PIERŚCIENIE I CIAŁA
Wykład 12

Punkt (2) z twierdzenia 4, wykład 11 można zapisać w ogólniejszej postaci zastępując zbiór $\{1, 2, ..., n\}$ przez dowolny zbiór n-elementowy $A = \{a_1, a_2, ..., a_n\}$. Wtedy dla permutacji $\sigma \in S_n$ przez f_σ oznaczamy permutację zbioru A zdefiniowaną wzorem $f_\sigma(a_i) = a_{\sigma(i)}$, a więc polegającą na spermutowaniu indeksów. Z twierdzenia 4, wykład 11 wynika, że grupa wszystkich permutacji zbioru A jest generowana przez permutacje f_τ i f_σ, gdzie $\tau = (1, 2)$, $\sigma = (1, 2, ..., n)$.

Twierdzenie 1. *Niech $p > 1$ będzie liczbą pierwszą. Jeśli podgrupa H grupy S_p zawiera cykl długości p i dowolną transpozycję, to $H = S_p$.*

Dowód. Dowód sprowadza się do wykazania, że cykl σ długości p i dowolna transpozycja τ generują całą grupę S_p. Możemy przyjąć, że $\sigma = (a_1, a_2, ..., a_p)$ i $\tau = (a_1, a_k)$ dla pewnego $1 < k \leqslant p$.

Mamy $\sigma^{k-1}(a_1) = a_k$. Ponadto σ^{k-1} ma rząd $p = \operatorname{rz}\sigma$. Rzeczywiście $l = \operatorname{rz}\sigma^{k-1}$ jest najmniejszą liczbą naturalną taką, że $\sigma^{(k-1)l} = I$. Ale z równości $p = \operatorname{rz}\sigma$ wynika, że p dzieli $(k-1)l$. Ponieważ p jest liczbą pierwszą i $k - 1 < p$, więc p dzieli l i stąd $l = p$. Pokazuje to, że $\sigma^{k-1} = (a_1, a_k, ..., a_m)$ zawiera wszystkie liczby $1, 2, ..., p$. Zatem τ i σ^{k-1} generują całą grupę S_p. Stąd również τ i σ generują grupę S_p. □

Grupy rozwiązalne

Przypomnijmy, że podzbiór H grupy G jest podgrupą, jeśli dla dowolnych elementów $a, b \in H$ mamy

$$ab^{-1} \in H.$$

Dla podgrupy H grupy G i elementu $a \in G$ oznaczamy

$$aH = \{ab : b \in H\}, \quad Ha = \{ba : b \in H\}.$$

Zbiory te nazywamy odpowiednio warstwą lewostronną i warstwą prawostronną elementu a względem podgrupy H. Jeśli $aH = Ha$ dla każdego $a \in G$, to mówimy, że H jest dzielnikiem normalnym (albo podgrupą niezmienniczą) grupy G. Wtedy wzór

$$a \sim b \Leftrightarrow ab^{-1} \in H,$$

gdzie $a, b \in G$ definiuje relację równoważności w G zgodną z działaniem w grupie. Oznacza to, że dla dowolnych $a, b, c, d \in G$ jeżeli $a \sim b$ i $c \sim d$, to

$$ac \sim bd.$$

Dzięki temu w zbiorze G/H wszystkich klas abstrakcji, czyli warstw aH, gdzie $a \in G$ możemy określić działanie

$$(aH)(bH) = (ab)H.$$

Zbiór G/H z tym działaniem jest grupą. Jej elementem neutralnym jest $H = eH$, gdzie e jest elementem neutralnym grupy G, zaś elementem odwrotnym do aH jest $a^{-1}H$.

Dla grupy skończonej G liczbę jej elementów nazywamy rzędem grupy G i oznaczamy przez $\operatorname{rz} G$. Z twierdzenia Lagrange'a wiemy, że jeśli H jest dzielnikiem normalnym skończonej grupy G, to $\operatorname{rz} H$ dzieli $\operatorname{rz} G$ i $\operatorname{rz} G/H = \frac{\operatorname{rz} G}{\operatorname{rz} H}$.

Oczywiście, jeśli G jest grupą przemienną, to każda jej podgrupa H jest dzielnikiem normalnym i grupa ilorazowa G/H jest przemienna. Możliwa jest jednak sytuacja, gdy cała grupa G nie jest przemienna, zaś grupa ilorazowa G/H jest przemienna.

Do badania przemienności grupy G/H można użyć tzw. komutanta. Dla $a, b \in G$ oznaczamy

$$[a, b] = aba^{-1}b^{-1}.$$

Element $[a, b] \in G$ nazywamy ***komutatorem*** elementów a, b. ***Komutantem*** $[G, G]$ grupy G nazywamy podgrupę generowaną przez wszystkie komutatory $[a, b] = aba^{-1}b^{-1}$, gdzie $a, b \in G$. Oczywiście jeśli G jest grupą przemienną to dla dowolnych $a, b \in G$ mamy $[a, b] = e$, gdzie e jest elementem neutralnym, więc $[G, G] = \{e\}$.

