

GRZEGORZ BOBIŃSKI

Teoria Galois

Wydział Matematyki i Informatyki
Uniwersytet Mikołaja Kopernika w Toruniu
2023

TEORIA GALOIS

SPIS TREŚCI

1	Rozszerzenia ciał	1
A	Konstrukcje geometryczne	7
2	Podstawowe Twierdzenie Teorii Galois	9
3	Ciało rozkładu wielomianu, domknięcie algebraiczne i normalność	20
B	Zasadnicze Twierdzenie Algebra	32
4	Grupa Galois wielomianu	34
5	Ciała skończone	36
6	Rozdzielczość	38
7	Rozszerzenia cykliczne	45
8	Rozszerzenia cyklotomiczne	57
9	Rozszerzenia pierwiastnikowe	58
C	Ogólne równanie stopnia n	62

TEORIA GALOIS

1. ROZSZERZENIA CIAŁ

DEFINICJA.

Mówimy, że ciało F jest ROZSZERZENIEM ciała K , jeśli K jest podciałem ciała F .

UWAGA.

Jeśli F jest rozszerzeniem ciała K , to F jest przestrzenią wektorową nad ciałem K .

DEFINICJA.

Jeśli F jest rozszerzeniem ciała K , to definiujemy STOPIEŃ $[F : K]$ rozszerzenia wzorem

$$[F : K] := \dim_K F.$$

TWIERDZENIE 1.1.

Jeśli F jest rozszerzeniem ciała E i E jest rozszerzeniem ciała K , to

$$[F : K] = [F : E] \cdot [E : K].$$

DOWÓD.

Ćwiczenie. □

OZNACZENIE.

Niech F będzie rozszerzeniem ciała K oraz X podzbiorem ciała F .

- (1) Przez $K(X)$ oznaczamy podciało ciała F generowane przez $K \cup X$. Jeśli $X = \{u_1, \dots, u_n\}$, to piszemy $K(u_1, \dots, u_n)$ zamiast $K(\{u_1, \dots, u_n\})$.
- (2) Przez $K[X]$ oznaczamy podpierścień ciała F generowany przez $K \cup X$. Jeśli $X = \{u_1, \dots, u_n\}$, to piszemy $K[u_1, \dots, u_n]$ zamiast $K[\{u_1, \dots, u_n\}]$.

DEFINICJA.

- (1) Ciało F nazywamy SKOŃCZENIE GENEROWANYM ROZSZERZENIEM ciała K , jeśli istnieją elementy $u_1, \dots, u_n$ ciała F takie, że $F = K(u_1, \dots, u_n)$.
- (2) Ciało F nazywamy PROSTYM rozszerzeniem ciała K , jeśli istnieje element u ciała F takie, że $F = K(u)$.

TWIERDZENIE 1.2.

Jeśli F jest rozszerzeniem ciała K oraz $u_i, i \in I$, elementami ciała F , to

$$K[\{u_i : i \in I\}] = \{f((u_i)) : f \in K[x_i : i \in I]\}.$$

oraz

$$K(\{u_i : i \in I\}) = \left\{ \frac{f((u_i))}{g((u_i))} : f, g \in K[x_i : i \in I], g((u_i)) \neq 0 \right\}.$$

TEORIA GALOIS

W szczególności, jeśli $v \in K[\{u_i : i \in I\}]$, to istnieje skończony podzbiór I_0 zbioru I taki, że $v \in K[\{u_i : i \in I_0\}]$.

Podobnie, jeśli $v \in K(\{u_i : i \in I\})$, to istnieje skończony podzbiór I_0 zbioru I taki, że $v \in K(\{u_i : i \in I_0\})$.

DOWÓD.

Ćwiczenie. □

OZNACZENIE.

Jeśli L i M są podciałami ciała F , to

$$LM := L(M) = M(L).$$

DEFINICJA.

Niech F będzie rozszerzeniem ciała K .

- (1) Element u ciała F nazywamy ALGEBRAICZNYM nad K , jeśli istnieje niezerowy wielomian $f \in K[x]$ taki, że $f(u) = 0$.
- (2) Element u ciała F nazywamy PRZESTĘPNYM nad K , jeśli nie istnieje niezerowy wielomian $f \in K[x]$ taki, że $f(u) = 0$.
- (3) F nazywam rozszerzeniem ALGEBRAICZNYM ciała K , jeśli wszystkie elementy ciała F są algebraiczne nad K .
- (4) F nazywam rozszerzeniem PRZESTĘPNYM ciała K , jeśli istnieje element ciała F , który jest przestępny nad K .

OZNACZENIE.

Jeśli $\sigma: F \rightarrow E$ jest izomorfizmem ciał oraz K podciałem ciała F , to przez $\sigma|_K$ oznaczamy izomorfizm $K \rightarrow \sigma(K)$ indukowany przez σ .

TWIERDZENIE 1.3.

Niech F będzie rozszerzeniem ciała K . Jeśli element $u \in F$ jest przestępny nad K , to istnieje izomorfizm $\sigma: K(x) \simeq K(u)$ taki, że $\sigma|_K = \text{Id}_K$ i $\sigma(x) = u$.

DOWÓD.

Z definicji $g(u) \neq 0$ dla każdego niezerowego wielomianu $g \in K[x]$. Definiujemy funkcję $\sigma: K(x) \rightarrow K(u)$ wzorem

$$\sigma\left(\frac{f}{g}\right) := \frac{f(u)}{g(u)} \quad (f, g \in K[x]).$$

Łatwo sprawdzić, że σ jest dobrze określonym homomorfizmem (a więc również monomorfizmem) ciał. Ponadto z Twierdzenia 1.2 wynika, że σ jest epimorfizmem. Ponieważ oczywiście $\sigma|_K = \text{Id}_K$, co kończy dowód. □

UWAGA/DEFINICJA.

Niech F będzie rozszerzeniem ciała K . Jeśli element $u \in F$ jest algebraiczny

TEORIA GALOIS

nad K , to istnieje jedyny wielomian unormowany $f \in K[x]$ taki, że

$$(f) = \{g \in K[x] : g(u) = 0\}.$$

Wielomian f jest nierozkładalny, nazywamy go wielomianem MINIMALNYM elementu u , a jego stopień STOPNIEM elementu u .

Twierdzenie 1.4.

Niech F będzie rozszerzeniem ciała K . Jeśli $u \in F$ jest elementem algebraicznym nad K stopnia n , to:

- (1) $K(u) = K[u]$.
- (2) Jeśli f jest wielomianem minimalnym elementu u , to istnieje izomorfizm $\sigma: K(u) \simeq K[x]/(f)$ taki, że $\sigma(k) = k + (f)$ dla $k \in K$ oraz $\sigma(u) = x + (f)$.
- (3) $[K(u) : K] = n$.
- (4) Elementy $1, u, \dots, u^{n-1}$ tworzą bazę przestrzeni $K(u)$ nad ciałem K .

Dowód.

Ćwiczenie. □

Uwaga.

Jeśli $\sigma: R \rightarrow S$ jest homomorfizmem pierścieni, to indukowany homomorfizm $R[x] \rightarrow S[x]$ będziemy oznaczać również przez σ . Zauważmy, że indukowany homomorfizm $R[x] \rightarrow S[x]$ jest izomorfizmem wtedy i tylko wtedy, gdy wyjściowy homomorfizm jest izomorfizmem.

Definicja.

Niech E i F będą rozszerzeniami ciała K . Homomorfizm $\sigma: E \rightarrow F$ nazywamy K -homomorfizmem, jeśli $\sigma|_K = \text{Id}_K$.

Uwaga.

Niech E i F będą rozszerzeniami ciała K . Homomorfizm $\sigma: E \rightarrow F$ jest K -homomorfizmem wtedy i tylko wtedy, gdy jest odwzorowaniem K -liniowym.

Dowód.

Założmy najpierw, że σ jest K -homomorfizmem. Oczywiście $\sigma(e_1 + e_2) = \sigma(e_1) + \sigma(e_2)$ dla dowolnych $e_1, e_2 \in E$, gdyż σ jest homomorfizmem ciał. Ponadto

$$\sigma(k \cdot e) = \sigma(k) \cdot \sigma(e) = k \cdot \sigma(e)$$

dla dowolnych $k \in K$ i $e \in E$, gdzie pierwsza równość wynika z faktu, że σ jest homomorfizmem ciał, a druga z faktu, że σ jest K -homomorfizmem.

TEORIA GALOIS

Założmy teraz, że homomorfizm σ jest K -liniowy. Wtedy dla dowolnego $k \in K$ mamy

$$\sigma(k) = \sigma(k \cdot 1) = k \cdot \sigma(1) = k \cdot 1 = k,$$

gdzie druga równość wynika z K -liniowości, a trzecia z faktu, że σ jest homomorfizmem ciał. $\square$

Twierdzenie 1.5.

Niech $\sigma: K \rightarrow L$ będzie izomorfizmem ciał, F rozszerzeniem ciała K , E rozszerzeniem ciała L , $u \in F$ i $v \in E$. Jeśli

- (1) elementy u i v są przestępne nad ciałami K i L , odpowiednio, lub
- (2) elementy u i v są algebraiczne nad ciałami K i L , odpowiednio, oraz $(\sigma f)(v) = 0$, gdzie f jest wielomianem minimalnym elementu u ,

to istnieje izomorfizm $\bar{\sigma}: K(u) \rightarrow L(v)$ taki, że $\sigma(u) = v$ oraz $\bar{\sigma}|_K = \sigma$.

Dowód.

- (1) Mamy izomorfizm $\sigma': K(x) \rightarrow L(x)$ indukowany przez izomorfizm $\sigma: K[x] \rightarrow L[x]$. Korzystając z Twierdzenia 1.3, otrzymujemy tezę.
- (2) Podobnie jak poprzednio mamy izomorfizm $\sigma': K[x]/(f) \rightarrow L(x)/(\sigma f)$ indukowany przez izomorfizm $\sigma: K[x] \rightarrow L[x]$, więc tezę otrzymujemy, korzystając z Twierdzenia 1.4(2). $\square$

Wniosek 1.6.

Niech E i F będą rozszerzeniami ciała K , $u \in E$ i $v \in F$. Założmy, że elementy u i v są algebraiczne nad ciałem K . Wtedy u i v mają ten sam wielomian minimalny wtedy i tylko wtedy, gdy istnieje K -izomorfizm $\sigma: K(u) \rightarrow K(v)$ taki, że $\sigma(u) = v$.

Dowód.

$\implies$: Wystarczy zastosować Twierdzenie 1.5(2) dla $\sigma = \text{Id}_K$.

$\impliedby$: Niech f i g będą wielomianami minimalnymi elementów u i v , odpowiednio. Wtedy

$$f(v) = f(\sigma(u)) = \sigma(f(u)) = \sigma(0) = 0,$$

gdzie równość $f(\sigma(u)) = \sigma(f(u))$ jest konsekwencją założenia $\sigma|_K = \text{Id}_K$. Zatem $g \mid f$. Analogicznie $f \mid g$. Ponieważ wielomiany f i g są unormowane, więc $f = g$. $\square$

Twierdzenie 1.7.

Niech K będzie ciałem i $f \in K[X]$, $\deg f > 0$.

TEORIA GALOIS

- (1) Istnieje rozszerzenie F ciała K oraz element $u \in F$ takie, że $F = K(u)$ i $f(u) = 0$.
- (2) Jeśli F jest rozszerzeniem ciała K takim, że $F = K(u)$ dla pewnego elementu $u \in F$ takiego, że $f(u) = 0$, to $[F : K] \leq \deg f$ oraz $[F : K] = \deg f$ wtedy i tylko wtedy, gdy wielomian f jest nierozkładalny.
- (3) Jeśli wielomian f jest nierozkładalny oraz F i E są rozszerzeniami ciała K takimi, że $F = K(u)$ i $E = K(v)$ dla pewnych pierwiastków u i v wielomianu f , to istnieje K -izomorfizm $\sigma: F \rightarrow E$.

Dowód.

