Wykład 3

$K \subset L$ rozszerzenie ciał.

Def. 4.1 ($a \in L$)

(1) a jest <u>algebraiczny</u> nad K, gdy $f(a)=0$ dla pewnego $0 \neq f \in K[X]$

(2) a jest <u>przestępny</u> nad K, gdy nie jest algebraiczny nad K.
(transcendental)

(3) Rozszerzenie ciał $K \subset L$ jest:

- <u>algebraiczne</u>, gdy $\forall a \in L$ a algebraiczny nad K
- <u>przestępne</u>, gdy nie jest algebraiczne.

(4) Liczba $a \in \mathbb{C}$ algebraiczna/przestępna, gdy jest algebraiczna/przestępna nad $\mathbb{Q}$.

<u>Przykłady</u> (1) i, $\sqrt{2}$, $\sqrt[n]{d}$, $d \in \mathbb{Q}$: algebraiczne

(2) $i^2+1=0$ $\quad (\sqrt{2})^2-2=0$ $\quad (\sqrt[n]{d})^n - d = 0$.

(2) Rozszerzenie $F(p) \subseteq F(p^n)$ jest algebraiczne
ciało mają p^n

$$\left(\text{bo}: \ a \in F(p^n) \Rightarrow a^{p^n} - a = 0 \right)$$

$$W(X) = X^{p^n} - X \in F(p)[X]$$

(3) e, π są <u>przestępne</u> (może później)

(4) $K \subset L = K(X)$: $X \in L$ przestępne nad K

bo: zał, że $0 \neq f \in K[X]$. $\hat{f}(X) = f \neq 0$, w $K(X)$

Uwaga 4,2. $L \supset K$, a algebraiczny $/K \Leftrightarrow I(a/K) \neq \{0\}$.

<u>Def.</u> ($K \subset L$ rozszerzenie ciał)

$[L : K] \overset{\text{def}}{=} \dim_K L$: wymiar L jako przestrzeni liniowej nad K.

stopień rozszerzenia

Uwaga 4,3. $a \in L \supset K$. Ⓔ

(1) a algebraiczny nad K

(2) $K[a] = K(a)$

(3) $[K(a) : K] < \infty$.

D-d

(1) ⇒ (2): $I(a/K) \triangleleft K[X]$ ideał pierwszy

$\Downarrow$ $K[X]$ PID

maksymalny

pierwszy:

$f \cdot g \in I(a/K)$

$\Updownarrow$

$(f \cdot g)(a) = 0$ w L $\quad (f \cdot g)(a) = f(a) \cdot g(a)$

$\Updownarrow$

$f(a) \cdot g(a) = 0$ w L $\quad \varphi_a : K[X] \longrightarrow L$

ewaluacyjna homomorfizm pierścieni.

$\Updownarrow$

$f(a) = 0 \vee g(a) = 0$

$\Updownarrow$

$f \in I(a/K) \vee g \in I(a/K)$

$L \supseteq K[a] \cong K[X]/_{I(a/K)}$ ciało, więc

$K[a] = K(a)$.

(2) ⇒ (3).

Możemy założyć, że $a \notin K$, więc $a \neq 0$.

$K[a]$: ciało, więc $a^{-1} \in K[a]$, tzn:

$a^{-1} = f(a)$ dla pewnego $f \in K[X]$

$\Downarrow$

$a \cdot f(a) = 1$. $\quad a^{-1} \neq 0 \Rightarrow f \neq 0$

A2R/3

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

$$0 = a \cdot f(a) - 1 = b_n a^{n+1} + b_{n-1} a^{n-2} + \dots + b_0 a^1 - 1$$

$$\Downarrow \; b_n \neq 0$$

$$a^{n+1} \in \mathrm{Lin}_K(1, a, a^2, \dots, a^n)$$

(*) $\forall m \quad a^m \in \mathrm{Lin}_K(1, a, \dots, a^n)$.

(a) $m = 0, \dots, n+1$: już mamy

(b) krok indukcyjny $m \longmapsto m+1$.

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

$$a^m = \sum_{i=0}^{n} c_i a^i, \quad c_i \in K$$

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

z (*): $\{1, a, a^2, \dots\} \subseteq \mathrm{Lin}_K(1, a, \dots, a^n)$

liniowo generuje $K[a] = K(a)$ nad K $\Rightarrow [K(a):K] \leq n+1$.