Twierdzenie 2. *Niech H będzie dzielnikiem normalnym grupy G. Grupa ilorazowa G/H jest przemienna wtedy i tylko wtedy, gdy*

$$[G, G] \subset H.$$

Dowód. Załóżmy, że grupa ilorazowa G/H jest przemienna. Wtedy dla dowolnych $a, b \in G$ mamy $(ab)H = (ba)H$, czyli $ab \sim ba$. Oznacza to, że

$$[a, b] = aba^{-1}b^{-1} = ab(ba)^{-1} \in H.$$

Stąd $[G, G] \subset H$.

Załóżmy teraz, że $[G, G] \subset H$. Dla dowolnych $a, b \in G$ mamy wtedy

$$ab(ba)^{-1} = aba^{-1}b^{-1} = [a, b] \in H,$$

czyli $ab \sim ba$. Oznacza to, że $(ab)H = (ba)H$. Zatem G/H jest grupą przemienną. □

Grupa G jest ***rozwiązalna***, gdy istnieje ciąg podgrup

$$\{e\} = H_0 \subset H_1 \subset \cdots \subset H_{k-1} \subset H_k = G$$

takich, że dla każdego $i = 1, ..., k$ są spełnione warunki:

(1) H_{i-1} jest dzielnikiem normalnym H_i,
(2) grupa ilorazowa H_i/H_{i-1} jest przemienna.

Twierdzenie 2 pokazuje, że warunek (2) jest równoważny temu, że $[H_i, H_i] \subset H_{i-1}$. Dla $i = 1$ warunek ten ma postać $[H_1, H_1] \subset H_0 = \{e\}$, czyli H_1 musi być grupą przemienną.

Niech $G^{(1)} = [G, G]$, $G^{(2)} = [G^{(1)}, G^{(1)}]$ i ogólnie $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Otrzymujemy w ten sposób ciąg podgrup

$$G \supset G^{(1)} \supset G^{(2)} \supset ...$$

grupy G. Z definicji rozwiązalności i twierdzenia 2 wynika, że grupa G jest rozwiązalna wtedy i tylko wtedy, gdy istnieje n takie, że $G^{(n)} = \{e\}$.

Twierdzenie 3. *Jeżeli H jest podgrupą grupy rozwiązalnej G, to H jest grupą rozwiązalną.*

Oczywiście każda grupa przemienna jest rozwiązalna. Każda grupa skończona, której rząd jest liczbą pierwszą jest grupą cykliczną. Jest to więc grupa przemienna i w konsekwencji grupa rozwiązalna. Grupa permutacji S_2 jest jedyną przemienną grupą permutacji S_n. Jest to więc grupa rozwiązalna.

Rozważmy teraz grupę permutacji S_n, gdzie $n \geqslant 3$. Przez A_n oznaczamy podzbiór grupy S_n wszystkich ***permutacji parzystych***, czyli takich, które są iloczynami parzystej liczby transpozycji. Zbiór A_n ma $\frac{n!}{2}$ elementów i jest to dzielnik normalny grupy S_n. Grupa ilorazowa S_n/A_n ma rząd 2, więc jest to grupa cykliczna.

Grupa S_3 jest rozwiązalna. Rzeczywiście, rozważmy ciąg

$$\{I\} = H_0 \subset H_1 = A_3 \subset H_2 = S_3.$$

Grupa S_3 ma rząd $3! = 6$, zaś A_3 ma rząd 3. Zatem A_3 jest grupą przemienną. Ponadto, $H_2/H_1 = S_3/A_3$ ma rząd 2, więc również ta grupa jest przemienna.

Grupa S_4 jest rozwiązalna. Rzeczywiście, rozważmy ciąg

$$\{I\} = H_0 \subset H_1 = V_4 \subset H_2 = A_4 \subset H_3 = S_4,$$

gdzie

$$V_4 = \{I, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Grupa V_4 jest przemienna. Grupa S_4 ma rząd $4! = 24$, zaś A_4 ma rząd 12. Zatem A_4/V_4 ma rząd 3, zaś S_4/A_4 ma rząd 2 i są to grupy przemienne.

Widzimy zatem, że dla $n \leqslant 4$ grupy S_n są rozwiązalne.

