PRZYKŁAD WIELOMIANU, KTÓREGO PIERWIASTKI NIE WYRAŻAJĄ SIĘ PRZEZ PIERWIASTNIKI.

PRZYPOMNIENIE:

TWIERDZENIE GALOIS. Niech $f \in \mathbb{Q}[x]$ - wielomian nierozkładalny. Pierwiastki wielomianu f wyrażają się przez pierwiastniki $\iff$ grupa Galois wielomianu f, $Gal(\mathbb{Q}_f/\mathbb{Q}) = Aut(\mathbb{Q}_f)$, jest rozwiązalna.

WNIOSEK. Jeśli grupa Galois $Gal(\mathbb{Q}_f/\mathbb{Q})$ nierozkładalnego wielomianu $f \in \mathbb{Q}[x]$ jest nierozwiązalna, to pierwiastki wielomianu f nie wyrażają się przez pierwiastniki.

UWAGA. Wiemy już też, że stopień takiego wielomianu f jak wyżej musi wynosić przynajmniej 5.

Naszym przykładem takiego wielomianu będzie

$$f(x) = x^5 - 6x + 3.$$

WŁASNOŚCI WIELOMIANU $x^5-6x+3=f$

(1) f jest nierozkładalny

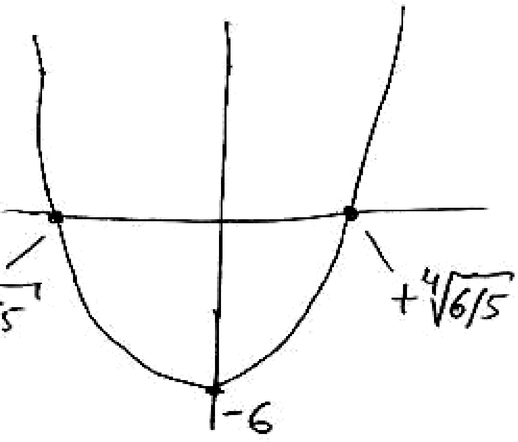
Wystarczy zastosować kryterium Eisensteina dla $p=3$.

WNIOSEK. f ma 5 różnych pierwiastków, zaś grupa Galois $Gal(\mathbb{Q}_f/\mathbb{Q})$ utożsamia się z pewną podgrupą permutacji tych pierwiastków, czyli podgrupą w grupie S_5.

(2) Wielomian $f = x^5 - 6x + 3$ ma dokładnie 3 pierwiastki rzeczywiste.

Uzasadnienie analityczne:

Pochodna $f'(x) = 5x^4 - 6$



Zatem funkcja f:

- rośnie na przedziale $(-\infty, -\sqrt[4]{6/5})$
- ma maximum w punkcie $x = -\sqrt[4]{6/5}$
- maleje na przedziale $(-\sqrt[4]{6/5}, +\sqrt[4]{6/5})$
- ma minimum w punkcie $x = \sqrt[4]{6/5}$
- rośnie na przedziale $(\sqrt[4]{6/5}, +\infty)$.

Obliczmy lub oszacujmy znaki wartości w punktach charakterystycznych:

* $f(0) = 3$
* $f(-\sqrt[4]{6/5}) = (-\sqrt[4]{6/5})^5 - 6 \cdot (-\sqrt[4]{6/5}) + 3 =$

