

▣ (Charakteryzacja rozszerzeń normalnych) Jeśli $K \subseteq L \subseteq \text{alg}(K)$, to następujące warunki równoważne:

- (i) L jest rozszerzeniem normalnym K ;
- (ii) jeśli $\varphi : L \rightarrow \text{alg}(K)$ jest K -monomorfizmem, to $\varphi(L) = L$;
- (iii) jeśli $f(x) \in K[x]$ nierozkładalny i ma pierwiastek w L , to ma wszystkie pierwiastki w L (rozkład liniowy).

Dowód:

- (i) $\implies$ (ii) UW: Przy homomorfizmie, pierwiastki danego wielomianu przechodzą na pierwiastki tego wielomianu.

(ii) $\implies$ (iii) $\blacksquare$ $K \subseteq L$ algebraiczne, $a, b \in L$ pierwiastki wielomianu $f(x)$ nierozkładalnego w $K[x]$.
Wówczas istnieje K -izomorfizm $\phi : K(a) \rightarrow K(b)$, taki że $\phi(a) = b$ i da się rozszerzyć na L .

(ii) $\implies$ (iii)

$\blacksquare$ WŁASNOŚCI:

1. Każde rozszerzenie algebraiczne zawarte w normalnym
2. $\bigcap$ normalnych – normalne
3. istn. najmniejsze normalne rozszerzenie dowolnego $L \supset K$ – domknięcie normalne ($\bigcap$)
4. złożenie normalnych – normalne (podkrata)

■ Automorfizmy ciała L tworzą grupę $Aut(L)$.

■ Niech $L \supseteq K$. Wtedy K -automorfizmy L (= stabilizujące każdy element K) tworzą podgrupę $Aut(L)$ oznaczaną $G(L/K)$ lub $Gal(L/K)$ zwaną grupą Galois rozszerzenia $L \supseteq K$.

■ Odwrotnie: dla $G \leq Aut(L)$, zbiór $L^G = \{a \in L : \forall \varphi \in G (\varphi(a) = a)\}$ elementów stałych dla G jest podciałem L .

Twierdzenia o rzędach grup i stopniach rozszerzeń

(1) ■ Jeśli $G \leq Aut(L)$, to $|G| = [L : L^G]$. $\left(\begin{array}{l} L \text{ normalne} \end{array} \right)$

(2) ■ Jeśli $L \supseteq K$ jest normalne, to $|G(L/K)| = [L : K]$. ($\text{char}(K) = 0$)

Tw. o istn. el. pierwotnego wzniesienia: Dla $a, b \in L/K \exists c :$
 $K(a, b) = K(c)$ $\Rightarrow$ ZAD
 $\Rightarrow$ WN. Każde wzniesienie skończone $[L : K] < \infty$, jest pojedyncze $= \overline{K(c)}$
 $\uparrow$
 el. pierwotny

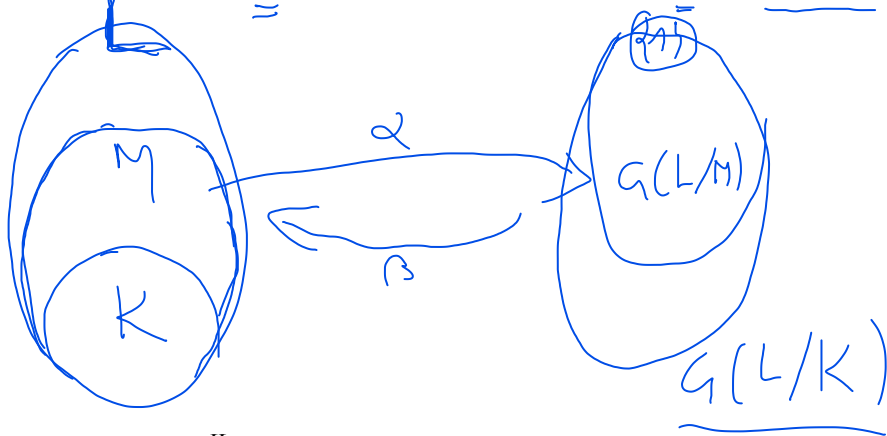
(1). $L = L^G(c)$, $c - n = \text{stop. } m_c(x) = [L : L^G]$
 z drug. strony c przedstawi na pierwiastku $m_c(x)$ w każdym aut. $\rightarrow$ to wyznacza automorfizm
 $\begin{array}{c} L \\ \uparrow \\ L^G \end{array} \xrightarrow{c \mapsto a, b} \in \text{określ. stab. gr } G$ — takich aut. jest dokładnie $n = |G|$

