Wykład 8.

Def. Zał., że $K \subset L$: skończone Galois.
Wtedy rozszerzenie $K \subset L$ jest abelowe [cykliczne],
gdy $G(L/K)$ jest abelowa [cykliczna].

TW. 9.3. Zał., że $K \subset L_1 \subset L$: rozszerzenia ciał.
Jeśli $K \subset L$: abelowe [cykliczne], to
$K \subset L_1$ i $L_1 \subset L$: też.

<u>D-d</u>. $G(L/L_1) \triangleleft G(L/K) \Rightarrow$

$\cancel{K \subset L}$ $K \subset L_1$ i $L_1 \subset L$: Galois i

$$G(L_1/K) \cong G(L/K) / G(L/L_1)$$

Dlatego $G(L/L_1)$ i $G(L_1/K)$: abelowe [cykliczne]

<u>Przykład</u> (1) $K \subset \hat{K}$, $\zeta \in \hat{K}$ pierwiastek pierwotny stopnia $n \geq 1$.

$$G(K(\zeta)/K) \hookrightarrow \mathbb{Z}_n^*$$
$$f \longmapsto l_f \text{ t. że } f(\zeta) = \zeta^{l_f},\ 0 < l_f < n.$$

Gdy char $= 0$, to jest $\cong$
Gdy char $= p$: niekoniecznie, ale: $K(\zeta) \supset K$ abelowe

(2) $p = \mathrm{char}\, K$, $(p \geq 0)$ $p \nmid n$, $a \in K$, $\sqrt[n]{a} \notin K$.

Zał, że $\zeta \in K$ pierwiastek pierwotny z 1 stopnia n.

Wtedy $L := K(\sqrt[n]{a}) \supseteq K$: Galois.

$W_{\sqrt[n]{a}}(X) = X^n - a$ (nie twierdzę, że nierozkładalny).

pierwiastki $W_{\sqrt[n]{a}}(X)$ w L: $\zeta^i \sqrt[n]{a}$: $i = 0, \dots, n-1$

$G(L/K) \ni f$ wyznaczony przez $f(\sqrt[n]{a}) = \zeta^{l_f} \sqrt[n]{a}$, $0 \leq l_f < n$

$$\begin{aligned} G(L/K) &\hookrightarrow \mathbb{Z}_n^+ \\ f &\longmapsto l_f \end{aligned}$$ monomorfizm, bo:

$f, g \in G(L/K)$, $f \mapsto l_f$, $g \mapsto l_g$

$(g \circ f)(\sqrt[n]{a}) = g(\zeta^{l_f} \sqrt[n]{a}) \underset{f|_K = id_K}{=} \zeta^{l_f} g(\sqrt[n]{a}) = \zeta^{l_f} \zeta^{l_g} \sqrt[n]{a} = \zeta^{l_f +_n l_g} \sqrt[n]{a}$

więc $l_{g \circ f} = l_g +_n l_f$.

Dlatego $G(L/K)$ cykliczna.

TW. 9.4. Zał, że $K \subset L$: cykliczne, $[L:K]=n$, $\zeta \in K$: pierwiastek pierwotny z 1 stopnia n (więc $p \nmid n$, gdy char $K = p$)

Wtedy $\exists a \in K \quad L = K(\sqrt[n]{a})$

D-d. Niech $\gamma \in G(L/K)$ generator (rzędu n).

Dla $b \in L$ niech $c(b) = \underbrace{b}_{=\gamma^0(b)} + \zeta\gamma(b) + \dots + \zeta^{n-1}\gamma^{n-1}(b)$.

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

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

~~Gd~~ $\boxed{\text{Jeśli } c(b) \neq 0}$, to $\{\gamma^0(c(b)), \gamma(c(b)), \dots, \gamma^{n-1}c(b)\}$ n - elementowy

pierwiastki wielomianu $W_{c(b)}(X) \in K[X]$

$$\Downarrow$$

$$\underset{\subseteq L}{[K(c(b)):K]} \geq n \Rightarrow K(c(b)) = L.$$

$\boxed{\text{założenie ad hoc}}$

$c(b)^n \in K$, 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 $i = 0, \dots, n-1$.

Dlatego $c(b) = \sqrt[n]{a}$ dla $a = c(b)^n \in K$ i

$L = K(\sqrt[n]{a})$.

Pod warunkiem, że $c(b) \neq 0$. Ale

Istnieje $b \in L$ t. że $c(b) \neq 0$, bo:

TW. 9.5 (Dedekinda, o liniowej niezależności charakterów)

Zał, że $\alpha_1, \dots, \alpha_n \in Aut(L)$, różne $\underbrace{a_1, \dots, a_n}_{\neq (0, \dots, 0)} \in L$

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

[tzn: $\alpha_1, \dots, \alpha_n$ są liniowo niezależne w przestrzeni L^L nad L]

<u>D-d</u>. Indukcja względem n.