- (1) Niech g będzie nierozkładalnym dzielnikiem wielomianu f . Wtedy ideał (g) jest maksymalny, zatem $F := K[x]/(g)$ jest ciałem. Ponieważ $K \cap (g) = (0)$, więc utożsamiając K z obrazem przy naturalnym rzutowaniu $K[x] \rightarrow F$, otrzymujemy, że F jest rozszerzeniem ciała K . Niech $u := x + (g)$. Wtedy łatwo widać, że $F = K(u)$ oraz $g(u) = 0$, a więc również $f(u) = 0$.
- (2) Niech g będzie nierozkładalnym dzielnikiem wielomianu f takim, że $g(u) = 0$. Z Twierdzenie 1.4(3) wynika, że $[F : K] = \deg g$, co kończy dowód.
- (3) Wynika z Wniosku 1.6. □

Twierdzenie 1.8.

Niech F będzie rozszerzeniem ciała K . Jeśli $[F : K] < \infty$, to F jest skończone generowanym rozszerzeniem algebraicznym ciała K .

Dowód.

Niech $n := [F : K]$. Jeśli elementy $v_1, \dots, v_n$ tworzą bazę liniową ciała F nad ciałem K , to $F = K(v_1, \dots, v_n)$.

Niech teraz $u \in F$. Wtedy elementy $1, u, \dots, u^n$ są liniowo zależne nad ciałem K , zatem istnieje wielomian $f \in K[x]$ taki, że $f(u) = 0$. □

Twierdzenie 1.9.

Niech F będzie rozszerzeniem ciała K oraz $F = K(X)$ dla pewnego podzbioru X ciała F . Jeśli każdy element zbioru X jest algebraiczny nad ciałem K , to F jest rozszerzeniem algebraicznym ciała K . Jeśli dodatkowo $|X| < \infty$, to $[F : K] < \infty$.

Dowód.

Zauważmy najpierw, że jeśli $v_1, \dots, v_n \in X$, to $[K(v_1, \dots, v_n) : K] < \infty$. Istotnie, z założenia dla każdego $i \in [1, n]$ element v_i jest algebraiczny nad ciałem K , więc jest również algebraiczny nad ciałem $K(v_1, \dots, v_{i-1})$. W szcze-

TEORIA GALOIS

gólności $[K(v_1, \dots, v_i) : K(v_1, \dots, v_{i-1})] < \infty$ na mocy Twierdzenie 1.4(3), a więc korzystając z Twierdzenia 1.1, otrzymujemy

$$[K(v_1, \dots, v_n) : K] = \prod_{i=1}^n [K(v_1, \dots, v_i) : K(v_1, \dots, v_{i-1})] < \infty.$$

Z powyższej obserwacji wynika w szczególności, że jeśli $|X| < \infty$, to $[F : K] < \infty$.

Ustalmy teraz element $u \in F$. Z Twierdzenia 1.2 wiemy, że istnieją elementy $v_1, \dots, v_n \in X$ takie, że $u \in K(v_1, \dots, v_n)$. Korzystając ponownie z powyższej obserwacji, otrzymujemy $[K(v_1, \dots, v_n) : K] < \infty$. Ponieważ $K(u) \subseteq K(v_1, \dots, v_n)$, więc również $[K(u) : K] < \infty$, zatem element u jest algebraiczny nad ciałem K na mocy Twierdzenia 1.8. $\square$

Twierdzenie 1.10.

Jeśli F jest rozszerzeniem algebraicznym ciała E , a E jest rozszerzeniem algebraicznym ciała K , to F jest rozszerzeniem algebraicznym ciała K .

Dowód.

Ustalmy element u ciała F . Ponieważ element u jest algebraiczny nad ciałem E , więc istnieją elementy $v_0, \dots, v_n$ ciała E takie, że $v_n \neq 0$ oraz

$$v_n u^n + \dots + v_1 u + v_0 = 0.$$

W szczególności, element u jest algebraiczny nad ciałem $K(v_0, \dots, v_n)$. Korzystając z Twierdzenia 1.9, wiemy, że

$$[K(v_0, \dots, v_n, u) : K(v_0, \dots, v_n)], [K(v_0, \dots, v_n) : K] < \infty$$

(w drugim przypadku korzystamy również z faktu, że elementy $v_0, \dots, v_n$ są algebraiczne nad ciałem K). Twierdzenie 1.1 implikuje, że

$$\begin{aligned} [K(v_0, \dots, v_n, u) : K] \\ = [K(v_0, \dots, v_n, u) : K(v_0, \dots, v_n)] \cdot [K(v_0, \dots, v_n) : K] < \infty, \end{aligned}$$

więc element u jest algebraiczny nad ciałem K na mocy Twierdzenia 1.8. $\square$

Twierdzenie 1.11.

Niech F będzie rozszerzeniem ciała K . Jeśli

$$E := \{u \in F : \text{element } u \text{ jest algebraiczny nad ciałem } K\},$$

to E jest podciałem ciała F .

Dowód.

Ustalmy elementy u i v zbioru E . Z Twierdzenia 1.9 otrzymujemy, że ciało $K(u, v)$ jest rozszerzeniem algebraicznym ciała K , a więc $K(u, v) \subseteq E$. W szczególności, elementy $u + v$, $u - v$, $u \cdot v$ i $\frac{u}{v}$ (gdy $v \neq 0$) należą do E . $\square$

TEORIA GALOIS

A. KONSTRUKCJE GEOMETRYCZNE

OZNACZENIE.

Niech P i Q będą dwoma różnymi punktami płaszczyzny $\mathbb{R}^2$.

- (1) Przez $L(P, Q)$ oznaczamy prostą przechodzącą przez punkty P i Q .
- (2) Przez $C(P, Q)$ oznaczamy okrąg o środku P i promieniu P i Q .

DEFINICJA.

Punktami KONSRTUOWALNYMI nazywamy elementy najmniejszego zbioru $\mathcal{C}$ punktów na płaszczyźnie $\mathbb{R}^2$ spełniającego warunki:

- (1) $\mathbb{Z}^2 \subseteq \mathcal{C}$;
- (2) jeśli $P_1, Q_1, P_2, Q_2 \in \mathcal{C}$ oraz $P_1 \neq Q_1$ i $P_2 \neq Q_2$, to:
 - (a) $L(P_1, Q_1) \cap L(P_2, Q_2) \subseteq \mathcal{C}$, o ile $L(P_1, Q_1) \neq L(P_2, Q_2)$,
 - (b) $L(P_1, Q_1) \cap C(P_2, Q_2) \subseteq \mathcal{C}$,
 - (c) $C(P_1, Q_1) \cap C(P_2, Q_2) \subseteq \mathcal{C}$, o ile $C(P_1, Q_1) \neq C(P_2, Q_2)$.

DEFINICJA.

Liczbę rzeczywistą c nazywamy KONSTRUOWALNĄ, jeśli punkt $(c, 0)$ jest konstruowalny.

UWAGA.

- (1) Każda liczba wymierna jest konstruowalna.
- (2) Jeśli liczba c jest konstruowalna, to liczba $\sqrt{c}$ jest konstruowalna.
- (3) Zbiór liczb konstruowalnych jest podciałem ciała $\mathbb{R}$.

LEMAT A.1.

Niech F będzie podciałem ciała $\mathbb{R}$, $P_1, Q_1, P_2, Q_2 \in F^2$, $P_1 \neq Q_1$ i $P_2 \neq Q_2$.

- (1) Jeśli $L(P_1, Q_1) \neq L(P_2, Q_2)$, to $L(P_1, Q_1) \cap L(P_2, Q_2) \subset F^2$.
- (2) $L(P_1, Q_1) \cap C(P_2, Q_2) \subset (F(\sqrt{u}))^2$, dla pewnej liczby $u \in F$.
- (3) Jeśli $C(P_1, Q_1) \neq C(P_2, Q_2)$, to $C(P_1, Q_1) \cap C(P_2, Q_2) \subset (F(\sqrt{u}))^2$, dla pewnej liczby $u \in F$.

DOWÓD.

Ćwiczenie. □

STWIERDZENIE A.2.

Jeśli liczba c jest konstruowalna, to liczba c jest algebraiczna stopnia 2^n , dla pewnej liczby $n \in \mathbb{N}$, nad ciałem $\mathbb{Q}$.

DOWÓD.

TEORIA GALOIS

Z Lematu A.1 wynika, że istnieje ciąg ciał

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_t$$

taki, że $c \in F_t$ oraz $[F_i : F_{i-1}] \in \{1, 2\}$ dla każdego $i \in [1, t]$. W szczególności stopień $[F_t : \mathbb{Q}]$ jest potęgą dwójki na mocy Twierdzenia 1.1. Ponieważ $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq F_t$, więc korzystając ponownie z Twierdzenia 1.1, wnioskujemy, że stopień $[\mathbb{Q}(c) : \mathbb{Q}]$ też jest potęgą dwójki. W szczególności liczba c jest algebraiczna nad ciałem $\mathbb{Q}$ wobec Twierdzenia 1.8, a jej stopień jest potęgą dwójki na mocy Twierdzenia 1.4(3). $\square$

WNIOSEK A.3.

Nie istnieje konstrukcja realizująca trysekcję kąta 60° .

Dowód.

Istnienie konstrukcji realizującej trysekcję kąta 60° oznaczałoby konstruowalność liczby $\cos 20^\circ$. Ze wzoru $\cos 3\alpha = 4\cos^3 \alpha - 3\cos \alpha$ wynika jednak, że liczba $\cos 20^\circ$ jest pierwiastkiem wielomianu $8x^3 - 6x - 1$, który jest nierozkładalny nad ciałem $\mathbb{Q}$. Zatem liczba $\cos 20^\circ$ jest algebraiczna stopnia 3 nad ciałem $\mathbb{Q}$, więc nie jest konstruowalna na mocy Stwierdzenia A.2. $\square$

WNIOSEK A.4.

Nie istnieje konstrukcja realizująca podwojenie sześcianu.

Dowód.

Istnienie konstrukcji realizującej podwojenie sześcianu oznaczałoby konstruowalność liczby $\sqrt[3]{2}$, która jednak jest pierwiastkiem wielomianu $x^3 - 2$ nierozkładalnego nad ciałem $\mathbb{Q}$. Zatem liczba $\sqrt[3]{2}$ jest algebraiczna stopnia 3 nad ciałem $\mathbb{Q}$, więc nie jest konstruowalna na mocy Stwierdzenia A.2. $\square$

TEORIA GALOIS

2. PODSTAWOWE TWIERDZENIE TEORII GALOIS

DEFINICJA.

Niech F będzie rozszerzeniem ciała K . Zbiór wszystkich K -automorfizmów ciała F tworzy grupę, którą nazywamy GRUPĄ GALOIS rozszerzenia F nad ciałem K i oznaczamy $\text{Aut}_K F$.

PRZYKŁAD.

Niech K będzie ciałem. Jeśli $a \in K^\times$ i $b \in K$ to odwzorowania $\sigma_a, \tau_b: K(x) \rightarrow K(x)$ dane wzorami

$$\sigma_a\left(\frac{f}{g}\right) := \frac{f(ax)}{g(ax)} \quad \text{ i } \quad \tau_b\left(\frac{f}{g}\right) := \frac{f(x+b)}{g(x+b)} \quad (f, g \in K[x], g \neq 0),$$

są K -automorfizmami ciała $K(x)$.

Jeśli $a_1 \neq a_2$, to $\sigma_{a_1} \neq \sigma_{a_2}$, więc $|\text{Aut}_K(K(x))| = \infty$, o ile $|K| = \infty$.

Jeśli $a \neq 1$ i $b \neq 0$, to $\tau_b \circ \sigma_a \neq \sigma_a \circ \tau_b$, więc grupa $\text{Aut}_K(K(x))$ jest nieabelowa, o ile $K \not\cong \mathbb{F}_2$.

STWIERDZENIE 2.1.

Niech F będzie rozszerzeniem ciała K i $u \in F$. Jeśli $\sigma, \tau: K(u) \rightarrow F$ są K -homomorfizmami i $\sigma(u) = \tau(u)$, to $\sigma = \tau$.

DOWÓD.

Łatwo pokazać, że zbiór $\{v \in K(u) : \sigma(v) = \tau(v)\}$ jest podciałem ciała $K(u)$ zawierającym K i u , a więc równym $K(u)$. $\square$

TWIERDZENIE 2.2.

