LEMAT 4. Jeśli $f \in \mathbb{Q}[x]$ jest wielomianem nierozkładalnym to grupa Galois $Gal(\mathbb{Q}_f/\mathbb{Q})$ działa tranzytywnie na pierwiastkach wielomianu $f$.

Dowód (SZKIC): niech $a, b$ – dowolne dwa różne pierwiastki wielomianu $f$. Mamy pokazać, że istnieje automorfizm $\varphi \in Gal(\mathbb{Q}_f/\mathbb{Q}) = Aut(\mathbb{Q}_f)$ taki, że $\varphi(a) = b$.

Automorfizm $\varphi$ będziemy konstruować indukcyjnie.

Krok 1 Najpierw opiszemy izomorfizm $\varphi_1 : \mathbb{Q}(a) \to \mathbb{Q}(b)$ o tej własności, że $\varphi_1(a) = b$.

Niech $n$ będzie stopniem wielomianu $f$.

Ponieważ zarówno $a$ jak i $b$ są pierwiastkami $f$, ciała $\mathbb{Q}(a)$ i $\mathbb{Q}(b)$ mają podobny opis:

$$(*)\quad \begin{aligned} \mathbb{Q}(a) &= \{\alpha_{n-1} a^{n-1} + \alpha_{n-2} a^{n-2} + \ldots + \alpha_1 a + \alpha_0 : \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Q}\} \\ \mathbb{Q}(b) &= \{\alpha_{n-1} b^{n-1} + \alpha_{n-2} b^{n-2} + \ldots + \alpha_1 b + \alpha_0 : \alpha_0, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{Q}\}. \end{aligned}$$

Możemy wtedy określić:

$$\varphi_1(\alpha_{n-1} a^{n-1} + \ldots + \alpha_1 a + \alpha_0) = \alpha_{n-1} b^{n-1} + \ldots + \alpha_1 b + \alpha_0$$

lub w skrócie, $\varphi_1(v(a)) = v(b)$ dla dowolnego wielomianu $v \in \mathbb{Q}[x]$ stopnia $\leq n-1$.

Sprawdzenie, że $\varphi_1$ jest izomorfizmem ciał wymaga weryfikacji 3 warunków:

(1) $\varphi_1(x+y) = \varphi_1(x) + \varphi_1(y)$ – BARDZO ŁATWE Z OKREŚLENIA $\varphi_1$ – POMIJAMY

(2) $\varphi_1(x \cdot y) = \varphi_1(x) \cdot \varphi_1(y)$ – TRUDNIEJSZE – ZARAZ ZROBIMY

(3) $\varphi_1$ jest wzajemnie jednoznaczne – wynika z jednoznaczności form $(*)$ w ciałach $\mathbb{Q}(a)$ i $\mathbb{Q}(b)$.

SPRAWDZENIE, ŻE $\varphi_1(x\cdot y)=\varphi_1(x)\cdot\varphi_1(y)$.

Niech $x=\alpha_{n-1}a^{n-1}+\alpha_{n-2}a^{n-2}+\ldots+\alpha_1 a+\alpha_0=g(a)$

$y=\beta_{n-1}a^{n-1}+\beta_{n-2}a^{n-2}+\ldots+\beta_1 a+\beta_0=h(a)$

Rozważmy wielomian $g(x)\cdot h(x)$.

Dzieląc go przez $f(x)$ dostaniemy iloraz i resztę o współczynnikach wymiernych:

$$g(x)\cdot h(x)=f(x)\cdot \underset{\substack{\uparrow\\ \text{iloraz}}}{q(x)}+\underset{\substack{\uparrow\\ \text{reszta}}}{r(x)}$$

Wielomian $r(x)$, jako reszta, ma stopień mniejszy niż $f(x)$, czyli stopień co najwyżej $n-1$.

Obliczmy:

$$\varphi_1(x\cdot y)=\varphi_1(g(a)\cdot h(a))=\varphi_1(g\cdot h(a))=$$
$$=\varphi_1(\underbrace{f(a)}_{=0}\cdot q(a)+r(a))=\varphi_1(r(a))=r(b)$$

$$\varphi_1(x)\cdot\varphi_1(y)=\varphi_1(g(a))\cdot\varphi_1(h(a))=g(b)\cdot h(b)=$$
$$=g\cdot h(b)=\underbrace{f(b)}_{=0}\cdot q(b)+r(b)=r(b)$$

Stąd $\varphi_1(x\cdot y)=\varphi_1(x)\cdot\varphi_1(y)$. $\square$ Koniec dowodu Kroku 1.

