ROCZNIKI POLSKIEGO TOWARZYSTWA MATEMATYCZNEGO
Seria II: WIADOMOŚCI MATEMATYCZNE X (1968)

wmptm 1897

Ministerstwo Nauki i Szkolnictwa Wyższego

J. BRZEZIŃSKI (Warszawa)

# Grupy Galois wielomianów stopnia czwartego

Niech $K$ oznacza dowolne ciało zawarte w ciele liczb zespolonych $C$. Rozważmy wielomian $f(x)$ o współczynnikach z ciała $K$. *Ciałem rozkładu* tego wielomianu nad $K$ nazywamy ciało, które otrzymujemy dołączając do $K$ pierwiastki wielomianu $f(x)$. Ciało to oznaczamy symbolem $K_f$.

Tak np. jeśli $f(x) = x^2-2$, to ciałem rozkładu tego wielomianu nad ciałem liczb wymiernych $Q$ jest ciało $Q(\sqrt{2})$, tzn. zbiór wszystkich liczb postaci $a+b\sqrt{2}$, gdzie $a$ i $b$ są liczbami wymiernymi.

Dla każdego wielomianu $f(x)$ można rozważać zbiór złożony ze wszystkich przekształceń $\varphi$ jego ciała rozkładu $K_f$, które spełniają warunki:

$$\begin{aligned} \varphi(a+b) &= \varphi(a)+\varphi(b) \quad \text{dla} \quad a,b \in K_f, \\ \varphi(ab) &= \varphi(a)\varphi(b) \quad \text{dla} \quad a,b \in K_f, \\ \varphi(a) &= a \quad \text{dla} \quad a \in K. \end{aligned}$$

Takie przekształcenia nazywamy *automorfizmami ciała $K_f$ stałymi na ciele $K$*. Można łatwo sprawdzić, że tworzą one grupę o skończonej liczbie elementów ([1], str. 446-450). Grupę tę nazywamy *grupą Galois* wielomianu $f$ nad ciałem $K$.

W przypadku ciała $Q(\sqrt{2})$ mamy dwa takie przekształcenia — są nimi tożsamość i przekształcenie, które liczbie $a+b\sqrt{2}$ przyporządkowuje liczbę $a-b\sqrt{2}$.

Jeśli $ax^2+bx+c$ jest wielomianem stopnia drugiego o współczynnikach z ciała $K$, to można bardzo łatwo ustalić, jaką grupę Galois ma ten wielomian. Korzystając bowiem ze znanych wzorów, które pierwiastki $x_1$ i $x_2$ tego wielomianu wyrażają za pomocą współczynników, stwierdzamy z łatwością, że

$$K_f = K(x_1,x_2) = K(\sqrt{\Delta}),$$

gdzie $\Delta = (x_1-x_2)^2 = b^2-4ac$. Jeśli teraz $\sqrt{\Delta} \in K$, to $K_f = K$ i grupa Galois wielomianu $f$ zawiera tylko jeden automorfizm, a mianowicie automorfizm tożsamościowy. Jeśli natomiast $\sqrt{\Delta} \notin K$, to w grupie Galois

są dwa automorfizmy: jednym jest tożsamość, a drugim przekształcenie, które liczbie $a+b\sqrt{\Delta}$ przyporządkowuje liczbę $a-b\sqrt{\Delta}$.

Ogólnie, można pytać o to, jakie grupy Galois mogą mieć wielomiany ustalonego stopnia $n$ o współczynnikach w ciele $K$ i jak określić, czy dla dwóch danych wielomianów stopnia $n$ grupy te są izomorficzne, czy nie są izomorficzne.

Problem ten był przedmiotem badań w końcu XIX wieku. O. Hölder w artykule *Galoische Theorie mit Anwendungen* zamieszczonym w pierwszej części Encyklopädie der Mathematischen Wissenschaften pisze, że problem ten dla wielomianów drugiego, trzeciego i czwartego stopnia został rozwiązany w dysertacji F. Hacka w 1895 roku. Koniec XIX wieku był okresem, w którym tego typu zagadnienia były bardzo modne. Wiele prac (np. [5]) dotyczących analogicznych zagadnień dla równań wyższych stopni pochodzi właśnie z tych czasów. Niestety praca F. Hacka jest w Polsce całkowicie niedostępna, zaś sam problem jest na tyle intrygujący, ciekawy i bywa często przedmiotem zainteresowania ze strony studentów słuchających wykładu teorii Galois, że odtworzenie jego rozwiązania wydawało się bardzo celowe(1). Znajomość rozwiązania tego problemu dostarcza zresztą wielu ciekawych przykładów ilustrujących zastosowania teorii Galois. Na zakończenie podamy jedno z takich nietrywialnych zastosowań.

