GRUPA GALOIS WIELOMIANU

PRZYPOMNIENIE.

TWIERDZENIE GALOIS. Niech $f \in Q[x]$ – wielomian nierozkładalny.
Pierwiastki wielomianu f wyrażają się przez pierwiastki $\Leftrightarrow$
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 (takie 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

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

↑ kolejność rozszerzań o pojedynczy pierwiastek dowolna;
(niektóre z tych rozszerzań mogą być trywialne).

PRZYKŁADY.

(1) $f(x) = x^2 - 2$, pierwiastki to $\sqrt{2}$ oraz $-\sqrt{2}$.

Zatem $Q_f = Q(\sqrt{2})(-\sqrt{2}) = Q(\sqrt{2}, -\sqrt{2})$.

Pokażmy, że $Q(\sqrt{2}, -\sqrt{2}) = Q(\sqrt{2})$, czyli $\underline{Q_f = Q(\sqrt{2})}$.

Z jednej strony, $Q(\sqrt{2}, -\sqrt{2}) = Q(\sqrt{2})(-\sqrt{2}) \subset Q(\sqrt{2})$.

Z drugiej strony, liczby $\sqrt{2}$ i $-\sqrt{2}$ należą do ciała $Q(\sqrt{2})$,
więc $Q(\sqrt{2}, -\sqrt{2}) \subset Q(\sqrt{2})$.

Stąd równość. □

(2) $f = x^4 - 2$.

pierwiastki to $\underbrace{\sqrt[4]{2}}_{a_1}, \underbrace{-\sqrt[4]{2}}_{a_2}, \underbrace{i\sqrt[4]{2}}_{a_3}, \underbrace{-i\sqrt[4]{2}}_{a_4}$

Rozszerzenie $Q(a_1) = Q(\sqrt[4]{2})$ nie jest jeszcze pełnym ciałem rozkładu wielomianu f, bo składa się z liczb postaci

$$a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} : a, b, c, d \in Q,$$

a więc z samych liczb rzeczywistych, i wobec tego nie zawiera pierwiastków a_3 i a_4.

Zachodzi natomiast $a_2 \in Q(\sqrt[4]{2})$, więc $Q(a_1, a_2) = Q(\sqrt[4]{2})$.

Rozważmy więc $Q(a_1, a_2, a_3) = Q(\sqrt[4]{2})(i\sqrt[4]{2})$

Pokażemy, że $Q(\sqrt[4]{2})(i\sqrt[4]{2}) = Q(\sqrt[4]{2})(i)$

Zawieranie $Q(\sqrt[4]{2})(i\sqrt[4]{2}) \subset Q(\sqrt[4]{2})(i)$

wynika z tego, że $\sqrt[4]{2}$ oraz $i\sqrt[4]{2}$ należą do $Q(\sqrt[4]{2})(i)$.

Zawieranie $Q(\sqrt[4]{2})(i) \subset Q(\sqrt[4]{2})(i\sqrt[4]{2})$ wynika z tego, że

$\sqrt[4]{2} \in Q(\sqrt[4]{2})(i\sqrt[4]{2})$ [oczywiste] oraz że

$i \in Q(\sqrt[4]{2})(i\sqrt[4]{2})$ [bo $i = i\sqrt[4]{2}/\sqrt[4]{2}$].

Zauważmy jeszcze, że $a_4 \in Q(a_1)(a_2)(a_3) = Q(\sqrt[4]{2})(i)$

Zatem $Q_f = Q(a_1)(a_2)(a_3)(a_4) = Q(\sqrt[4]{2})(i)$ składa się z liczb

postaci $a + b\sqrt[4]{2} + c\sqrt[4]{4} + d\sqrt[4]{8} + a'i + b'i\sqrt[4]{2} + c'i\sqrt[4]{4} + d'i\sqrt[4]{8}$ $\quad a, b, c, d, a', b', c', d' \in Q$

(3)

(3) $f(x) = x^2 - x - 2 = (x+1)(x-2)$.

pierwiastki: $-1, 2$

Ponieważ $Q(-1,2) = Q$, więc samo dato Q jest dieten rozkładu wielomianu $x^2 - x - 2$.

