## Wykład 6.

$$K \underset{\text{alg.}}{\subseteq} L$$

Def. (1) $\text{sep}_L(K) = \{a \in L : a/K \text{ rozdzielny}\}$

rozdzielcze domknięcie $K$ w $L$

(2) $\text{rad}_L(K) = \{a \in L : a/K \text{ czysto nierozdzielny}\}$

czysto nierozdzielcze (radykalne) domknięcie $K$ w $L$

Wniosek 7.2

(1) $$\underbrace{K \subseteq \text{sep}_L(K), \ \text{rad}_L(K)}_{\text{podciała}} \subseteq L \subseteq \hat{K}, \quad \text{sep}_L(K) \cap \text{rad}_L(K) = K.$$

D-d. • $\text{sep}_L(K)$ : ciało : wniosek 6.9

• $\text{rad}_L(K)$ : ciało, bo : $\text{rad}_L(K) = L \cap \bigcap_{f \in G(\hat{K}/K)} \text{Fix}(f)$

$$\text{Fix}(f) = \{a \in \hat{K} : f(a) = a\} \ \underline{\text{ciało}}.$$

• dla $a \in \text{sep}_L(K) \cap \text{rad}_L(K)$

$W_a(X) = X - a$ : wiel. minimalny dla $a/K$.

Def (1) $\hat{K}^s = \text{sep}_{\hat{K}}(K)$ : rozdzielcze domknięcie $K$

(2) $\hat{K}^r = \text{rad}_{\hat{K}}(K)$ : czysto nierozdzielcze domknięcie $K$

Uwaga 7.3 (1) $\text{sep}_L(K) = \hat{K}^s \cap L$, $\text{rad}_L(K) = \hat{K}^r \cap L$

[Gdy $K \subseteq L \subseteq \hat{K}$]

(2) Zał, że $K \subseteq L \subseteq M \subseteq \hat{K}$. Wtedy

$$K \underset{\text{rad}}{\subseteq} L \underset{\text{rad}}{\subseteq} M \iff K \underset{\text{rad}}{\subseteq} M$$

(3) gdy char $K=0$, to $sep_L(K) = K^{alg}(L)$

i $rad_L(K) = K$,

oraz $\hat{K}^s = \hat{K}$ i $\hat{K}^r = K$,

**Fakt 7.4** Zał., że $K \subseteq L \subseteq \hat{K}$, $K_s = sep_L(K)$, $K_r = rad_L(K)$, $L' = K_s \cdot K_r$ : złożenie ciał $K_s$ i $K_r$ w $L$,

tzn: ciało generowane (w $L$) przez $K_s \cup K_r$, tzn: $L' = K_s(K_r) = K_r(K_s)$

Wtedy:

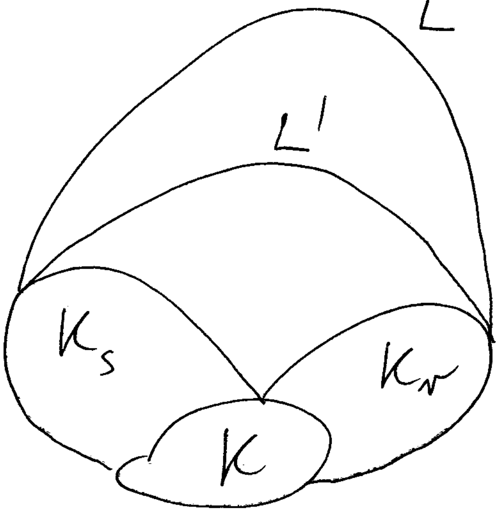
(1) $[L' : K] = [K_s : K] \cdot [K_r : K]$

(2) Gdy $K \underset{\text{normalne}}{\subseteq} L$, to $K_s \cdot K_r = L$

(3) $K_s \underset{\text{radykalne}}{\subseteq} L$, $K_r \underset{\text{rozdzielcze}}{\subseteq} L'$

D-d: Gdy char $K=0$, to jest trywialne, bo wtedy: $K_s = L$, $K_r = K$, $L' = L$.