Obecnie naszkicujemy rozwiązanie omawianego problemu dla wielomianów stopnia trzeciego, a następnie szczegółowe rozwiązanie dla wielomianów stopnia czwartego.

**1. Kilka uwag o wielomianach stopnia trzeciego.** Niech $K$ będzie ciałem charakterystyki 0, $\bar{K}$ domknięciem algebraicznym ciała $K$ i $x_1, x_2, x_3$ pierwiastkami wielomianu

$$f(x) = x^3+ax^2+bx+c$$

o współczynnikach w ciele $K$ (2). *Wyróżnikiem* wielomianu $f$ nazywamy

$$\Delta = (x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2 = a^2b^2+18abc-4a^3c-4b^3-27c^2.$$

Jak wiadomo ([1], str. 466), zachodzi równość

$$K(x_1,x_2,x_3) = K(\sqrt{\Delta},x_i), \tag{1}$$

tzn. ciało rozkładu wielomianu $f$ nad $K$ powstaje z ciała $K$ przez dołączenie $\sqrt{\Delta}$ (tzn. takiego elementu $a$ ciała $\bar{K}$, że $a^2 = \Delta$) oraz któregokolwiek z pierwiastków wielomianu $f$.

(1) Wydaje się ono tym bardziej celowe, że w pewnych współczesnych źródłach podawane są błędne informacje o grupach Galois wielomianów stopnia czwartego. Jaskrawym tego przykładem jest książka [4].

(2) Dla uproszczenia można stale zakładać, że $K$ jest ciałem liczbowym. Jednakże założenie, że charakterystyka ciała $K$ jest równa 0 jest założeniem zbyt mocnym. Wystarcza zakładać, że charakterystyka jest różna od 2 i 3.

Z faktu tego wynika łatwo, że jeśli wielomian $f$ nie ma pierwiastków w ciele $K$ (tzn. jest nierozkładalny w $K$), to stopień ciała rozkładu $K(x_1, x_2, x_3)$ nad $K$ jest równy trzy lub sześć w zależności od tego, czy $\sqrt{\Delta} \in K$, czy $\sqrt{\Delta} \notin K$. W pierwszym przypadku grupą Galois wielomianu $f$ jest grupa permutacji parzystych trzech elementów (grupa $A_3$), a w drugim, grupa wszystkich permutacji trzech elementów (grupa $S_3$). Tak więc, jeśli potrafimy rozstrzygnąć czy wielomian o współczynnikach z ciała $K$ ma pierwiastki w tym ciele (np. potrafimy to zrobić w przypadku ciała $Q$ liczb wymiernych), to potrafimy prosto odpowiedzieć na pytanie: jaki jest stopień ciała rozkładu wielomianu stopnia trzeciego i jaką ten wielomian ma grupę Galois. Obecnie naszym celem będzie znalezienie odpowiedzi na analogiczne pytanie dotyczące wielomianów stopnia czwartego.

**2. Fakty pomocnicze.** Niech

$$f(x) = x^4 + px^2 + qx + r \tag{2}$$

będzie wielomianem o współczynnikach w ciele $K$ charakterystyki 0 i niech $x_1$, $x_2$, $x_3$, $x_4$ będą pierwiastkami wielomianu $f$ w algebraicznym domknięciu $\overline{K}$ ciała $K$. Rozpatrzmy dowolny rozkład wielomianu $f(x)$ w ciele $\overline{K}$ na iloczyn dwu wielomianów stopnia drugiego:

$$x^4 + px^2 + qx + r = (x^2 + ax + b)(x^2 + a_1 x + b_1). \tag{3}$$

Pierwiastkami jednego z czynników (załóżmy, że pierwszego) są więc albo $x_1$ i $x_2$, albo $x_1$ i $x_3$, albo $x_1$ i $x_4$. Porównując współczynniki po obu stronach równości (3) otrzymujemy następujący układ równań:

$$\begin{aligned} a + a_1 &= 0, \\ b + b_1 + aa_1 &= p, \\ ab_1 + a_1 b &= q, \\ bb_1 &= r. \end{aligned}$$

Układ ten jest równoważny układowi:

$$\begin{aligned} b + b_1 &= p + a^2, \\ a(b_1 - b) &= q, \\ bb_1 &= r. \end{aligned}$$

Mnożymy teraz obie strony pierwszego równania przez $a$. Z kolei podnosimy do kwadratu obie strony pierwszego i drugiego równania, a następnie tak otrzymane równania odejmujemy stronami, zastępując pojawiający się iloczyn $bb_1$ przez $r$. W ten sposób uzyskujemy równanie:

$$a^6 + 2pa^4 + (p^2 - 4r)a^2 - q^2 = 0.$$

Wielomian

$$r(f) = t^3+2pt^2+(p^2-4r)t-q^2$$

nazywamy *rezolwentą* wielomianu (2).

