PIERŚCIENIE I CIAŁA
Wykład 13

Wielomiany rozdzielcze

Z wykładu 12 wiemy, że jeżeli wielomianu $f \in K[x]$ ma parami różne pierwiastki i E jest ciałem jego rozkładu, to $\operatorname{rz}\operatorname{Aut}(E/K) = (E : K)$, a więc E jest rozszerzeniem Galois ciała K. Istotne jest tu założenie, że pierwiastki wielomianu są parami różne. Mówimy, że wielomian nierozkładalny $f \in K[x]$ jest ***rozdzielczy***, jeśli nie ma pierwiastków wielokrotnych w swoim ciele rozkładu, czyli jego pierwiastki są parami różne.

Twierdzenie 1. *Niech K będzie ciałem.*

(1) *Jeżeli* $\operatorname{char} K = 0$*, to każdy nierozkładalny wielomian $f \in K[x]$ jest rozdzielczy.*

(2) *Jeżeli* $\operatorname{char} K = p > 0$*, to nierozkładalny wielomian $f \in K[x]$ nie jest rozdzielczy wtedy i tylko wtedy, gdy*

$$f(x) = b_0 + b_1 x^p + b_2 x^{2p} + ... + b_n x^{np} \tag{1}$$

dla pewnych $b_0, b_1, b_2, ..., b_n \in K$.

Dowód. Załóżmy, że wielomian

$$f(x) = a_0 + a_1 x + ... + a_m x^m \in K[x]$$

jest nierozkładalny. Wielomian f nie jest rozdzielczy gdy ma w ciele rozkładu E pierwiastek wielokrotny $a \in E$, co jest równoważne temu, że $f'(a) = 0$. Ale f jest wielomianem nierozkładalnym, więc różni się ewentualnie jedynie stałym czynnikiem od wielomianu minimalnego elementu a. Zatem $\operatorname{st} f = m$ jest najmniejszym stopniem niezerowego wielomianu, którego pierwiastkiem jest a. Ponieważ $f'(a) = 0$ i $\operatorname{st} f' < \operatorname{st} f = m$, więc $f' = 0$. Ale

$$f'(x) = a_1 + 2 \cdot a_2 x + ... + m \cdot a_m x^{m-1},$$

więc równość $f'(x) = 0$ oznacza, że $k \cdot a_k = 0$ dla każdego $k = 1, 2, ..., m$. Jeżeli $\operatorname{char} K = 0$, to dostajemy $a_k = 0$ dla $k = 1, 2, ..., m$, czyli f jest wielomianem stałym, co jest sprzeczne z założeniem, że f jest nierozkładalny.

Jeżeli $\operatorname{char} K = p$ i p dzieli k, to $k \cdot a = 0$ dla każdego $a \in K$. Zatem z równości $k \cdot a_k = 0$ dla $k = 1, 2, ..., m$ wynika, że $a_k = 0$ dla k, które nie są wielokrotnościami p, zaś a_{kp}, czyli współczynniki przy x^{kp} nie muszą być zerami. Stąd f ma postać (1). □

Jeżeli $\operatorname{char} K = p > 0$, to istnieją wielomiany nierozkładalne w $K[x]$, które nie są rozdzielcze.

Uwaga 1. Niech K, L będą ciałami i $f : K \to L$ będzie homomorfizmem. Wtedy f jest funkcją różnowartościową. Rzeczywiście, jeśli $f(a) = f(b)$, dla $a, b \in K$, to $a = b$, bo gdyby $a \neq b$, to $a - b \neq 0$ więc istniałby element odwrotny $(a - b)^{-1}$. Z równości $f(a) = f(b)$ dostajemy

$$f(a - b) = f(a) - f(b) = 0$$

i mnożąc obie strony przez $f((a - b)^{-1})$ mamy

$$0 = f(a - b) f((a - b)^{-1}) = f((a - b)(a - b)^{-1}) = f(1) = 1.$$

Sprzeczność ta pokazuje, że $a = b$.

Niech K będzie ciałem skończonym i $\operatorname{char} K = p$. Wtedy p jest liczbą pierwszą. Funkcję $\theta : K \to K$ zdefiniowaną wzorem

$$\theta(a) = a^p \tag{2}$$

dla $a \in K$ nazywamy automorfizmem Frobeniusa. Aby uzasadnić tę nazwę sprawdzimy, że θ jest automorfizmem. Ponieważ $\operatorname{char} K = p$, więc dla $a, b \in K$ mamy

$$\theta(a+b) = (a+b)^p = a^p + b^p = \theta(a) + \theta(b). \tag{3}$$

Ponadto

$$\theta(ab) = (ab)^p = a^p b^p = \theta(a)\theta(b)$$

oraz $\theta(0) = 0$, $\theta(1) = 1$. Zatem θ jest homomorfizmem.