dlatego zał., że char $K = p > 0$



AL2R/6 ③

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

$$[L':K] = \underbrace{[K_r(K_s):K_r]} \cdot [K_r:K]$$

Wystarczy pokazać, że $\parallel$ ← ~~to mamy A, więc wystarczy~~

$[K_s:K]$ ~~pokazać A, tzn:~~

W tym celu wystarczy pokazać, że:

$$\forall K \underset{\substack{\uparrow\\ \text{skończ}}}{\subseteq} K_r^0 \subseteq K_r \ \forall K \underset{\substack{\uparrow\\ \text{skończ.}}}{\subseteq} K_s^0 \subseteq K_s \quad [K_s^0:K] = [K_r^0(K_s^0):K_r^0].$$

Zad. z listy 4: Załóżmy, że $K \subseteq L, M \subseteq \hat{K}$ rozszerzenia ciał t. że $L \cap M = K$. Jeśli $\forall K \underset{\text{sk}}{\subseteq} L_0 \subseteq L \ \forall K \underset{\text{sk.}}{\subseteq} M_0 \subseteq M$

$$[L_0(M_0):L_0] = [M_0:K],$$

to $[L(M):L] = [M:K]$

Niech $K \underset{\text{skończ}}{\subseteq} K_r^0 \subseteq K_r$, $K \underset{\text{skończ.}}{\subseteq} K_s^0 \subseteq K_s$

z tw. Abela niech $a \in K_s^0$ t. że $K_s^0 = K(a)$.

Wtedy też $K_r^0(K_s^0) = K_r^0(a)$ i

$[K_s^0:K] = \deg(a/K)$, $[K_r^0(a):K_r^0] = \deg(a/K_r^0)$

Wystarczy pokazać, że $\deg(a/K) = \deg(a/K_r^0)$.

Niech $n = [K(a):K] = \deg(a/K)$

$1, a, \ldots, a^{n-1}$ ; baza liniowa $K(a)/K$.

$\Downarrow$

$\forall l > 0 \quad 1, a^{p^l}, \ldots, \overset{\Downarrow}{a^{(n-1)\cdot p^l}}$ : też baza $K(a)/K$ (†)

bo: [**Lemat** $a/K$ rozdzielczy, $p = \mathrm{char}\, K \Rightarrow$
$K(a) = K(a^p)$ (zad 7 z listy 4)]

Dlatego również $K(a) = K(a^{p^l})$, więc (†).

Pokażemy, że $1, a, \ldots, a^{n-1}$ : baza $K_r^0(a)/K_r^0$:

- liniowa niezależność:

$\sum k_i a^i = 0$, $k_i \in K_r^0$. Niech $l$ t.że $k_i^{p^l} \in K$ dla wszystkich $i$

$$\Downarrow$$

$$\sum \underset{\overset{\uparrow}{K}}{k_i^{p^l}} (a^i)^{p^l} = 0 \underset{(\dagger)}{\Longrightarrow} \forall i \; k_i = 0.$$

$[K_r^0(a) : K_r^0] \leq [K(a) : K] = n$, ~~więc $1, \ldots, a$~~

więc $1, a, \ldots, a^{n-1}$ : baza $K_r^0(a)/K_r^0$.

(2) bso $[L:K] < \infty$, [bo: $L = \bigcup\{L_0 : K \underset{\overset{\uparrow}{\text{normalne skończone}}}{\subseteq} L_0 \subseteq L\}$]

(a) $L \supseteq K_r$ : rozdzielcze, bo:

niech $a \in L$. $a = a_1, a_2, \ldots, a_n$ : wszystkie różne pierwiastki $W_a(X) \in K[X]$.

Niech $V(X) = \prod_{i=1}^{n} (X - a_i)$. Dla $f \in G(\hat{K}/K)$
$f[L] = L$, więc:

~~$\forall l \geq 0$ $1, a_s^{p^l}, \ldots, a_s^{(n-1)p^l}$ : baza $K[a_s]/K$~~

~~bo: Lemat, $a/K$ rozdzielczy $\Rightarrow K[a] = K[a^p]$~~ char $K = p$.

---

f permutuje $\{a_1, \ldots, a_n\}$. Stąd $f(V(X)) = V(X)$

więc $V(X) \in K_r[X]$, f zachowuje współczynniki $V(X)$

Czyli: a rozdzielczy$/K_r$.

(b) $L \supseteq K_s$ radykalne, bo ~~$L = K_s(K_r)$~~.

~~$[\forall x \in L\ \exists l\ x^{p^l} \in K_s]$~~

Z uwagi 6,6(3): Jeśli $a \in L$ to dla pewnego $l$ $a^{p^l}$: rozdzielczy$/K$, czyli $a^{p^l} \in K_s$, Czyli: a: radykalny$/K_s$.

