GRUPA GALOIS WIELOMIANU JAKO GRUPA PERMUTACJI JEGO PIERWIASTKÓW

PRZYPOMNIENIE.

TWIERDZENIE GALOIS. Niech $f \in Q[x]$ – wielomian nierozkładalny. Pierwiastki wielomianu f wyrażają się przez pierwiastniki $\Longleftrightarrow$ grupa Galois wielomianu f, $Gal(Q_f/Q)$, jest rozwiązalna.

CIAŁO ROZKŁADU Q_f WIELOMIANU $f \in Q[x]$

jest to najmniejsze ciało liczbowe zawierające wszystkie (także zespolone) pierwiastki wielomianu f.

UWAGA. Jeśli $a_1, a_2, \dots, a_n$ to pełen zbiór pierwiastków wielomianu $f \in Q[x]$, to jego ciałem rozkładu Q_f jest ciało

$$Q(a_1)(a_2)\dots(a_n) = Q(a_1, \dots, a_n)$$

GRUPA GALOIS $Gal(Q_f/Q)$ WIELOMIANU $f \in Q[x]$

jest to grupa

$$Gal(Q_f/Q) := Aut(Q_f/Q) = Aut(Q_f)$$

automorfizmów ciała rozkładu Q_f wielomianu f stałych na podciele Q

czyli grupa wszystkich automorfizmów ciała rozkładu Q_f.

LEMAT 1. Niech $\mathbb{Q}_f$ będzie ciałem rozkładu wielomianu

$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ o współczynnikach z $\mathbb{Q}$,

i niech u będzie dowolnym pierwiastkiem wielomianu f.

Wówczas dla dowolnego automorfizmu $\varphi \in Gal(\mathbb{Q}_f/\mathbb{Q}) = Aut(\mathbb{Q}_f)$

$\varphi(u)$ jest także pierwiastkiem wielomianu f.

Dowód:

Skoro u jest pierwiastkiem f, to spełnia równanie

$$a_n u^n + a_{n-1} u^{n-1} + \dots + a_1 u + a_0 = 0.$$

Wtedy, nakładając automorfizm φ na obie strony tej równości, i przekształcając, otrzymujemy:

$$0 = \varphi(0) = \varphi\left(a_n u^n + a_{n-1} u^{n-1} + \dots + a_1 u + a_0\right) =$$

$$= \varphi(a_n u^n) + \varphi(a_{n-1} u^{n-1}) + \dots + \varphi(a_1 u) + \varphi(a_0) =$$

$$= \varphi(a_n) \cdot \varphi(u^n) + \varphi(a_{n-1}) \cdot \varphi(u^{n-1}) + \dots + \varphi(a_1) \varphi(u) + \varphi(a_0) =$$

$$= a_n \cdot \varphi(u^n) + a_{n-1} \varphi(u^{n-1}) + \dots + a_1 \cdot \varphi(u) + a_0 =$$

$$= a_n [\varphi(u)]^n + a_{n-1} [\varphi(u)]^{n-1} + \dots + a_1 \cdot \varphi(u) + a_0.$$

Stąd wynika, że $\varphi(u)$ rzeczywiście jest pierwiastkiem wielomianu

$f(x) = a_n x^n + \dots + a_1 x + a_0$. □

UWAGA. Powyższe wyliczenie pokazuje też, że dla dowolnego wielomianu $h \in \mathbb{Q}[x]$ i dowolnego automorfizmu φ ciała liczbowego zachodzi równość

$$\varphi(h(a)) = h(\varphi(a)).$$

Wykorzystamy ją później.

WNIOSEK 1. Każdy automorfizm $\varphi \in Gal(\mathbb{Q}_f/\mathbb{Q})$ wyznacza pewną permutację zbioru R_f pierwiastków wielomianu f.

Dowód: Z lematu 1, ograniczenie $\varphi|_{R_f}$ automorfizmu φ do zbioru R_f jest przekształceniem $\varphi|_{R_f}: R_f \to R_f$. Ponieważ φ jest różnowartościowy, również $\varphi|_{R_f}$ jest różnowartościowym przekształceniem $R_f \to R_f$.