Z uwagi 1 wynika, że θ jest funkcją różnowartościową. Zatem obraz $\theta(K)$ ma tyle samo elementów co K, którego jest podzbiorem. Stąd $\theta(K) = K$.

Ponieważ $\theta(K) = K$ i θ jest funkcją różnowartościową, więc dla każdego $a \in K$ istnieje dokładnie jedno $c \in K$ takie, że $c^p = \theta(c) = a$, czyli c jest pierwiastkiem stopnia p z a.

Twierdzenie 2. *Jeżeli K jest ciałem skończonym, to każdy wielomian nierozkładalny $f \in K[x]$ jest rozdzielczy.*

Dowód. Ponieważ K jest ciałem skończonym, więc $\operatorname{char} K = p > 0$ jest liczbą pierwszą. Załóżmy, że istnieje nierozkładalny wielomian $f \in K[x]$, który nie jest rozdzielczy. Z twierdzenia 1 wiemy, że f ma postać

$$f(x) = b_0 + b_1 x^p + b_2 x^{2p} + ... + b_n x^{np} \tag{4}$$

dla pewnych $b_0, b_1, b_2, ..., b_n \in K$. Dla każdego k w ciele K istnieje c_k takie, że $c_k^p = b_k$. Zatem

$$\begin{aligned} f(x) &= c_0^p + c_1^p x^p + c_2^p x^{2p} + ... + c_n^p x^{np} = c_0^p + (c_1 x)^p + (c_2 x^2)^p + ... + (c_n x^n)^p = \\ &= (c_0 + c_1 x + c_2 x^2 + ... + c_n x^n)^p, \end{aligned}$$

co jest sprzeczne z nierozkładalnością f. □

Pierwiastki z 1

Niech K będzie ciałem. Pierwiastkiem stopnia n z 1 nazywamy dowolny pierwiastek wielomianu $f(x) = x^n - 1 \in K[x]$. Jest to więc taki element $a \in K$, dla którego $a^n = 1$. Wszystkie takie pierwiastki są elementami ciała rozkładu E wielomianu f będącego rozszerzeniem ciała K.

Niech $K = \mathbb{F}_q$ będzie q-elementowym ciałem skończonym. Wtedy $q = p^n$ dla pewnej liczby pierwszej p i $n \in \mathbb{N}$. Z dowodu twierdzenia 10, wykład 10, wiemy, że K jest izomorficzne z ciałem rozkładu wielomianu

$$f(x) = x^q - x = x(x^{q-1} - 1) \in \mathbb{Z}_p[x]$$

i każdy niezerowy element ciała K jest pierwiastkiem wielomianu $x^{q-1} - 1$. Widzimy zatem, że każdy niezerowy element ciała skończonego jest pierwiastkiem z 1.

Dla dowolnego ciała K niech U_n oznacza zbiór wszystkich pierwiastków stopnia n z 1 należących do K. Zatem

$$U_n = \{a \in K : a^n = 1\}.$$

Jeżeli $a, b \in U_n$, to

$$(ab)^n = a^n b^n = 1,$$

więc $a, b \in U_n$. Ponadto $(a^{-1})^n = (a^n)^{-1} = 1$, czyli $a^{-1} \in U_n$. Widzimy więc, że U_n z mnożeniem jest podgrupą grupy $(K^*, \cdot)$, gdzie $K^* = K \setminus \{0\}$.

Twierdzenie 3. *Niech K będzie ciałem i $K^* = K \setminus \{0\}$. Każda skończona podgrupa G grupy $(K^*, \cdot)$ jest grupą cykliczną.*

Dowód. Niech $a \in G$ będzie elementem o największym rzędzie spośród wszystkich elementów grupy G. Wykażemy, że a jest generatorem grupy G, czyli dowolny element $b \in G$ różny od 1 można zapisać jako $b = a^l$ dla pewnego $l \in \mathbb{N}$.

Niech $\operatorname{rz} a = N$ i załóżmy, że $\operatorname{rz} b = n$ nie dzieli N. Wtedy $m = \mathrm{NWD}(n, N) \neq n$, więc $p = \frac{n}{m} > 1$. Ponadto liczba p jest względnie pierwsza z N i $\operatorname{rz} b^m = p$. Zatem rzędy elementów a i b^m są względnie pierwsze, a stąd

$$\operatorname{rz}(ab^m) = \operatorname{rz} a \operatorname{rz} b^m = Np.$$

Zatem ab^m ma rząd $Np > N$, co jest sprzeczne z założeniem, że a ma największy rząd w grupie G.