Niech F i E będą rozszerzeniami ciała K i $f \in K[x]$. Jeśli $u \in F$ jest pierwiastkiem wielomianu f oraz $\sigma: F \rightarrow E$ jest K -homomorfizmem, to $\sigma(u)$ też jest pierwiastkiem wielomianu f .

DOWÓD.

Ćwiczenie. $\square$

WNIOSEK 2.3.

Niech F będzie rozszerzeniem ciała K i $f \in K[x]$. Jeśli $u \in F$ jest pierwiastkiem wielomianu f , to $|\text{Aut}_K(K(u))| \leq m$, gdzie m jest liczbą parami różnych pierwiastków wielomianu f .

DOWÓD.

Na mocy Stwierdzenia 2.1 automorfizm $\sigma \in \text{Aut}_K(K(u))$ jest jednoznacznie wyznaczony przez wartość $\sigma(u)$, która musi być pierwiastkiem wielomianu f na mocy Twierdzenia 2.2. $\square$

PRZYKŁADY.

TEORIA GALOIS

- (1) $\text{Aut}_K K = \{\text{Id}_K\}$.
- (2) $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = \{\text{Id}_{\mathbb{Q}(\sqrt[3]{2})}\}$.
Istotnie, jeśli $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt[3]{2}))$, to $\sigma(\sqrt[3]{2})$ jest pierwiastkiem wielomianu $x^3 - 2$ na mocy Twierdzenia 2.2. Ponieważ pierwiastki wielomianu różne od $\sqrt[3]{2}$ są liczbami zespolonymi, więc $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$.
- (3) Korzystając z równości $\mathbb{C} = \mathbb{R}(\iota)$, łatwo pokazać że $\text{Aut}_{\mathbb{R}} \mathbb{C} \simeq \mathbb{Z}_2$.
Podobnie $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) \simeq \mathbb{Z}_2$.
- (4) Jeśli $\sigma \in \text{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3})$, to $\sigma(\sqrt{2}) = \pm\sqrt{2}$ oraz $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Stąd łatwo widać, że $\text{Aut}_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}, \sqrt{3}) \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Twierdzenie 2.4.

Niech F będzie rozszerzeniem ciała K .

- (1) Jeśli $H \leq \text{Aut}_K F$, to

$$H' := \{u \in F : \sigma(u) = u \text{ dla wszystkich } \sigma \in H\}$$

jest podciałem ciała F zawierającym K .

- (2) Jeśli E jest podciałem ciała F zawierającym K , to

$$E' := \{\sigma \in \text{Aut}_K F : \sigma(u) = u \text{ dla wszystkich } u \in E\}$$

jest podgrupą grupy $\text{Aut}_K F$.

Dowód.

Ćwiczenie. □

Uwaga.

Niech F będzie rozszerzeniem ciała K . Wtedy:

- (1) $F' = \{\text{Id}_F\}$;
- (2) $K' = \text{Aut}_K F$;
- (3) $\{\text{Id}_F\}' = F$.

Ponadto, jeśli E jest podciałem ciała F zawierającym K , to $E' = \text{Aut}_E F$.

Definicja.

Niech F będzie rozszerzeniem ciała K . Jeśli $K = (\text{Aut}_K F)'$, to F nazywamy **ROZSZERZENIEM GALOIS** ciała K .

Uwaga.

Niech F będzie rozszerzeniem ciała K . Jeśli $L := (\text{Aut}_K F)'$, to:

- (1) $K \subseteq L$;
- (2) $\text{Aut}_L F = \text{Aut}_K F$;

TEORIA GALOIS

- (3) F jest rozszerzeniem Galois ciała L .

PRZYKŁADY.

- (1) $\mathbb{C}$ jest rozszerzeniem Galois ciała $\mathbb{R}$.
 (2) $\mathbb{Q}(\sqrt{3})$ jest rozszerzeniem Galois ciała $\mathbb{Q}$.

LEMAT 2.5.

Niech F będzie rozszerzeniem ciała K .

- (1) $F' = \{\text{Id}_F\}$ i $K' = \text{Aut}_K F$.
 (2) $\{\text{Id}_F\}' = F$.
 (3) Jeśli E i L są podciałami ciała F zawierającymi ciało K takimi, że $L \subseteq E$, to $E' \subseteq L'$.
 (4) Jeśli $H, G \leq \text{Aut}_K F$ i $H \subseteq G$, to $G' \subseteq H'$.
 (5) Jeśli L jest podciałem ciała F zawierającym K , to $L \subseteq L''$.
 (6) Jeśli $H \leq \text{Aut}_K F$, to $H \subseteq H''$.
 (7) Jeśli E jest podciałem ciała F zawierającym K , to $E' = E'''$.
 (8) Jeśli $H \leq \text{Aut}_K F$, to $H' = H'''$.

DOWÓD.

Punkty (1)–(6) wynikają bezpośrednio z definicji.

- (7) Z punktu (5) wiemy, że $L \subseteq L''$, więc $L''' \subseteq L'$ na mocy punktu (3). Z drugiej strony, $L' \subseteq (L')'' = L'''$ na mocy (6), co kończy dowód równości $L' = L'''$.

- (8) Analogiczny do dowodu punktu (7). □

UWAGA.

Niech F będzie rozszerzeniem ciała K .

- (1) F jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy $K'' = K$.
 (2) Ogólniej, jeśli E jest podciałem ciała F zawierającym ciało K , to F jest rozszerzeniem Galois ciała E wtedy i tylko wtedy, gdy $E'' = E$.

TWIERDZENIE 2.6.

Niech F będzie rozszerzeniem ciała K . Wtedy odwzorowanie

$$\begin{aligned} \{E : E \text{ jest podciałem ciała } F, K \subseteq E \text{ i } E'' = E\} \\ \rightarrow \{H : H \leq \text{Aut}_K F \text{ i } H'' = H\}, \quad E \mapsto E', \end{aligned}$$

jest dobrze określoną bijekcją.

TEORIA GALOIS

Dowód.

Poprawność definicji wynika Lematu 2.5(8). Odwzorowanie odwrotne, poprawność definicji którego wynika z Lematu 2.5(7), dane jest wzorem $H \mapsto H'$. $\square$

LEMAT 2.7.

Niech F będzie rozszerzeniem ciała K . Jeśli $u \in F$ jest elementem algebraicznym nad K oraz f jest wielomianem minimalnym elementu u , to odwzorowanie

$$\text{Aut}_K F / \text{Aut}_{K(u)} F \rightarrow \{v \in F : f(v) = 0\}, \quad \sigma \cdot \text{Aut}_{K(u)} F \mapsto \sigma(u),$$

jest dobrze zdefiniowaną injekcją. W szczególności,

$$[\text{Aut}_K F : \text{Aut}_{K(u)} F] \leq \deg f.$$

Dowód.

Niech X zbiorem pierwiastków wielomianu f . Z Twierdzenia 2.2 wiemy, że działanie grupy $\text{Aut}_K F$ na zbiorze X dane wzorem

$$\sigma * v := \sigma(v) \quad (\sigma \in \text{Aut}_K F, v \in X),$$

jest dobrze określone. Ponadto grupa $\text{Aut}_{K(u)} F$ jest stabilizatorem elementu $u \in X$ na mocy Stwierdzenia 2.1. Stąd funkcja

$$\text{Aut}_K F / \text{Aut}_{K(u)} F \rightarrow \text{Aut}_K F * u, \quad \sigma \cdot \text{Aut}_{K(u)} F \mapsto \sigma(u),$$

jest dobrze zdefiniowaną bijekcją, gdzie $\text{Aut}_K F * u \subseteq X$ jest orbitą przy działaniu grupy $\text{Aut}_K F$ na zbiorze X . Ostatnia nierówność wynika z nierówności $|X| \leq \deg f$. $\square$

LEMAT 2.8.

Niech F będzie rozszerzeniem ciała K . Jeśli E i L są podciałami ciała F zawierającymi ciało K takimi, że $L \subseteq E$ i $[E : L] < \infty$, to $[L' : E'] \leq [E : L]$. W szczególności, jeśli $[F : K] < \infty$, to $|\text{Aut}_K F| < \infty$.

Dowód.

Dowód będzie indukcyjny ze względu na $n := [E : L]$.

Gdy $n = 1$, to teza jest oczywista.

Założmy, że $n > 1$ i wybierzmy element $u \in E \setminus L$. Ponieważ $[E : L] < \infty$, więc element u jest algebraiczny nad ciałem L na mocy Twierdzenia 1.8. Niech m będzie stopniem elementu u . Na mocy Twierdzeń 1.4(3) i 1.1

$$[L(u) : L] = m \quad \text{ i } \quad [E : L(u)] = \frac{n}{m}.$$

TEORIA GALOIS

Ponieważ $u \notin L$, więc $m > 1$. Jeśli dodatkowo $m < n$, to z założenia indukcyjnego wiemy, że

$$[L' : (L(u))'] \leq m \quad \text{ i } \quad [(L(u))' : E'] \leq \frac{n}{m},$$

więc

$$[L' : E'] = [L' : (L(u))'] \cdot [(L(u))' : E'] \leq m \cdot \frac{n}{m} = n.$$

Jeśli natomiast $m = n$, to $E = L(u)$ i nierówność $[L' : E'] \leq n$ wynika z Lematu 2.7. $\square$

LEMAT 2.9.

Niech F będzie rozszerzeniem ciała K . Jeśli $H, G \leq \text{Aut}_K F$, $H \subseteq G$ i $[G : H] < \infty$, to $[H' : G'] \leq [G : H]$.

Dowód.

Niech $n := [G : H]$ i $\sigma_1, \dots, \sigma_n$ będą reprezentantami różnych klas abstrakcji ze zbioru G/H .

Niech $u_1, \dots, u_m$ będą G' -liniowo niezależnymi elementami ciała H' .

Niech V będzie zbiorem wszystkich ciągów $(v_1, \dots, v_m) \in H'^m$ takich, że

$$\begin{aligned} \sigma_1(u_1) \cdot v_1 + \sigma_1(u_2) \cdot v_2 + \dots + \sigma_1(u_m) \cdot v_m &= 0 \\ \sigma_2(u_1) \cdot v_1 + \sigma_2(u_2) \cdot v_2 + \dots + \sigma_2(u_m) \cdot v_m &= 0 \\ \dots & \\ \sigma_n(u_1) \cdot v_1 + \sigma_n(u_2) \cdot v_2 + \dots + \sigma_n(u_m) \cdot v_m &= 0 \end{aligned}$$

Przypuśćmy, że $V \neq \{0\}$ i wybierzmy element $(v_1, \dots, v_m) \in V \setminus \{0\}$ o minimalnej liczbie niezerowych wyrazów. Bez straty ogólności możemy założyć, że $v_1 = 1$ i $\sigma_1 \in H$. Wtedy otrzymujemy $\sigma_1(u_i) = u_i$, dla każdego $j \in [1, m]$, więc pierwsze równanie przyjmuje postać

$$u_1 \cdot v_1 + u_2 \cdot v_2 + \dots + u_m \cdot v_m = 0.$$

Z G' -linowej niezależności elementów $u_1, \dots, u_m$ wynika, że istnieje $j \in [1, m]$ takie, że $v_j \notin G'$. Oczywiście $j \neq 1$, gdyż $v_1 = 1$. Bez straty ogólności założymy, że $v_2 \notin G'$, i wybierzmy automorfizm $\sigma \in G$ taki, że $\sigma(v_2) \neq v_2$.

Niech V' będzie zbiorem wszystkich ciągów $(v'_1, \dots, v'_m) \in H'^m$ takich, że

$$\begin{aligned} (\sigma \circ \sigma_1)(u_1) \cdot v'_1 + (\sigma \circ \sigma_1)(u_2) \cdot v'_2 + \dots + (\sigma \circ \sigma_1)(u_m) \cdot v'_m &= 0 \\ (\sigma \circ \sigma_2)(u_1) \cdot v'_1 + (\sigma \circ \sigma_2)(u_2) \cdot v'_2 + \dots + (\sigma \circ \sigma_2)(u_m) \cdot v'_m &= 0 \\ \dots & \\ (\sigma \circ \sigma_n)(u_1) \cdot v'_1 + (\sigma \circ \sigma_n)(u_2) \cdot v'_2 + \dots + (\sigma \circ \sigma_n)(u_m) \cdot v'_m &= 0 \end{aligned}$$

TEORIA GALOIS

Wtedy $V = V'$. Istotnie, $\sigma \circ \sigma_1, \dots, \sigma \circ \sigma_n$ będą reprezentantami różnych klas abstrakcji ze zbioru G/H . Ponadto, jeśli $i \in [1, n]$, to istnieje $i' \in [1, n]$ takie, że $(\sigma \circ \sigma_i)^{-1} \circ \sigma_{i'} \in H$, i wtedy

$$(\sigma \circ \sigma_i)(u_j) = \sigma_{i'}(u_j),$$

dla każdego $j \in [1, m]$, gdyż $u_j \in H'$.