Z przeprowadzonych rozważań wynika następujący prosty wniosek, który odnotujemy jako

LEMAT 1. *Jeśli wielomian* (2) *nie ma pierwiastków w ciele* $K$ *i jest w tym ciele rozkładalny, to jego rezolwenta ma pierwiastek w* $K$.

Dowód. Jeśli wielomian (2) nie ma pierwiastków w $K$, to jego rozkład w $K$ musi mieć postać (3). Zatem $a \in K$, czyli pierwiastek $a^2$ rezolwenty należy do ciała $K$.

Jak zauważyliśmy, w zależności od wyboru rozkładu (3) współczynnik $a$ jest równy albo $-(x_1+x_2)$, albo $-(x_1+x_3)$, albo $-(x_1+x_4)$. Zatem elementy

$$t_1 = (x_1+x_2)^2, \quad t_2 = (x_1+x_3)^2, \quad t_3 = (x_1+x_4)^2$$

są pierwiastkami rezolwenty. Z tego, że $x_1+x_2+x_3+x_4 = 0$ wynikają równości

$$(x_1+x_2)^2 = (x_3+x_4)^2, \quad (x_1+x_3)^2 = (x_2+x_4)^2, \quad (x_1+x_4)^2 = (x_2+x_3)^2.$$

LEMAT 2. *Jeśli wielomian* (2) *nie ma pierwiastków wielokrotnych, to jego rezolwenta* $r(f)$ *też nie ma pierwiastków wielokrotnych.*

Dowód. Można bardzo łatwo sprawdzić, że zachodzi równość:

$$(4) \quad (t_1-t_2)^2(t_2-t_3)^2(t_3-t_1)^2 = \\ = (x_1-x_2)^2(x_1-x_3)^2(x_1-x_4)^2(x_2-x_3)^2(x_2-x_4)^2(x_3-x_4)^2.$$

Wynika z niej natychmiast, że jeśli $x_i \neq x_j$ dla $i \neq j$, to $t_i \neq t_j$ dla $i \neq j$. Jeśli więc wielomian $f$ nie ma pierwiastków wielokrotnych, to elementy $t_i$ $(i = 1, 2, 3)$ są trzema, parami różnymi, pierwiastkami rezolwenty (a więc wszystkimi jej pierwiastkami[3]).

Udowodnimy teraz zasadniczy

LEMAT 3. *Jeśli wielomian* (2) *nie ma pierwiastków wielokrotnych, to*

$$K(x_1, x_2, x_3, x_4) = K(t_1, t_2, t_3, x_i).$$

(Tak więc ciało rozkładu wielomianu (2) powstaje przez dołączenie któregokolwiek z jego pierwiastków do ciała rozkładu rezolwenty.)

Dowód. Oznaczmy ciało $K(t_1, t_2, t_3, x_i)$ przez $L$ i dla ustalenia uwagi przyjmijmy, że $x_i = x_1$. Zauważmy, że pierwiastki $x_2, x_3, x_4$ są

---

[3]) Można sprawdzić, że elementy $t_i$ są wszystkimi pierwiastkami rezolwenty również wtedy, gdy wielomian $f$ ma pierwiastki wielokrotne. Z tego faktu nie będziemy korzystali.

elementami algebraicznymi stopnia $\leqslant 2$ nad $L$, bo są one odpowiednio pierwiastkami wielomianów

$$f_i(x) = (x_1+x)^2 - t_{i-1} \qquad (i = 2, 3, 4)$$

o współczynnikach w ciele $L$. Przypuśćmy, że któryś z wielomianów $f_i(x)$ jest nierozkładalny w ciele $L$. Wówczas wielomian $f_i(x)$ jest dzielnikiem wielomianu $f(x)$ (bo $x_i$ jest wspólnym pierwiastkiem wielomianów $f$ i $f_i$). Zatem wielomian $f_i(x)$ ma oprócz $x_i$ jeszcze jeden pierwiastek wspólny z wielomianem $f$, tzn.

$$f_i(x_i) = f_i(x_j) = 0 \qquad \text{dla} \qquad i \neq j.$$

Tak więc

$$(x_1+x_i)^2 = (x_1+x_j)^2 \qquad \text{dla} \qquad i \neq j,$$

co jak wiemy nie może mieć miejsca na podstawie lematu 2. Zatem wielomiany $f_i(x)$ są rozkładalne w ciele $L$, a więc ich pierwiastki należą do tego ciała. Stąd $K(x_1, x_2, x_3, x_4) \subset L$. Przeciwne zawieranie jest oczywiste.