Twierdzenie 4. *Grupa permutacji S_5 nie jest rozwiązalna.*

Dowód. Załóżmy, że S_5 jest grupą rozwiązalną, czyli istnieje ciąg podgrup

$$\{I\} = H_0 \subset H_1 \subset \cdots \subset H_{k-1} \subset H_k = S_5$$

takich, że H_{i-1} jest dzielnikiem normalnym H_i oraz $[H_i, H_i] \subset H_{i-1}$ dla każdego $i = 1, ..., k$.

Rozważmy podzbiór C grupy S_5 zawierający wszystkie cykle (i, j, k) długości 3. Wykażemy, że jeśli H_i zawiera wszystkie cykle długości 3, to H_{i-1} zawiera wszystkie cykle długości 3. Zauważmy w tym celu, że dla dowolnego cyklu (i, j, k) mamy

$$\begin{aligned}(i,j,k) &= (i,l,k)(k,j,m)(k,l,i)(m,j,k) = (i,l,k)(k,j,m)(i,l,k)^{-1}(k,j,m)^{-1} = \\ &= [(i,l,k),(k,j,m)].\end{aligned}$$

Jeżeli więc $C \subset H_i$, to $C \subset [H_i, H_i] \subset H_{i-1}$. Wychodząc od tego, że $C \subset H_k = S_5$ dochodzimy więc do wniosku, że C zawiera się w kolejnych podgrupach H_i i w końcu $C \subset H_0 = \{I\}$, co nie jest prawdą. Zatem S_5 nie jest grupą rozwiązalną. □

Dla $n > 5$ grupa S_n zawiera podgrupę izomorficzną z S_5. Rzeczywiście S_n jest grupą permutacji zbioru $\{1, 2, ..., n\}$ i ograniczając się do permutacji σ takich, że $\sigma(i) = i$ dla $i = 6, 7, ..., n$ otrzymujemy podgrupę izomorficzną z S_5. Stąd i z twierdzenia, że podgrupa grupy rozwiązalnej jest rozwiązalna dostajemy następujący wniosek.

Wniosek 1. *Jeżeli $n \geqslant 5$, to grupa permutacji S_n nie jest rozwiązalna.*

Automorfizmy ciał

Niech K będzie ciałem. Izomorfizm $\phi : K \to K$ przekształcający wzajemnie jednoznacznie K na K nazywamy ***automorfizmem***. Zbiór wszystkich takich automorfizmów oznaczmy przez $\mathrm{Aut}(K)$. Jest to grupa z działaniem złożenia funkcji.

Niech $\phi \in \mathrm{Aut}(\mathbb{Q})$. Wtedy $\phi(1) = 1$, więc

$$\phi(n) = \phi(\underbrace{1 + ... + 1}_{n \text{ razy}}) = \underbrace{\phi(1) + ... + \phi(1)}_{n \text{ razy}} = n$$

dla każdego $n \in \mathbb{N}$. Następnie, jeśli $n \in \mathbb{Z}$, $n < 0$, to $-n \in \mathbb{N}$, więc $\phi(n) = \phi(-(-n)) = -\phi(-n) = -(-n) = n$.

Dla dowolnej liczby wymiernej $a = \frac{n}{m}$, gdzie $n, m \in \mathbb{Z}$, $m \neq 0$ mamy

$$\phi(a) = \phi(nm^{-1}) = \phi(n)\phi(m^{-1}) = \phi(n)\phi(m)^{-1} = nm^{-1} = a.$$

Zatem $I(a) = a$ jest jedynym automorfizmem ciała $\mathbb{Q}$.

Podobnie, jeśli $p \in \mathbb{N}$ jest liczbą pierwszą, $p > 1$, to $I(a) = a$ jest jedynym automorfizmem ciała $\mathbb{Z}_p$.

Ponadto takie samo rozumowanie pokazuje, że jeśli E jest rozszerzeniem ciała $\mathbb{Q}$ i $\phi \in \mathrm{Aut}(E)$, to $\phi(a) = a$ dla każdego $a \in \mathbb{Q}$.

Twierdzenie 5. $\mathrm{Aut}(\mathbb{R}) = \{I\}$.

Dowód. Niech $\phi \in \mathrm{Aut}(\mathbb{R})$. Jak już wiemy $\phi(a) = a$ dla każdego $a \in \mathbb{Q}$.

Załóżmy, że $x \in \mathbb{R}$, $x > 0$. Wtedy $\sqrt{x} \in \mathbb{R}$ i

$$\phi(x) = \phi(\sqrt{x}^2) = \phi(\sqrt{x})^2 \geqslant 0,$$

przy czym ϕ jest funkcją różnowartościową, więc $\phi(x) \neq \phi(0) = 0$. Stąd $\phi(x) > 0$.

Niech teraz $x, y \in \mathbb{R}$, $x < y$. Wtedy $y - x > 0$, więc

$$0 < \phi(y - x) = \phi(y) - \phi(x),$$

czyli $\phi(x) < \phi(y)$.