2.2. Automorfizmy ciała

Definicja 2.2.1. *Automorfizmem ciała L nazywamy wzajemnie jednoznaczne odwzorowanie $\varphi: L \to L$, które spełnia warunki:*

1) $\varphi(a+b) = \varphi(a) + \varphi(b)$ *dla dowolnych* $a, b \in L$

2) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ *dla dowolnych* $a, b \in L$

Przykłady 2.2.2.

Niech $\varphi: C \to C$ będzie funkcją zespoloną zapisaną wzorem $\varphi(z) = \bar{z}$, czyli $\varphi(x+iy) = x - iy$.

Korzystając ze znanych własności sprzężenia dla liczb zespolonych pokażę, że to odwzorowanie spełnia warunki automorfizmu. Oczywiście φ jest odwzorowaniem wzajemnie jednoznacznym.

1) $\varphi(z_1 + z_2) = \overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2 = \varphi(z_1) + \varphi(z_2)$;

2) $\varphi(z_1 \cdot z_2) = \overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2 = \varphi(z_1) \cdot \varphi(z_2)$.

Przykład 2.2.3.

W ciele $L = Q(\sqrt{2})$ łatwo wskazać dwa automorfizmy - są nimi tożsamość i przekształcenie, które liczbie $p + q\sqrt{2}$ przyporządkowuje liczbę $p - q\sqrt{2}$.

- Tożsamość oczywiście jest automorfizmem.
- Sprawdzimy czy drugie przekształcenie spełnia definicję automorfizmu:

  1) $\varphi((p_1 + q_1\sqrt{2}) + (p_2 + q_2\sqrt{2})) = \varphi((p_1 + p_2) + (q_1 + q_2)\sqrt{2}) = (p_1 + p_2) - (q_1 + q_2)\sqrt{2} =$
  $(p_1 - q_1\sqrt{2}) + (p_2 - q_2\sqrt{2}) = \varphi(p_1 + q_1\sqrt{2}) + \varphi(p_2 + q_2\sqrt{2})$;

  2) $\varphi((p_1 + q_1\sqrt{2}) \cdot (p_2 + q_2\sqrt{2})) = \varphi((p_1p_2 + 2q_1q_2) + (p_1q_2 + p_2q_1)\sqrt{2}) =$
  $= (p_1p_2 + 2q_1q_2) - (p_1q_2 + p_2q_1)\sqrt{2} = (p_1 - q_1\sqrt{2})(p_2 - q_2\sqrt{2}) = \varphi(p_1 + q_1\sqrt{2}) \cdot \varphi(p_2 + q_2\sqrt{2})$.

  Przekształcenie to zachowuje dodawanie i mnożenie, więc spełnia definicję automorfizmu.

Poniższy fakt zbiera własności automorfizmów, które wykorzystamy w kolejnych twierdzeniach.

Fakt 2.2.4.

Dla dowolnego automorfizmu φ ciała liczbowego L zachodzi:

1) $\varphi(0)=0$;
2) $\varphi(1)=1$;
3) dla $a,b\in L$ mamy $\varphi(a-b)=\varphi(a)-\varphi(b)$;
4) dla $a,b\in L$ i $b\neq 0$ wtedy $\varphi\left(\frac{a}{b}\right)=\frac{\varphi(a)}{\varphi(b)}$;
5) dla $a_1,a_2,...,a_n\in L$ zachodzi $\varphi(a_1+a_2+...+a_n)=\varphi(a_1)+\varphi(a_2)+...+\varphi(a_n)$;
6) dla $a_1,a_2,...,a_n\in L$ mamy $\varphi(a_1\cdot a_2\cdot...\cdot a_n)=\varphi(a_1)\cdot\varphi(a_2)\cdot...\cdot\varphi(a_n)$.