W dalszym ciągu zajmować się będziemy wielomianami stopnia czwartego postaci

$$f(x) = x^4+px^2+qx+r,$$

które nie mają pierwiastków w ciele $K$ i nie mają pierwiastków wielokrotnych. Rozpatrzmy następujące przypadki:

I. Rezolwenta nie ma pierwiastków w ciele $K$.

II. Rezolwenta ma tylko jeden pierwiastek w ciele $K$.

III. Rezolwenta ma wszystkie pierwiastki w ciele $K$.

Zanim przystąpimy do dyskusji tych przypadków zauważmy, że z równości (4) wynika, że wyróżniki wielomianów $f$ i $r(f)$ są sobie równe (lewa strona tej równości jest wyróżnikiem $\Delta(r(f))$, a prawa wyróżnikiem $\Delta(f)$).

Przypomnijmy, że jeśli $\Delta \neq 0$, to $\sqrt{\Delta} \in K$ wtedy i tylko wtedy, gdy do grupy Galois wielomianu $f$ należą tylko parzyste permutacje pierwiastków.

Istotnie, jeśli do grupy Galois wielomianu $f$ należą tylko parzyste permutacje pierwiastków, to $\sqrt{\Delta}$ jest niezmienniczy ze względu na wszystkie automorfizmy ciała rozkładu, a więc należy do $K$. Odwrotnie, jeśli $\sqrt{\Delta} \in K$, to do grupy Galois wielomianu $f$ należą tylko permutacje parzyste. Gdyby bowiem do grupy tej należała pewna permutacja nieparzysta, to z jednej strony $\sqrt{\Delta}$ musiałby w wyniku tej permutacji zmienić znak, a z drugiej nie uległby zmianie (ponieważ jest on elementem ciała $K$). Mielibyśmy więc $\sqrt{\Delta} = -\sqrt{\Delta}$, co oznacza, że $\Delta = 0$.

**3. Przypadek I.** Niech $\Delta$ oznacza wyróżnik wielomianu $f$. Rozpatrzmy dwie możliwości:

(a) $\sqrt{\Delta} \in K$. W tym przypadku $(K(t_1, t_2, t_3): K) = 3$. Wielomian $f$ jest nierozkładalny w ciele $K$ (bo ani on, ani jego rezolwenta nie mają pierwiastków w tym ciele — Lemat 1), a więc wielomian $f$ jest również nierozkładalny w ciele $K(t_1, t_2, t_3)$ (bo stopień wielomianu $f$ jest względnie pierwszy ze stopniem rozszerzenia $K(t_1, t_2, t_3)$ nad $K$; [1], str. 425, zadanie 3). Zatem

$$(K(t_1, t_2, t_3, x_i): K) = 12.$$

Tak więc ciało rozkładu wielomianu $f$ nad $K$ ma stopień 12. Ponieważ $\sqrt{\Delta} \in K$, więc do grupy Galois wielomianu $f$ mogą należeć tylko parzyste permutacje pierwiastków $x_i$. Ponieważ grupa Galois wielomianu $f$ ma rząd 12, więc zawiera wszystkie permutacje parzyste czterech elementów. Jest to więc grupa $A_4$.

(b) $\sqrt{\Delta} \notin K$. W tym przypadku $(K(t_1, t_2, t_3) : K) = 6$. Wielomian $f$ jest nierozkładalny w ciele $K$ z tych samych względów co w przypadku (a); zatem żaden z pierwiastków wielomianu $f$ nie należy do ciała $K(t_1, t_2, t_3)$ (w przeciwnym razie ciało to zawierałoby podciało stopnia czwartego nad $K$). Pierwiastki wielomianu $f$ są więc elementami algebraicznymi stopnia drugiego lub czwartego nad $K(t_1, t_2, t_3)$. Oznacza to zatem, że $(K(t_1, t_2, t_3, x_i): K) = 12$ lub 24.

Gdyby zachodziła pierwsza możliwość, to grupą Galois wielomianu $f$ musiałaby być podgrupa rzędu 12 grupy $S_4$. Wiadomo, że jedyną taką podgrupą jest grupa permutacji parzystych $A_4$. Gdyby jednak grupą Galois wielomianu $f$ była grupa $A_4$, to $\sqrt{\Delta}$ byłby elementem niezmienniczym ze względu na wszystkie automorfizmy, tzn. musiałby należeć do ciała $K$. Przeczy to jednak przyjętemu założeniu. Pozostaje więc tylko druga możliwość, tzn. $(K(x_1, x_2, x_3, x_4): K) = 24$ i grupą Galois wielomianu $f$ jest grupa $S_4$.