Z (a) i (b): $L \supseteq K_r \cdot K_s$ rozszerzenie rozdzielcze i radykalne, więc $L = K_r K_s$

(3). $L \supseteq K_s$ radykalne: jak wyżej.

· $L' \supseteq K_r$: rozdzielcze; bo $L' = K_r[K_s]$.

---

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

Def $[L:K]_s = [sep_L(K):K]$ stopień rozdzielczy ciała L nad K.

$[L:K]_r = [L:sep_L(K)]$ stopień radykalny L/K nierozdzielczy.

Więc: $[L:K] = [L:K]_s \cdot [L:K]_r$.

$$K \underset{\substack{\uparrow \\ \text{rozdzielcze}}}{\subseteq} sep_L(K) \underset{\substack{\uparrow \\ \text{radykalne.}}}{\subseteq} L$$

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

(1) $K \subseteq L$ rozdzielcze $\Rightarrow [L:K] = |\{f|_L : f \in G(\hat{K}/K)\}|$.

(2) Ogólnie: $[L:K]_s = \longrightarrow$ $\| $ $|\{f : L \longrightarrow \hat{K} :$ homomorfizm ciał, $f|_K = id\}|$

D-d.

Najpierw gdy $[L:K] < \infty$. $G(\hat{K}/K) \ni$

(1) Z tw. Abela $L = K(a)$. $f|_L$ wyznaczone jednoznacznie przez $f(a)$

$$f(a) \in \{\text{pierwiastki } \underset{\substack{\cap \\ K[X]}}{W_a(X)}\} \Leftarrow \text{jest ich } n = [L:K]$$

(2) $L \supseteq K_s$: radykalne, więc $f|_L$ wyznaczone przez $f|_{K_s}$.

Dlatego: $|\{f|_L : f \in G(\hat{K}/K)\}| =$

$$= |\{f|_{K_s} : f \in G(\hat{K}/K)\}| = [K_s : K] = [L : \overset{\substack{sep_L(K) \\ \|}}{K_s}]$$

Przypadek ogólny $[L:K]$ można zredukować do przypadku $[L:K] < \infty$ (ćwiczenie). (wskazówka: rozważyć odpowiednią bazę liniową $L$ nad $K$ )

**Uwaga** $[L:K]_r<\infty \Rightarrow [L:K]_r$ jest potęgą $p$.

(char $K=p>0$)

D-d Indukcja wzgl. $[L:K]_r = [L:K_s]$.

$$K_s \overset{\parallel}{} \ \mathrm{sep}_L(K)$$

BSO $K=K_s$.

~~Niech $a\in L\setminus K_s$~~

Niech $a\in L\setminus K$. Wtedy $a/K$ radykalny $\Rightarrow$ $a^{p^l}\in K$ ($l$: minimalne).

Niech $a'=a^{p^{l-1}}$. Wtedy $a'\in L\setminus K$ i $(a')^p\in K$, dlatego

$$\underset{K[X]}{\underset{\cap}{W_{a'}}}(X) = X^p-(a')^p \quad \text{i} \quad K \underset{\text{stopień } p.}{\subseteq} K(a') \underset{\text{radykalne.}}{\subseteq} L$$

$$[L:K(a')] < [L:K]$$

⇓ zał. indukc.

$$[L:K(a')] = p^r \Rightarrow [L:K]=p^{r+1}.$$

---

Norma i ślad.

$B\subseteq V$ baza

$V$: p. liniowa/$K$, $\dim V<\infty$, $f: V\longrightarrow V$ liniowe

1. $\det(f)=\det(m_B(f))\in K$

   $\det(f\circ g)=\det(f)\cdot\det(g)$.

2. $Tr(f)=Tr(m_B(f))\in K$.

   ślad

   suma wyrazów na głównej przekątnej $m_B(f)$

$\mathrm{Tr}(f+g) = \mathrm{Tr}(f) + \mathrm{Tr}(g)$

$\mathrm{Tr}(\underset{\underset{K}{\cap}}{\lambda} f) = \lambda \mathrm{Tr}(f)$ $\quad \mathrm{Tr}: \mathrm{End}(V) \longrightarrow K$

liniowe.

(fakty z algebry liniowej)

---

Teraz: $K \subseteq L$ skończone rozszerzenie ciał.