Dowód:

1) Z definicji automorfizmu wiemy, że $\varphi(a)=\varphi(a+0)=\varphi(a)+\varphi(0)$. Tak więc $\varphi(a)+\varphi(0)=\varphi(a)$ czyli $\varphi(0)=0$.
2) Rozumowanie jest podobne jak w punkcie pierwszym.

$$\varphi(a)=\varphi(a\cdot 1)=\varphi(a)\cdot\varphi(1)$$

$$\varphi(a)=\varphi(a)\cdot\varphi(1)$$

$$\varphi(1)=1.$$

3) Korzystając z definicji automorfizmu i wcześniej udowodnionej własności 1) pokażę, że $\varphi(-b)=-\varphi(b)$.

$$0=\varphi(0)=\varphi(b-b)=\varphi(b+(-b))=\varphi(b)+\varphi(-b)$$

$$0=\varphi(b)+\varphi(-b)$$

$$\varphi(-b)=-\varphi(b)$$

Własności 3) dowodzi poniższa równość:

$$\varphi(a-b)=\varphi(a+(-b))=\varphi(a)+\varphi(-b)=\varphi(a)-\varphi(b)$$

4) Dowód tej własności jest podobny do poprzedniego.
5) Jest to dowód indukcyjny względem n.

Dla $n=1$ własność 5) jest spełniona, bo $\varphi(a_1)=\varphi(a_1)$. Zakładam, że równość ta zachodzi dla n, czyli $\varphi(a_1+a_2+...+a_n)=\varphi(a_1)+\varphi(a_2)+...+\varphi(a_n)$.

Sprawdzam, czy zachodzi dla $n+1$.

$$\varphi(a_1+a_2+...+a_n+a_{n+1})=\varphi((a_1+a_2+...+a_n)+a_{n+1})=\varphi(a_1+a_2+...+a_n)+\varphi(a_{n+1})=$$

$$=\varphi(a_1)+\varphi(a_2)+...+\varphi(a_n)+\varphi(a_{n+1})$$

Własność zachodzi dla dowolnego n.

6) Dowód tej własności opiera się na indukcji względem n.

Wprowadzam oznaczenie *Aut(L)* – zbiór wszystkich automorfizmów ciała L.

Definicja 2.2.5. *Automorfizm* $\varphi:L\to L$ *jest stały na podciele K, jeśli dla dowolnego* $a\in K$ *zachodzi* $\varphi(a)=a$.

Fakt 2.2.6.

Każdy automorfizm ciała liczbowego L jest stały na podciele liczb wymiernych.

Dowód:

Dowód ten będzie opierał się na konstrukcji liczb wymiernych. Najpierw pokażę, że automorfizm jest stały na liczbach naturalnych, potem całkowitych i wymiernych.

Z własności udowodnionych w fakcie 2.2.4 wiemy, że $\varphi(0)=0$ i $\varphi(1)=1$

Dla liczb naturalnych mamy $n=\underbrace{1+1+...+1}_{n\,razy}$

$$\varphi(n)=\varphi(\underbrace{1+1+...+1}_{n\,razy})=\underbrace{\varphi(1)+\varphi(1)+...+\varphi(1)}_{n\,razy}=\underbrace{1+1+...+1}_{n\,razy}=n$$

Korzystając z własności 3) faktu 2.2.4 łatwo pokazać, że automorfizm jest stały na liczbach całkowitych ujemnych, czyli liczbach postaci $-n$, gdzie $n\in N$. Dla takich liczb mamy $\varphi(-n)=-\varphi(n)=-n$, a więc są zachowywane przez φ.

Aby twierdzenie było prawdziwe dla wszyśtkich liczb wymiernych, należy pokazać, że zachodzi dla wszystkich ułamków $\frac{p}{q}$, takich że $p,q\in Z$ i $q\neq 0$.

Korzystając z własności 4) faktu 2.2.4 otrzymujemy $\varphi\left(\frac{p}{q}\right)=\frac{\varphi(p)}{\varphi(q)}=\frac{p}{q}$, co kończy dowód faktu.