Krok 2 (reprezentujący ogólny krok indukcyjny)

- Najpierw pokażę, że jeśli $Q(a) = Q_f$, to także $Q(b) = Q_f$, a wtedy $\varphi_1$ jest poszukiwanym automorfizmem $Q_f \to Q_f$ takim, że $\varphi(a) = b$.

Niech $a_1, \dots, a_n$ - wszystkie pierwiastki $f$ (wśród nich są $a$ i $b$).

Zachodzi: $Q(b) = \varphi_1(Q(a)) = \varphi_1[Q(a_1, \dots, a_n)] =$

$$= Q(\varphi_1(a_1), \dots, \varphi_1(a_n)) \underset{\substack{\uparrow \\ \text{bo } \varphi_1 \text{ permutuje wtedy} \\ \text{pierwiastki wielomianu } f}}{=} Q(a_1, \dots, a_n) = Q_f. \quad \square$$

- Jeśli jednak $Q(a) \neq Q_f = Q(a_1, \dots, a_n)$, to przynajmniej jeden pierwiastek wielomianu $f$ nie należy do $Q(a)$ (bo inaczej $Q(a_1, \dots, a_n) \subset Q(a) \subset Q(a_1, \dots, a_n)$, czyli jest równość).

Niech $c$ będzie takim pierwiastkiem $f$ nie należącym do $Q(a)$.

Dla dowolnego wielomianu $w \in Q(a)[x]$,

$$w(x) = \alpha_k x^k + \alpha_{k-1} x^{k-1} + \dots + \alpha_1 x + \alpha_0, \quad \alpha_i \in Q(a),$$

oznaczmy

$$w^{\varphi_1}(x) := \varphi_1(\alpha_k) x^k + \varphi_1(\alpha_{k-1}) x^{k-1} + \dots + \varphi_1(\alpha_1) \cdot x + \varphi_1(\alpha_0).$$

Jest to wielomian z $Q(b)[x]$ $\Big(\overset{\text{współczynniki}}{\varphi_1(\alpha_i)} \in Q(b)\Big)$.

Operacja $w \mapsto w^{\varphi_1}$ ma następujące własności:

1. $(w_1 \cdot w_2)^{\varphi_1} = w_1^{\varphi_1} \cdot w_2^{\varphi_1}$ dla dowolnych $w_1, w_2 \in Q(a)[x]$
2. jeśli $w \in Q[x] \subset Q(a)[x]$ to $w^{\varphi_1} = w$ (bo $\varphi_1(\alpha) = \alpha$ dla $\alpha \in Q$).
3. jeśli $w = \underset{\in Q(a)}{\alpha_0}$ jest wielomianem stopnia $0$, to $w^{\varphi_1} = \varphi_1(\alpha) \in Q(b)$.
4. $(w^{\varphi_1})^{\varphi_1^{-1}} = w$, gdzie $v \mapsto v^{\varphi_1^{-1}}$ jest podobną operacją z $Q(b)[x]$ do $Q(a)[x]$.

Niech $h$ będzie wielomianem minimalnym nad ciałem $Q(a)$ dla $c$.

WŁASNOŚCI:

(1) Ponieważ $f(c)=0$, $f$ jest krotnością $h$ nad ciałem $Q(a)$, tzn. $f(x)=h(x)\cdot g(x)$ dla pewnego $g\in Q(a)[x]$.

(2) wielomian $h^{\varphi_1}\in Q(b)[x]$ jest nierozkładalny, bo gdyby się rozkładał jako $h^{\varphi_1}=w\cdot v$ $w,v\in Q(b)[x]$, to mielibyśmy

$h=h^{\varphi_1\varphi_1^{-1}}=w^{\varphi_1^{-1}}\cdot v^{\varphi_1^{-1}}$, czyli $h$ byłby rozkładalny nad $Q(a)$, wbrew minimalności.

(3) dowolny pierwiastek wielomianu $h^{\varphi_1}$ jest pierwiastkiem $f$,

bo $f=f^{\varphi_1}=(h\cdot g)^{\varphi_1}=h^{\varphi_1}\cdot g^{\varphi_1}$

więc jeśli $h^{\varphi_1}(z)=0$ to również $f(z)=0$.