Widzimy więc, że n dzieli N. Elementy $a_k = a^{k\frac{N}{n}}$ dla $k = 0, 1, ..., n-1$ są parami różne i $a_k^n = a^{kN} = 1$, więc są to pierwiastki wielomianu $f = x^n - 1$. Zatem $a_0, a_1, ..., a_{n-1}$ są wszystkimi pierwiastkami tego wielomianu. Ale $b^n = 1$, czyli również b jest pierwiastkiem wielomianu f. Stąd $b = a_k = a^{k\frac{N}{n}}$ dla pewnego k. □

Wszystkich pierwiastków stopnia n z 1 jest skończenie wiele. Z twierdzenia 3 wynika więc następujący wniosek.

Wniosek 1. *Niech K będzie ciałem i niech U_n oznacza zbiór wszystkich pierwiastków stopnia n z 1 należących do K. Wtedy $(U_n, \cdot)$ jest grupą cykliczną.*

Generatory grupy U_n nazywamy pierwiastkami pierwotnymi z 1. Dla wielomianu $f(x) = x^n - 1 \in K[x]$ mamy $f'(x) = nx^{n-1}$, więc jeśli $\operatorname{char} K = 0$, to f i f' nie mają wspólnych pierwiastków i w konsekwencji f nie ma pierwiastków wielokrotnych. W ciele rozkładu E wielomianu f istnieje zatem n różnych pierwiastków $\omega_0 = 1, \omega_1, ..., \omega_{n-1}$ stopnia n z 1.

Równania wielomianowe rozwiązalne przez pierwiastniki

Niech E będzie rozszerzeniem ciała K i $n \in \mathbb{N}$, $n > 1$. Mówimy, że $a \in E$ jest pierwiastkiem stopnia n z $b \in K$, jeśli $a^n = b$. Oznacza to, że a jest pierwiastkiem wielomianu $f(x) = x^n - b$.

Jeśli c jest jednym z pierwiastków f i ω jest pierwiastkiem pierwotnym stopnia n z 1 w pewnym rozszerzeniu ciała K, to

$$(c\omega^l)^n = c^n \omega^{nl} = c^n = b,$$

więc $c, c\omega, c\omega^2, ..., c\omega^{n-1}$ są wszystkimi pierwiastkami wielomianu f. Stąd $K(c, \omega)$ jest ciałem rozkładu wielomianu f.

Twierdzenie 4. *Jeżeli ciało K zawiera pierwiastek pierwotny stopnia n z 1 i E jest ciałem rozkładu wielomianu $f(x) = x^n - b \in K[x]$, to grupa $\operatorname{Aut}(E/K)$ jest cykliczna.*

Dowód. Niech $\omega \in K$ będzie pierwiastkiem pierwotnym stopnia n z 1 i c będzie jednym z pierwiastków wielomianu f w pewnym rozszerzeniu ciała K. Ponieważ $\omega \in K$, więc $K(c)$ jest ciałem rozkładu f, czyli $E = K(c)$ i $\phi(\omega) = \omega$ dla każdego $\phi \in \mathrm{Aut}(E/K)$.

Jeżeli $\phi \in \mathrm{Aut}(E/K)$, to $\phi(c)$ jest pierwiastkiem f, więc $\phi(c) = c\omega^k$ dla pewnego $k \in \{0, 1, ..., n-1\}$ i ϕ jest jednoznacznie wyznaczone przez $\phi(c)$. Zatem oznaczając przez U_n grupę wszystkich pierwiastków stopnia n z 1 otrzymujemy funkcję różnowartościową $F : \mathrm{Aut}(E/K) \to U_n$, która automorfizmowi $\phi \in \mathrm{Aut}(E/K)$ przyporządkowuje $F(\phi) = \omega^k$, gdzie $\phi(c) = c\omega^k$.