Zauważmy, że $(\sigma(v_1), \dots, \sigma(v_m)) \in V' = V$, zatem $(v_1 - \sigma(v_1), \dots, v_m - \sigma(v_m)) \in V$. Ponieważ $v_2 - \sigma(v_2) \neq 0$, więc $(v_1 - \sigma(v_1), \dots, v_m - \sigma(v_m)) \in V \setminus \{0\}$. Z drugiej strony,

$$v_1 - \sigma(v_1) = 1 - \sigma(1) = 1 - 1 = 0$$

oraz

$$v_j - \sigma(v_j) = 0 - \sigma(0) = 0 - 0 = 0,$$

jeśli $v_j = 0$, więc $(v_1 - \sigma(v_1), \dots, v_m - \sigma(v_m))$ ma mniej niezerowych współrzędnych niż $(v_1, \dots, v_m)$, sprzeczność.

Zatem $V = 0$, co oznacza, że $m \leq n$, i kończy dowód. $\square$

LEMAT 2.10.

Niech F będzie rozszerzeniem ciała K .

- (1) Jeśli E i L są podciałami ciała F zawierającymi ciało K takimi, że $L \subseteq E$, $[E : L] < \infty$ i $L'' = L$, to $E'' = E$ i $[L' : E'] = [E : L]$.
- (2) Jeśli $H, G \leq \text{Aut}_K F$, $H \subseteq G$, $H'' = H$ i $[G : H] < \infty$, to $G'' = G$ i $[H' : G'] = [G : H]$.
- (3) Jeśli $[F : K] < \infty$ i $K'' = K$, to:
 - (a) $E'' = E$ dla każdego podciała ciała F zawierającego ciało K ;
 - (b) $H'' = H$ dla każdej podgrupy grupy $\text{Aut}_K F$,
 - (c) $|\text{Aut}_K F| = [F : K]$.

UWAGA.

Niech F będzie rozszerzeniem ciała K . Ponieważ $\{\text{Id}_F\}'' = \{\text{Id}_F\}$ (Lemat 2.5(1) i (2)), więc Lemat 2.10(2) implikuje, że jeśli G jest skończoną podgrupą grupy $\text{Aut}_K F$, to $G'' = G$.

DOWÓD.

- (1) Z Lematu 2.5(5) wiemy, że $E \subseteq E''$. Zatem stosując założenie $L'' = L$ oraz Lematy 2.9 i 2.8, otrzymujemy, że

$$[E : L] \leq [E'' : L] = [E'' : L''] \leq [L' : E'] \leq [E : L],$$

skąd $[L' : E'] = [E : L] = [E'' : L]$. Ponieważ $E \subseteq E''$ i $[E : L] < \infty$, druga z równości oznacza, że $E'' = E$.

TEORIA GALOIS

- (2) Podobnie jak (1).
- (3) Jeśli E jest podciałem ciała F zawierającym ciało K , to $[E : K] \leq [F : K] < \infty$, więc równość $E'' = E$ wynika z punktu (1). Podobnie, jeśli H jest podgrupą grupy $\text{Aut}_K F$, to z Lematu 2.8 wiemy, że

$$[H : \{\text{Id}_F\}] = |H| \leq |\text{Aut}_K F| \leq [F : K] < \infty.$$

Wykorzystując równość $\{\text{Id}_F\}'' = \{\text{Id}_F\}$, równość $H'' = H$ otrzymujemy z punktu (2).

Na zakończenie przypomnijmy, że $\text{Aut}_K F = K'$ i $\{\text{Id}_F\} = F'$ (Lemat 2.5(1)), zatem

$$|\text{Aut}_K F| = [\text{Aut}_K F : \{\text{Id}_F\}] = [K' : F'] = [F : K]$$

na mocy punktu (1). □

DEFINICJA.

Niech F będzie rozszerzeniem ciała K . Podciało E ciała F zawierające ciało K nazywamy STABILNYM, jeśli $\sigma(E) \subseteq E$ dla każdego automorfizmu $\sigma \in \text{Aut}_K F$.

UWAGA.

Niech F będzie rozszerzeniem ciała K . Jeśli E jest stabilnym podciałem ciała F zawierającym ciało K oraz $\sigma \in \text{Aut}_K F$, to $\sigma|_E \in \text{Aut}_K E$ ($(\sigma|_E)^{-1} = (\sigma^{-1}|_E)$).

LEMAT 2.11.

Niech F będzie rozszerzeniem ciała K .

- (1) Jeśli E jest stabilnym podciałem ciała K zawierającym ciało K , to podgrupa E' jest dzielnikiem normalnym grupy $\text{Aut}_K F$.
- (2) Jeśli H jest dzielnikiem normalnym grupy $\text{Aut}_K F$, to podciało H' jest stabilne.

DOWÓD.

- (1) Ustalmy automorfizmy $\sigma \in \text{Aut}_K F$ i $\tau \in E'$ oraz element $u \in E$. Ponieważ podciało E jest stabilne, więc $\sigma^{-1}(u) \in E$, zatem $\tau(\sigma^{-1}(u)) = \sigma^{-1}(u)$, gdyż $\tau \in E'$. Stąd

$$(\sigma \circ \tau \circ \sigma^{-1})(u) = \sigma(\tau(\sigma^{-1}(u))) = \sigma(\sigma^{-1}(u)) = u,$$

więc $\sigma \circ \tau \circ \sigma^{-1} \in E'$.

TEORIA GALOIS

- (2) Ustalmy automorfizmy $\sigma \in \text{Aut}_K F$ i $\tau \in H$ oraz element $u \in H'$. Ponieważ H jest dzielnikiem normalnym grupy $\text{Aut}_K F$, więc $\sigma^{-1} \circ \tau \circ \sigma \in H$. Stąd $(\sigma^{-1} \circ \tau \circ \sigma)(u) = u$, a więc $\tau(\sigma(u)) = \sigma(u)$. Z dowolności automorfizmu τ wynika, że $\sigma(u) \in H'$. $\square$

LEMAT 2.12.

Niech F będzie rozszerzeniem Galois ciała K . Jeśli E jest stabilnym podciałem ciała F zawierającym ciało K , to E jest rozszerzeniem Galois ciała K .

DOWÓD.

Ustalmy element $u \in E \setminus K$. Ponieważ F jest rozszerzeniem Galois ciała K , więc istnieje automorfizm $\sigma \in \text{Aut}_K F$ taki, że $\sigma(u) \neq u$. Korzystając ze stabilności podciała E , otrzymujemy, że $\tau := \sigma|_E \in \text{Aut}_K E$. Ponieważ $\tau(u) = \sigma(u) \neq u$, więc z dowolności elementu u wynika, że E jest rozszerzeniem Galois ciała K . $\square$

OZNACZENIE.

Niech K będzie ciałem. Jeśli $f, g \in K[x]$, to piszemy $f \sim g$ (i mówimy, że wielomiany f i g są stowarzyszone), jeśli $f \mid g$ i $g \mid f$.

LEMAT 2.13.

Niech F będzie rozszerzeniem Galois ciała K . Jeśli $f \in K[x]$ jest wielomianem nierozkładalnym posiadającym pierwiastek w ciele F , to istnieją parami różne elementy $u_1, \dots, u_n \in F$ takie, że $f \sim (x - u_1) \cdots (x - u_n)$.

DOWÓD.

Niech $u_1, \dots, u_n \in F$ będą parami różnymi pierwiastkami wielomianu f i $g := (x - u_1) \cdots (x - u_n)$. Jeśli $\sigma \in \text{Aut}_K F$, to σ permutuje elementy $u_1, \dots, u_n$ na mocy Twierdzenia 2.2. Stąd $\sigma(g) = g$. Ponieważ F jest rozszerzeniem Galois ciała K , więc oznacza to, że $g \in K[x]$. Ponadto $g \mid f$ oraz $\deg g > 0$. Z nierozkładalności wielomianu wynika, że $f \sim g$. $\square$

LEMAT 2.14.

Niech F będzie rozszerzeniem ciała K . Jeśli E jest podciałem ciała F zawierającym ciało K , które jest algebraicznym rozszerzeniem Galois ciała K , to podciało E stabilne.

DOWÓD.

Ustalmy element u ciała E i niech $f \in K[x]$ będzie wielomianem minimalnym elementu u (wielomian f istnieje, gdyż E jest rozszerzeniem algebraicznym ciała K). Z Lematu 2.13 i unormowania wielomianu f wiemy, że istnieją parami różne elementy $u_1, \dots, u_n \in E$ takie, że $f = (x - u_1) \cdots (x - u_n)$. W szczególności, jeśli $v \in F$ jest pierwiastkiem wielomianu f , to $v \in E$.

TEORIA GALOIS

Ustalmy $\sigma \in \text{Aut}_K F$. Z Twierdzenia 2.2 wiemy, że $f(\sigma(u)) = 0$, zatem $\sigma(u) \in E$ na mocy powyższej obserwacji. Z dowolności automorfizmu σ wynika, że podciało E jest stabilne. $\square$

WNIOSEK 2.15.

Niech F będzie algebraicznym rozszerzeniem Galois ciała K . Jeśli E jest podciałem ciała F zawierającym ciało K takim że $E'' = E$, to E jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy podgrupa $\text{Aut}_E F$ jest dzielnikiem normalnym grupy $\text{Aut}_K F$.

UWAGA.

W dowodzie Twierdzenia 3.10 pokażemy, że jeśli E jest podciałem ciała F zawierającym ciało K , to $E'' = E$.

Dowód.

Założmy najpierw, że E jest rozszerzeniem Galois ciała K . Ponieważ F , a więc również E , jest rozszerzeniem algebraicznym ciała K , więc podciało E jest stabilne na mocy Lematu 2.14, zatem Lemat 2.11(1) implikuje, że podgrupa $\text{Aut}_E F$ jest dzielnikiem normalnym grupy $\text{Aut}_K F$.

Założmy teraz, że podgrupa $\text{Aut}_E F$ jest dzielnikiem normalnym grupy $\text{Aut}_K F$. Wtedy podciało $(\text{Aut}_E F)' = E''$ jest stabilne na mocy Lematu 2.11(2). Ponieważ $E'' = E$, więc E jest stabilnym podciałem ciała F zawierającym ciało K , skąd E jest rozszerzeniem Galois ciała K wobec Lematu 2.12. $\square$

OZNACZENIE.

Niech F będzie rozszerzeniem ciała K . Jeśli E jest podciałem ciała F zawierającym ciało K , to

$$\begin{aligned} \text{Ext}_E F &:= \\ &\{\tau \in \text{Aut}_K E : \text{istnieje automorfizm } \sigma \in \text{Aut}_K F \text{ taki, że } \tau = \sigma|_E\}. \end{aligned}$$

UWAGA.

Niech F będzie rozszerzeniem ciała K . Jeśli E jest podciałem ciała F zawierającym ciało K , to zbiór $\text{Ext}_E F$ jest podgrupą grupy $\text{Aut}_K E$.

LEMAT 2.16.

Niech F będzie rozszerzeniem ciała K . Jeśli E jest stabilnym podciałem ciała F zawierającym ciało K , to

$$\text{Ext}_E F \simeq \text{Aut}_K F / \text{Aut}_E F.$$

Dowód.