GRUPA PRZEKSZTAŁCEŃ

Zbiór G złożony z przekształceń $g: X \to X$ zbioru X nazywamy grupą przekształceń gdy

(0) wszystkie przekształcenia $g \in G$ są wzajemnie jednoznaczne

(1) jeśli $g \in G$, to również przekształcenie odwrotne $g^{-1} \in G$
(zamkniętość na odwrotność)

(2) jeśli $g_1, g_2 \in G$, to również złożenie $g_1 \circ g_2 \in G$
(zamkniętość na składanie).

UWAGA. Grupa przekształceń z działaniem składania to szczególny przypadek grupy.

NAJPOPULARNIEJSZE PRZYKŁADY:

(1) Zbiór wszystkich permutacji zbioru $\{1, 2, \dots, n\}$ - grupa S_n.

(2) Zbiory symetrii figur.

(3) Zbiór wszystkich izometrii płaszczyzny.

My pokażemy, że zbiór wszystkich automorfizmów ciała L, oznaczony przez $Aut(L)$, jest grupą przekształceń.

Fakt 2.2.7.

Zbiór wszystkich automorfizmów ciała L jest grupą przekształceń.

Dowód:

Sprawdzam, czy zbiór $Aut(L)$ ze składaniem przekształceń spełnia definicje grupy przekształceń.

1) Każdy automorfizm ciała L jest z definicji przekształceniem wzajemnie jednoznacznym.
2) Niech $\varphi \in Aut(L)$. Należy pokazać, że $\varphi^{-1} \in Aut(L)$, czyli φ^{-1} spełnia definicję automorfizmu.

   φ^{-1} jest przekształceniem wzajemnie jednoznacznym.

   φ^{-1} zachowuje dodawanie, bo

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad / \text{ nakładamy } \varphi^{-1}$$

$$\varphi^{-1}(\varphi(a+b)) = \varphi^{-1}(\varphi(a) + \varphi(b))$$

$$a+b = \varphi^{-1}(\varphi(a) + \varphi(b))$$

$$\varphi^{-1}(\varphi(a)) + \varphi^{-1}(\varphi(b)) = \varphi^{-1}(\varphi(a) + \varphi(b))$$

   Elementy $\varphi(a)$ i $\varphi(b)$ mogą być dowolnymi elementami ciała L. Oznaczam $\varphi(a) = a'$, $\varphi(b) = b'$. Powyższą równość możemy zapisać jako:

$$\varphi^{-1}(a') + \varphi^{-1}(b') = \varphi^{-1}(a' + b').$$

   W podobny sposób pokazujemy, że φ^{-1} zachowuje mnożenie.

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

$$\varphi^{-1}(\varphi(a \cdot b)) = \varphi^{-1}(\varphi(a) \cdot \varphi(b))$$

$$a \cdot b = \varphi^{-1}(\varphi(a) \cdot \varphi(b))$$

$$\varphi^{-1}(\varphi(a)) \cdot \varphi^{-1}(\varphi(b)) = \varphi^{-1}(\varphi(a) \cdot \varphi(b))$$

   Stosując takie samo podstawienie otrzymujemy:

$$\varphi^{-1}(a') \cdot \varphi^{-1}(b') = \varphi^{-1}(a' \cdot b')$$

3) Należy pokazać, że złożenie dwóch automorfizmów jest automorfizmem.

   Niech $\varphi_1, \varphi_2 \in Aut(L)$. Wtedy $\varphi_1 \circ \varphi_2$ jest przekształceniem wzajemnie jednoznacznym.