Aby wykazać nasze twierdzenie załóżmy, że istnieje $x \in \mathbb{R}$ takie, że $\phi(x) \neq x$. Wtedy $x < \phi(x)$ lub $\phi(x) < x$. W pierwszym przypadku istnieje $q \in \mathbb{Q}$ takie, że

$$x < q < \phi(x). \tag{1}$$

Wobec tego, co już wykazaliśmy z lewej nierówności dostajemy $\phi(x) < \phi(q) = q$, co jest sprzeczne z prawą nierównością w (1).

Podobnie pokazujemy, że nierówność $\phi(x) < x$ prowadzi do sprzeczności. Zatem $\phi(x) = x$ dla każdego $x \in \mathbb{R}$. □

Punktem stałym automorfizmu $\phi \in \mathrm{Aut}(K)$ nazywamy element $a \in K$ taki, że $\phi(a) = a$. Niech E będzie rozszerzeniem ciała K. Automorfizm $\phi \in \mathrm{Aut}(E)$ nazywamy K-***automorfizmem***, jeśli $\phi(a) = a$ dla każdego $a \in K$, czyli każdy $a \in K$ jest punktem stałym ϕ. Zbiór $\mathrm{Aut}(E/K)$ wszystkich K-automorfizmów ciała E jest podgrupą grupy wszystkich automorfizmów $\mathrm{Aut}(E)$. Grupę $\mathrm{Aut}(E/K)$ nazywamy ***grupą Galois rozszerzenia*** E ciała K.

Np. jeśli E jest rozszerzeniem ciała $\mathbb{Q}$, to każdy automorfizm $\phi \in \mathrm{Aut}(E)$ jest $\mathbb{Q}$-automorfizmem, więc $\mathrm{Aut}(E/\mathbb{Q}) = \mathrm{Aut}(E)$.

Przykład 1. Jeśli $\phi \in \mathrm{Aut}(\mathbb{C})$, to $\phi(a) = a$ dla każdego $a \in \mathbb{Q}$. Jednak ϕ nie musi być równe I. Np. $\phi_1(z) = \overline{z}$ jest automorfizmem ciała $\mathbb{C}$, przy czym istnieją jeszcze inne automorfizmy.

Natomiast $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{I, \phi_1\}$. Rzeczywiście, jeśli $\phi \in \mathrm{Aut}(\mathbb{C}/\mathbb{R})$, to $\phi(a) = a$ dla każdego $a \in \mathbb{R}$, więc

$$\phi(a+bi) = \phi(a) + \phi(b)\phi(i) = a + b\phi(i)$$

dla $a, b \in \mathbb{R}$. Ponadto $\phi(i)^2 = \phi(i^2) = \phi(-1) = -1$, więc $\phi(i) = i$ albo $\phi(i) = -i$. W pierwszym przypadku $\phi(a+bi) = a+bi$, zaś w drugim $\phi(a+bi) = a-bi = \overline{a+bi}$. Zatem $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \neq \mathrm{Aut}(\mathbb{C})$.

Twierdzenie 6. *Niech E będzie rozszerzeniem ciała K i $a \in E$ będzie elementem algebraicznym nad K, którego wielomianem minimalnym jest $f \in K[x]$. Wtedy dla każdego $\phi \in \mathrm{Aut}(E/K)$ obraz $\phi(a)$ jest pierwiastkiem wielomianu f, więc $\phi(a)$ jest również elementem algebraicznym nad K.*

Ponadto funkcja $F : \mathrm{Aut}(K(a)/K) \to E$ określona wzorem $F(\phi) = \phi(a)$ jest różnowartościowa i wobec tego $\operatorname{rz}\mathrm{Aut}(K(a)/K)$ *jest równy liczbie różnych pierwiastków wielomianu f.*

Dowód. Niech $f(x) = a_0 + a_1x + ... + a_nx^n$. Ponieważ każdy element $c \in K$ jest punktem stałym ϕ, więc

$$\begin{aligned} f(\phi(a)) &= a_0 + a_1\phi(a) + ... + a_n\phi(a)^n = \phi(a_0) + \phi(a_1)\phi(a) + ... + \phi(a_n)\phi(a)^n = \\ &= \phi(a_0 + a_1a + ... + a_na^n) = \phi(f(a)) = \phi(0) = 0. \end{aligned}$$