Ponadto funkcja F jest homomorfizmem, gdyż jeśli $\phi, \psi \in \mathrm{Aut}(E/K)$ i $\phi(c) = c\omega^k$, $\psi(c) = c\omega^l$, to

$$\phi(\psi(c)) = \phi(c\omega^l) = \phi(c)\phi(\omega)^l = c\omega^k\omega^l,$$

co oznacza, że

$$F(\phi \circ \psi) = \omega^k\omega^l = F(\phi)F(\psi).$$

Zatem grupa $\mathrm{Aut}(E/K)$ jest izomorficzna z podgrupą $F(\mathrm{Aut}(E/K))$ grupy cyklicznej U_n i w konsekwencji $\mathrm{Aut}(E/K)$ jest grupą cykliczną. □

Przypomnijmy, że rozszerzenie E ciała K jest rozszerzeniem Galois, gdy

$$K = \mathrm{Fix}(E, \mathrm{Aut}(E/K)).$$

Twierdzenie 5 (Galois)**.** *Niech L będzie skończonym rozszerzeniem Galois ciała K i E będzie ciałem takim, że $K \subset E \subset L$. Ciało E jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy grupa* $\mathrm{Aut}(L/E)$ *jest dzielnikiem normalnym grupy* $\mathrm{Aut}(L/K)$*. Wówczas* $\mathrm{Aut}(E/K)$ *jest izomorficzna z grupą ilorazową* $\mathrm{Aut}(L/K)/\mathrm{Aut}(L/E)$*.*

Niech E będzie rozszerzeniem ciała K. Rozszerzeniem dwumianowym ciała K nazywamy rozszerzenie postaci $K(a)$, gdzie a jest n-tym pierwiastkiem z b dla pewnego $b \in K$ i $n \in \mathbb{N}$, $n > 1$.

Niech E będzie rozszerzeniem ciała K. Mówimy, że element $a \in E$ ***wyraża się przez pierwiastniki*** nad K, jeżeli istnieje ciąg rozszerzeń

$$K = K_0 \subset K_1 \subset ... \subset K_n \tag{5}$$

taki, że K_{m+1} jest dwumianowym rozszerzeniem ciała K_m dla $m = 0, ..., n-1$ i $a \in K_n$. Zatem $K_{m+1} = K_m(c)$, gdzie c jest pierwiastkiem wielomianu postaci $f(x) = x^{p_m} - b$, gdzie $p_m \in \mathbb{N}$ oraz $b \in K_m$. Dołączając do K_m pierwiastek pierwotny stopnia p_m z 1 i stosując twierdzenie 4 możemy zastąpić wyjściowy ciąg rozszerzeń (5) przez ciąg, dla którego $\mathrm{Aut}(K_{m+1}/K_m)$ są grupami cyklicznymi.

Twierdzenie 6.
1) Jeżeli $K = K_0 \subset K_1 \subset ... \subset K_n$ jest jak wyżej i $a \in K_n$, to każdy element $b \in K(a)$ wyraża się przez pierwiastniki nad K.
2) Jeżeli a^k, gdzie $k \in \mathbb{Z} \setminus \{0\}$ wyraża się przez pierwiastniki, to a wyraża się przez pierwiastniki nad K.

Dowód. 1) Mamy $K \subset K_n$ i $a \in K_n$, a więc $K(a) \subset K_n$. Jeżeli więc $b \in K(a)$, to $b \in K_n$, czyli b wyraża się przez pierwiastniki nad K.

2) Załóżmy, że $k > 0$ i niech $K = K_0 \subset K_1 \subset ... \subset K_n$ będzie ciągiem rozszerzeń dwumianowych takich, że $a^k \in K_n$. Oczywiście a jest pierwiastkiem wielomianu $f(x) =$

$x^k - a^k \in K_n[x]$. Zatem $K_n(a)$ jest rozszerzeniem dwumianowym ciała K_n i wystarczy do naszego ciągu rozszerzeń dołączyć $K_{n+1} = K_n(a)$. Jeżeli $k < 0$, to zamiast a^k rozważamy $a^{-k} \in K_n$. □

Niech a będzie elementem algebraicznym nad ciałem K. Mówimy, że a ma stopień n, jeśli wielomian minimalny $f \in K[x]$ ma stopień n.

Niech $z \in \mathbb{C}$ będzie liczbą algebraiczną stopnia 2. Zatem z jest pierwiastkiem wielomianu stopnia 2 o współczynnikach wymiernych, czyli wielomianu postaci

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

gdzie $a, b, c \in \mathbb{Q}$. Jak wiemy

$$z = \frac{-b \pm \sqrt{\Delta}}{2a},$$

gdzie $\Delta = b^2 - 4ac$. Liczba $\sqrt{\Delta}$ jest pierwiastkiem wielomianu $x^2 - \Delta \in \mathbb{Q}[x]$, więc $\mathbb{Q}\left(\sqrt{\Delta}\right)$ jest rozszerzeniem dwumianowym ciała $\mathbb{Q}$. Ponieważ $z \in \mathbb{Q}\left(\sqrt{\Delta}\right)$, więc pierwiastek z wyraża się przez pierwiastniki nad ciałem $\mathbb{Q}$, do którego należą współczynniki wielomianu. Ciało $\mathbb{Q}$ można tutaj zastąpić przez dowolne ciało K charakterystyki 0.