(3) $\Rightarrow$ (1): $\{1, a, a^2, \dots\}$ nieskończony układ $\Rightarrow$

liniowo zależny nad K:

$$\sum_{i=0}^{k} b_i a^{n_i} = 0 \quad \text{dla pewnych } b_i \in K, \; b_k \neq 0$$

$$0 \leq n_0 < n_1 < \dots < n_k$$

$\Downarrow$

a algebraiczny nad K.

Def. 4.4. $K \subset L \ni a$: algebraiczny nad K,

$I(a/K) = (f)$, $f \in K[X]$, $f \neq 0$

bso: f unormowany, tzn: (monic) wiodący współczynnik $= 1$.

jedyny!

(1) ten f nazywamy wielomianem minimalnym a nad K.

(2) $\deg(a/K) := \deg f$.
stopień a nad K

Uwaga 4.5.

(1) $f \in K[X]$ jest wielomianem unormowanym minimalnego stopnia t. że $f(a) = 0$.

(2) $\deg f = [K(a) : K]$

D-d (1) $\dashv$.

(2) Niech $n = \deg f$. $f = X^n + b_{n-1}X^{n-1} + \dots + b_0$, $(b_i \in K)$

$\cdot\ f(a) = 0 \Rightarrow a^n \in Lin_K(1, \dots, a^{n-1}) \underset{\text{d-d } 4.3}{\Longrightarrow}$

$Lin_K(1, a, \dots, a^{n-1}) \supseteq K[a] \underset{4.3}{=} K(a) \Longrightarrow$

- $\mathrm{Lin}_K(1, a, \dots, a^{n-1}) = K(a)$.

- $1, a, \dots, a^{n-1}$: układ lin. niezależny nad K

bo: jeśli nie, to dla pewnego $r < n$

$$a^r \in \mathrm{Lin}_K(1, a, \dots, a^{r-1})$$

$$\Downarrow$$

$$\exists\ g \in I(a/K) \quad \deg g = r < n \quad \text{↯}.$$

Przykład. $X^2 - 2$ wielomian minimalny dla $\sqrt{2}/\mathbb{Q}$

$X^3 - 3$ —"— —"— $\sqrt[3]{3}/\mathbb{Q}$.

- Jeśli $K \subset L \ni a$ algebraiczny $/K$, $\deg(a/K) = n$,

to $K(a) = K[a] = \{\underbrace{\sum_{i=0}^{n-1} b_i a^i}_{\text{przedstawienie jednoznaczne}} : b_i \in K\}$

i $\{1, a, \dots, a^{n-1}\}$ baza liniowa $K(a)$ nad K.

np. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

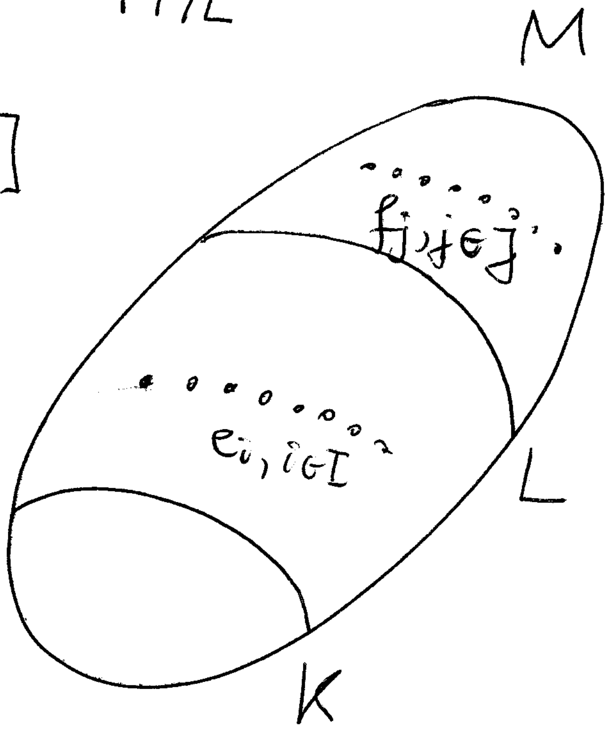
Fakt 4.6. $K \subset L \subset M$ rozszerzenia ciał.

Wtedy $[M:K] = [M:L] \cdot [L:K]$.