   $\varphi_1 \circ \varphi_2$ zachowuje dodawanie, ponieważ mamy

$$\varphi_1 \circ \varphi_2(a+b) = \varphi_1(\varphi_2(a+b)) = \varphi_1(\varphi_2(a) + \varphi_2(b)) = \varphi_1(\varphi_2(a)) + \varphi_1(\varphi_2(b)) =$$

$$= \varphi_1 \circ \varphi_2(a) + \varphi_1 \circ \varphi_2(b)$$

Podobnie $\varphi_1 \circ \varphi_2$ zachowuje mnożenie, gdyż

$$\varphi_1 \circ \varphi_2(a \cdot b) = \varphi_1(\varphi_2(a \cdot b)) = \varphi_1(\varphi_2(a) \cdot \varphi_2(b)) = \varphi_1(\varphi_2(a)) \cdot \varphi_1(\varphi_2(b)) = \varphi_1 \circ \varphi_2(a) \cdot \varphi_1 \circ \varphi_2(b)$$

W powyższych równościach korzystałam z założenia, że φ_1 i φ_2 są automorfizmami.

Def. Jeśli $K \subset L$ są ciałami, to zbiór automorfizmów ciała L stałych na podciele K oznaczamy przez $Aut(L/K)$.

Są to takie automorfizmy $\varphi: L \to L$, że $\forall x \in K \ \varphi(x) = x$.

FAKT. Zbiór $Aut(L/K)$ jest grupą przekształceń.

Dowód:

Zamkniętość na odwrotność

Niech $\varphi \in Aut(L/K)$ i niech $x \in K$.

Zachodzi $\varphi(x) = x$, więc zachodzi także $\varphi^{-1}(x) = x$,

czyli $\varphi^{-1} \in Aut(L/K)$. □

Zamkniętość na składanie

Niech $\varphi_1, \varphi_2 \in Aut(L/K)$.

Wówczas dla dowolnego $x \in K$ zachodzi

$$\varphi_1 \circ \varphi_2 (x) = \varphi_1(\varphi_2(x)) = \varphi_1(x) = x$$

czyli $\varphi_1 \circ \varphi_2 \in Aut(L/K)$. □

Definicja. Grupę Galois rozszerzenia $K \subset L$ to grupa $Aut(L/K)$ automorfizmów ciała L stałych na podciele K.
Oznaczamy ją także jako $Gal(L/K)$.

Definicja. Grupę Galois wielomianu $f \in \mathbb{Q}[x]$ to grupa $Gal(\mathbb{Q}_f/\mathbb{Q})$ [automorfizmów ciała rozkładu $\mathbb{Q}_f$ stałych na $\mathbb{Q}$].

UWAGA. $Gal(\mathbb{Q}_f/\mathbb{Q}) = Aut(\mathbb{Q}_f)$, gdyż każdy automorfizm ciała liczbowego jest stały na podciele $\mathbb{Q}$.

Przykład 2.3.3.

Aby wyznaczyć grupę Galois $Gal((Q(\sqrt{2})/Q)$ należy wyznaczyć wszystkie automorfizmy ciała $Q(\sqrt{2})$ stałe na podciele Q.

$$\varphi(p+q\sqrt{2}) = \varphi(p) + \varphi(q\sqrt{2}) = \varphi(p) + \varphi(q)\cdot\varphi(\sqrt{2})$$

$$= p + q\cdot\varphi(\sqrt{2}).$$ Aby znaleźć automorfizm wystarczy znać obraz $\varphi(\sqrt{2})$. Mamy zależność:

$$(\sqrt{2})^2 = 2$$

$$(\varphi(\sqrt{2}))^2 = \varphi((\sqrt{2})^2) = \varphi(2) = 2$$

$$(\varphi(\sqrt{2}))^2 = 2 \Rightarrow \varphi(\sqrt{2}) = \sqrt{2} \text{ lub } \varphi(\sqrt{2}) = -\sqrt{2}$$

Grupa Galois tego rozszerzenia składa się z dwóch automorfizmów: identyczności i automorfizmu, który liczbie $p+q\sqrt{2}$ przyporządkowuje liczbę $p-q\sqrt{2}$.

UWAGA. Ponieważ $Q(\sqrt{2})$ jest ciałem rozkładu wielomianu $f=X^2-2$, powyższa grupa złożona z dwóch automorfizmów to grupa Galois $Gal(Q_f/Q)$ wielomianu X^2-2.