Z wykładów 1 i 2 wiemy, że istnieją wzory pozwalające rozwiązać równania trzeciego i czwartego stopnia, w których również pojawiają się pierwiastki (odpowiednio trzeciego i czwartego stopnia) z wyrażeń algebraicznych zawierających współczynniki wielomianów. Pokazuje to, że pierwiastki takich równań również wyrażają się przez pierwiastniki nad ciałem $\mathbb{Q}$. Także w tym przypadku ciało $\mathbb{Q}$ można tutaj zastąpić przez dowolne ciało K charakterystyki 0.

Mając dany ciąg rozszerzeń

$$K = K_0 \subset K_1 \subset ... \subset K_n$$

taki, że K_{m+1} jest dwumianowym rozszerzeniem ciała K_m i $\mathrm{Aut}(K_{m+1}/K_m)$ jest grupą cykliczną otrzymujemy ciąg grup

$$\{I\} = \mathrm{Aut}(K_n/K_n) \subset \mathrm{Aut}(K_n/K_{n-1}) \subset ... \subset \mathrm{Aut}(K_n/K),$$

i z twierdzenia 5 wynika, że dla każdego $m = 0, 1, ..., n-1$ grupa $\mathrm{Aut}(K_{m+1}/K_m)$ jest izomorficzna z grupą ilorazową $\mathrm{Aut}(K_n/K_m)/\mathrm{Aut}(K_n/K_{m+1})$.

Zatem $\mathrm{Aut}(K_n/K_m)/\mathrm{Aut}(K_n/K_{m+1})$ jest grupą cykliczną. W ten sposób badanie, czy $a \in K_n$ wyraża się przez pierwiastniki nad K można sprowadzić do badania, czy grupa $\mathrm{Aut}(K_n/K)$ jest rozwiązalna.

Niech $f \in K[x]$ i $E \supset K$ będzie ciałem rozkładu wielomianu f. Grupę $\mathrm{Aut}(E/K)$ nazywamy ***grupą Galois wielomianu*** f.

Wielomianowi $f \in K[x]$ odpowiada grupa automorfizmów $\mathrm{Aut}(E/K)$, gdzie $E = K(a_1, a_2, ..., a_n)$ jest ciałem rozkładu wielomianu f, czyli $a_1, a_2, ..., a_n \in E$ są pierwiastkami f. Z twierdzenia 6, wykład 12 wynika, że dla dowolnego automorfizmu $\phi \in \mathrm{Aut}(E/K)$ obraz pierwiastka wielomianu f jest pierwiastkiem f, więc jeśli f ma jedynie pierwiastki jednokrotne, czyli $a_i \neq a_j$ dla $i \neq j$, to zbiór $\{\phi(a_1), \phi(a_2), ..., \phi(a_n)\}$ powstaje przez permutację zbioru $\{a_1, a_2, ..., a_n\}$. W tym przypadku $\mathrm{Aut}(E/K)$ można więc utożsamiać z pewną podgrupą grupy permutacji S_n. Pozwala to przenieść problem, czy pierwiastki wielomianu f wyrażają się przez pierwiastniki nad K na grunt teorii grup.

Twierdzenie 7. *Załóżmy, że K jest ciałem o charakterystyce 0 i wielomian $f \in K[x]$,* $\operatorname{st} f \geqslant 1$ *ma jedynie pierwiastki jednokrotne. Wówczas równanie $f(x) = 0$ jest rozwiązalne przez pierwiastniki nad K, tj. pierwiastki f wyrażają się przez pierwiastniki nad K wtedy i tylko wtedy, gdy grupa Galois wielomianu f jest rozwiązalna.*

W przypadku ciała o charakterystyce 0, dzieląc wielomian f przez $\mathrm{NWD}(f, f')$ możemy zastąpić f przez wielomian, który ma takie same pierwiastki jak f, ale jednokrotne, więc założenie o jednokrotności pierwiastków f w twierdzeniu 7 nie jest bardzo ograniczające.

Grupę Galois wielomianu można utożsamiać z pewną podgrupą grupy permutacji S_n. Jak wiemy grupa S_n dla $n \leqslant 4$ jest rozwiązalna, więc także każda jej podgrupa jest rozwiązalna. Z twierdzenia 7 wynika zatem to, co zostało wykazane bezpośrednio: jeżeli K jest ciałem o charakterystyce 0 i $f \in K[x]$, $\operatorname{st} f \leqslant 4$, to równanie $f(x) = 0$ jest rozwiązalne przez pierwiastniki nad K.