**4. Przypadek II.** Załóżmy, że $t_1 = (x_1+x_2)^2 \in K$. Z równości (1) wynika, że w rozpatrywanym przypadku $\sqrt{\Delta} \notin K$. Istotnie, gdyby $\sqrt{\Delta} \in K$, to ciało rozkładu rezolwenty byłoby równe $K(\sqrt{\Delta}, t_1) = K$ wbrew temu, że nie wszystkie pierwiastki rezolwenty należą do ciała $K$.

Do grupy Galois wielomianu $f$ mogą należeć tylko takie permutacje pierwiastków, które zachowują element $t_1$. Z założenia, że wielomian $f$ nie ma pierwiastków wielokrotnych oraz z tego, że $(x_1+x_2)^2 = (x_3+x_4)^2$ wynika, że permutacjami takimi są:

$$a = (1), \quad b = (1, 2), \quad c = (3, 4), \quad d = (1, 2)(3, 4), \quad e = (1, 3)(2, 4),$$
$$f = (1, 4)(2, 3), \quad g = (1, 3, 2, 4), \quad h = (1, 4, 2, 3).$$

Można łatwo sprawdzić, że grupa utworzona przez te permutacje jest izomorficzna z grupą symetrii kwadratu, którą oznaczać będziemy symbolem $D_4$.

Grupą Galois wielomianu $f$ jest więc pewna podgrupa grupy utworzonej przez permutację $a$-$h$. Z tego, że $\sqrt{\Delta} \notin K$ wynika, że podgrupa ta musi zawierać przynajmniej jedną permutację nieparzystą. Oprócz tego żaden pierwiastek wielomianu $f$ nie może być niezmienniczy ze względu na wszystkie permutacje należące do tej podgrupy. W przeciwnym razie pierwiastek ten musiałby należeć do ciała $K$. Można łatwo sprawdzić, że grupa permutacji $a$-$h$, zawiera tylko 3 podgrupy czyniące zadość tym wymogom:

(*) $\{a, b, c, d\}$ — grupa czwórkowa $V_4$,

(**) $\{a, d, g, h\}$ — grupa cykliczna $C_4$,

(***) $\{a, b, c, d, e, f, g, h\}$ — grupa symetrii kwadratu $D_4$.

Zanim przystąpimy do dalszej dyskusji zauważmy, że

$$p+t_1 = x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_3+x_3x_4+(x_1+x_2)^2 = x_1x_2+x_3x_4$$

(należy skorzystać z tego, że $(x_1+x_2)^2 = -(x_1+x_2)(x_3+x_4)$). Symbolem $\Delta_1$ oznaczać będziemy wyróżnik wielomianu:

$$x^2-(p+t_1)x+r, \tag{5}$$

tzn.

$$\Delta_1 = (p+t_1)^2-4r.$$

Pierwiastkami wielomianu (5) są oczywiście $x_1x_2$ i $x_3x_4$.

(a) *Grupą Galois wielomianu $f$ jest grupa* (*) *wtedy i tylko wtedy, gdy* $x_1x_2 \in K$.

Istotnie, jeśli grupą Galois wielomianu $f$ jest grupa (*), to ponieważ element $x_1x_2$ jest niezmienniczy ze względu na wszystkie permutacje należące do niej, więc należy on do ciała $K$.

Odwrotnie, jeśli $x_1x_2 \in K$ i grupą Galois wielomianu $f$ nie jest grupa (*), to musi nią być jedna z grup (**) albo (***). W obu przypadkach musi wówczas zachodzić równość $x_1x_2 = x_3x_4$. Ponieważ jednocześnie $x_1+x_2 = (-x_3)+(-x_4)$, więc $x_1 = -x_3$ lub $x_1 = -x_4$. Zatem rezolwenta ma oprócz pierwiastka $t_1 = (x_1+x_2)^2$ jeszcze jeden pierwiastek w ciele $K$, a mianowicie $(x_1+x_3)^2$ lub $(x_1+x_4)^2$. Jeśli więc $x_1x_2 \in K$, to grupą Galois wielomianu $f$ jest grupa (*). Zauważmy teraz, że $x_1x_2 \in K$ wtedy i tylko wtedy, gdy $\sqrt{\Delta_1} \in K$.

Istotnie, jeśli $\sqrt{\Delta_1} \in K$, to wielomian (5) ma pierwiastki w ciele $K$, tzn. $x_1x_2 \in K$. Odwrotnie, jeśli $x_1x_2 \in K$, to $x_3x_4 \in K$, czyli wielomian (5) ma pierwiastki w $K$, tzn. jego wyróżnik jest kwadratem elementu ciała $K$.