(4) dowolny pierwiastek $d$ wielomianu $h^{\varphi_1}$ nie należy do $Q(b)$, bo gdyby $d\in Q(b)$ to mielibyśmy:

$$0=\varphi_1^{-1}(0)=\varphi_1^{-1}(h^{\varphi_1}(d))=h^{\varphi_1\varphi_1^{-1}}(\varphi_1^{-1}(d))=h(\varphi_1^{-1}(d))$$

a to oznacza, że $h$ miałby pierwiastek w $Q(a)$, wbrew nierozkładalności nad $Q(a)$ (wynikającej z minimalności).

Opiszemy teraz izomorfizm $\varphi_2: Q(a)(c)\to Q(b)(d)$ będący rozszerzeniem izomorfizmu $\varphi_1$ takim, że $\varphi_2(c)=d$.

Jeśli stopień $c$ nad $Q(a)$ wynosi $k$, to każdy element $z\in Q(a)(c)$ ma jednoznacznie postać

$$z=\gamma_{k-1}c^{k-1}+\dots+\gamma_1 c+\gamma_0,\quad \gamma_i\in Q(a),$$

czyli postać $z=v(c)$ gdzie $v\in Q(a)[x]$, $\deg v\le k-1$.

Określmy

$$\varphi_2(z) = \varphi_2(v(c)) := v^{\varphi_1}(d).$$

Sprawdzamy rozmaite warunki na $\varphi_2$:

- jeśli $z_1 = v_1(c)$, $z_2 = v_2(c)$, to

$$\varphi_2(z_1+z_2) = \varphi_2(v_1(c)+v_2(c)) = \varphi_2((v_1+v_2)(c)) =$$

$$= (v_1+v_2)^{\varphi_1}(d) = (v_1^{\varphi_1} + v_2^{\varphi_1})(d) = v_1^{\varphi_1}(d) + v_2^{\varphi_1}(d) =$$

$$= \varphi_2(v_1(c)) + \varphi_2(v_2(c)) = \varphi_2(z_1) + \varphi_2(z_2).$$

- podobnie pokazuje się, że $\varphi_2(z_1 \cdot z_2) = \varphi_2(z_1) \cdot \varphi_2(z_2)$

- gdy $z \in Q(a)$, to $z = v(c)$ dla wielomianu stałego $v$ (o współczynniku równym $z$);

wtedy $\varphi_2(z) = \varphi_2(v(c)) = v^{\varphi_1}(d) = \varphi_1(z)$

bo $v^{\varphi_1}$ to wielomian stały o współczynniku $\varphi_1(z)$.

Zatem $\varphi_2$ jest rozszerzeniem $\varphi_1$.

- Podobny argument, z wielomianem $v(x) \overset{=1\cdot x}{=} x$, pokazuje że

$$\varphi_2(c) = \varphi_2(v(c)) = v^{\varphi_1}(d) = d$$

bo $v^{\varphi_1}(x) = \varphi_1(1)\cdot x = 1 \cdot x = x$

Stąd też wynika, że obraz $\varphi_2(Q(a)(c))$ jest całe $Q(b)(d)$.

- Różnowartościowość $\varphi_2$ wynika z jednoznaczności przedstawień elementów z $Q(a)(c)$ i $Q(b)(d)$ w postaci

$\gamma_{k-1}c^{k-1} + \dots + \gamma_1 c + \gamma_0$ i $\gamma_{k-1}d^{k-1} + \dots + \gamma_1 d + \gamma_0$, odpowiednio,

gdzie $\gamma_0, \gamma_1, \dots, \gamma_{k-1} \in Q(a), Q(b)$ odpowiednio.

albo z istnienia podobnie określonego izomorfizmu $\psi_2 : Q(b)(d) \to Q(a)(c)$ takiego, że $\psi_2(b) = a$, $\psi_2(d) = c$, o którym nietrudno stwierdzić, że jest odwrotny do $\varphi_2$.

Kontynuując to rozumowanie przez indukcję, powtarzając kroki analogiczne jak krok 2, otrzymujemy w końcu izomorfizm

$$\varphi_n : \mathbb{Q}(a_1,\dots,a_n) \to \mathbb{Q}(a_1,\dots,a_n)$$

czyli automorfizm ciała $\mathbb{Q}_f$, taki że $\varphi_n(a) = b$.

Stąd tranzytywność grupy $Gal(\mathbb{Q}_f/\mathbb{Q}) = Aut(\mathbb{Q}_f)$ na zbiorze pierwiastków wielomianu $f$. $\square$