta(r) = r \cdot 1$ jest homomorfizmem R-algebr.

2. Gdy R jest ciałem, to $\eta : R \hookrightarrow S$ jest włożeniem i R jest podciałem pierścienia S .
3. Na odwrót, gdy S jest pierścieniem z 1 i $R \subseteq S$ jest podciałem, to S jest R-algebrą.

Kategorię R-algebr oznaczamy przez Alg_R .

Założmy, że S jest R-algebrą z 1 , a M jest R-modułem. Wtedy

$$S \otimes_R M$$

jest produktem tensorowym R-modułów i działa w oczywisty sposób jako R-moduł, ale też jako S-moduł:

$$S \ni s : S \otimes_R M \rightarrow S \otimes_R M$$

takie, że $s \cdot (s' \otimes m) = (ss') \otimes m$ dla wszystkich $s' \in S$ oraz $m \in M$.

Dowód. Rozważmy homomorfizmy R-modułów

$$S \xrightarrow{s} S$$

$$M \xrightarrow{\text{id}} M$$

jak wyżej. Wtedy

$$(s) \otimes \text{id} : S \otimes M \rightarrow S \otimes M$$

jest homomorfizmem R-modułów. Czyli $(S \otimes M, +, s)_{s \in S}$ jest S-modułem z działaniem $s \otimes \text{id}$. ☕

Przykłady:

1. Jeśli G jest \mathbb{Z} -modułem (grupą abelową), to $\mathbb{Q} \otimes_{\mathbb{Z}} G$ jest \mathbb{Q} -modułem, tzn. przestrzenią liniową nad \mathbb{Q} .
2. Jeśli V jest przestrzenią liniową nad \mathbb{R} , to $\mathbb{C} \otimes_{\mathbb{R}} V$ jest przestrzenią liniową nad \mathbb{C} . Nazywamy to wtedy *kompleksyfikacją* V.

Dla S_1, S_2 R-algebr z 1 mamy $S_1 \otimes_R S_2$ jako R-algebrę z działaniem dla tensorów prostych $s_1 \otimes s_2, s'_1 \otimes s'_2 \in S_1 \otimes_R S_2$ zadany przez

$$(s_1 \otimes s_2)(s'_1 \otimes s'_2) = (s_1 s'_1) \otimes (s_2 s'_2)$$

a na dowolne tensory przedłużamy korzystając z dwuliniowości:

$$\left(\sum s_1^i \otimes s_2^i\right) \left(\sum s'_1^j \otimes s'_2^j\right) = \sum (s_1^i s'_1^j) \otimes (s_2^i s'_2^j)$$

15.3 Radykały

Dla ideału $I \triangleleft R$ definiujemy jego **radykał** jako

$$\sqrt{I} = \{a \in R : (\exists n > 0) a^n \in I\}$$

wtedy $I \subseteq \sqrt{I} \triangleleft R$.

Twierdzenie 15.5. [Nullstellensatz Hilberta] Niech $I \triangleleft K[\bar{X}]$ i $f \in K[\bar{X}]$ taki, że

$$Z_{K^{\text{alg}}}(I) \subseteq Z_{K^{\text{alg}}}(f).$$

Wtedy $f \in \sqrt{I}$.

Tutaj dla $K \subseteq L$ rozszerzenia ciał definiujemy

$$Z_L(I) = \{\bar{a} \in K^n : (\forall g \in I) g(\bar{a}) = 0\}$$

Dowód. Załóżmy nie wprost, że $f \notin \sqrt{I}$. Niech $J \triangleleft K[\bar{X}]$ będzie ideałem maksymalnym wśród ideałów $I' \supseteq \sqrt{I}$ takich, że $f \notin \sqrt{I'}$. Pokażemy, że J jest ideałem pierwszym.

Załóżmy, że $g \cdot h \in J$, ale $g, h \notin J$. Wtedy $f \in \sqrt{(J, g)}$ i $f \in \sqrt{(J, h)}$. W takim razie istnieją n, k takie, że

$$f^n \in (J, g) \quad f^n = j_1 + w_1 \cdot g$$

$$f^k \in (J, h) \quad f^k = j_2 + w_2 \cdot h$$

W takim razie

$$f^{n+k} = f^n \cdot f^k = (j_1 + w_1 \cdot g)(j_2 + w_2 \cdot h) \in (J, gh) \subseteq J \implies f \in \sqrt{J}.$$



Dla J i f jak wyżej w $K[\bar{X}]/J = K[\bar{a}]$, gdzie $\bar{a} = \bar{X}/J$, jest:

- $f(\bar{a}) \neq 0$, bo $f \notin J$
- $\bar{a} \in Z(J)$
- $K[\bar{a}]$ jest dziedziną.

Mamy

$$K[\bar{a}] \subseteq K[\bar{a}]_0 \subseteq K[\bar{a}]_0^{\text{alg}},$$

gdzie $K[\bar{a}]_0$ jest ciałem ułamków, a $K[\bar{a}]_0^{\text{alg}}$ jest algebraicznym domknięciem $K[\bar{a}]_0$. W $K[\bar{x}]_0^{\text{alg}}$ istnieje takie \bar{x} , że $\bar{x} \in Z(J) \setminus Z(f)$.

Twierdzenie. [z teorii modeli] Jeśli $L_1 \subseteq L_2$ są ciałami algebraicznie domkniętymi, to $L_1 \prec L_2$, tzn. dla każdego zdania ϕ w języku pierścieni z parametrami w L_1 mamy $L_2 \models \phi \iff L_1 \models \phi$.

Ponieważ

$$K[\bar{a}]_0^{\text{alg}} \models \exists \bar{x} \in Z(J) \setminus Z(f)$$

jest zdaniem w języku pierścieni i $K^{\text{alg}} \prec K[\bar{a}]_0^{\text{alg}}$, to również

$$K^{\text{alg}} \models \exists \bar{x} \in Z(J) \setminus Z(f).$$

Uwaga 15.6. Załóżmy, że K jest ciałem algebraicznie domkniętym takim, że układ równań wielomianowych

$$f_1(\bar{x}) = \dots = f_k(\bar{x}) = 0$$

nie ma rozwiązań w K , tzn. $Z_K(f_1, \dots, f_n) \subseteq Z_K(1)$. Wtedy $1 \in (f_1, \dots, f_k)$.