Tak więc jeśli rezolwenta ma tylko jeden pierwiastek w ciele $K$ i $\sqrt{\Delta_1} \in K$, to grupą Galois wielomianu $f$ jest grupa $V_4$.

(b) *Grupą Galois wielomianu $f$ jest grupa (**) wtedy i tylko wtedy, gdy* $x_1x_2 \in K(\sqrt{\Delta}) \setminus K$.

Konieczność tego warunku wynika stąd, że $x_1x_2$ jest niezmiennicze ze względu na permutacje parzyste należące do grupy (**) i nie jest niezmiennicze ze względu na wszystkie permutacje. Gdyby bowiem $x_1x_2$ było niezmiennicze ze względu na pozostałe permutacje, to mielibyśmy $x_1x_2 = x_3x_4$ i podobnie jak w przypadku (a) uzyskalibyśmy sprzeczność.

Załóżmy, że $x_1x_2 \in K(\sqrt{\Delta}) \setminus K$. Grupą Galois wielomianu $f$ nie może być wówczas ani grupa (*), ani grupa (***).

Istotnie, gdyby grupą Galois wielomianu $f$ była grupa (*), to mielibyśmy $x_1x_2 \in K$. Gdyby natomiast grupą Galois wielomianu $f$ była grupa (***), to ponieważ permutacja $e$ jest parzysta, więc mielibyśmy $x_1x_2 = x_3x_4$, co, jak już wiemy, prowadzi do sprzeczności. Tak więc, jeśli $x_1x_2 \in K(\sqrt{\Delta}) \setminus K$, to grupą Galois wielomianu $f$ jest grupa (**).

Podobnie jak w (a) rozważmy wielomian (5). Warunek $x_1x_2 \in K(\sqrt{\Delta}) \setminus K$ jest równoważny warunkowi $\sqrt{\Delta_1/\Delta} \in K$. Istotnie, $x_1x_2 \in K(\sqrt{\Delta}) \setminus K$ wtedy i tylko wtedy, gdy $K(\sqrt{\Delta}) = K(x_1x_2)$. Ta równość ma z kolei miejsce wtedy i tylko wtedy, gdy wyróżniki wielomianów minimalnych dla $\sqrt{\Delta}$ i $x_1x_2$ nad $K$ różnią się czynnikiem, który jest kwadratem w ciele $K$. Wyróżnikami tymi są odpowiednio $4\Delta$ i $\Delta_1$, tzn. $\sqrt{\Delta_1/\Delta} \in K$.

Tak więc, jeśli rezolwenta ma tylko jeden pierwiastek w ciele $K$ i $\sqrt{\Delta_1/\Delta} \in K$, to grupą Galois wielomianu $f$ jest grupa $C_4$.

Z przeprowadzonych rozważań wynika, że

(c) *jeśli nie zachodzą przypadki* (a) *i* (b), *to grupą Galois wielomianu $f$ jest grupa* (***).

Tak więc, jeśli rezolwenta ma tylko jeden pierwiastek w ciele $K$, $\sqrt{\Delta_1} \notin K$ i $\sqrt{\Delta_1/\Delta} \notin K$, to grupą Galois wielomianu $f$ jest grupa $D_4$.

**5. Przypadek III.** Ponieważ $t_1, t_2, t_3, \in K$, więc do grupy Galois wielomianu $f$ mogą należeć tylko takie permutacje, które zachowują elementy $t_1, t_2, t_3$. Z założenia, że wielomian $f$ nie ma pierwiastków wielokrotnych wynika, że permutacjami takimi są:

$$a = (1), \quad b = (1,2)(3,4), \quad c = (1,3)(2,4), \quad d = (1,4)(2,3).$$

Permutacje te tworzą grupę czwórkową, która zawiera trzy podgrupy rzędu drugiego:

(*') $\{a, b\}$ lub $\{a, c\}$ lub $\{a, d\}$ — grupy cykliczne $C_2$,

(**') $\{a, b, c, d\}$ — grupa czwórkowa $V_4$.

W dyskusji tego przypadku istotną rolę odgrywać będą wyróżniki $\Delta_i$ $(i = 1, 2, 3)$ wielomianów:

$$x^2-(p+t_i)x+r \quad (i = 1, 2, 3).$$

Pierwiastkami tych wielomianów są odpowiednio $x_1x_2$ i $x_3x_4$, $x_1x_3$ i $x_2x_4$, $x_1x_4$ i $x_2x_3$.

