Wykład 5. A2R/5 (1)

Def. Rozszerzenie ciał $K \subseteq L$ jest <u>skończone</u>, gdy $[L:K] < \infty$.

TW. 6.4. Rozszerzenie skończone $L \supseteq K$ jest normalne $\iff$ L jest ciałem rozkładu pewnego wielomianu $W \in K[X]$, nad K.

<u>D-d</u>. Bso $K \subseteq L \subseteq \hat{K}$.

$\Leftarrow$. $L = K(\underbrace{a_1, \dots, a_n}_{\text{wszystkie pierwiastki } W \text{ w } \hat{K}})$

$f \in G(\hat{K}/K) \Rightarrow f(W) = W \Rightarrow f[\{a_1, \dots, a_n\}] = \{a_1, \dots, a_n\}$

$\Rightarrow f[L] = L$.

$\Rightarrow$: $L = K(a_1, \dots, a_n)$ dla pewnych $a_1, \dots, a_n \in L$. (bo $K \underset{\text{skończ}}{\subset} L$)

a_i / K algebraiczne dla $i = 1, \dots, n$.

Niech $W \in K[X]$ t. że $W(a_i) = 0$ $(i = 1, \dots, n)$.

~~z tw. 6.3: W rozkłada się w L[~~

$\underset{K[X]}{\underset{\cap}{W_i(x)}}$: wiel. minimalny dla a_i / K

$W = W_1 \cdot W_2 \cdot \ldots \cdot W_n$.

Z tw. 6.3: każde W_i rozkłada się

w $L[X]$ na iloczyn czynników liniowych

$\Rightarrow$ W rozkłada się w $L[X]$ na iloczyn czynników liniowych

i $L = K(a_1, \dots, a_n) = K($pierwiastki W w $L)$.

L: ciało rozkładu W nad K.

<u>Przykład</u> $K \subset L$ ciała skończone $\Rightarrow$ $K \subset L$ normalne

bo: $|L| = p^n$ $\quad W_{p^n-1}(X) = X^{p^n-1} - 1$

L: ciało rozkładu W nad K.

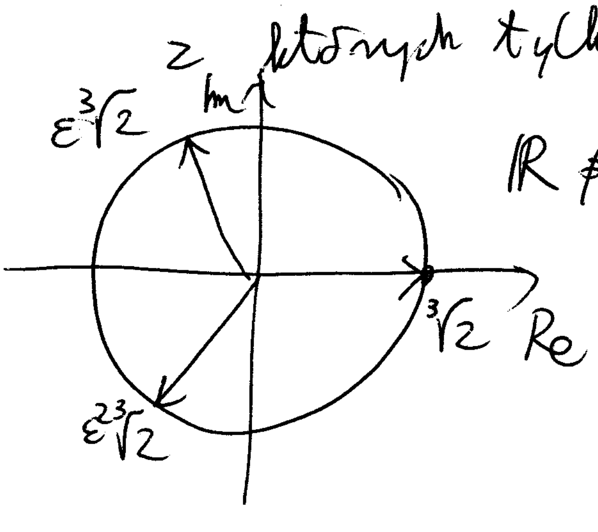
<u>Przykład</u>. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$: rozszerzenie skończone,

ale nie normalne,

bo: (1) X^3-2 nierozkładalny$/\mathbb{Q}$ (kryterium Eisensteina)

(2) w ciele $\mathbb{C}$ ma 3 pierwiastki,

z których tylko jeden $\in \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$,



$\mathbb{R} \not\ni \varepsilon$: pierwiastek ~~pierwot.~~ stopnia 3 z 1

Def. ($K \subseteq L \subseteq \hat{K}$)

L_1 := ciało generowane przez $\bigcup\{f[L] : f \in G(\hat{K}/K)\}$

normalne domknięcie ciała L w $\hat{K}$.

Uwaga 6.5. (1) Rozszerzenie $K \subseteq L_1$ jest normalne.

(2) Jeśli $\underset{\text{normalne}}{K \subseteq L_2}$ i $L \subseteq L_2$, to $\exists f : L_1 \xrightarrow{\text{monomorfizm}} L_2$

$f|_K = id$.