Rozważmy odwzorowanie $\varphi: \text{Aut}_K F \rightarrow \text{Ext}_E F$ dane wzorem

$$\varphi(\sigma) := \sigma|_E \quad (\sigma \in \text{Aut}_K F).$$

TEORIA GALOIS

Ponieważ podciało E jest stabilne, więc funkcja φ jest dobrze zdefiniowanym homomorfizmem. Z definicji grupy $\text{Ext}_E F$ wynika, że $\text{Im } \varphi = \text{Ext}_E F$. Ponadto łatwo widzieć, że $\text{Ker } \varphi = \text{Aut}_E F$, zatem teza wynika z Pierwszego Twierdzenia o Izomorfizmie. $\square$

Twierdzenie 2.17 (Podstawowe Twierdzenie Teorii Galois).

Niech F będzie skończenie wymiarowym rozszerzeniem Galois ciała K . Wtedy odwzorowanie

$$\begin{aligned} \{E : E \text{ jest podciałem ciała } F \text{ i } K \subseteq E\} \\ \rightarrow \{H : H \leq \text{Aut}_K F\}, \quad E \mapsto E', \end{aligned}$$

jest bijekcją taką, że:

- (1) jeśli E i L są podciałami ciała F zawierającymi ciało K takimi, że $L \subseteq E$, to

$$[E : L] = [L' : E'];$$

w szczególności, $[F : K] = |\text{Aut}_K F|$;

- (2) jeśli E jest podciałem ciała F zawierającym ciało K , to F jest rozszerzeniem Galois ciała E ;
- (3) jeśli E jest podciałem ciała F zawierającym ciało K , to E jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy podgrupa $\text{Aut}_E F$ jest dzielnikiem normalnym grupy $\text{Aut}_K F$;
- (4) jeśli E jest podciałem ciała F będącym rozszerzeniem Galois ciała K , to $\text{Aut}_K E \simeq \text{Aut}_K F / \text{Aut}_E F$.

Dowód.

Ponieważ F jest skończenie wymiarowym rozszerzeniem Galois ciała K , więc z Lematu 2.10(3) wiemy, że $E'' = E$ dla każdego podciała ciała E zawierającego ciało K oraz $H'' = H$ dla każdej podgrupy H grupy $\text{Aut}_K F$. Zatem odwzorowanie

$$\begin{aligned} \{E : E \text{ jest podciałem ciała } F \text{ i } K \subseteq E\} \\ \rightarrow \{H : H \leq \text{Aut}_K F\}, \quad E \mapsto E', \end{aligned}$$

jest bijekcją na mocy Twierdzenia 2.6.

- (1) Jeżeli E i L są podciałami ciała F zawierającymi ciało K takimi, że $L \subseteq E$, to $L'' = L$ na mocy Lematu 2.10(3). Ponieważ $[E : L] \leq [F : K] < \infty$, więc Lemat 2.10(1) implikuje, że $[L' : E'] = [L : E]$.

TEORIA GALOIS

- (2) Korzystając ponownie z Lematu 2.10(3), wiemy, że jeśli E jest podciałem ciała F zawierającym ciało K , to $E'' = E$.
- (3) Ponieważ $[F : K] < \infty$, więc z Twierdzenia 1.8 wiemy, że E jest rozszerzeniem algebraicznym ciała K . Ponadto $E'' = E$ dla każdego podciała ciała E zawierającego ciało K (Lemat 2.10(3) po raz kolejny), więc teza wynika z Wniosku 2.15.
- (4) Niech E będzie podciałem ciała F będącym rozszerzeniem Galois ciała K . Podobnie jak powyżej pokazujemy, że podciało E jest stabilne, więc z Lematu 2.16 wiemy, że $\text{Ext}_E F \simeq \text{Aut}_K F / \text{Aut}_E F = K' / E'$. W szczególności, $|\text{Ext}_E F| = [K' : E']$. Z drugiej strony, z punktu (1) wiemy, że $[K' : E'] = [E : K] = |\text{Aut}_K E|$ (druga z równości jest konsekwencją założenia, że E jest rozszerzeniem Galois ciała K). Zatem $|\text{Ext}_E F| = |\text{Aut}_K E|$. Ponieważ $\text{Ext}_E F \leq \text{Aut}_K E$ i $|\text{Aut}_K F| = [E : K] \leq [F : K] < \infty$, więc $\text{Ext}_E F = \text{Aut}_K F$, co kończy dowód. $\square$

Twierdzenie 2.18 (Artin).

Niech F będzie ciałem i $G \leq \text{Aut } F$. Jeśli

$$K := \{u \in F : \sigma(u) = u \text{ dla każdego } \sigma \in G\},$$

to F jest rozszerzeniem Galois ciała K . Jeśli dodatkowo $|G| < \infty$, to $[F : K] < \infty$ i $\text{Aut}_K F = G$.

Dowód.

Oczywiście $G \leq \text{Aut}_K F$ oraz $K = G'$. Zatem $K'' = G''' = G' = K$, gdzie druga równość wynika z Lematu 2.5(8). Innymi słowy, F jest rozszerzeniem Galois ciała K .

Założmy teraz dodatkowo, że $|G| < \infty$. Z Lematu 2.9 wiemy, że

$$[F : K] = [\{\text{Id}\}' : G'] \leq [G : \{\text{Id}\}] = |G| < \infty.$$

W szczególności F jest skończone wymiarowym rozszerzeniem Galois ciała K . Z Lematu 2.10(3) wiemy zatem, że $G = G'' = K' = \text{Aut}_K F$, co kończy dowód. $\square$

TEORIA GALOIS

3. CIAŁO ROZKŁADU WIELOMIANU, DOMKNIĘCIE ALGEBRAICZNE I NORMALNOŚĆ

DEFINICJA.

Niech K będzie ciałem i $f \in K[x]$, $f \neq 0$. Rozszerzenie F ciała K nazywamy CIAŁEM ROZKŁADU wielomianu f (nad ciałem K), jeśli istnieją elementy $u_1, \dots, u_n \in F$ takie, że

$$F = K(u_1, \dots, u_n) \quad \text{i} \quad f \sim (x - u_1) \cdots (x - u_n).$$

Ogólniej, jeśli $S \subseteq K[x] \setminus \{0\}$, to rozszerzenie F ciała K nazywamy CIAŁEM ROZKŁADU (wielomianów ze) zbioru S (nad ciałem K), jeśli istnieją elementy $u_{f,i} \in F$, $f \in S$, $i \in [1, n_f]$, gdzie $n_f := \deg f$, takie, że

$$F = K(u_{f,i} : f \in S \text{ i } i \in [1, n_f]) \quad \text{i} \quad f \sim (x - u_{f,1}) \cdots (x - u_{f,n_f})$$

dla każdego $f \in S$.

PRZYKŁADY.

- (1) $\mathbb{Q}(\sqrt{2})$ jest ciałem rozkładu wielomianu $x^2 - 2 \in \mathbb{Q}[x]$.
- (2) $\mathbb{C}$ jest ciałem rozkładu wielomianu $x^2 + 1 \in \mathbb{R}[x]$.
- (3) $\mathbb{Q}(\sqrt[3]{2})$ nie jest ciałem rozkładu wielomianu $x^3 - 2 \in \mathbb{Q}[x]$.

UWAGA.

Niech K będzie ciałem i F ciałem rozkładu zbioru $S \subseteq K[x] \setminus \{0\}$.

- (1) Ciało F jest rozszerzeniem algebraicznym ciała K na mocy Twierdzenia 1.9.
- (2) Jeśli $|S| < \infty$, to $[F : K] < \infty$ oraz istnieje wielomian $f \in K[x]$ taki, że F jest ciałem rozkładu wielomianu f .
- (3) Jeśli E jest podciałem ciała F zawierającym ciało K , to F jest ciałem rozkładem zbioru S nad E .

Twierdzenie 3.1.

Niech K będzie ciałem. Jeśli $f \in K[x]$ i $n := \deg f > 0$, to istnieje ciało F rozkładu wielomianu f takie, że $[F : K] \leq n!$.

Dowód.

Dowód będzie indukcyjny ze względu na n . Gdy $n = 1$, to teza jest oczywista. Załóżmy zatem, że $n > 1$. Na mocy Twierdzenia 1.7 istnieje rozszerzenie E ciała K oraz element $u \in E$ takie, że $E = K(u)$, $f(u) = 0$ oraz $[E : K] \leq n$. Ponieważ $f(u) = 0$, więc istnieje wielomian $g \in E[x]$ taki, że $f = (x - u) \cdot g$. Wtedy $\deg g = n - 1$, więc z założenia indukcyjnego istnieje ciało F rozkładu

TEORIA GALOIS

wielomianu g nad ciałem E takie, że $[F : E] \leq (n-1)!$. Wtedy F jest ciałem rozkładu wielomianu f nad ciałem K oraz

$$[F : K] = [F : E] \cdot [E : K] \leq n \cdot (n-1)! = n!$$

na mocy Twierdzenia 1.1. □

Twierdzenie 3.2.

Dla ciała F następujące warunki są równoważne.

- (1) Dla każdego wielomianu $f \in F[x]$, jeśli $\deg f > 0$, to istnieje element $u \in F$ taki, że $f(u) = 0$.
- (2) Dla każdego wielomianu $f \in F[x]$, jeśli $f \neq 0$, to istnieją elementy $u_1, \dots, u_n \in F$ takie, że $f \sim (x - u_1) \cdots (x - u_n)$.
- (3) Jeśli wielomian $f \in F[x]$ jest nierozkładalny, to $\deg f = 1$.
- (4) Jeśli E jest rozszerzeniem algebraicznym ciała F , to $E = F$.
- (5) Istnieje podciało K ciała F takie, że ciało F jest rozszerzeniem algebraicznym ciała K i dla każdego wielomianu $f \in K[x] \setminus \{0\}$ istnieją elementy $u_1, \dots, u_n \in F$ takie, że $f \sim (x - u_1) \cdots (x - u_n)$.

Dowód.

- (1) $\iff$ (2): Ćwiczenie.
- (2) $\iff$ (3): Ćwiczenie.
- (3) $\implies$ (4): Niech E będzie rozszerzeniem algebraicznym ciała F . Ustalmy element $u \in E$. Jeśli $f \in F[x]$ jest wielomianem minimalnym elementu u , to z założenia $\deg f = 1$, więc $f \sim x - u$, zatem $u \in F$.
- (4) $\implies$ (3): Niech $f \in K[x]$ będzie wielomianem nierozkładalnym. Z Twierdzenia 1.7 wiemy, że istnieje rozszerzenie E ciała F takie, że $[E : F] = \deg f$. Z Twierdzenia 1.8 wiemy, że E jest rozszerzeniem algebraicznym ciała F , a więc z założenia $E = F$. Stąd $\deg f = [E : F] = 1$.
- (2) $\implies$ (5): Wystarczy przyjąć $K = F$.
- (5) $\implies$ (4): Niech E będzie rozszerzeniem algebraicznym ciała F i ustalmy element $u \in E$. Z Twierdzenia 1.10 wiemy, że E jest rozszerzeniem algebraicznym ciała K , więc istnieje niezerowy wielomian $f \in K[x]$ taki, że $f(u) = 0$. Ponieważ z założenia istnieją elementy $u_1, \dots, u_n \in F$ takie, że $f \sim (x - u_1) \cdots (x - u_n)$, więc istnieje $i \in [1, n]$ takie, że $u = u_i \in F$. □

DEFINICJA.

Ciało F spełniające równoważne warunki z Twierdzenia 3.2 nazywamy ALGEBRAICZNIE DOMKNIĘTYM.

TEORIA GALOIS

PRZYKŁAD.

Zasadnicze Twierdzenie Algebry (Twierdzenie B.3) orzeka, że ciało $\mathbb{C}$ liczb zespolonych jest algebraicznie domknięte.

TWIERDZENIE 3.3.

Następujące warunki są równoważne dla rozszerzenia F ciała K .

- (1) F jest rozszerzeniem algebraicznym ciała K i ciało F jest algebraicznie domknięte.
- (2) F jest ciałem rozkładu zbioru $K[x] \setminus \{0\}$.
- (3) F jest ciałem rozkładu zbioru $\{f \in K[x] : f \text{ jest nierozkładalny}\}$.

Dowód.