Dla wykazania, że funkcja F jest różnowartościowa załóżmy, że $\phi_1, \phi_2 \in \mathrm{Aut}(K(a)/K)$ są takie, że $\phi_1(a) = \phi_2(a)$. Bazą rozszerzenia $K(a)$ jest ciąg $1, a, ..., a^{n-1}$, gdzie $n = \operatorname{st} f$ i każdy element $u \in K(a)$ ma postać $u = b_0 + b_1a + ... + b_{n-1}a^{n-1}$, gdzie $b_0, b_1, ..., b_{n-1} \in K$. Ponieważ ϕ_1, ϕ_2 są K-automorfizmami, więc

$$\begin{aligned} \phi_1(u) &= \phi_1(b_0) + \phi_1(b_1)\phi_1(a) + ... + \phi_1(b_{n-1})\phi_1(a)^{n-1} = \\ &= b_0 + b_1\phi_1(a) + ... + b_{n-1}\phi_1(a)^{n-1} = \\ &= b_0 + b_1\phi_2(a) + ... + b_{n-1}\phi_2(a)^{n-1} = \\ &= \phi_2(b_0) + \phi_2(b_1)\phi_2(a) + ... + \phi_2(b_{n-1})\phi_2(a)^{n-1} = \phi_2(u), \end{aligned}$$

czyli $\phi_1 = \phi_2$. □

Przykład 2. Niech $E = \mathbb{Q}(\sqrt{2})$. Wielomianem minimalnym $\sqrt{2}$ jest $x^2 - 2$. Zatem dla dowolnego automorfizmu $\phi \in \mathrm{Aut}(E/\mathbb{Q})$ mamy

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

więc $\phi(\sqrt{2}) = \sqrt{2}$ albo $\phi(\sqrt{2}) = -\sqrt{2}$. Grupa $\mathrm{Aut}(E/\mathbb{Q})$ składa się zatem z dwóch automorfizmów: $I(a+b\sqrt{2}) = a+b\sqrt{2}$ i $\phi(a+b\sqrt{2}) = a-b\sqrt{2}$ dla $a, b \in \mathbb{Q}$. Stąd grupa $\mathrm{Aut}(E/\mathbb{Q})$ jest izomorficzna z grupą S_2 permutacji zbioru dwuelementowego $\{\sqrt{2}, -\sqrt{2}\}$.

Przykład 3. Niech $E = \mathbb{Q}(\sqrt[3]{2})$. Wielomianem minimalnym $\sqrt[3]{2}$ jest $x^3 - 2$, zatem dla dowolnego automorfizmu $\phi \in \mathrm{Aut}(E/\mathbb{Q})$ mamy $\phi(\sqrt[3]{2})^3 = 2$ i stąd $\phi(\sqrt[3]{2}) = \sqrt[3]{2}$. Dowolny element $u \in \mathbb{Q}(\sqrt[3]{2})$ ma postać $u = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$, gdzie $a, b, c \in \mathbb{Q}$, więc

$$\phi(u) = a + b\phi(\sqrt[3]{2}) + c\phi\Big(\sqrt[3]{2}^2\Big) = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 = u.$$

Zatem $\mathrm{Aut}(E/\mathbb{Q}) = \{I\}$.

Niech H będzie podgrupą grupy automorfizmów $\mathrm{Aut}(K)$. Przez $\mathrm{Fix}(K,H)$ oznaczamy zbiór elementów ciała K, które są ***punktami stałymi*** wszystkich automorfizmów z podgrupy H, czyli

$$\mathrm{Fix}(K,H) = \{a \in K : \phi(a) = a \text{ dla każdego } \phi \in H\}.$$

Twierdzenie 7. *Zbiór* $\mathrm{Fix}(K,H)$ *jest podciałem ciała* K*.*

Dowód. Mamy $0, 1 \in \mathrm{Fix}(K,H)$. Ponadto, jeśli $a, b \in \mathrm{Fix}(K,H)$, to dla dowolnego $\phi \in H$ mamy

$$\phi(a-b) = \phi(a) - \phi(b) = a - b,$$

więc $a - b \in \mathrm{Fix}(K,H)$. Jeśli dodatkowo $b \neq 0$, to

$$\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = ab^{-1},$$

więc $ab^{-1} \in \mathrm{Fix}(K,H)$. □

Rozszerzenie E ciała K jest ***rozszerzeniem Galois***, jeśli

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

Twierdzenie 8. *Niech* E *będzie rozszerzeniem skończonym ciała* K*. Wtedy* $\mathrm{rz}\,\mathrm{Aut}(E/K) \leqslant (E:K)$ *i równość* $(E:K) = \mathrm{rz}\,\mathrm{Aut}(E/K)$ *zachodzi wtedy i tylko wtedy, gdy* E *jest rozszerzeniem Galois.*

Przykład 4. Niech $E = \mathbb{Q}(\sqrt[3]{2})$. Z przykładu 3 wiemy, że $\mathrm{Aut}(E/\mathbb{Q}) = \{I\}$. Stąd $\mathrm{Fix}(E, \mathrm{Aut}(E/\mathbb{Q})) = E \neq \mathbb{Q}$, zatem E nie jest rozszerzeniem Galois.