<u>D-d</u>

(1) z ~~definicji lub~~ Uwagi 6.2.

(2) bso $K \subset L \subset L_2 \subset \hat{K}$. i $K \subset L \subset L_1 \subset \hat{K}$.

Niech $f \in G(\hat{K}/K)$, $f[L] \subseteq L_2$ (bo $\underset{\text{normalne}}{K \subset L_2}$)

więc $\bigcup\{f[L] : f \in G(\hat{K}/K)\} \subseteq L_2$

$$\Downarrow$$

$L_1 \subseteq L_2$.

<u>Rozszerzenia rozdzielcze.</u>

Def. (1) $a \in \hat{K}$ jest <u>rozdzielczy</u> nad K, gdy

$W_a(X) \in K[X]$ ma w $\hat{K}$ tylko pierwiastki

wielomian minimalny a/K jednokrotne.

(2) $\underset{\text{algebr}}{K \subset L}$: <u>rozszerzenie rozdzielcze</u>, gdy $\forall a \in L$

a/K rozdzielczy.

(3) Wielomian $W(X) \in K[X]$ jest <u>rozdzielczy</u>, gdy W ma tylko pierwiastki ~~...~~ jednokrotne w $\hat{K}$.

Uwaga 6.6. Zał, że $W(X) \in K[X]$ nierozkładalny, $\deg W > 0$, wtedy

(1) $W(X)$ rozdzielczy $\Leftrightarrow$ $W(X)$ i $W'(X)$ są względnie pierwsze

(2) $\mathrm{char}\, K = 0 \Rightarrow W$ rozdzielczy

(3) $\mathrm{char}\, K = p > 0 \Rightarrow$ (W nierozdzielczy $\Leftrightarrow$ $W(X) \in K[X^p]$)

tzn. $W(X) = V(X^p)$ dla pewnego $V(X) \in K[X]$.

<u>D-d</u> Zad. z listy 4.

<u>Przykłady</u> (1). $K \subseteq L$ rozdzielcze, $K \subseteq L_1 \subseteq L$ $\Rightarrow L_1 \subseteq L$ rozdzielcze (ćw)

(2) $\mathrm{char}\, K = 0 \Rightarrow$ każde rozszerzenie algebraiczne ciała K jest rozdzielcze

(3) $K \subseteq L$: ciała skończone $\Rightarrow K \subseteq L$ rozdzielcze

(bo: L : ciało rozkładu wielomianu $X^{p^n} - X$ o pierwiastkach jednokrotnych)

(4) Przykład rozszerzenia nierozdzielczego:

$K = F_p(X)$ ciało funkcji wymiernych

$\cap\!|$

$L = K(\sqrt[p]{X})$ $\quad W_a(T) = T^p - X \in K[T]$

$\quad\quad\; \overset{\shortparallel}{a}$ $\quad$ wielomian nierozkładalny

$W_a' = 0$ (Eisenstein)

w ciele L: $W_a(T) = (T-a)^p$; a: p-krotny pierwiastek.

Lemat 6, 7.

(1) $a \in \hat{K} \Rightarrow |\{f(a) : f \in G(\hat{K}/K)\}| \leq \deg(a/K)$.

(2) a/K rozdzielczy $\Leftrightarrow$ w (1) jest $=$.

<u>D-d</u>.

$\{f(a) : f \in G(\hat{K}/K)\} \underset{6.1}{=} \{$ pierwiastki wielomianu minimalnego $W_a(X) \in K[X]$ a nad K. $\}$

$\deg(a/K) \overset{?}{=} \deg W_a$.

<u>Def</u>. Element $a \in L$ nazywamy <u>elementem pierwotnym</u> rozszerzenia $K \subseteq L$, gdy $L = K(a)$.

TW. 6.8 (Abela, o elemencie pierwotnym).

$K \subset L$ rozszerzenie skończone, $L = K(a_1, \ldots, a_n)$ i $a_1, \ldots, a_n$ rozdzielcze$/K \Rightarrow \exists\, a^* \in L$ rozdzielczy$/K$

$L = K(a^*)$.