(1) $\implies$ (3): Ponieważ ciało F jest algebraicznie domknięte, więc na mocy Twierdzenia 3.2(2) dla każdego wielomianu nierozkładalnego $f \in K[x] \subseteq F[x] \setminus \{0\}$ istnieją elementy $u_{f,1}, \dots, u_{f,n_f} \in F$, gdzie $n_f := \deg f$, takie, że $f \sim (x - u_{f,1}) \cdots (x - u_{f,n_f})$. Aby pokazać, że

$$F = K(u_{f,i} : f \in K[x] \text{ nierozkładalny i } i \in [1, n_f]),$$

ustalmy element $u \in F$. Ponieważ F jest rozszerzeniem algebraicznym ciała K , więc istnieje wielomian minimalny $f \in K[x]$ elementu u . Wtedy $u = u_{f,i}$ dla pewnego $i \in [1, n_f]$, zatem

$$F \subseteq K(u_{f,i} : f \in K[x] \text{ nierozkładalny i } i \in [1, n_f]).$$

Inkluzja $K(u_{f,i} : f \in K[x] \text{ nierozkładalny i } i \in [1, n_f]) \subseteq F$ jest oczywista.

(3) $\implies$ (2): Z założenia dla każdego wielomianu nierozkładalnego $f \in K[x]$ istnieją elementy $u_{f,1}, \dots, u_{f,n_f} \in F$, gdzie $n_f := \deg f$, takie, że

$$f \sim (x - u_{f,1}) \cdots (x - u_{f,n_f}).$$

Ponadto $F = K(u_{f,i} : f \in K[x] \text{ nierozkładalny i } i \in [1, n_f])$. Jeśli $g \in K[x] \setminus \{0\}$, to istnieją wielomiany nierozkładalne $f_1, \dots, f_m \in K[x]$ takie, że

$$g \sim f_1 \cdots f_m \sim \prod_{j \in [1, m]} (x - u_{f_j,1}) \cdots (x - u_{f_j, n_{f_j}}).$$

Kładąc $u_{g, n_{f_1} + \dots + n_{f_{j-1}} + i} := u_{f_j, i}$ dla $j \in [1, m]$ i $i \in [1, n_{f_j}]$ (oraz wszystkich wielomianów $g \in K[x] \setminus \{0\}$), otrzymujemy

$$\begin{aligned} F &= K(u_{f,i} : f \in K[x] \text{ nierozkładalny i } i \in [1, n_f]) \\ &= K(u_{g,i} : g \in K[x] \setminus \{0\} \text{ i } i \in [1, \deg g]). \end{aligned}$$

TEORIA GALOIS

(2) $\implies$ (1): Z założenia dla każdego wielomianu $f \in K[x]$ istnieją elementy $u_{f,1}, \dots, u_{f,n_f} \in F$, gdzie $n_f := \deg f$, takie, że $f \sim (x - u_{f,1}) \cdots (x - u_{f,n_f})$. Ponadto $F = K(u_{f,i} : f \in K[x] \setminus \{0\} \text{ i } i \in [1, n_f])$. Z definicji element $u_{f,i}$ jest algebraiczny nad ciałem K dla każdego wielomianu $f \in K[x] \setminus \{0\}$ oraz $i \in [1, n_f]$, więc ciało F jest rozszerzeniem algebraicznym ciała K na mocy Twierdzenia 1.9. Korzystając z Twierdzenia 3.2(5), otrzymujemy, że ciało F jest algebraicznie domknięte. $\square$

DEFINICJA.

Ciało F spełniające równoważne warunki z Twierdzenia 3.3 nazywamy DOMKNIĘCIEM ALGEBRAICZNYM ciała K .

PRZYKŁAD.

Ciało $\mathbb{C}$ jest domknięciem algebraicznym ciała $\mathbb{R}$ liczb rzeczywistych.

LEMAT 3.4.

Jeśli F jest rozszerzeniem algebraicznym ciała K , to $|F| \leq \aleph_0 \cdot |K|$.

DOWÓD.

Łatwo pokazać, że $|K[x]| = \aleph_0 \cdot |K|$. Rozważmy odwzorowanie $\Phi: F \rightarrow K[x]$ dane wzorem

$$\Phi(u) := \text{wielomian minimalny elementu } u \quad (u \in F).$$

Wtedy $|\Phi^{-1}(f)| \leq \aleph_0$ dla każdego wielomianu $f \in K[x]$, więc

$$|F| \leq \aleph_0 \cdot |K[x]| = \aleph_0 \cdot \aleph_0 \cdot |K| = \aleph_0 \cdot |K|. \quad \square$$

TWIERDZENIE 3.5.

Dla każdego ciała K istnieje jego algebraiczne domknięcie.

DOWÓD.

Wybierzmy zbiór S taki, że $|S| > \aleph_0 \cdot |K|$ i $K \subset S$. Oznaczmy przez $\mathcal{E}$ zbiór (!) wszystkich rozszerzeń algebraicznych E ciała K takich, że $E \subseteq S$. Oczywiście $K \in \mathcal{E}$. W zbiorze $\mathcal{E}$ wprowadzamy relację częściowego porządku poprzez warunek: $E_1 \preceq E_2$, jeśli ciało E_2 jest rozszerzeniem ciała E_1 . Jeśli $(E_i)_{i \in I}$ jest łańcuchem elementów zbioru $\mathcal{E}$, to $\bigcup_{i \in I} E_i \in \mathcal{E}$, zatem z Lematu Kuratowskiego–Zorna wynika, że w zbiorze $\mathcal{E}$ istnieje element maksymalny. Pokażemy, że jeśli E jest elementem maksymalnym w zbiorze $\mathcal{E}$, to E jest domknięciem algebraicznym ciała K . Oczywiście ciało E jest rozszerzeniem algebraicznym ciała K , więc musimy jedynie pokazać, że ciało E jest algebraicznie domknięte.

Niech F będzie rozszerzeniem algebraicznym ciała E . Z Twierdzenia 1.10 wiemy, że wtedy F jest rozszerzeniem algebraicznym ciała K , więc $|F| \leq \aleph_0 \cdot |K|$

TEORIA GALOIS

na mocy Lematu 3.4. Korzystając ponownie z Lematu 3.4, wiemy, że również $|E| \leq \aleph_0 \cdot |K|$. Ponieważ $|S| > \aleph_0 \cdot |K|$, więc $|S - E| > \aleph_0 \cdot |K|$. Stąd

$$|F - E| \leq |F| \leq \aleph_0 \cdot |K| < |S - E|,$$

więc istnieje iniekcja $\xi: F \rightarrow S$ taka, że $\xi(u) = u$ dla wszystkich $u \in E$. Utożsamiając F z $\xi(F)$, możemy założyć, że $F \subseteq S$, a więc $F \in \mathcal{E}$. Z maksymalności ciała E wynika, że $F = E$, co kończy dowód. $\square$

WNIOSEK 3.6.

Niech K będzie ciałem. Jeśli $S \subseteq K[x] \setminus \{0\}$, to istnieje ciało rozkładu wielomianów ze zbioru S nad ciałem K .

DOWÓD.

Niech F będzie domknięciem algebraicznym ciała K oraz

$$X := \{u \in F : \text{istnieje wielomian } f \in S \text{ taki, że } f(u) = 0\}.$$

Wtedy ciało $K(X)$ jest ciałem rozkładu zbioru S . $\square$

TWIERDZENIE 3.7.

Niech $\sigma: K \rightarrow L$ będzie izomorfizmem ciał i $S \subseteq K[x] \setminus \{0\}$. Jeśli F jest ciałem rozkładu zbioru S nad ciałem K , a E jest ciałem rozkładu zbioru $\sigma(S)$ nad ciałem L , to istnieje izomorfizm $\bar{\sigma}: F \rightarrow E$ taki, że $\bar{\sigma}|_K = \sigma$.

DOWÓD.

Niech $\mathcal{S}$ będzie zbiorem wszystkich trójek (M, N, τ) takich, że M jest podciałem ciała F zawierającym ciało K , N jest podciałem ciała E zawierającym ciało L oraz $\tau: M \rightarrow N$ jest izomorfizmem takim, że $\tau|_K = \sigma$. W zbiorze $\mathcal{S}$ wprowadzamy relację częściowego porządku poprzez warunek: $(M_1, N_1, \tau_1) \preceq (M_2, N_2, \tau_2)$, jeśli $M_1 \subseteq M_2$, $N_1 \subseteq N_2$ i $\tau_2|_{M_1} = \tau_1$. Korzystając z Lematu Kuratowskiego–Zorna, łatwo pokazać, że w zbiorze $\mathcal{S}$ istnieje element maksymalny. Pokażemy, że jeśli trójka (M, N, τ) jest elementem maksymalnym w zbiorze $\mathcal{S}$, to $M = F$ i $N = E$, co zakończy dowód.

Aby pokazać, że $M = F$, wystarczy udowodnić, że jeśli $f \in S$, $g \in K[x]$ jest unormowanym dzielnikiem nierozkładalym wielomianu f i $g(u) = 0$ dla pewnego $u \in F$, to $u \in M$. W powyższej sytuacji wiemy jednak, że istnieje element $v \in E$ taki, że $(\sigma g)(v) = 0$. Zauważmy, że $\sigma g = \tau g$, zatem korzystając z Twierdzenia 1.5(2), wiemy, że istnieje izomorfizm $\bar{\tau}: M(u) \rightarrow N(v)$ taki, że $\bar{\tau}|_M = \tau$. Wobec maksymalności trójki (M, N, τ) oznacza to, że $M(u) = M$, tzn. $u \in M$.

Równość $N = E$ pokazujemy analogicznie. $\square$

WNIOSEK 3.8.

Niech $S \subseteq K[x] \setminus \{0\}$. Jeśli F i E są ciałami rozkładu zbioru S nad ciałem K ,

TEORIA GALOIS

to ciała F i E są K -izomorficzne. W szczególności, jeśli F i E są domknięciami algebraicznymi ciała K , to ciała E i F są K -izomorficzne.

DOWÓD.

Pierwsza część wynika z Twierdzenia 3.7 zastosowanego dla $\sigma := \text{Id}_K$. Druga jest szczególną wersją pierwszej na mocy Twierdzenia 3.3(2). $\square$

DEFINICJA.

Niech K będzie ciałem. Wielomian nierozkładalny $f \in K[x]$ nazywamy ROZDZIELCZYM, jeśli f ma tylko pierwiastki jednokrotne w swoim ciele rozkładu.

UWAGA.

Niech K będzie ciałem. Wielomian $f \in K[x]$ ma tylko pierwiastki jednokrotne w swoim ciele rozkładu wtedy i tylko wtedy, gdy wielomian f i jego pochodna są względnie pierwsze. W konsekwencji, wielomian nierozkładalny jest rozdzielnym wtedy i tylko wtedy, gdy jego pochodna jest niezerowa. W szczególności, jeśli $\text{char } K = 0$, to każdy wielomian nierozkładalny jest rozdzielnym.

DEFINICJA.

Niech F będzie rozszerzeniem ciała K .

- (1) Element u ciała F nazywamy ROZDZIELCZYM nad ciałem K , jeśli element u jest algebraiczny nad ciałem K oraz wielomian minimalny elementu u nad ciałem K jest rozdzielnym.
- (2) Ciało F nazywamy rozszerzeniem ROZDZIELCZYM ciała K , jeśli każdy element ciała F jest rozdzielnym nad ciałem K .

UWAGA.

Niech K będzie ciałem. Jeśli $\text{char } K = 0$, to każde rozszerzenie algebraiczne ciała K jest rozdzielnym.

TWIERDZENIE 3.9.

Następujące warunki są równoważne dla rozszerzenia F ciała K .

- (1) F jest algebraicznym rozszerzeniem Galois ciała K .
- (2) F jest rozszerzeniem rozdzielnym ciała K , które jest ciałem rozkładu pewnego zbioru wielomianów z $K[x] \setminus \{0\}$.
- (3) F jest ciałem rozkładu pewnego zbioru wielomianów rozdzielnych z $K[x]$.

DOWÓD.

(1) $\implies$ (2): Dla każdego elementu $u \in F$ oznaczamy przez f_u wielomian minimalny elementu u nad ciałem K (taki wielomian istnieje, gdyż F jest rozszerzeniem algebraicznym ciała K). Z Lematu 2.13 wiemy, że dla każdego

TEORIA GALOIS

elementu $u \in F$ istnieją parami różne elementy $v_1, \dots, v_{n_u} \in F$, takie, że $f_u = (x - v_1) \cdots (x - v_{n_u})$. W szczególności wielomian f_u jest rozdzielnym dla każdego $u \in F$ oraz F jest ciałem rozkładu zbioru $\{f_u : u \in F\}$.