Wzory na rozwiązania równań 2, 3 i 4 stopnia pokazują, jakiego stopnia pierwiastki występują w tych rozwiązaniach. Na przykład dla wielomianu stopnia 2 mamy pierwiastek kwadratowy. Dla ciał o charakterystyce większej od 0 sytuacja jest bardziej skomplikowana.

Przykład 1. Niech $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Mamy $f(0) = f(1) = 1$, więc wielomian f nie ma pierwiastków w $\mathbb{Z}_2$, a zatem jest nierozkładalny. Niech a będzie pierwiastkiem wielomianu f w pewnym rozszerzeniu ciała $\mathbb{Z}_2$. Ponieważ $f'(x) = 1$, więc a nie jest pierwiastkiem podwójnym i jeśli b jest drugim pierwiastkiem f, to $a + b = 1$, czyli $b = 1 - a = 1 + a$. Stąd $\mathbb{Z}_2(a)$ jest ciałem rozkładu wielomianu f.

Mamy $\mathbb{Z}_2 = \{0, 1\}$, więc jedynym niezerowym pierwiastkiem z elementu należącego do $\mathbb{Z}_2$ jest 1, zatem rozszerzenie ciała $\mathbb{Z}_2$ o ten pierwiastek jest tym samym ciałem. Ale $f(a) = 0$, czyli $a^2 + a + 1 = 0$ i mnożąc obie strony tej równości przez $a + 1$ dostajemy $a^3 + 1 = 0$, czyli $a^3 = 1$. Zatem a jest pierwiastkiem trzeciego stopnia z 1. Rozszerzenie $\mathbb{Z}_2(a)$ ciała $\mathbb{Z}_2$ o pierwiastek równania kwadratowego jest więc rozszerzeniem dwumianowym, ale o pierwiastek trzeciego stopnia.

Z twierdzenia 7 wynika też wniosek, który pozwala stwierdzić, że równanie wielomianowe $f(x) = 0$ stopnia większego niż 4 nie jest rozwiązalne przez pierwiastniki nad K.

Wniosek 2. *Jeżeli $f \in \mathbb{Q}[x]$ ma jedynie pierwiastki jednokrotne i grupa Galois wielomianu f jest izomorficzna z S_n, gdzie $n \geqslant 5$, to równanie $f(x) = 0$ nie jest rozwiązalne przez pierwiastniki nad $\mathbb{Q}$.*

Kolejne twierdzenie opisuje klasę wielomianów, których grupa Galois wielomianu f jest izomorficzna z S_n. W jego dowodzie skorzystamy z twierdzenia, które jest w pewnym sensie odwrotne do twierdzenia Lagrange'a o tym, że dla podgrupy H grupy skończonej G rząd podgrupy H dzieli rząd grupy G.

Twierdzenie 8 (Cauchy'ego)**.** *Niech G będzie grupą skończoną. Jeżeli liczba pierwsza p dzieli rzad grupy G, to istnieje element $a \in G$ rzędu p, a więc grupa G ma podgrupę cykliczną H generowaną przez a, dla której* $\operatorname{rz} H = p$.

Twierdzenie 9. *Jeżeli wielomian $f \in \mathbb{Q}[x]$ jest nierozkładalny,* $\operatorname{st} f = p > 2$ *jest liczbą pierwszą i f ma $p - 2$ różne pierwiastki rzeczywiste, to grupa Galois wielomianu f jest izomorficzna z S_p.*

Dowód. Niech $c_1, ..., c_p$ będą pierwiastkami wielomianu f. Z założenia wiemy, że $p-2$ spośród nich to liczy rzeczywiste, a pozostałe dwa należą do $\mathbb{C} \setminus \mathbb{R}$. Możemy przyjąć, że $c_1, c_2 \in \mathbb{C} \setminus \mathbb{R}$, a ponieważ f ma współczynniki rzeczywiste, więc $c_2 = \overline{c_1}$. Zatem funkcja $\phi_1(z) = \overline{z}$ jest automorfizmem ciała $E = \mathbb{Q}(c_1, ..., c_p)$ rozkładu wielomianu f takim, że $\phi_1(x) = x$ dla $x \in \mathbb{R}$, czyli $\phi_1 \in \mathrm{Aut}(E/\mathbb{Q})$.