(2) $L = K(c)$ ~~A ten sam argument.~~ ???

Główne twierdzenia teorii Galois

(w przypadku rozszerzeń skończonych i $\text{char}(K) = 0$)

■ Dla rozszerzenia normalnego $L \supseteq K$ istnieje $\frac{1-1}{na}$ odpowiedniość pomiędzy podciałami $L \supseteq M \supseteq K$ oraz podgrupami $\{1\} \leq H \leq G(L/K)$ dana funkcją $\alpha : M \rightarrow G(L/M)$;

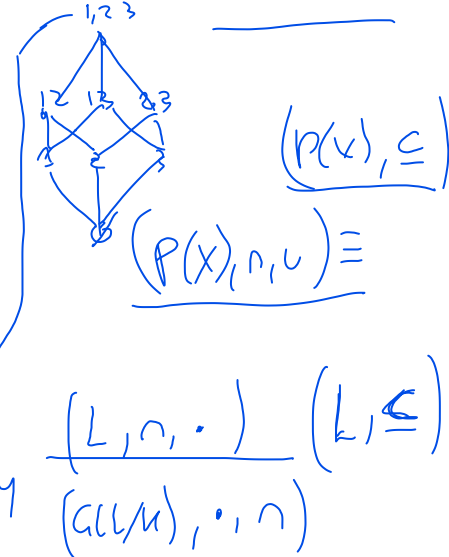


funkcja $\beta : H \rightarrow L^H$ jest odwrotna do α ;

→ ponadto $M_1 \supseteq M_2 \iff G(L/M_1) \subseteq G(L/M_2)$ (antyizomorfizm).

Skoro L/K jest normalne, to każde L/M też, natomiast:

■ M/K jest normalne $\iff G(L/M) \triangleleft G(L/K)$. (stąd ta sama nazwa!)



$$\begin{aligned} \alpha(M_1 \cap M_2) &= \alpha(M_1) \cap \alpha(M_2) \\ \alpha(M_1 M_2) &= \alpha(M_1) \alpha(M_2) \end{aligned}$$

D-d: α, β wzajemnie odwrotne

$$\textcircled{1} \quad L^{G(L/M)} \supseteq M \quad \text{oryginalnie} \quad \left| \begin{aligned} &\subseteq \text{Zł. } a \in L/M \\ &\text{wz. wz. ma } \text{rk} > 1, \exists b \end{aligned} \right.$$

$$L^{G(L/M)} = M$$

$$\textcircled{2} \quad G(L/L^H) \cong H \quad \text{oryginalnie}$$

automorfizmy które
fixują L^H

$$G(L/L^H) = H$$

$$\begin{aligned} &\subseteq \\ |G(L/L^H)| &= \\ &= [L : L^H] = |H| \end{aligned}$$