$n = 1$: Oczywiste. $c = 1$: $a_1 \alpha_1(1) = a_1 \neq 0$.

<u>Krok indukcyjny</u> $n \mapsto n+1$.

Nie wprost: Zał, że $\forall x \in L \ \sum^{n+1} a_i \alpha_i(x) = 0$

niech $a \in L$ dowolne $\neq 0$

$$\Rightarrow \forall x \in L \ \sum^{n+1} a_i \alpha_i(ax) = 0$$

$$\sum^{n+1} (a_i \alpha_i(a)) \alpha_i(x) = 0 \ / \cdot \alpha_{n+1}(a)^{-1}$$

$$\forall x \in L \ \sum_{i=1}^{n+1} a_i \alpha_i(a) \alpha_{n+1}(a)^{-1} \alpha_i(x) = 0$$

$$\Downarrow \quad \sum^{n+1} a_i \alpha_i(x) = 0$$

$$\forall x \in L \quad \sum_{i=1}^{n+1} \Big(\underbrace{a_i - a_i \alpha_i(a) \alpha_{n+1}(a)^{-1}}_{=0,\ \text{gdy}\ i=n+1} \Big) \cdot \alpha_i(x) = 0$$

$$\Downarrow$$

$$\sum_{i=1}^{n} \left(a_i - a_i \alpha_i(a) \alpha_{n+1}(a)^{-1} \right) \alpha_i(x) = 0$$

$\Downarrow$ zał. ind.

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

Czyli: $\alpha_i(a) = \alpha_{n+1}(a)$ gdy $a_i \neq 0$.

$$\Downarrow$$

$$\forall a \in L,\ a \neq 0 \quad \alpha_i(a) = \alpha_{n+1}(a)$$

$$\Downarrow$$

$$\alpha_i = \alpha_n \quad \lightning$$

Def. Zał., że $K \subset L$: skończone rozszerzenie ciał.

(1) $K \subset L$: rozszerzenie <u>rozwiązalne</u>, gdy $K \subset L$: Galois i $G(L/K)$ rozwiązalna.

(2) $K \subset L$: rozszerzenie ciał przez pierwiastniki, gdy [radicals]

$\exists k\ \exists\ L_0 \supset L_1 \supset \dots \supset L_i \supset L_{i+1} \supset \dots \supset L_k = K$, $L_0 \supseteq L$, $\forall i < k$

L_i: ciało rozkładu wielomianu $X^{n_i} - b_i \in L_{i+1}$ nad L_{i+1} ($p \nmid n_i$ gdy char $K = p$)

lub

wielomianu $\underline{X^p - X - b_i}$ $(p = \mathrm{char}\, K)$ nad L_{i+1}.

$b_i \in L_{i+1}$

TW. 9.6. Zał, że $K \subset L$: rozszerzenie skończone ciał.

Wtedy $K \subset L$: rozszerzenie przez pierwiastniki $\iff$

$\exists\, L' \supset K$, $L \subset L'$

rozwiązalne.

ćwiczenie

D-d. $\Rightarrow$ we may assume $K \subseteq L_0$: Galois (by extending the sequence) then:

ciąg normalny grup.

(*) $G(L_0/L_k) \rhd G(L_0/L_{k-1}) \rhd \ldots \rhd G(L_0/L_1) \rhd \{e\}$.

faktory tego ciągu: $G(L_i/L_{i+1})$.

Wystarczy pokazać, że $L_i \supset L_{i+1}$: rozwiązalne.

[wtedy można rozdrobnić ciąg (*) by miał faktory abelowe]

alternatywnie:

Ćw. $H \lhd G$, H rozwiązalna i G/H rozwiązalna $\Rightarrow$ G rozwiązalna]

Przypadek (a) ; $X^{n_i} - b_i^{\in L_{i+1}}$. Niech $a_i = \sqrt[n_i]{b_i} \in L_i$

$(p \nmid n_i)$

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

$\uparrow$

pierwiastek pierwotny z 1 stopnia n_i.