Automorfizmy $\phi \in \mathrm{Aut}(E/\mathbb{Q})$ można utożsamiać z permutacjami zbioru $\{c_1, ..., c_p\}$, a więc również z elementami grupy S_p. Grupę $\mathrm{Aut}(E/\mathbb{Q})$ można zatem utożsamiać z podgrupą H grupy S_p. Automorfizmowi ϕ_1 odpowiada transpozycja $(1, 2)$.

Ponieważ wielomian f jest nierozkładalny, więc $(\mathbb{Q}(c_1) : \mathbb{Q}) = \mathrm{st}\, f = p$. Zatem

$$(E : \mathbb{Q}) = (E : \mathbb{Q}(c_1))(\mathbb{Q}(c_1) : \mathbb{Q}) = (E : \mathbb{Q}(c_1))p,$$

czyli $(E : \mathbb{Q})$ dzieli się przez p.

Wielomian f ma jedynie pierwiastki jednokrotne, co wobec twierdzenia 9, wykład 12 pokazuje, że E jest rozszerzeniem Galois ciała $\mathbb{Q}$ i w konsekwencji $\mathrm{rz}\,\mathrm{Aut}(E/\mathbb{Q}) = (E : \mathbb{Q})$. Zatem p dzieli $\mathrm{rz}\, H = \mathrm{rz}\,\mathrm{Aut}(E/\mathbb{Q})$. Korzystając z twierdzenia Cauchy'ego widzimy, że istnieje automorfizm $\phi \in \mathrm{Aut}(E/\mathbb{Q})$, któremu odpowiada permutacja rzędu p. Ale taka permutacja to cykl długości p. Zatem H zawiera transpozycję $(1, 2)$ i cykl długości p, co wobec twierdzenia 1, wykład 12 dowodzi, że $H = S_p$, czyli grupa $\mathrm{Aut}(E/\mathbb{Q})$ jest izomorficzna z S_p. □

Z wniosku 1, wykład 12 wiemy, że dla $p \geqslant 5$ grupa S_p nie jest rozwiązalna. Twierdzenia 7 i 9 dają nam więc następujący wniosek.

Wniosek 3. *Jeżeli wielomian $f \in \mathbb{Q}[x]$ jest nierozkładalny,* $\mathrm{st}\, f = p \geqslant 5$ *jest liczbą pierwszą i f ma $p-2$ różne pierwiastki rzeczywiste, to równanie $f(x) = 0$ nie jest rozwiązalne przez pierwiastniki nad $\mathbb{Q}$.*

Opiszemy klasę wielomianów, dla których grupa Galois jest izomorficzna z S_n. Potrzebne nam będzie następujące twierdzenie pomocnicze.

Twierdzenie 10. *Jeżeli wszystkie pierwiastki wielomianu*

$$f(x) = x^n + a_{n-3}x^{n-3} + ... + a_1x + a_0 \in \mathbb{R}[x]$$

są liczbami rzeczywistymi, to $a_0 = a_1 = ... = a_{n-3} = 0$, czyli $f(x) = x^n$.

Dowód. Załóżmy, że f ma pierwiastki $c_1, ..., c_n \in \mathbb{R}$. Ze wzorów Viete'a otrzymujemy:

$$\sum_{i=1}^{n} c_i = 0, \quad \sum_{i<j}^{n} c_ic_j = 0.$$

Stąd

$$0 = \left(\sum_{i=1}^{n} c_i\right)^2 = \sum_{i=1}^{n} c_i^2 + 2\sum_{i<j}^{n} c_ic_j = \sum_{i=1}^{n} c_i^2.$$

Ponieważ $c_1, ..., c_n$ są liczbami rzeczywistymi, więc z równości $\sum_{i=1}^{n} c_i^2 = 0$ wynika, że $c_1 = c_2 = ... = c_n = 0$. Zatem $f = x^n$. □

Twierdzenie 11. *Niech $q > 1$ będzie liczbą pierwszą i $f(x) = x^5 - 2qx - q$. Wtedy równanie $f(x) = 0$ nie jest rozwiązalne przez pierwiastniki nad $\mathbb{Q}$.*

Dowód. Liczba q dzieli wszystkie współczynniki f oprócz pierwszego i q^2 nie dzieli wyrazu wolnego, więc na mocy kryterium Eisensteina wielomian f jest nierozkładalny.

Wykażemy, że f ma trzy pierwiastki rzeczywiste. Niech $g(x) = x^4 - 2x - 1$. Wtedy $g'(x) = 4x^3 - 2 > 0$ dla $x > \frac{1}{\sqrt[3]{2}}$. Zatem g jest funkcją rosnącą w przedziale $(\frac{1}{\sqrt[3]{2}}, +\infty)$. Stąd i z nierówności $q \geqslant 2$ wynika, że $g(q) \geqslant g(2) > 0$.