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

D-d 1°. K skończone. Wtedy L też skończone i L^* cykliczna. Niech $a^* \in L^*$ generator.
a^*: dobry: $L = K(a^*)$.

2°. K nieskończone: indukcja względem n.

Krok indukcyjny $n-1 \longrightarrow n$ $(n > 1)$

$\underbrace{K(a_1, \ldots, a_{n-1}}, a_n) = K(\underset{\underset{a_n}{\parallel}}{a}, b)$,

$\left.\begin{array}{l} K(a_1, \ldots, a_{n-1}) = K(b) \\ b/K \text{ rozdzielny} \end{array}\right]$ z zał. indukcyjnego

Niech $n = \deg(b/K)$, $m = \deg(a/K(b))$.

Z lematu 6.7:

$\underset{\underset{id_{\hat{K}}}{\parallel}}{f_1}, \ldots, f_n \in G(\hat{K}/K)$ $\ni f_1(b), \ldots, f_n(b) \in$ parami $\neq$

$f_{1,1}, \ldots, f_{1,m} \in G(\hat{K}/K(b))$ t. że

$f_{1,1}(a), \ldots, f_{1,m}(a)$ parami $\neq$.

$$\begin{array}{ccccc}
K(b)(a) & \xrightarrow[f_{1,j}]{j=1,\ldots,m} & K(b, f_{1,j}(a)) & \xrightarrow[i=1,\ldots,n]{f_i} & K(f_i(b), f_i(f_{1,j}(a))) \\
\cup & & \subseteq & & \subseteq \\
K(b) & & \xrightarrow[i=1,\ldots,n]{f_i} & & K(f_i(b)) \\
\cup & & & & \cup \\
K & & & & K
\end{array}$$

Dla $i=1,\dots,n$, $j=1,\dots,m$ niech

$$f_{i,j} = f_i \circ f_{1,j} \in G(\hat{K}/K).$$

(*) $\langle i,j\rangle \neq \langle i',j'\rangle \Rightarrow \langle f_{i,j}(a), f_{i,j}(b)\rangle \neq \langle f_{i',j'}(a), f_{i',j'}(b)\rangle$.

<u>bo:</u> $\cdot\ f_{ij}(b) = f_i(f_{1,j}(b)) = f_i(b)$.

$f_{1,j} \in G(\hat{K}/K(b))$

1° $i \neq i' \Rightarrow f_{ij}(b) = f_i(b) \neq f_{i'}(b) = f_{i'j}(b)$.

2° $i = i'$ & $j \neq j'$.

$$f_{ij}(a) = f_i(f_{1,j}(a)) \underset{\uparrow}{\neq} f_i(f_{1,j'}(a)) = f_{ij'}(a).$$

bo $f_{1,j}(a) \neq f_{1,j'}(a)$

~~Dlatego $\{\langle f_{ij}(a), f_{ij}(b)\rangle : \langle i,j\rangle \in \{1,\dots,n\}\times\{1,\dots,m\}\}$ parami~~ ~~różne~~.

• K <u>nieskończone</u> $\Rightarrow$ istnieje $c \in K$ t.że

dla $\langle i,j\rangle \neq \langle i',j'\rangle$ $\cancel{f_{ij}(b) + f_{ij}(a)\cdot c \neq f_{i'j'}(b) + f_{i'j'}(a)\cdot c}$

$$f_{ij}(b) + f_{ij}(a)\cdot c \neq f_{i'j'}(b) + f_{i'j'}(a)\cdot c.$$

bo: $$F(X) = \prod_{\langle i,j\rangle \neq \langle i',j'\rangle} \left[f_{ij}(b) + f_{ij}(a)\cdot X - (f_{i'j'}(b) + f_{i'j'}(a)\cdot X)\right]$$

$c \in K$ niepierwiastek F.

(+) $K(b,a) = K(a^*)$, gdzie $a^* = b + a\cdot c$.

$\uparrow$ element pierwotny

$\supseteq$: jasne.