(2) $\implies$ (3): Niech F jest rozszerzeniem rozdzielczym ciała K , które jest ciałem rozkładu pewnego zbioru $S \subseteq K[x] \setminus \{0\}$. Niech T będzie zbiorem unormowanych nierozkładalnych dzielników wielomianów ze zbioru S . Wtedy oczywiście F jest ciałem rozkładu zbioru T . W szczególności, jeśli $f \in T$, to istnieje element $u \in F$ taki, że $f(u) = 0$. Wtedy f jest wielomianem minimalnym elementu u , więc musi być wielomianem rozdzielczym wobec rozdzielnosci elementu u .

(3) $\implies$ (1): Niech F będzie ciałem rozkładu pewnego zbioru T wielomianów rozdzielczych z $K[x]$. Wtedy F jest rozszerzeniem algebraicznym ciała K (jako ciałem rozkładu zbioru wielomianów). Aby pokazać, że F jest rozszerzeniem Galois rozważymy dwa przypadki.

1°. Załóżmy najpierw, że $[F : K] < \infty$. Z Lematu 2.8 wiemy, że $|\text{Aut}_K F| \leq [F : K] < \infty$. Niech

$$L := \{u \in F : \sigma(u) = u \text{ dla wszystkich } \sigma \in \text{Aut}_K F\}.$$

Wtedy F jest rozszerzeniem Galois ciała L oraz $\text{Aut}_L F = \text{Aut}_K F$ na mocy Twierdzenia 2.18. Korzystając z Twierdzenia 2.17(1), wiemy, że $[F : L] = |\text{Aut}_K F|$. Przez indukcję na $[F : K]$ pokażemy, że $[F : K] = |\text{Aut}_K F|$, co wobec równości $[F : L] = |\text{Aut}_K F|$ będzie oznaczać, że $K = L$, i zakończy dowód. Jeśli $[F : K] = 1$, to teza jest oczywista, więc załóżmy, że $[F : K] > 1$.

Ponieważ $[F : K] > 1$, więc istnieje wielomian $f \in T$ taki, że $\deg f > 1$. Niech u będzie pierwiastkiem wielomianu f . Wtedy $[K(u) : K] = \deg f$ na mocy Twierdzenia 1.4(3) oraz f ma $\deg f$ różnych pierwiastków (jako wielomian rozdzielczy). Z Lematu 2.7 wiemy, że odwzorowanie

$$\text{Aut}_K F / \text{Aut}_{K(u)} F \rightarrow \{v \in F : f(v) = 0\}, \quad \sigma \cdot \text{Aut}_{K(u)} F \mapsto \sigma(u),$$

jest dobrze zdefiniowaną injekcją. Pokażemy, że jest ono również surjekcją, a więc $[\text{Aut}_K F : \text{Aut}_{K(u)} F] = \deg f$. Istotnie, niech $v \in F$ będzie pierwiastkiem wielomianu f . Z Wniosku 1.6 wiemy, że istnieje izomorfizm $\tau : K(u) \rightarrow K(v)$ taki, że $\tau|_K = \text{Id}_K$ i $\tau(u) = v$. Ponieważ F jest ciałem rozkładu zbioru T nad $K(u)$ i $K(v)$, więc Twierdzenie 3.7 implikuje istnienie automorfizmu $\sigma \in \text{Aut}_K F$ takiego, że $\sigma|_{K(u)} = \tau$. W szczególności $\sigma(u) = v$, co kończy dowód surjektywności.

Niech T' będzie zbiorem dzielników nierozkładalnych wielomianów ze zbioru T nad ciałem $K(u)$. Wtedy T' jest zbiorem wielomianów rozdzielczych oraz

TEORIA GALOIS

F jest ciałem rozkładu wielomianów ze zbioru T' nad ciałem $K(u)$. Ponadto

$$[F : K(u)] = \frac{[F:K]}{[K(u):K]} < [F : K]$$

na mocy Twierdzenia 1.1, więc korzystając z założenia indukcyjnego, wiemy, że $[F : K(u)] = |\text{Aut}_{K(u)} F|$. Korzystając ponownie z Twierdzenia 1.1, równości $[\text{Aut}_K F : \text{Aut}_{K(u)} F] = \deg f$ udowodnionej powyżej oraz Twierdzenia Lagrange'a, otrzymujemy

$$\begin{aligned} [F : K] &= [F : K(u)] \cdot [K(u) : K] = |\text{Aut}_{K(u)} F| \cdot \deg f \\ &= |\text{Aut}_{K(u)} F| \cdot [\text{Aut}_K F : \text{Aut}_{K(u)} F] = |\text{Aut}_K(F)|, \end{aligned}$$

co kończy dowód w tym przypadku.

2°. Załóżmy teraz, że $[F : K] = \infty$. Ustalmy element $u \in F \setminus K$. Na mocy Twierdzenia 1.2 istnieje skończony podzbiór $T' \subset T$ taki, że $u \in E$, gdzie E jest ciałem rozkładu zbioru T' . Korzystając z Twierdzenia 1.9 wiemy, że wtedy $[E : K] < \infty$, zatem E jest rozszerzeniem Galois ciała K na mocy części 1°. W szczególności, istnieje automorfizm $\tau \in \text{Aut}_K E$ taki, że $\tau(u) \neq u$. Ponieważ F jest ciałem rozkładu zbioru T nad ciałem E , więc Twierdzenie 3.7 implikuje istnienie automorfizmu σ ciała F takiego, że $\sigma|_E = \tau$. Wtedy $\sigma \in \text{Aut}_K F$ i $\sigma(u) \neq u$. Z dowolności elementu u wynika, że F jest rozszerzeniem Galois ciała K . $\square$

Twierdzenie 3.10 (Uogólnione podstawowe twierdzenie teorii Galois).

Niech F będzie algebraicznym rozszerzeniem Galois ciała K . Wtedy odwzorowanie

$$\begin{aligned} \{E : E \text{ jest podciałem ciała } F \text{ i } K \subseteq E\} \\ \rightarrow \{H : H \leq \text{Aut}_K F \text{ i } H'' = H\}, \quad E \mapsto E', \end{aligned}$$

jest bijekcją. Ponadto:

- (1) jeśli E jest podciałem ciała F zawierającym ciało K , to F jest rozszerzeniem Galois ciała E ;
- (2) jeśli E jest podciałem ciała F zawierającym ciało K , to E jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy podgrupa $\text{Aut}_E F$ jest dzielnikiem normalnym grupy $\text{Aut}_K F$;
- (3) jeśli E jest podciałem ciała F będącym rozszerzeniem Galois ciała K , to $\text{Aut}_K E \simeq \text{Aut}_K F / \text{Aut}_E F$.

Dowód.

Korzystając z Twierdzenia 2.6, aby udowodnić bijektywność powyższego odwzorowania, wystarczy pokazać, że $E'' = E$ dla każdego podciała E ciała F zawierającego ciało K , co wynika z punktu (1) udowodnionego poniżej.

- (1) Niech E będzie podciałem ciała F zawierającym ciało K . Z Twierdzenia 3.9 wiemy, że F jest ciałem rozkładu pewnego zbioru T wielomianów rozdzielnych z $K[x]$. Zatem F jest również ciałem rozkładu zbioru T nad ciałem E . Korzystając ponownie z Twierdzenia 3.9, wnioskujemy, że F jest rozszerzeniem Galois ciała E .
- (2) Wiemy już, że $E'' = E$ dla każdego podciała E ciała F zawierającego ciało K , zatem teza wynika z Wniosku 2.15.
- (3) Ponieważ z założenia $E = E'' = (\text{Aut}_E F)'$ oraz $\text{Aut}_E F \trianglelefteq \text{Aut}_K F$ na mocy punktu (1), więc z Lematu 2.11(2) wynika, że podciało E' jest stabilne. Korzystając z Lematu 2.16, otrzymujemy, że $\text{Aut}_K F / \text{Aut}_E F \simeq \text{Ext}_E F$. Ale z Twierdzenia 3.9 wiemy, że F jest ciałem rozkładu nad ciałem K , a więc również nad E , więc $\text{Ext}_E F = \text{Aut}_K E$ na mocy Twierdzenia 3.7. $\square$

DEFINICJA.

Rozszerzenie algebraiczne F ciała K nazywamy NORMALNYM, jeśli wielomian nierozkładalny $f \in K[x]$ posiada pierwiastek w ciele F wtedy i tylko wtedy, gdy istnieją wielomiany $f_1, \dots, f_n \in F[x]$ takie, że

$$f = f_1 \cdots f_n \quad \text{oraz} \quad \deg f_i = 1 \quad \text{dla każdego } i \in [1, n].$$

TWIERDZENIE 3.11.

Dla rozszerzenia algebraicznego F ciała K następujące warunki są równoważne:

- (1) F jest rozszerzeniem normalnym ciała K ;
- (2) F jest ciałem rozkładu pewnego zbioru wielomianów z $K[x] \setminus \{0\}$;
- (3) jeśli $\overline{K}$ jest domknięciem algebraicznym ciała K zawierającym ciało F i $\sigma: F \rightarrow \overline{K}$ jest K -homomorfizmem, to $\sigma(F) = F$.

Dowód.

(1) $\implies$ (2): Niech $\{u_i : i \in I\}$ będzie bazą liniową ciała F nad ciałem K . Jeśli $f_i \in K[x]$ jest wielomianem minimalnym elementu u_i dla $i \in I$, to normalność rozszerzenia F implikuje, że F jest ciałem rozkładu zbioru $\{f_i : i \in I\}$.

(2) $\implies$ (3): Niech F będzie ciałem rozkładu zbioru $S \subseteq K[x] \setminus \{0\}$. Wtedy istnieją elementy $u_{f,i} \in F$, $f \in S$, $i \in [1, n_f]$, gdzie $n_f := \deg f$, takie, że

$$F = K(u_{f,i} : f \in S \text{ i } i \in [1, n_f]) \quad \text{i} \quad f \sim (x - u_{f,1}) \cdots (x - u_{f,n_f})$$

TEORIA GALOIS

dla każdego $f \in S$. Niech $\sigma: F \rightarrow \overline{K}$ będzie K -homomorfizmem. Jeśli $f \in S$ i $i \in [1, n_f]$, to na mocy Twierdzenia 2.2 istnieje indeks $j \in [1, n_f]$ taki, że $\sigma(u_{f,i}) = u_{f,j}$. Z różnowartościowości homomorfizmu σ wynika, że dla każdego $f \in S$ homomorfizm σ permutuje elementy zbioru $\{u_{f,i} : i \in [1, n_f]\}$. Stąd

$$\begin{aligned}\sigma(F) &= K(\sigma(u_{f,i}) : f \in S \text{ i } i \in [1, n_f]) \\ &= K(u_{f,i} : f \in S \text{ i } i \in [1, n_f]) = F.\end{aligned}$$

(3) $\implies$ (1): Niech $\overline{K}$ będzie domknięciem algebraicznym ciała F . Korzystając z Twierdzenia 1.10, wiemy, że $\overline{K}$ jest również domknięciem algebraicznym ciała K . Niech $f \in K[x]$ będzie wielomianem nierozkładalnym i $u \in F$ pierwiastkiem wielomianu f . Wiemy, że istnieją elementy $u_1, \dots, u_n \in \overline{K}$ takie, że $f \sim (x - u_1) \cdots (x - u_n)$. Musimy pokazać, że $u_1, \dots, u_n \in F$.

Ustalmy $i \in [1, n]$. Na mocy Wniosku 1.6 istnieje K -izomorfizm $\sigma: K(u) \rightarrow K(u_i)$. Ponieważ $\overline{K}$ jest ciałem rozkładu zbioru $K[x] \setminus \{0\}$ nad ciałem K (a więc również ciałami $K(u)$ i $K(u_i)$) na mocy Twierdzenia 3.3(2), więc na mocy Twierdzenia 3.7 istnieje automorfizm $\tau \in \text{Aut}_K F$ taki, że $\tau|_{K(u)} = \sigma$. W szczególności $\tau \circ \iota: F \rightarrow \overline{K}$, gdzie $\iota: F \rightarrow \overline{K}$ jest naturalnym włożeniem, jest K -homomorfizmem. Z założenia $(\tau \circ \iota)(F) = F$, a więc $u_i = \sigma(u) = (\sigma \circ \iota)(u) \in F$. $\square$

WNIOSEK 3.12.