PRZYKŁAD: $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

$$\Rightarrow M/K \text{ normalne} \Rightarrow G(L/M) \triangleleft G(L/K)$$

$$\varphi \in G(L/K) \quad \varphi|_M : M \rightarrow \text{alg}(M)$$



$$\xrightarrow{\uparrow +w} \Rightarrow \varphi|_M = \text{id}$$

$$\zeta : G(L/K) \rightarrow G(M/K) \quad \varphi \mapsto \varphi|_M$$

— homomorfizm

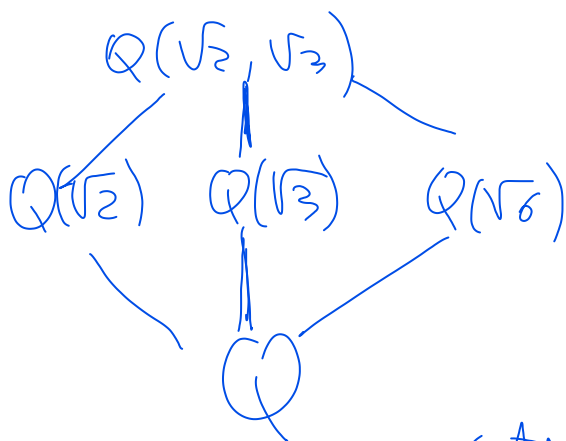
$$\psi \in \text{Ker } \zeta \Leftrightarrow \zeta(\psi) = \text{id} \Leftrightarrow \psi|_M = \text{id} \Leftrightarrow \psi \in G(L/M)$$

$\text{Ker } \zeta = G(L/M)$ jest podgrupą normalną i co więcej

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

DODATKOWY
FAKT

$L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ — jakie podgrupy



$$G(L/\mathbb{Q}) \quad x^2=2 \quad x^2=3$$

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}):\mathbb{Q}]$$

4 2 2

baza $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$

automorfizmy — wyznaczone przez
obrazy $\sqrt{2}, \sqrt{3}$

$$x^2=2$$

$$\sqrt{2} \rightarrow \pm\sqrt{2}$$

$$x^2=3$$

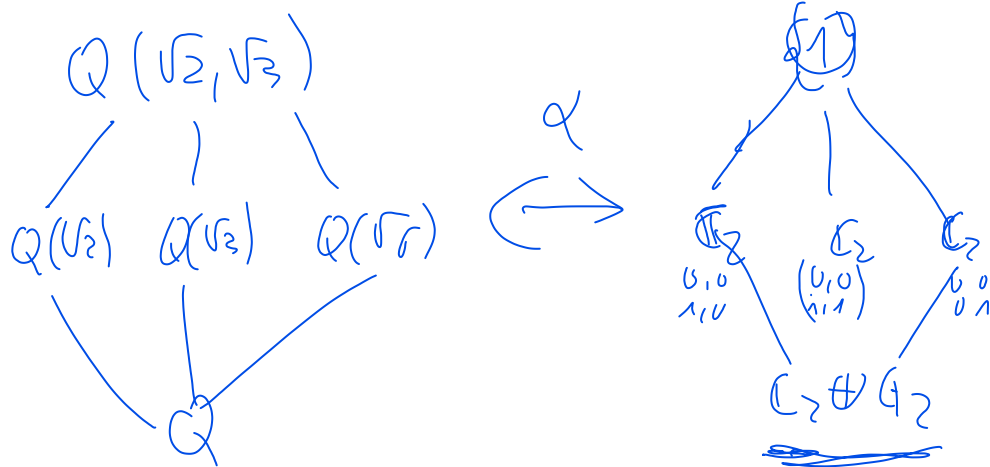
$$\sqrt{3} \rightarrow \pm\sqrt{3}$$

4 możliwości

permutacje

$$\begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ -\sqrt{2} & \sqrt{2} & -\sqrt{3} & \sqrt{3} \end{pmatrix}$$

$$\underline{C_2 \oplus C_2}$$



$$\alpha(\mathbb{Q}(\sqrt{2})) \rightarrow \{id, (\sqrt{3}, -\sqrt{3})\}$$

triv.

$$\mathbb{Q}(\sqrt{6}) \rightarrow \{id, (\sqrt{3}, \sqrt{3})(\sqrt{2}, -\sqrt{2})\}$$

Zad

Grupa Galois wielomianu

$$G_{\mathbb{Q}}((x^2-2)(x^2-3))$$

$\uparrow$
 $\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3}$

DEF. Grupa Galois wielomianu $f \in K[x]$ stopnia ≥ 1 ^{to} $G_K(f) = G(L/K)$, gdzie $L = K(a_1, \dots, a_n)$ ciało rozkładu f .