Przykład 5. Niech $E = \mathbb{Q}(\sqrt{2})$. Z przykładu 2 wiemy, że $\mathrm{Aut}(E/\mathbb{Q})$ składa się zatem z dwóch elementów: I, ϕ, gdzie $\phi(a+b\sqrt{2}) = a - b\sqrt{2}$ dla $a, b \in \mathbb{Q}$. Jeśli więc $u = a + b\sqrt{2} \in \mathrm{Fix}(E, \mathrm{Aut}(E/\mathbb{Q}))$, to

$$a + b\sqrt{2} = u = \phi(u) = a - b\sqrt{2}.$$

Stąd $2b\sqrt{2} = 0$, czyli $b = 0$, a zatem $u = a \in \mathbb{Q}$. Oznacza to, że $\mathrm{Fix}(E, \mathrm{Aut}(E/\mathbb{Q})) = \mathbb{Q}$, czyli $E = \mathbb{Q}(u)$ jest rozszerzeniem Galois. Wynika to także z równości $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = 2 = \mathrm{rz}\,\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$.

Przykład 5 jest szczególnym przypadkiem następującego twierdzenia.

Twierdzenie 9. *Niech* $E = K(a_1, ..., a_n)$ *będzie ciałem rozkładu wielomianu* $f \in K[x]$*, przy czym pierwiastki* $a_1, ..., a_n$ *wielomianu* f *są parami różne. Wtedy*

$$\mathrm{rz}\,\mathrm{Aut}(E/K) = (E:K),$$

a więc E *jest rozszerzeniem Galois ciała* K*.*

Dowód. Element a_1 ma pewien wielomian minimalny $f_1 \in K[x]$. Wielomian minimalny f_1 dzieli f i z jednoznaczności rozkładu $f(x) = a(x-a_1)...(x-a_n)$ w $E[x]$ wynika, że pierwiastki wielomianu f_1 (będące również pierwiastkami f) są parami różne. Z twierdzenia 6 wynika, że liczba wszystkich K-automorfizmów $\phi_1 : K(a_1) \to K(a_1)$ jest równa liczbie pierwiastków wielomianu f_1, a więc stopniowi tego wielomianu. Zatem $\mathrm{rz}\,\mathrm{Aut}(K(a_1)/K) = (K(a_1) : K)$.

Podobnie a_2 ma pewien wielomian minimalny $f_2 \in K(a_1)[x]$, który ma parami różne pierwiastki. Dla dowolnego $\phi_1 \in \mathrm{Aut}(K(a_1)/K)$ wielomian $g = \phi_1(f_2)$ również ma parami

różne pierwiastki. Mamy $K(a_1, a_2) = (K(a_1))(a_2)$ i z dowodu twierdzenia 6 wynika, że liczba wszystkich automorfizmów $\phi_2 : K(a_1, a_2) \to K(a_1, a_2)$ takich, że $\phi_2(u) = \phi_1(u)$ dla $u \in K(a_1)$ jest równa $(K(a_1, a_2) : K(a_1))$.

Postępując dalej w ten sposób dochodzimy do wniosku, że $\operatorname{rz}\operatorname{Aut}(E/K)$, czyli liczba wszystkich K-automorfizmów $\phi : E \to E$ jest równa

$$(K(a_1) : K) \cdot (K(a_1, a_2) : K(a_1)) \cdot ... \cdot (K(a_1, a_2, ..., a_n) : K(a_1, a_2, ..., a_{n-1})) =$$
$$= (K(a_1, ..., a_n) : K). \qquad \square$$

Niech L będzie rozszerzeniem ciała K i E będzie ciałem takim, że $K \subset E \subset L$. Jeśli $\phi \in \operatorname{Aut}(L/E)$, to $\phi(u) = u$ dla wszystkich $u \in E$, a więc w szczególności dla wszystkich $u \in K$. Wynika stąd, że $\operatorname{Aut}(L/E)$ jest podgrupą grupy $\operatorname{Aut}(L/K)$.

Niech L będzie rozszerzeniem ciała K. Ciału pośredniemu E, czyli takiemu, że $K \subset E \subset L$ odpowiada więc podgrupa $\Psi_1(E) = \operatorname{Aut}(L/E)$ grupy $\operatorname{Aut}(L/K)$.

Z kolei podgrupie H grupy $\operatorname{Aut}(L/K)$ odpowiada ciało $\Psi_2(H) = \operatorname{Fix}(L, H)$ pośrednie między K i L.