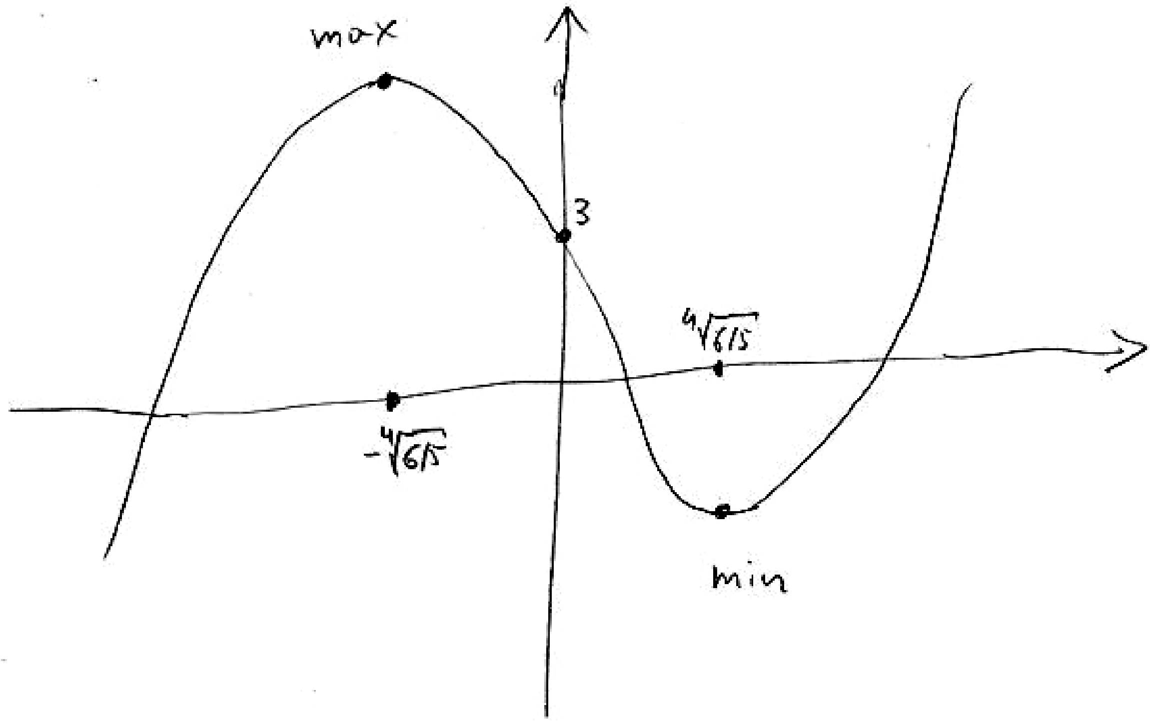
$$= -\frac{6}{5}\sqrt[4]{6/5} + 6\sqrt[4]{6/5} + 3 =$$

$$= 4\frac{4}{5} \cdot \sqrt[4]{6/5} + 3 > 0$$ (maksimum jest dodatnie)

* $f(\sqrt[4]{6/5}) = \frac{6}{5}\sqrt[4]{6/5} - 6\sqrt[4]{6/5} + 3 = -4\frac{4}{5}\sqrt[4]{6/5} + 3 < 0$

(minimum jest ujemne).

Szkicujemy orientacyjny wykres funkcji f :



Wykorzystujemy tu jeszcze informację, że

$$\lim_{x\to+\infty}(x^5-6x+3)=+\infty, \quad \lim_{x\to-\infty}(x^5-6x+3)=-\infty.$$

Z ciągłości, monotoniczności na wskazanych przedziałach, z oszacowania wartości minimum i maksimum, oraz z wyliczenia granic przy $x\to\pm\infty$, wynika że f ma dokładnie 3 pierwiastki (rzeczywiste). $\square$

(3) Jeśli pewna nierzeczywista zespolona liczba z_0 jest pierwiastkiem wielomianu $f = x^5 - 6x + 3$, to liczba sprzężona $\overline{z_0}$ także jest pierwiastkiem tego wielomianu.

Uzasadnienie

Skorzystamy z własności sprzężenia względem działań dodawania, mnożenia i potęgowania, oraz z tego, że sprzężenie liczby rzeczywistej to ta sama liczba.

Skoro z_0 jest pierwiastkiem f, to zachodzi

$$z_0^5 - 6 \cdot z_0 + 3 = 0.$$

Sprzęgamy obie strony tej równości, i przekształcamy:

$$0 = \overline{0} = \overline{z_0^5 - 6z_0 + 3} = \overline{z_0^5} - \overline{6z_0} + \overline{3} =$$

$$= (\overline{z_0})^5 - \overline{6} \cdot \overline{z_0} + 3 = (\overline{z_0})^5 - 6\,\overline{z_0} + 3$$

Zatem $(\overline{z_0})^5 - 6\,\overline{z_0} + 3 = 0$

czyli $\overline{z_0}$ jest pierwiastkiem $f = x^5 - 6x + 3$. $\square$

TWIERDZENIE. Jeśli wielomian f jest nierozkładalny nad $\mathbb{Q}$, zaś jego stopień wynosi 5, oraz f ma dokładnie 3 pierwiastki rzeczywiste, i dwa pierwiastki zespolone sprzężone (nierzeczywiste), to grupa Galois tego wielomianu nie jest rozwiązalna.