Grupa Galois wielomianu f wyznaczone przez permutacje $a_1, \dots, a_n$ utożsamiamy z $G \leq S_n$.

TEORIA GRUP (cd)

DEF. G nazywamy grupą rozwiązalną jeśli istnieje ciąg podgrup normalnych

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_n = \{1\}$$

taki że każda grupa ilorazowa G_{i+1}/G_i jest abelowa (wieża abelowa podgrup).

$$G_i \trianglelefteq G_{i+1}$$

$$\begin{array}{l} G_0 \supseteq G_1 \supseteq \dots \\ \textcircled{1} G_{i+1} \trianglelefteq G_i \\ \textcircled{2} G_i / G_{i+1} \text{ jest abelowa} \end{array}$$

Każda grupa abelowa jest rozwiązalna ($G \triangleright \{1\}$)

Każda podgrupa grupy rozwiązalnej jest rozwiązalna.

Dowód:

$$H \subseteq G, \text{ wieża abelowa}, G \cap H \supseteq G_1 \cap H \supseteq \dots \supseteq G_n \cap H \cong \{1\}$$

$$\textcircled{1} G_{i+1} \cap H \trianglelefteq G_i \cap H \quad (?)$$

$$x \cdot (G_{i+1} \cap H) \cdot x^{-1} = \underbrace{x G_{i+1} x^{-1}}_{G_{i+1}} \cap \underbrace{x H x^{-1}}_{H} \subseteq G_{i+1} \cap H \quad \square$$

$$x \in G_i \cap H$$

$$\textcircled{2} (G_i \cap H) / (G_{i+1} \cap H) \text{ abelowa?} \quad xy(G_{i+1} \cap H) = yx(G_{i+1} \cap H)$$

$$xy \in G_i \cap H \quad = \quad xy G_{i+1} \cap xy H = yx G_{i+1} \cap yx H = yx G_{i+1} \cap yx H = !$$

Spośród wielu faktów potrzebne nam będą jeszcze dwa:

$\Downarrow$
 $\Rightarrow S_5$ też nie jest rozwiązalna.

■ A_5 nie jest rozwiązalna (bo jest prosta nieabelowa)

■ Niech $G \triangleright H$. Jeśli H i G/H rozwiązalne, to G też rozwiązalna.

$$\begin{array}{l} \text{Dł.} \\ \text{km.} \end{array} \quad \varphi: G \rightarrow G/H \quad \parallel \quad \begin{array}{l} H \triangleright H_1 \triangleright \dots \triangleright H_n = \langle 1 \rangle \\ G/H = F_0 \triangleright F_1 \triangleright \dots \triangleright F_m = \langle 1 \rangle \end{array}$$

$$G = \varphi^{-1}(G/H) \triangleright \varphi^{-1}(F_1) \triangleright \dots \triangleright \varphi^{-1}(F_m) = H \triangleright H_1 \triangleright \dots \triangleright \langle 1 \rangle$$

rekursywnie

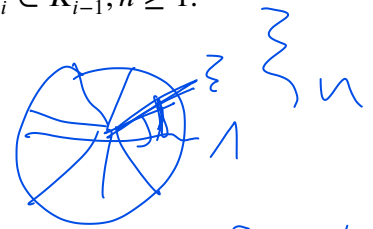
Prypomnijmy:

$$\underline{\text{char } K = 0}$$

DEF. $a \in \text{alg}(K)$ jest **pierwiastnikowy** nad K (wyrażalny przez pierwiastniki), jeśli istnieje ciąg $K = K_0 \subset K_1 \subset \dots \subset K_r \ni a$, taki że $K_i = K_{i-1}(x^n - a_i)$ – ciało rozkładu wielomianu, $a_i \in K_{i-1}, n \geq 1$.