D-d Niech $\{e_i : i\in I\}$ baza liniowa L/K

$\{f_j : j\in J\}$ —//— M/L,

$|I| = [L:K]$, $|J| = [M:L]$



Pdk, że układ:

$$X := \{\underset{\substack{\| \\ e_i\cdot f_j}}{g_{ij}} : i\in I, j\in J\} \leftarrow \text{baza } M/K.$$

(a) X układ lin. niezależny nad K:

$$\sum_{i,j} \overset{\in K}{k_{ij}}\, e_i f_j = 0$$

$$\| $$

$$\sum_j \Big(\underbrace{\sum_i k_{ij} e_i}_{\in L}\Big) f_j \overset{\{f_j\} \text{ baza } M/L}{\Longrightarrow} \forall j\in J\ \sum_i k_{ij} e_i = 0$$

$$\Downarrow \{e_i\} \text{ baza } L/K$$

$$\forall j\in J\ \forall i\in I\ k_{ij} = 0.$$

(b) generowanie M/K

niech $m\in M$

$$\| $$

$$\sum_j \underset{\in L}{l_j} f_j = \sum_{i,j} k_{ij} (e_i\cdot f_j).$$

$$l_j = \sum_i k_{ij} e_i$$

Wn. 4.7. $(K \subset L)$

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

jest podciałem ciała L, $K \subset K_{alg}(L)$.

D-d. Niech $a, b \in K_{alg}(L)$. Wtedy:

$[K(a):K] < \infty \Rightarrow \forall x \in K(a)$ x algebraiczny$/K$

(bo $[\underset{K(a)}{\underset{\cap}{K(x)}} : K] \leq [K(a):K] < \infty$)

Więc $K(a) \subseteq K_{alg}(L)$.

$K \subset K(a) \subset K(a,b) \subset L$

$$[K(a,b):K] = \underbrace{[K(a):K]}_{<\infty} \cdot [\overbrace{K(a)(b)}^{K(a,b)} : K(a)] < \infty.$$

$\underset{<\infty}{} \Rightarrow \Uparrow$

$\Uparrow$

$b : \text{alg}/K \Rightarrow b \text{ alg}/K(a)$

Stąd: $\forall c \in K(a,b)$

$[\underset{K(a,b)}{\underset{\cap}{K(c)}} : K] \leq [K(a,b):K] < \infty$ więc $c \in K_{alg}(L)$.

Stąd: $K(a,b) \subseteq K_{alg}(L)$ i $K_{alg}(L)$ ciało.

Def. 4.8. A2R 9/3

(1) $K_{alg}(L)$ nazywamy <u>algebraicznym domknięciem</u> ciała K w ciele L.

~~(2)~~ np. $\mathbb{Q}_{alg}(\mathbb{C}) \overset{ozn.}{=} \hat{\mathbb{Q}} = \mathbb{Q}^{alg}$; ciało liczb algebraicznych

(2) K jest <u>algebraicznie domknięte</u> w L, gdy $K_{alg}(L) = K$.

<u>Przykład</u> (1) $\hat{\mathbb{Q}}$ jest przeliczalne (bo $\mathbb{Q}[X]$ przeliczalny) więc jest dużo liczb przestępnych.

(2) K jest algebraicznie domknięte w $K(X)$.

(3) $\frac{1}{\sqrt[3]{2}+\sqrt{3}} \in \mathbb{Q}[\sqrt{3}, \sqrt[3]{2}]$

$L = \mathbb{Q}[\sqrt[3]{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{3}][\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}[\sqrt{3}]\}$

$\sqrt[3]{2} + \sqrt{3} \in L \Rightarrow \frac{1}{\sqrt[3]{2}+\sqrt{3}} \in L$ jest tej postaci.

Wn. 5.1. ($K \subset L \subset M$ rozszerzenia ciał)

$K \subset M$ jest algebraiczne $\iff \begin{cases} K \subset L \text{ jest algebraiczne} \\ \quad i \\ L \subset M \text{ jest algebraiczne.} \end{cases}$

D-d $\Rightarrow$: jasne.

$\Leftarrow$: Niech $m \in M$.

$L \underset{alg.}{\subset} M \Rightarrow f(m) = 0$ dla pewnego $0 \neq f \in L[X]$, $f = \sum_{i=0}^{n} a_i X^i$, $a_i \in L$, $a_n \neq 0$

więc m : algebraiczne nad $K(a_0, \dots, a_n)$

$$[K(m):K] \leq [\underbrace{K(a_0, \dots, a_n, m)}_{alg./K} : K] =$$

$$= [K(a_0, \dots, a_n)(m) : K(a_0, \dots, a_n)] \cdot [K(\overline{a_0 \dots a_n}) : K] < \infty.$$

$$\qquad < \infty \qquad\qquad\qquad < \infty$$

Wn. 5.2. $K_{alg}(L)$ jest algebraicznie domknięte w L ($K \subset L$ ciała)

(tzn : ~~K_{alg}~~ $(K_{alg}(L))_{alg}(L) = K_{alg}(L)$)