Twierdzenie 10 (Galois)**.** *Niech L będzie skończonym rozszerzeniem Galois ciała K. Wtedy powyższe odwzorowania Ψ_1, Ψ_2 są funkcjami różnowartościowymi. Ponadto są one względem siebie odwrotne, tzn. jeżeli H jest podgrupą $\operatorname{Aut}(L/K)$, to*

$$\operatorname{Aut}(L/\operatorname{Fix}(L, H)) = H$$

oraz jeżeli $K \subset E \subset L$, to

$$\operatorname{Fix}(L, \operatorname{Aut}(L/E)) = E.$$

W szczególności L jest rozszerzeniem Galois ciała E.

Przykład 6. Niech $E = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$. Wielomian $f(x) = x^3 - 2$ jest wielomianem minimalnym liczby $\sqrt[3]{2}$, wiec $(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = 3$. Wielomian $g(x) = x^2 + 3$ jest nierozkładalny w $\mathbb{Q}(\sqrt[3]{2})[x]$, gdyż jego pierwiastki $\sqrt{3}i$ oraz $-\sqrt{3}i$ nie należą do ciała $\mathbb{Q}(\sqrt[3]{2})$. Stąd $\left((\mathbb{Q}(\sqrt[3]{2}))(\sqrt{3}i) : \mathbb{Q}(\sqrt[3]{2})\right) = 2$ i ponieważ $E = (\mathbb{Q}(\sqrt[3]{2}))(\sqrt{3}i)$, więc

$$(E : \mathbb{Q}) = \left((\mathbb{Q}(\sqrt[3]{2}))(\sqrt{3}i) : \mathbb{Q}(\sqrt[3]{2})\right)(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = 6.$$

Zauważmy, że $\omega_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \in \mathbb{Q}(\sqrt{3}i) \subset E$. Liczba ω_1 jest pierwiastkiem trzeciego stopnia z 1. Również $\omega_1^2 \in E$, więc wszystkie trzy zespolone pierwiastki trzeciego stopnia z 1, tj. 1, ω_1 i ω_1^2 należą do E.

Niech ϕ_1, ϕ_2 będą $\mathbb{Q}$-automorfizmami ciała E takimi, że

$$\phi_1(\sqrt[3]{2}) = \sqrt[3]{2}\omega_1, \quad \phi_1(\omega_1) = \omega_1,$$
$$\phi_2(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \phi_2(\omega_1) = \omega_1^2.$$

Wtedy

$$\phi_2(\sqrt[3]{2}\omega_1) = \phi_2(\sqrt[3]{2})\phi_2(\omega_1) = \sqrt[3]{2}\omega_1^2, \quad \phi_2(\sqrt[3]{2}\omega_1^2) = \phi_2(\sqrt[3]{2})\phi_2(\omega_1)^2 = \sqrt[3]{2}\omega_1^4 = \sqrt[3]{2}\omega_1$$

oraz

$$\phi_1(\sqrt[3]{2}\omega_1) = \phi_1(\sqrt[3]{2})\phi_1(\omega_1) = \sqrt[3]{2}\omega_1^2, \quad \phi_1(\sqrt[3]{2}\omega_1^2) = \phi_1(\sqrt[3]{2})\phi_2(\omega_1)^2 = \sqrt[3]{2}\omega_1^3 = \sqrt[3]{2},$$
$$\phi_1(\sqrt[3]{2}) = \sqrt[3]{2}\omega_1.$$

Rozważmy grupę permutacji S_3 zbioru $\{1,2,3\}$. Jej generatorami są: transpozycja $\tau = (1,2)$ i cykl $\sigma = (1,2,3)$. Z powyższych wzorów widać, że jeśli zamiast zbioru $\{1,2,3\}$ weźmiemy zbiór

$$\{\sqrt[3]{2}\omega_1, \sqrt[3]{2}\omega_1^2, \sqrt[3]{2}\},$$

to transpozycji τ odpowiada ϕ_2, zaś cyklowi σ odpowiada ϕ_1. Funkcja $F : S_3 \to \mathrm{Aut}(E/\mathbb{Q})$ taka, że $F(\tau) = \phi_2$, $F(\sigma) = \phi_1$ jest zatem izomorfizmem grupy S_3 na podgrupę H grupy $\mathrm{Aut}(E/\mathbb{Q})$. Ale $\mathrm{rz}\, H = \mathrm{rz}\, S_3 = 6$ i z twierdzenia 8 wiemy, że $\mathrm{rz}\,\mathrm{Aut}(E/\mathbb{Q}) \leqslant (E:\mathbb{Q}) = 6$, więc $H = \mathrm{Aut}(E/\mathbb{Q})$. Zatem grupa automorfizmów $\mathrm{Aut}(E/\mathbb{Q})$ jest izomorficzna z S_3.