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

$L_i \supset L_{i+1}$: Galois, $\Rightarrow$ Galois & $G(\overbrace{L_{i+1}(\zeta_{n_i}, a_i)}^{L_i}/L_{i+1}(\zeta_{n_i}))$

bo "$X^{n_i} - b_i$" rozdzielony

przykład (b) $\cong$ $\mathbb{Z}_{n_i}^{+}$ cykliczna $\Downarrow$ abelowa

również $L_{i+1} \subset L_{i+1}(\zeta_{n_i})$: Galois

& $G(L_{i+1}(\zeta_{n_i})/L_{i+1}) \hookrightarrow \mathbb{Z}_{n_i}^{*}$

abelowa

Stąd: $G(L_i/L_{i+1}) \rhd G(L_i/L_{i+1}(\zeta_{n_i})) \rhd \{e\}$

faktor $\cong G(L_{i+1}(\zeta_{n_i})/L_{i+1})$ abelowy

więc $G(L_i/L_{i+1})$: rozwiązalna stopnia ≤ 2.

Przypadek (b): $X^p - X - b_i$, $p = \mathrm{char}\, K$.

$b_i \in L_{i+1}$

Niech $L_i \ni a$ pierwiastek.

Wtedy $a+1$: też pierwiastek (bo: $(a+1)^p - (a+1) - b_i =$
$= a^p + 1^p - a - 1 - b_i =$
$= a^p - a - b_i = 0$)

Dlatego $a, a+1, \dots, a+(p-1) \in L_i$ wszystkie pierwiastki $X^p - X - b_i$

Stąd $L_i = L_{i+1}(a)$

$G(L_i/L_{i+1}) \ni f$ wyznaczony przez $f(a) = a + l_f$

$$G(L_i/L_{i+1}) \ni f \longmapsto l_f \in \mathbb{Z}_p^+$$

daje $G(L_i/L_{i+1}) \hookrightarrow \mathbb{Z}_p^+$

(wistocie $\cong$)

wnsc $L_i \supset L_{i+1}$: cykliczne $\Rightarrow$ rozwiązalne.

$\Leftarrow$: Niech $K \subset L$: rozwiązalne. Pdk, że jest pierwiastnikowe.

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

ciąg normalny podgrup o faktorach abelowych

bso: cykliczne, proste.

tzn. $\cong \mathbb{Z}_q$, q: l. pierwsze

wtedy:

$$\begin{array}{ccccccccc} L = L^{G_0} & \supset & L^{G_1} & \supset \dots \supset & L^{G_{k-1}} & \supset & K \\ \shortparallel & & \shortparallel & & \shortparallel & & \shortparallel \\ L_0 & \supset & L_1 & \supset \dots \supset & L_{k-1} & \supset & L_k \end{array}$$

: ciąg rozszerzeń cyklicznych, prostych.

Wystarczy pokazać

Claim. Jeśli $K \underset{\text{cykliczne}}{\subset} L \subset \hat{K}$ i $G(L/K)$: prosta,

to $K \subset L$: pierwiastnikowe.

D-d. $[L:K]=n$, $G(L/K) \cong \mathbb{Z}_n^+$, n: l. pierwsza,

Przypadek (a) $\underset{\text{char } K}{p} \neq n$ lub $\operatorname{char} K = 0$.

Niech $\zeta \in \hat{K}$ pierwiastek pierwotny z 1, stopnia n

$$K \subset K(\zeta) \underset{\text{Galois}}{\subset} L(\zeta), \quad \underbrace{[L(\zeta):K(\zeta)]}_{m} \,\Big|\, [L:K]$$

(bo: $G(L(\zeta)/K(\zeta)) \hookrightarrow G(L/K) \cong \mathbb{Z}_n^+$ prosta,)

więc nawet: $m=1$ lub $m=n$

z tw. 9.4: $L(\zeta) = K(\zeta)(\sqrt[n]{a})$ dla pewnego $a \in K(\zeta)$
(gdy $m=n$.)

Gdy $m=1$: trywialne.

Przypadek (b): $\underset{\text{char}\,K}{\underset{\parallel}{p}} = n$.

Niech $\gamma \in G(L/K)$ generator.

$$K \ni \underset{t}{\underset{\parallel}{\mathrm{Tr}_{L/K}(b)}} = \sum_{i=0}^{p-1} \gamma^i(b) \neq 0$$ dla pewnego $b \in L$ (tw. Dedekinda o charakterach, 9.5)

Dla $b' = \frac{1}{t} b$, $\mathrm{Tr}_{L/K}(b') = 1$.

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

Wtedy $\gamma(a) = \gamma^2(b') + 2\gamma^3(b') + \dots + (p-1)\underbrace{\gamma^p(b')}_{= b'} =$

$= a - \mathrm{Tr}_{L/K}(b') = a - 1$

więc $\gamma(a) \neq a$ oraz $a \notin K$.

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

więc $a^p - a \in Fix(\gamma) = K$. Niech $c = a^p - a$

Stąd: a: pierwiastek $X^p - X - c$

oraz L: ciało rozkładu $X^p - X - c$ nad K,

więc $K \subset L$: pierwiastnikowe.