$\subseteq$: $f_{ij}(a^*)$; $1 \leq i \leq n$, $1 \leq j \leq m$: parami $\neq$ (wybór c)

$\Rightarrow \deg(a^*/K) \geq n \times m$

$$n \times m \leq [K(a^*):K] \leq [K(a,b):K] =$$

$$= \underbrace{[K(b):K]}_{=n} \cdot \underbrace{[K(b;a):K(b)]}_{=m} = n \times m$$

Dlatego: wszędzie tu są $=$ i $K(a^*) = K(a,b)$.

Stąd też (z Lematu 6.7) a^*/K rozdzielczy.

<u>Wniosek</u> 6.9. (1) Jeśli $L = K(a_1, \dots, a_n)$, a_i/K rozdzielcze ($i = 1, \dots, n$), to $L \supset K$ rozdzielcze.

(2) $\underbrace{K \subset L \subset M}_{\text{rozdzielcze}} \Rightarrow \underbrace{K \subset M}_{\text{rozdzielcze}}$

<u>D-d</u> (1) $L = K(a)$, a/K rozdzielczy

Zał, że $b \in L$ nie rozdzielczy $/K$.

$L = K(b,a).$ $\quad \underset{\underset{[K(a):K]}{\shortparallel}}{\overset{\overset{n\times m}{\shortparallel}}{\deg(a/K)}} = \underset{\underset{[K(b):K]}{\shortparallel}}{\overset{\overset{n}{\shortparallel}}{\deg(b/K)}} \cdot \underset{\underset{[K(a,b):K(b)]}{\shortparallel}}{\overset{\overset{m}{\shortparallel}}{\deg(a/K(b))}}$ A2R/5

$b = g(a),\ g \in K[X]$,

$= \left|\{f(a) : f \in G(\hat{K}/K)\}\right| = \left|\{(f(b), f(a)) : f \in G(\hat{K}/K)\}\right| \leq$

$= n \times m$

bo a/K rozdzielczy

tu $k < n$ możliwości

bo b/K nierozdzielczy

Lemat 6.7

Przy ustalonym $f(b)$ jest $\leq m$ możliwości na $f(a)$

bo: $\deg(a/K(b)) = m. = \deg(f(a)/K(f(b)))$.

razem: $\leq k \times m < n \times m$ ↯.

---

(2) Podobny dowód.

Rozszerzenia radykalne (czysto nierozdzielcze)

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

<u>Def.</u> (1) $a \in L$ czysto nierozdzielczy (radykalny) $/K$,

gdy $W_a(X) \in K[X]$ ma tylko jeden pierwiastek w $\hat{K}$.
wiel. minimalny a/K

Def. (2) $K \subseteq L$ radykalne (czysto nierozdzielcze), gdy:
$\forall a \in L$ a/K radykalny.

Uwaga 7.1. (1) char $K=0 \Rightarrow$ [a/K czysto nierozdzielczy $\Leftrightarrow a \in K$]

(2) a/K radykalny $\Leftrightarrow \forall f \in G(\hat{K}/K)\ f(a)=a$

(3) char $K=p \Rightarrow$ (a/K radykalny $\Leftrightarrow \exists n \geq 0\ a^{p^n} \in K$).

D-d (1) $W_a(X)$ ma tylko pierwiastki jednokrotne, gdy char $K=0$.

(2) Oczywiste.

(3) $\Leftarrow$ Oczywiste. Lub: $W_a(X) \in K[X]$ dzieli $X^{p^n} - a^{p^n} = (X-a)^{p^n} \in K[X]$.

$\Rightarrow$. $\deg(a/K)=n$, indukcja względem n

$$W_a(X) = (X-a)^n \qquad W_a'(X) = n \cdot (X-a)^{n-1}$$

$W_a(X) \in \hat{K}[X]$, $W_a'(X) \in K[X]$, $n \cdot (X-a)^{n-1} \in I(a/K)$ gdy $n > 1$

Jeśli $n>1$, to $W_a'(X)=0$, więc $p \mid n$.

$n = p \cdot n_1 \qquad W_a(X) = (X^p - a^p)^{n_1}$

i a^p: radykalny$/K$. $\deg(a^p/K) \leq n_1 < n$ | Z zał. indukc. $\exists k \geq 0\ (a^p)^{p^k} = a^{p^{k+1}} \in K$.