(Dla $\text{char}(K) = 0$!!!) ciało $r(K)$

■ $G_K(x^n - a)$ jest rozwiązalna dla $a \in K$



LEM1: $G_K(x^n - 1)$ jest abelowa

$$\varphi \varphi(\zeta) = \varphi(\zeta^r) = (\zeta^r)^s = \zeta^{rs} = \varphi \varphi(\zeta)$$

$$= K(\zeta_n) \quad \zeta_n^r \quad \varphi: \zeta_n \rightarrow \zeta_n^r$$

$$\varphi: \zeta_n \rightarrow \zeta_n^s$$

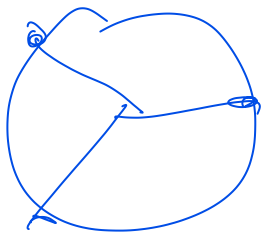
LEM2: $G_K(x^n - a)$ jest abelowa, jeśli $\zeta_n, a \in K$.

$$b^n = a \quad b, \zeta_n^r b \quad r = 0, \dots, n-1$$

$$\varphi: b \rightarrow \zeta_n^r b$$

$$\varphi: b \rightarrow \zeta_n^s b$$

argument taki sam



PRZYKŁAD: $G_Q(x^3 - 2)$

$$\sqrt[3]{2}, \sqrt[3]{2}, \sqrt[3]{2} \quad \sqrt[3]{2}^3 = 1$$

$$L = \mathbb{Q}(x^3 - 2) = \mathbb{Q}(\sqrt[3]{2}, \zeta) = (\underbrace{\mathbb{Q}(\zeta)}) (\sqrt[3]{2})$$

$$[L : \mathbb{Q}] = \underline{\underline{6}} \quad \frac{x^3 - 1}{x - 1} = \underline{\underline{x^2 + x + 1}}$$

$$\frac{x^{3.1}}{x-1} = \underline{\underline{x^2 + x + 1}}$$

st. 2

$x^{3.2}$

st. 3

ant. w/2 name jms $\varphi \left(\sqrt[3]{2} \right)$

$\sqrt[3]{2} \rightarrow \sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$

$\omega \rightarrow \omega, \omega^2$

$=6$

$$\rightarrow \left(\begin{pmatrix} \sqrt[3]{2} \\ \psi(\sqrt[3]{2}) \end{pmatrix}, \begin{pmatrix} \sqrt[3]{2} \\ \psi(\sqrt[3]{2}) \end{pmatrix}, \begin{pmatrix} \sqrt[3]{2} \\ \psi(\sqrt[3]{2}) \end{pmatrix} \right) \leftarrow \text{wird.}$$

$$G(L/Q) \cong S_3$$

~~Bazın $L/\mathbb{Q}$: $1, \sqrt[3]{2}, \zeta, \zeta\sqrt[3]{2}, \zeta^2, \zeta^2\sqrt[3]{2}$~~

$1, \sqrt[3]{2}, \sqrt[3]{4}, \zeta, \zeta\sqrt[3]{2}, \zeta\sqrt[3]{4}$

~~$\times$~~

$$\frac{\text{el. pr. } Q(\zeta + \sqrt[3]{2})}{\text{wrt. min}} \quad \triangleright \quad \frac{Q(\zeta, \sqrt[3]{2})}{(a+b\zeta)(1+\sqrt[3]{2})} = \frac{x^6 + 3x^5 + 6x^4 - 3x^3 + 9x + 9}{2??}$$

■ Niech $[L : K] < \infty$ i p będzie największym dzielnikiem pierwszym $p \mid [L : K]$. Wtedy następujące warunki są równoważne:

(i) $L \subseteq r_p(K)$,

(ii) $L \subseteq r(K)$,

(iii) $G(L/K)$ jest rozwiązalna.

WNIOSEK: Dla $f \in K[x]$, jeśli $G_K(f)$ nie jest rozwiązalna, to pierwiastki równania $f(x) = 0$ nie dadzą się wyrazić wzorami przy pomocy działań arytmetycznych i pierwiastników stopnia n .