$\Rightarrow$ $L$: przestrzeń liniowa $/K$, $\dim_K L = [L:K]$

$\underset{a}{\overset{\Downarrow}{}} \mapsto f_a : L \longrightarrow L$ $\quad f_a(x) = a \cdot x$ : $K$-liniowe przekształcenie

Def. (1) $\underset{\text{norma}}{N_{L/K}}(a) = \det(f_a)$

(2) $\underset{\text{ślad}}{\mathrm{Tr}_{L/K}}(a) = \mathrm{Tr}(f_a)$

Fakt 8.1. ($K \subseteq L$ skończone).

Niech $\{f_1, \ldots, f_k\} = \{f : L \xrightarrow{\text{homo}} \hat{K} : f|_K = \mathrm{id}\}$.

Ⓩ $k = [L:K]_s$, $a \in L$,

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

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

<u>D-d</u> ~~2~~ 1°. $L = K(a)$, gdzie $a/K$ rozdzielczy

Niech $W_a(X) \in K[X]$ wiel. minimalny dla $a/K$. $L \subseteq \hat{K}$.

$$\overset{\|}{}\; X^k + a_{k-1}X^{k-1} + \dots + a_1X + a_0$$

$b_1 = a, \dots, b_n \in \hat{K}$ pierwiastki $W_a$.

<u>bso</u> $b_i = f_i(a)$

<u>więc</u> w $\hat{K}[X]$

$$W_a(X) = \prod_{i=1}^{k}(X - b_i)$$

$$a_{k-1} = -\sum_{i=1}^{k} b_i, \quad a_0 = (-1)^k \prod_{i=1}^{k} b_i.$$

Z zad 4 z listy 5: $N_{L/K}(a) = (-1)^k a_0 = \prod_{i=1}^{k} f_i(a)$

$$Tr_{L/K}(a) = -a_{k-1} = \sum_{i=1}^{k} f_i(a).$$

2°. Przypadek ogólny:

(1) Niech $a \in L$

$$[L : \underset{\substack{\| \\ sep_L(K)}}{K_s}] = [L : K]_r = p^l \overset{\text{zad}}{\Rightarrow} a^{p^l} \in K_s$$

$$N_{L/K}(a)^{p^l} = N_{L/K}(\underset{\substack{\uparrow \\ K_s}}{a^{p^l}}) \underset{\substack{\uparrow \\ \text{zad}}}{=} N_{K_s/K}(a^{p^l})^{[L:K_s]} = N_{K_s/K}(a^{p^l})^{p^l}$$

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

$$N_{K_s/K}(b) \underset{\substack{\uparrow \\ \text{zad}}}{=} N_{K(b)/K}(b)^{[K_s : K(b)]} \underset{\substack{\uparrow \\ \text{zad}}}{=} \prod_{i=1}^{k} f_i(b)$$

(tu: $f_1, \dots, f_k : L \xrightarrow[K]{} \hat{K}$ wszystkie $\Rightarrow f_1|_{K_s}, \dots, f_k|_{K_s} : K_s \xrightarrow{K} \hat{K}$ też wszystkie, parami $\neq$)

Dlatego

$$N_{L/K}(a) = N_{K_s/K}(\underset{\substack{\shortparallel \\ a^{p^l}}}{b}) = \prod_{i=1}^{k} f_i(a^{p^l}) = \left[\prod_{i=1}^{k} f_i(a)\right]^{p^l}.$$

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

i $Tr_{L/K}(a) = 0$ ~~(zad z listy)~~

1°. $a \in K_s \Rightarrow Tr_{L/K}(a) \underset{\substack{\uparrow \\ \text{zad}}}{=} \underbrace{[L:K_s]}_{p^l} \cdot Tr_{K_s/K}(a) = 0$

2°. $a \notin K_s \Rightarrow W_a(X) \in K[X^p]$ (Uwaga 6.6(4))

$$\shortparallel$$
$$X^{tp} + a_{(t-1)p}X^{(t-1)p} + \dots$$

stąd: $a_{tp-1} = 0 = Tr_{L/K}(a)$.

Jeśli $[L:K]_r = 1$, to $L = K_s$, $K \subset L$ rozdzielcze

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

$$Tr_{L/K}(a) = [L:K(a)] \cdot Tr_{K(a)/K}(a) \underset{\substack{\uparrow \\ \text{liczenie} \\ \text{homomorfizmów}: L \xrightarrow[K]{} \hat{K}}}{=} \sum_{i=1}^{k} f_i(a).$$