(a′) *Grupą Galois wielomianu f jest jedna z grup* (*′) *wtedy i tylko wtedy, gdy odpowiednio* $x_1+x_2, x_1x_2 \in K$ *lub* $x_1+x_3, x_1x_3 \in K$, *lub* $x_1+x_4, x_1x_4 \in K$.

Konieczność warunku jest oczywista. Dla dowodu dostateczności zauważmy, że grupa (**′) nie spełnia żadnego z tych warunków. Gdyby bowiem dla grupy (**′) był spełniony np. pierwszy warunek, tzn. $x_1+x_2$, $x_1x_2 \in K$, to mielibyśmy $x_1+x_2 = x_3+x_4$ i $x_1x_2 = x_3x_4$. Stąd $x_1 = x_3$ lub $x_1 = x_4$, co z założenia nie zachodzi. Z kolei zauważmy (tj. w przypadku IIa), że warunki $x_1x_2 \in K$, $x_1x_3 \in K$, $x_1x_4 \in K$ są odpowiednio równoważne warunkom $\sqrt{\Delta_1} \in K$, $\sqrt{\Delta_2} \in K$, $\sqrt{\Delta_3} \in K$.

Ponieważ $x_1+x_2$, $x_1+x_3$, $x_1+x_4$ są odpowiednio równe (z dokładnością do znaku) $\sqrt{t_1}$, $\sqrt{t_2}$, $\sqrt{t_3}$, więc grupą Galois wielomianu $f$ jest jedna z grup (*′) wtedy i tylko wtedy, gdy $\sqrt{\Delta_i}$, $\sqrt{t_i} \in K$ dla pewnego $i = 1, 2, 3$.

Tak więc, jeśli rezolwenta ma wszystkie pierwiastki w ciele $K$ i istnieje takie $i$, że $\sqrt{\Delta_i}$, $\sqrt{t_i} \in K$, to grupą Galois wielomianu $f$ jest grupa $C_2$.

Z przeprowadzonych rozważań wynika, że

(b′) *jeśli nie zachodzi przypadek* (a), *to grupą Galois wielomianu f jest grupa* (**′).

Tak więc, jeśli rezolwenta ma wszystkie pierwiastki w ciele $K$ i dla każdego $i = 1, 2, 3$ $\sqrt{t_i}$ lub $\sqrt{\Delta_i}$ nie należy do $K$, to grupą Galois wielomianu $f$ jest grupa $V_4$.

Uzyskane wyniki ilustruje tabela 1.

Na zakończenie podamy zapowiedziany we wstępie przykład ilustrujący zastosowania uzyskanych wyników. Pochodzi on od A. Schinzla.

Jak wiadomo, wielomian $x^4+1$ jest nierozkładalny nad ciałem liczb wymiernych, mimo że dla każdej liczby pierwszej $p$ jest rozkładalny modulo $p$ (tzn. jest rozkładalny nad ciałem skończonym $Z_p$). Okazuje się, że przeprowadzone rozważania pozwalają rozstrzygnąć, czy dowolny wielomian stopnia czwartego o współczynnikach całkowitych ma analogiczną własność, czy jej nie ma. Co więcej, podana tabela pozwala konstruować wielomiany, które mają tę własność.

Na mocy twierdzenia Frobeniusa ([2], str. 151) dla każdej permutacji pierwiastków należącej do grupy Galois danego wielomianu o współczynnikach całkowitych istnieje nieskończenie wiele takich liczb pierwszych $p$, że dany wielomian modulo $p$ rozkłada się na czynniki nierozkładalne, których stopnie są odpowiednio równe długościom cykli, na które

TABELA 1

Oznaczenia:

$K$ — ciało o charakterystyce 0;
$f = x^4+px^2+qx+r$; $p,q,r \in K$;
Pierwiastki wielomianu $f$: $x_1, x_2, x_3, x_4$;
Rezolwenta wielomianu $f$: $r(f) = t^3+2pt^2+(p^2-4r)\,t-q^2$;
Pierwiastki rezolwenty: $t_1, t_2, t_3$;
Wyróżnik rezolwenty: $\Delta = 16p^2r-4p^3q^2-128p^2r^2+144pq^2r+256r^3-27q^4$;
$\Delta_i = (p+t_i)^2-4r \quad (i = 1, 2, 3)$.