Ponieważ jednak zbiór R_f jest skończony (bo każdy wielomian ma conajwyżej tyle pierwiastków, ile wynosi jego stopień), każde różnowartościowe przekształcenie $R_f \to R_f$ jest wzajemnie jednoznaczne, czyli jest permutacją zbioru R_f. Zatem φ wyznacza permutację $\varphi|_{R_f}$ zbioru R_f. $\square$

UWAGA. Przyporządkowanie $\varphi \mapsto \varphi|_{R_f}$ jest homomorfizmem grupy $Gal(\mathbb{Q}_f/\mathbb{Q})$ w grupę $S(R_f)$ permutacji zbioru pierwiastków wielomianu $f \in \mathbb{Q}[x]$.

Aby się o tym przekonać, należy sprawdzić, że dla dowolnych $\varphi_1, \varphi_2 \in Gal(\mathbb{Q}_f/\mathbb{Q})$ zachodzi

$$\varphi_1|_{R_f} \circ \varphi_2|_{R_f} = (\varphi_1 \circ \varphi_2)_{R_f}.$$

To jest jednak oczywiste, bo dla dowolnego $u \in R_f$ mamy

$$\varphi_1|_{R_f} \circ \varphi_2|_{R_f}(u) = \varphi_1|_{R_f}(\varphi_2(u)) = \varphi_1(\varphi_2(u)) =$$
$$= (\varphi_1 \circ \varphi_2)(u) = (\varphi_1 \circ \varphi_2)|_{R_f}(u). \quad \square$$

LEMAT 2 Homomorfizm $\Omega: Gal(\mathbb{Q}_f/\mathbb{Q}) \to S(R_f)$ zadany przez $\Omega(\varphi) = \varphi|_{R_f}$ jest różnowartościowy.

Dowód: aby pokazać, że homomorfizm grup jest różnowartościowy, wystarczy pokazać, że jego jądro zawiera tylko element neutralny. Elementem neutralnym grupy $S(R_f)$ jest trywialna permutacja zbioru R_f, czyli przekształcenie tożsamościowe id_{R_f}.

Załóżmy więc, że $\varphi \in Ker(\Omega)$, czyli że $\Omega(\varphi) = id_{R_f}$. Mamy uzasadnić, że wówczas $\varphi = id_{\mathbb{Q}_f}$ (automorfizm tożsamościowy, będący elementem neutralnym grupy $Gal(\mathbb{Q}_f/\mathbb{Q}) = Aut(\mathbb{Q}_f)$).

To, że $\Omega(\varphi) = id_{R_f}$ oznacza, że dla każdego $u \in R_f$ zachodzi $\varphi(u) = u$. Niech $u_1, \dots, u_k$ będzie zbiorem wszystkich pierwiastków wielomianu f. Dla każdego z nich mamy $\varphi(u_i) = u_i$.

Wiemy też, że $\mathbb{Q}_f = \mathbb{Q}(u_1)(u_2)\dots(u_k)$.

Krok 1 Pokażemy, że $\varphi(a) = a$ dla każdego $a \in \mathbb{Q}(u_1)$.

Ciało $\mathbb{Q}(u_1)$ składa się z elementów postaci

$$a = q_{p-1} u_1^{p-1} + q_{p-2} u^{p-2} + \dots + q_1 u + q_0$$

gdzie $q_0, q_1, \dots, q_{p-1} \in \mathbb{Q}$ i gdzie p jest stopniem elementu u_1.

Mamy więc

$$\varphi(a) = \varphi(q_{p-1} u_1^{p-1} + \dots + q_1 u + q_0) =$$
$$= \varphi(q_{p-1})\, \varphi(u_1)^{p-1} + \dots + \varphi(q_1)\varphi(u_1) + \varphi(q_0) =$$
$$= q_{p-1} u_1^{p-1} + \dots + q_1 u_1 + q_0 = a.$$

Krok 2 Indukcyjnie, pokażemy że jeśli $\varphi(a)=a$ dla wszystkich $a\in Q(u_1)\dots(u_j)$, to zachodzi też $\varphi(a)=a$ dla wszystkich $a\in Q(u_1)\dots(u_j)(u_{j+1})$.

Niech $a\in Q(u_1)\dots(u_j)(u_{j+1})=[Q(u_1)\dots(u_j)](u_{j+1})$.