Grupę S_3 można interpretować jako grupę izometrii trójkąta równobocznego, przy czym transpozycji odpowiada symetria osiowa, zaś cyklowi obrót wokół środka trójkąta. Nietrywialne podgrupy grupy S_3 rozpatrywanej jako grupa izometrii trójkąta równobocznego to grupa obrotów mająca rząd 3 i trzy grupy symetrii względem trzech osi mające rząd 2. Odpowiadają im podgrupy grupy $\mathrm{Aut}(E/\mathbb{Q})$: $H_1 = (\phi_1)$, $H_2 = (\phi_2)$, $H_3 = (\phi_2 \circ \phi_1)$ i $H_4 = (\phi_2 \circ \phi_1^2)$.

Ponieważ $\phi_1(\omega_1) = \omega_1$, więc $\mathrm{Fix}(E, H_1) = \mathbb{Q}(\omega_1)$. Z równości $\phi_2(\sqrt[3]{2}) = \sqrt[3]{2}$ wynika z kolei, że $\mathrm{Fix}(E, H_2) = \mathbb{Q}(\sqrt[3]{2})$.

Ponadto,

$$\phi_1(\sqrt[3]{2}\omega_1) = \phi_1(\sqrt[3]{2})\phi_1(\omega_1) = \sqrt[3]{2}\omega_1^2,$$

zatem

$$(\phi_2 \circ \phi_1)(\sqrt[3]{2}\omega_1) = \phi_2(\sqrt[3]{2}\omega_1^2) = \phi_2(\sqrt[3]{2})\phi_2(\omega_1)^2 = \sqrt[3]{2}\omega_1^4 = \sqrt[3]{2}\omega_1,$$

więc $\mathrm{Fix}(E, H_3) = \mathbb{Q}(\sqrt[3]{2}\omega_1)$.

Następnie,

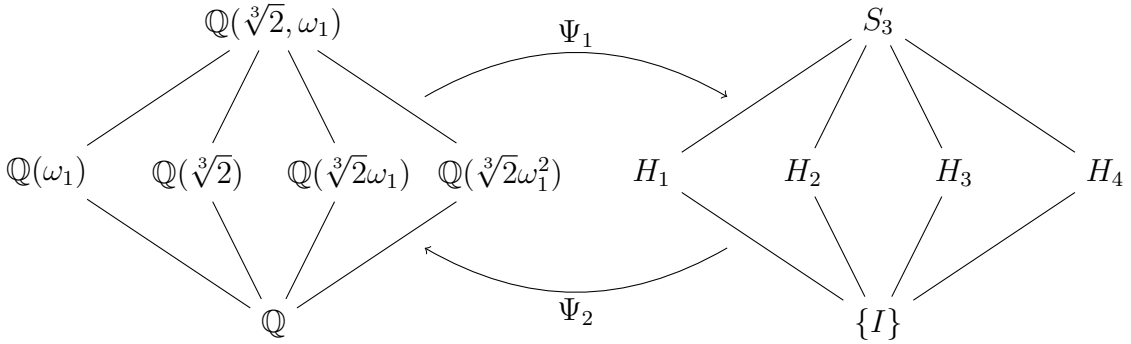
$$\phi_1^2(\sqrt[3]{2}\omega_1^2) = \phi_1(\phi_1(\sqrt[3]{2})\phi_1(\omega_1)^2) = \phi_1(\sqrt[3]{2}\omega_1\omega_1^2) = \phi_1(\sqrt[3]{2}) = \sqrt[3]{2}\omega_1,$$

zatem

$$(\phi_2 \circ \phi_1^2)(\sqrt[3]{2}\omega_1^2) = \phi_2(\sqrt[3]{2}\omega_1) = \sqrt[3]{2}\omega_1^2,$$

więc $\mathrm{Fix}(E, H_4) = \mathbb{Q}(\sqrt[3]{2}\omega_1^2)$.

Z twierdzenia 10 wynika, że wszystkie ciała pośrednie między $\mathbb{Q}$ i $\mathbb{Q}(\sqrt[3]{2}, \omega_1)$, to: $\mathbb{Q}(\omega_1)$, $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\omega_1)$ i $\mathbb{Q}(\sqrt[3]{2}\omega_1^2)$.



Ponadto zgodnie z twierdzeniem 8 mamy $(\mathbb{Q}(\omega_1) : \mathbb{Q}) = \mathrm{rz}\, H_1 = 3$, $(\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}) = \mathrm{rz}\, H_2 = 2$, $(\mathbb{Q}(\sqrt[3]{2}\omega_1) : \mathbb{Q}) = \mathrm{rz}\, H_3 = 2$ i $(\mathbb{Q}(\sqrt[3]{2}\omega_1^2) : \mathbb{Q}) = \mathrm{rz}\, H_4 = 2$.