Mamy $f(q) = q^5 - 2q^2 - q = qg(q)$, więc $f(q) > 0$. Ponadto

$$f(-q) = -q^5 + 2q^2 - q = -q(q^4 - 2q + 1) < -qg(q) < 0,$$

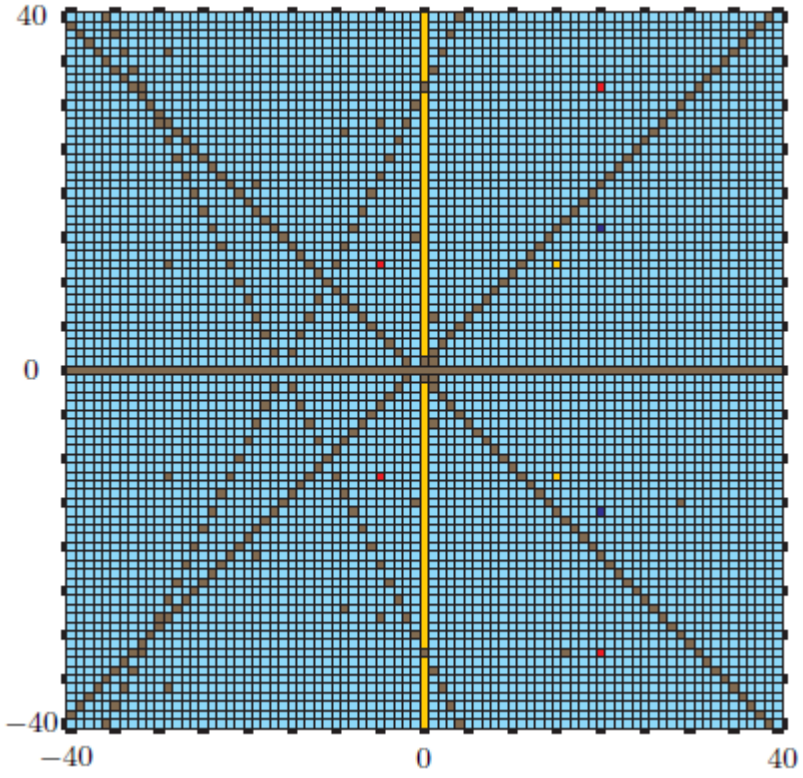
$f(-1) = -1 + q > 0$ i $f(0) = -q < 0$. Nierówności te pokazują, że f ma pierwiastek w każdym z przedziałów: $(-q, -1)$, $(-1, 0)$ i $(0, q)$.

Z twierdzenia 10 wynika, że f nie może mieć jedynie pierwiastków rzeczywistych. Zatem oprócz trzech pierwiastków rzeczywistych f ma dwa wzajemnie sprzężone pierwiastki w zbiorze $\mathbb{C} \setminus \mathbb{R}$. Stąd f ma jedynie trzy pierwiastki rzeczywiste i wniosek 3 pokazuje, że równanie $f(x) = 0$ nie jest rozwiązalne przez pierwiastniki nad $\mathbb{Q}$. □

Można powiedzieć, że dla większości wielomianów stopnia co najmniej 5 pierwiastki nie wyrażają się przez pierwiastniki nad $\mathbb{Q}$. Poniżej zostało to zilustrowane dla wielomianów postaci

$$f_{a,b}(x) = x^5 + ax + b,$$

gdzie $-40 \leqslant a, b \leqslant 40$.



Rysunek 1. Ilustracja z książki B. Everitt *Symmetries of Equations: An Introduction to Galois Theory*

Na poziomej osi mamy wartości parametru a, zaś na pionowej parametru b. Punkt (a, b) odpowiada wielomianowi $f_{a,b}$, przy czym:

- kolor brązowy oznacza, że wielomian jest rozkładalny, a więc jego pierwiastki są pierwiastkami wielomianów niższych stopni i wyrażają się przez pierwiastniki,
- kolory: żółty i czerwony oznaczają, że wielomian jest nierozkładalny, ale jego pierwiastki wyrażają się przez pierwiastniki,
- kolory: granatowy i niebieski oznaczają, że grupą Galois wielomianu jest odpowiednio A_5 i S_5, więc jego pierwiastki nie wyrażają się przez pierwiastniki.

Z ilustracji tej wynika, że dla zdecydowanej większości wielomianów $f_{a,b}$ ich pierwiastki nie wyrażają się przez pierwiastniki.