Założenia:

Wielomian $f$ nie ma pierwiastków w ciele $K$ i nie ma pierwiastków wielokrotnych.

| $K(x_1, x_2, x_3, x_4)/K$ | Rezolwenta nie ma pierwiastków w ciele $K$ | | Rezolwenta ma tylko jeden pierwiastek $t_i$ w ciele $K$ | | | Rezolwenta ma wszystkie pierwiastki w ciele $K$ | |
|---|---|---|---|---|---|---|---|
| | $\sqrt{\Delta} \in K$ | $\sqrt{\Delta} \notin K$ | $\sqrt{\Delta_i} \in K$ | $\sqrt{\frac{\Delta_i}{\Delta}} \in K$ | $\sqrt{\frac{\Delta_i}{\Delta}} \notin K$ | Istnieje $i$ takie, że $\sqrt{t_i}$, $\sqrt{\Delta_i} \in K$ | Dla każdego $i$ $\sqrt{t_i}$ lub $\sqrt{\Delta_i} \notin K$ |
| Stopień rozszerzenia | 12 | 24 | 4 | 4 | 8 | 2 | 4 |
| Grupa Galois | $A_4$ | $S_4$ | $V_4$ | $C_4$ | $D_4$ | $C_2$ | $V_4$ |
| Przykład nad $Q$ | $x^4+x+\frac{3}{4}$ | $x^4-2x-2$ | $x^4-4$ | $x^4+2x+\frac{1}{2}$ | $x^4-2$ | $x^4-10x^2+16$ | $x^4+1$ |

rozkłada się ta permutacja. Jeśli więc grupa Galois danego wielomianu stopnia czwartego zawiera cykl długości 4, to dla nieskończenie wielu liczb pierwszych $p$ wielomian ten modulo $p$ jest nierozkładalny. Z przeprowadzonych rozważań wynika, że jedynie wielomiany nierozkładalne stopnia czwartego, których grupą Galois jest grupa czwórkowa $V_4$ mogą być rozkładalne dla każdej liczby pierwszej $p$ (wszystkie inne z występujących grup dla wielomianów nierozkładalnych stopnia czwartego zawierają cykl długości 4). Z drugiej strony widzimy, że ma to miejsce w dwóch przypadkach — wtedy, gdy wielomian spełnia warunki podane w trzeciej albo w ostatniej pionowej rubryce tabeli. Jeśli wielomian spełnia warunki podane w trzeciej rubryce, to — jak wynika z rozważań w przypadku IIa — jest on rozkładalny nad ciałem liczb wymiernych, jeśli natomiast spełnia on warunki podane w ostatniej rubryce, to — jak

wynika z rozważań w przypadku III — jest on nad tym ciałem nierozkładalny. Tak więc jeśli wielomian stopnia czwartego o współczynnikach całkowitych jest rozkładalny modulo $p$ dla każdej liczby pierwszej $p$ i nierozkładalny nad ciałem liczb wymiernych, to musi on spełniać warunki podane w ostatniej rubryce tabeli. Okazuje się, że twierdzenie odwrotne jest również prawdziwe. Istotnie, załóżmy, że wielomian stopnia czwartego o współczynnikach całkowitych spełnia warunki podane w ostatniej rubryce tabeli. Jak stwierdziliśmy, wielomian ten jest nierozkładalny nad ciałem liczb wymiernych. Gdyby był on nierozkładalny nad ciałem $Z_p$ dla pewnej liczby pierwszej $p$, to jego grupą Galois nad tym ciałem byłaby grupa cykliczna (bowiem grupą Galois każdego rozszerzenia ciała skończonego jest grupa cykliczna) rzędu 4. Z twierdzenia Dedekinda ([3] str. 198) wynika, że ta grupa cykliczna jest izomorficzna z podgrupą grupy Galois rozważanego wielomianu nad ciałem liczb wymiernych. Ponieważ grupa czwórkowa nie zawiera oczywiście podgrupy izomorficznej z grupą cykliczną rzędu 4, więc przypuszczenie, że rozważany wielomian jest dla pewnej liczby pierwszej $p$ nierozkładalny modulo $p$, prowadzi do sprzeczności.

Można łatwo przeliczyć, że jeśli $a$ i $b$ są liczbami całkowitymi takimi, że $\sqrt{a}, \sqrt{b} \notin Q$, to wielomian $x^4+2(a+b)x^2+(a-b)^2$ ma rozważaną własność, tzn. jest nierozkładalny nad ciałem liczb wymiernych i dla każdej liczby pierwszej $p$ jest rozkładalny modulo $p$.

## Prace cytowane

[1] G. Birkhoff, S. MacLane, *Przegląd algebry współczesnej*, Warszawa 1966.

[2] H. Mann, *Introduction to algebraic number theory*, Columbus 1956.

[3] A. Mostowski, M. Stark, *Algebra wyższa*, tom III, Warszawa 1967.

[4] М. М. Постников, *Теория Галуа*, Москва 1963.

[5] Д. Селиванов, *Об уравнениях пятой степени с целыми коэффициентами*, Ст. Петербург 1889.