UWAGA: założenia tego twierdzenia spełnia wielomian x^5-6x+3.

DOWÓD: Niech $\mathbb{Q}_f$ będzie ciałem rozkładu wielomianu f.

(A) Jednym z automorfizmów ciała $\mathbb{Q}_f$ jest sprzężenie zespolone

Uzasadnienie: sprzężenie zespolone $s(z)=\bar{z}$ jest automorfizmem ciała $\mathbb{C}$, i dlatego jest też izomorfizmem ciała $\mathbb{Q}_f$ na ciało $s(\mathbb{Q}_f)=\overline{\mathbb{Q}_f}=\{\bar{z} : z\in \mathbb{Q}_f\}$. Pokażę, że $s(\mathbb{Q}_f)=\mathbb{Q}_f$, skąd wyniknie że $s: \mathbb{Q}_f\to\mathbb{Q}_f$ jest automorfizmem.

Mamy 3 rzeczywiste pierwiastki f; v_1, v_2, v_3, oraz dwa zespolone z_0 i $\bar{z}_0$. Zatem

$$\mathbb{Q}_f = \mathbb{Q}(v_1, v_2, v_3, z_0, \bar{z}_0).$$

Zachodzi też

$$s(\mathbb{Q}_f) = s(\mathbb{Q}(v_1,v_2,v_3,z_0,\bar{z}_0)) = \mathbb{Q}(s(v_1), s(v_2), s(v_3), s(z_0), s(\bar{z}_0))$$

$$= \mathbb{Q}(v_1, v_2, v_3, \bar{z}_0, \underset{\substack{\uparrow \\ \text{bo } \bar{\bar{z}}_0 = z_0}}{z_0}) = \mathbb{Q}_f. \quad \square$$

Automorfizm $\overbrace{s}^{\text{sprzężenia zespolonego}}$ ciała $\mathbb{Q}_f$ indukuje permutację pierwiastków wielomianu f, która jest transpozycją elementów z_0 i $\bar{z}_0$, natomiast elementy v_1, v_2, v_3 pozostają nieruszone.

(B) Grupa Galois $Gal(\mathbb{Q}_f/\mathbb{Q})$ wielomianu f zawiera element rzędu 5.

<u>Uzasadnienie:</u>

Z nierozkładalności f, grupę $Gal(\mathbb{Q}_f/\mathbb{Q})$ możemy traktować jako podgrupę w grupie permutacji pięciu pierwiastków wielomianu f, czyli podgrupę w grupie S_5.

Z jednego z twierdzeń z poprzedniego wykładu, $Gal(\mathbb{Q}_f/\mathbb{Q})$ jest <u>tranzytywną</u> podgrupą w grupie permutacji S_5.

Twierdzę, że każda tranzytywna podgrupa $G < S_5$ ma rząd podzielny przez 5. Rzeczywiście, niech $H = \{g \in G : g(1) = 1\}$. H jest podgrupą w G, bo jest zamknięte na składanie elementów i na odwrotność. Oznaczmy przez g_2, g_3, g_4, g_5 takie elementy z G t. że $g_2(1) = 2$, $g_3(1) = 3$, $g_4(1) = 4$ i $g_5(1) = 5$ (istnieją dzięki tranzytywności grupy G).

Zauważmy, że warstwy $g_iH = \{g_ih : h \in H\}$ składają się z permutacji przekształcających 1 na i, więc są parami rozłączne i rozłączne z H.

Co więcej warstwa g_iH składa się ze <u>wszystkich</u> permutacji z G które przekształcają 1 na i. Tak jest, bo jeśli $g \in G$ i $g(1) = i$ to $g = g_i(g_i^{-1}g)$, natomiast $g_i^{-1}g \in H$ bo $g_i^{-1}g(1) = g_i^{-1}(i) = 1$, to zaś oznacza że $g \in g_iH$.

W takim razie mamy $G = H \sqcup g_2H \sqcup g_3H \sqcup g_4H \sqcup g_5H$ (suma rozłączna). Ponieważ jednak wszystkie warstwy g_iH mają tą samą liczbę elementów co H, zachodzi $|G| = 5 \cdot |H|$, czyli $5 \mid |G|$.