Do (ii) $\Rightarrow$ (iii) szkielet

$$\left\{ \begin{array}{l} L \subseteq r(K) \\ K \subseteq K_1 \subseteq \dots \subseteq K_r \\ \quad \quad \quad L \subseteq \end{array} \right\} \quad x^n - a$$

Wystarczy domniemyć indukcyjne, że $G(K_r/K)$ jest rozwiązalne

$r=1$

WNIOSEK $G(x^n - a)$ jest rozwiązalna

$$K \subseteq_{\text{norm}} M \subseteq_{\text{norm}} L \quad \text{normalna}$$

$$G(L/K) \triangleright G(L/M) \triangleright \dots$$

$$\frac{G(L/K)}{G(L/M)} \cong G(M/K) - \text{abel} \Rightarrow G(L/K) \text{ normalna}$$

$$r > 1 \quad K \subseteq_{\text{norm}} K_1 \quad K_1 \subseteq \dots \subseteq K_r \quad G(K_r/K_1) \text{ normalna}$$

$$K \subseteq K_1 \subseteq K \subseteq \sqrt{}$$

$$G(K_r/K) \cong G(K_r/K_1)$$

■ Jeśli $f \in \mathbb{Q}[x]$ nierozkładalny stopnia p pierwszego i f ma dokładnie $p-2$ pierwiastków rzeczywistych, to $G(f) \cong S_p$. (nierozwiązalna dla $p \geq 5$)

$\frac{p-1}{p=5}$ pierw. z_1, z_2, r_1, r_2, r_3
 $\begin{matrix} \in \mathbb{R} \\ a+bi & a-bi & - & - & - \end{matrix}$

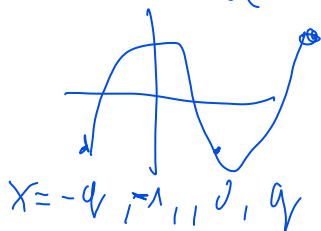
z_1
 $\varphi: a+bi \rightarrow a-bi$
 jest automorf.

ten automorfizm odp. transpozycja (z_1, z_2)

z dróg i w rham $p = [Q(z_1):Q]$ dzieli $[Q(f):Q]$
 $p \mid |G(f)| \leq S_p \Rightarrow$ zsum cych p -pierw. $= |G(f)|$
~~+ transp. $\Rightarrow$ jest S_p~~

WNIOSEK 1: $x^5 - 2qx - q$, gdzie q - liczba pierwsza, jest nierozwiązalny przez pierwiastniki.

$G(f) \cong S_5 \not\subseteq A_5$, niemoż. Kryt. Eisen. S_p



$$f' = 5x^4 - 2q \rightarrow \text{dwa pierwiastki}$$

WNIOSEK 2: Istnieją liczby algebraiczne nie należące do $r(\mathbb{Q})$.

$$x^5 - x - 1$$

Wszystkie pierwiastki $x^5 - 2qx - q \notin r(\mathbb{Q})$

gdyby $a \in r(\mathbb{Q}) \rightarrow$ rozkład w $r(\mathbb{Q})$

WNIOSEK 3: „Wzory” na rozwiązywanie równań $f(x) = 0$ dla $\deg f = 5$ nie istnieją.

Ogólniej: TWIERDZENIE RUFFINIEGO-ABELA

▣ $L = K(a_1, \dots, a_n)$, $a_1, \dots, a_n$ - algebraicznie niezależne nad K , $f(x) = x^n + a_1x^{n-1} + \dots + a_n \in K[x]$,
to $G_K(f) \cong S_n$.

WNIOSEK: Równanie $f(x) = 0$ dla wielomianu $f \in \mathbb{Q}[x]$ jest rozwiązalne w pierwiastnikach $\iff n \leq 4$.

$$K \subseteq K_1 \subseteq K_r$$

$$\underline{G(K_r/K)} \triangleright \underline{G(K_r/K_1)} \triangleright d_1$$

$$\frac{G(K_r/K)}{G(K_r/K_1)} \cong \frac{G(K_1/K)}{\text{row.}}$$

$$\text{TW, } \frac{G \triangleright M}{\text{row}} \quad \frac{G/M}{\text{row}} \Rightarrow G \text{ row.}$$