To ostatnie ciało składa się z elementów postaci

$$a=b_{p-1}u_{j+1}^{p-1}+b_{p-2}u_{j+1}^{p-2}+\dots\ b_1u_{j+1}+b_0$$

gdzie $b_0,b_1,\dots,b_{p-1}\in Q(u_1)\dots(u_j)$ i gdzie p jest stopniem pierwiastka u_{j+1} nad ciałem $Q(u_1)\dots(u_j)$.

Jak poprzednio, wyliczamy że $\varphi(a)=a$ korzystając z tego że $\varphi(b_i)=b_i$ (z założenia indukcyjnego, bo $b_i\in Q(u_1)\dots(u_j)$) oraz że $\varphi(u_{j+1})=u_{j+1}$ (z założenia że $\varphi\in\operatorname{Ker}\Omega$).

Krok 3 Z twierdzenia o indukcji, $\varphi(a)=a$ dla dowolnego $a\in Q(u_1)\dots(u_k)=Q_f$, czyli $\varphi=id_{Q_f}$. $\square$

WNIOSEK. Obraz $\Omega[Gal(Q_f/Q)]$ jest podgrupą w grupie permutacji $S(R_f)$ izomorficzną z grupą $Gal(Q_f/Q)$ (wynika bezpośrednio z różnowartościowości homomorfizmu Ω).

<u>LEMAT 3</u> Jeśli wielomian $f \in Q[x]$ jest nierozkładalny, to nie posiada pierwiastków wielokrotnych, a więc jego stopień jest równy liczbie jego pierwiastków.

<u>Dowód</u> Załóżmy NIE WPROST, że b jest pierwiastkiem wielokrotnym wielomianu f. Traktując f jako wielomian o współczynnikach z Q_f, możemy podzielić go przez wielomian $(x-b)^2$, który również ma współczynniki z Q_f, i dostaniemy iloraz $g(x) \in Q_f[x]$ oraz resztę ZERO (to wynika z tego, że b jest pierwiastkiem przynajmniej 2-krotnym). Zachodzi więc

$$f(x) = (x-b)^2 \cdot g(x).$$

Pochodna $f'(x)$ jest wielomianem stopnia $st(f') = st(f) - 1$, a oblicza się ją tak:

$$f'(x) = [(x-b)^2 \cdot g(x)]' = [(x-b)^2]' \cdot g(x) + (x-b)^2 \cdot g'(x) =$$

$$= 2(x-b) \cdot g(x) + (x-b)^2 g'(x) =$$

$$= (x-b)[2 \cdot g(x) + (x-b) g'(x)].$$

Zatem $f'(b) = 0$.

Zauważmy jednak, że jeśli $f(x) = a_n x^n + .. + a_1 x + a_0 \in Q[x]$ to $f'(x) = n \cdot a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + .. + 2a_2 x + a_1 \in Q[x]$.

Zatem $f'(x)$ jest wielomianem z $Q[x]$ stopnia mniejszego niż f, co przeczy minimalności wielomianu f (wynikającej z jego nierozkładalności).

To sprzeczność dowodzi LEMATU. $\square$

WNIOSEK. Jeśli $f \in \mathbb{Q}[x]$ jest nierozkładalnym wielomianem stopnia n, to jego grupę Galois $Gal(\mathbb{Q}_f/\mathbb{Q})$ utożsamiamy z pewną podgrupą w grupie permutacji S_n (n elementów).

WNIOSEK (z twierdzenia Galois)

Wielomian, którego pierwiastki nie wyrażają się przez pierwiastniki musi mieć stopień $n \geqslant 5$.

Dowód: Jeśli stopień wielomianu wynosi $n \leqslant 4$, to jego grupa Galois jest (izomorficzna z) podgrupą w grupie permutacji co najwyżej 4 elementów. Wiemy już, że wszystkie takie grupy są rozwiązalne. Z twierdzenia Galois wynika zatem, że wielomiany stopni $\leqslant 4$ mają wszystkie pierwiastki wyrażalne przez pierwiastniki. Żeby więc pierwiastek nie wyraził się przez pierwiastniki, wielomian musi mieć stopień przynajmniej 5. □

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: elementarny, ale trochę długi – pomijamy. □