W szczególności, 5 jest dzielnikiem rzędu grupy Galois

$Gal(\mathbb{Q}_f/\mathbb{Q})$.

Jedno z twierdzeń dowodzonych kilka wykładów wstecz mówiło, że jeśli liczba pierwsza p jest dzielnikiem rzędu $|G|$ grupy G, to w grupie G jest element rzędu p. Stąd wynika, że w naszej podgrupie tranzytywnej $Gal(\mathbb{Q}_f/\mathbb{Q}) < S_5$ jest element rzędu 5. $\square$

(C) Jedynym rodzajem elementu rzędu 5 w grupie S_5 jest 5-cykl. Zatem podgrupa $Gal(\mathbb{Q}_f/\mathbb{Q}) < S_5$ zawiera 5-cykl.

Uzasadnienie:

W grupie S_5 są następujące rodzaje elementów, mających następujące rzędy

rodzaj	przykład	rząd
transpozycje	(12)	2
3-cykl	(145)	3
4-cykl	(2513)	4
5-cykl	(13254)	5
kombinacje 2 rozłącznych transpozycji	(13)(25)	2
kombinacje rozłącznych 2-cyklu i 3 cyklu	(13)(245)	6

Widać, że jedynie 5-cykle mają rząd 5. $\square$

(D) Jedyna podgrupa $G < S_5$ zawierająca transpozycję oraz 5-cykl jest cała grupa S_5.

(Zatem grupa Galois $Gal(\mathbb{Q}_f/\mathbb{Q})$ to grupa S_5).

Uzasadnienie:

Przyjmijmy (przenumerowując elementy 1, 2, 3, 4, 5 jeśli trzeba) że do naszej grupy G należy transpozycja (12).

Cykl c długości 5, który należy do G, cyklicznie przestawia wszystkie elementy $1, 2, .., 5$.

Łatwo też sprawdzić, że wszystkie potęgi c^2, c^3, c^4 także są 5-cyklami.

Jeśli $c(1) \neq 2$, to dla jednej z potęg $i = 2, 3, 4$ zachodzi $c^i(1) = 2$. Do grupy G należy zatem taki 5-cykl b, że $b(1) = 2$.

Przenumerowując kolejność elementów 3, 4, 5 jeśli trzeba, możemy założyć że $b = (12345) \in G$.

Tak więc możemy przyjąć, że $(12) \in G$ oraz $(12345) \in G$.

Pokażemy teraz, że każda transpozycja elementów sąsiednich $(k\ k{+}1)$ należy do G.

Mamy $b^{k-1} = \begin{pmatrix} 1 & 2 & \cdots & 5 \\ k & k+1 & \cdots & \end{pmatrix} \in G$, $(b^{k-1})^{-1} = \begin{pmatrix} k & k+1 & \cdots & \\ 1 & 2 & \cdots & 5 \end{pmatrix} \in G$

a zatem

$$b^{k-1} \cdot (12) \cdot (b^{k-1})^{-1} = \begin{pmatrix} 1 & 2 & \cdots & 5 \\ k & k+1 & \cdots & \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} k & k+1 & \cdots & \\ 1 & 2 & \cdots & 5 \end{pmatrix} = (k\ k{+}1) \in G.$$

Zauważmy wreszcie, że każda permutacja zbioru 1, 2, 3, 4, 5 daje się uzyskać jako kombinacja transpozycji elementów sąsiednich: (12), (23), (34) oraz (45).

Zatem każdy element $\sigma \in S_5$ należy do podgrupy G, czyli $G = S_5$. $\square$

(E) Grupa $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ nie jest rozwiązalna.

<u>Uzasadnienie:</u>

Ponieważ $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) < S_5$ zawiera transpozycję oraz pewien 5-cykl, z punktu (D) wiemy, że $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q}) = S_5$.

Wiemy też, że grupa S_5 nie jest rozwiązalna, więc $\mathrm{Gal}(\mathbb{Q}_f/\mathbb{Q})$ nie jest rozwiązalna.

WNIOSEK.

Pierwiastki wielomianu $X^5 - 6x + 3$ nie wyrażają się przez pierwiastniki.