Niech F będzie rozszerzeniem algebraicznym ciała K .

- (1) F jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy F jest normalnym rozszerzeniem rozdzielczym ciała K .
- (2) Jeśli $\text{char } K = 0$, to F jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy F jest rozszerzeniem normalnym ciała K .

Dowód.

- (1) Z Twierdzenia 3.9 wiemy, że F jest rozszerzeniem Galois ciała K wtedy i tylko wtedy, gdy jest rozszerzeniem rozdzielczym ciała K , które jest ciałem rozkładu pewnego zbioru wielomianów z $K[x] \setminus \{0\}$. Wobec Twierdzenia 3.11 ostatni warunek jest równoważny temu, że F jest rozszerzeniem normalnym ciała K .
- (2) Wynika z części pierwszej oraz obserwacji, że gdy $\text{char } K = 0$, to każde rozszerzenie algebraiczne ciała K jest rozdzielcze. $\square$

STWIERDZENIE 3.13.

Niech $L = K(X)$ będzie rozszerzeniem algebraicznym ciała K , a S zbiorem wielomianów minimalnych nad ciałem K elementów zbioru X . Jeśli F jest ciałem rozkładu zbioru S nad ciałem L , to

TEORIA GALOIS

- (1) F jest rozszerzeniem normalnym ciała K ;
- (2) jeśli E jest podciałem ciała F zawierającym ciało L , które jest rozszerzeniem normalnym ciała K , to $E = F$.

Dowód.

- (1) Ponieważ $L = K(X)$, więc F jest również ciałem rozkładu zbioru S nad ciałem K , a zatem rozszerzeniem normalnym ciała K na mocy Twierdzenia 3.11.
- (2) Niech E będzie podciałem ciała F zawierającym ciało L , które jest rozszerzeniem normalnym ciała K . Ponieważ $L \subseteq E$, więc z definicji rozszerzenia normalnego dla każdego $v \in X$ istnieją elementy $u_{v,1}, \dots, u_{v,n_v} \in E$ takie, że $f_v = (x - u_{v,1}) \cdots (x - u_{v,n_v})$, gdzie $f_v \in K[x]$ jest wielomianem minimalnym elementu v nad ciałem K oraz $n_v := \deg f_v$, $v \in X$. Ponieważ $F = L(u_{v,i} : v \in X \text{ i } i \in [1, n_v])$ z definicji ciała rozkładu, więc mamy ciąg inkluzji

$$E \subseteq F = L(u_{v,i} : v \in X \text{ i } i \in [1, n_v]) \subseteq E(u_{v,i} : v \in X \text{ i } i \in [1, n_v]) = E,$$

gdzie ostatnia równość wynika z faktu, że elementy $u_{v,i}$, $v \in X$ i $i \in [1, n_v]$, należą do ciała E . Zatem $E = F$. □

Twierdzenie 3.14.

Niech L będzie rozszerzeniem algebraicznym ciała K . Wtedy istnieje dokładnie jedno z dokładnością do L -izomorfizmu rozszerzenie F ciała L takie, że

- (1) F jest rozszerzeniem normalnym ciała K ;
- (2) jeśli E jest podciałem ciała F zawierającym ciało L , które jest rozszerzeniem normalnym ciała K , to $E = F$.

Definicja.

Ciało F spełniające warunki z Twierdzenia 3.14 nazywamy **DOMKNIECIEM NORMALNYM** ciała L nad ciałem K .

Dowód.

Istnienie ciała spełniającego powyższe warunki wynika ze Stwierdzenia 3.13. Niech zatem X będzie zbiorem takim, że $L = K(X)$, oraz F będzie ciałem skonstruowanym w Stwierdzeniu 3.13. Załóżmy także, że M jest rozszerzeniem ciała L takim, że

- (1) M jest rozszerzeniem normalnym ciała K ;
- (2) jeśli N jest podciałem ciała M zawierającym ciało L , które jest rozszerzeniem normalnym ciała K , to $N = M$.

TEORIA GALOIS

Ponieważ M jest rozszerzeniem normalnym ciała K , więc dla każdego $u \in X$ istnieją elementy $v_{u,1}, \dots, v_{u,n_u} \in M$ takie, że $f_u = (x - v_{u,1}) \cdots (x - v_{u,n_u})$, gdzie $f_u \in K[x]$ jest wielomianem minimalnym elementu u nad ciałem K oraz $n_u := \deg f_u$, $u \in X$. Niech $N := K(v_{u,i} : u \in X \text{ i } i \in [1, n_u])$. Wtedy N jest ciałem rozkładu zbioru S nad ciałem K , gdzie $S := \{f_u : u \in X\}$, więc N jest rozszerzeniem normalnym ciała K na mocy Twierdzenia 3.11. Ponadto $L \subseteq N$, gdyż dla każdego $u \in X$ istnieje $i \in [1, n_u]$ takie, że $u = v_{u,i}$. Zatem z założenia $N = M$. Innymi słowy, M jest ciałem rozkładu zbioru S nad ciałem K , a więc również nad ciałem L . Korzystając z Twierdzenia 3.7, otrzymujemy, że istnieje E -izomorfizm $\sigma: F \rightarrow M$. $\square$

Twierdzenie 3.15.

Niech L będzie rozszerzeniem algebraicznym ciała K . Jeśli F jest domknięciem normalnym ciała L nad ciałem K , to:

- (1) jeśli rozszerzenie L jest rozdzielcze, to F jest rozszerzeniem Galois ciała K ;
- (2) $[F : K] < \infty$ wtedy i tylko wtedy, gdy $[L : K] < \infty$.

Dowód.

Korzystając z Twierdzenia 3.14 i Stwierdzenia 3.13, możemy założyć, że F jest ciałem rozkładu zbioru S nad ciałem L , gdzie S jest zbiorem wielomianów minimalnych elementów (pewnego) zbioru X nad ciałem K , $X \subseteq L$ i $L = K(X)$.

- (1) Jeśli rozszerzenie L jest rozdzielcze, to wszystkie wielomiany ze zbioru S są rozdzielcze, a więc F jest rozszerzeniem Galois ciała K na mocy Twierdzenia 3.9.
- (2) Oczywiście $[L : K] < \infty$, jeśli $[F : K] < \infty$. Jeśli $[L : K] < \infty$, to możemy założyć, że $|X| < \infty$, więc również $|S| < \infty$, a zatem $[F : K] < \infty$. $\square$

TEORIA GALOIS

B. ZASADNICZE TWIERDZENIE ALGEBRY

LEMAT B.1.

Jeśli F jest skończenie wymiarowym rozszerzeniem rozdzielczym nieskończonego ciała K , to istnieje element $u \in F$ taki, że $F = K(u)$.

DOWÓD.

Niech E będzie domknięciem normalnym ciała F nad ciałem K . Ponieważ F jest skończenie wymiarowym rozszerzeniem rozdzielczym nieskończonego ciała K , więc z Twierdzenia 3.15 wiemy, że E jest skończenie wymiarowym rozszerzeniem Galois ciała K . W szczególności, z Twierdzenia 2.17 wynika, że istnieje tylko skończenie wiele podciał L ciała E takich, że $K \subseteq L$. W konsekwencji, istnieje tylko skończenie wiele podciał L ciała F takich, że $K \subseteq L$.

Ponieważ $[F : K] < \infty$, więc istnieje element $u \in F$ taki, że

$$[K(u) : K] = \max\{[K(w) : K] : w \in F\}.$$

Przypuśćmy, że $K(u) \neq K$. Wybierzmy element $v \in F \setminus K(u)$. Ponieważ ciało K jest nieskończone oraz istnieje tylko skończenie wiele podciał L ciała F takich, że $K \subseteq L$, więc istnieją elementy $a, b \in K$ takie, że $a \neq b$ oraz $K(u + a \cdot v) = K(u + b \cdot v)$. Wtedy

$$(a - b) \cdot v = (u + a \cdot v) - (u + b \cdot v) \in K(u + a \cdot v).$$

Stąd $v = (a - b)^{-1} \cdot (a - b) \cdot v \in K(u + a \cdot v)$ (gdyż $a - b \in K^\times$) oraz $u = (u + a \cdot v) - a \cdot v \in K(u + a \cdot v)$. Zatem $K(u) \subset K(u + a \cdot v)$, sprzeczność z wyborem elementu u . Zatem $K(u) = K$. $\square$

LEMAT B.2.

Nie istnieje rozszerzenia stopnia 2 ciała $\mathbb{C}$.

DOWÓD.

Gdyby F było rozszerzeniem stopnia 2 ciała $\mathbb{C}$, to F byłoby rozszerzeniem algebraicznym ciała $\mathbb{C}$ (na mocy Twierdzenia 1.8) oraz istniałby element $u \in F$ taki, że $F = \mathbb{C}(u)$. Twierdzenia 1.4 implikowałyby zatem, że wielomian minimalny elementu u byłby stopnia 2, co jest jednak niemożliwe, gdyż łatwo pokazać, że każdy wielomian stopnia 2 o współczynnikach w ciele $\mathbb{C}$ posiada pierwiastek zespolony. $\square$

TWIERDZENIE B.3 (ZASADNICZE TWIERDZENIE ALGEBRY).

Ciało $\mathbb{C}$ jest algebraicznie domknięte.

DOWÓD.

Ustalmy wielomian $f \in \mathbb{C}[x]$ taki, że $\deg f > 0$. Z Twierdzenia 1.7 wiemy,

TEORIA GALOIS

że istnieją rozszerzenie F ciała $\mathbb{C}$ oraz element $u \in F$ takie, że $F = \mathbb{C}(u)$, $f(u) = 0$ i $[F : \mathbb{C}] < \infty$. W szczególności z Twierdzenia 1.1 wiemy, że $[F : \mathbb{R}] = 2 \cdot [F : \mathbb{C}] < \infty$, więc Twierdzenie 1.8 implikuje, że F jest rozszerzeniem algebraicznym ciała $\mathbb{R}$.

Niech E będzie domknięciem normalnym ciała F nad ciałem $\mathbb{R}$. Wtedy E jest rozszerzeniem Galois ciała $\mathbb{R}$ takim, że $[E : \mathbb{R}] < \infty$ na mocy Twierdzenia 3.15. W szczególności $|\text{Aut}_{\mathbb{R}} E| = [E : \mathbb{R}] < \infty$ na mocy Twierdzenia 2.17(1). Jeśli $|\text{Aut}_{\mathbb{R}} E| = 2^n \cdot m$ dla $n \in \mathbb{N}$ i $m \in \mathbb{N}_+$ takich, że $2 \nmid m$, to z Pierwszego Twierdzenia Sylowa wiemy, że istnieje podgrupa $G \leq \text{Aut}_{\mathbb{R}} E$ taka, że $|G| = 2^n$. Niech

$$K := \{u \in E : \sigma(u) = u \text{ dla wszystkich } \sigma \in G\}.$$

Wtedy $[K : \mathbb{R}] = [\text{Aut}_{\mathbb{R}} E : G] = m$ na mocy na mocy Twierdzenia 2.17(1). Z Lematu B.1 wiemy, że istnieje element $u \in K$ taki, że $K = \mathbb{R}(u)$. Jeśli f jest wielomianem minimalnym elementu u , to f jest wielomianem nierozkładalnym stopnia m nad ciałem $\mathbb{R}$ (na mocy Twierdzenia 1.4(3)), więc $m = 1$, gdyż $2 \nmid m$. W szczególności, $|\text{Aut}_{\mathbb{R}} E| = 2^n$, a więc istnieje $l \in \mathbb{N}$ takie, że $|\text{Aut}_{\mathbb{C}} E| = 2^l$, gdyż $\text{Aut}_{\mathbb{C}} E \leq \text{Aut}_{\mathbb{R}} E$.

Gdyby $l > 0$, to na mocy Pierwszego Twierdzenia Sylowa istniałaby podgrupa H grupy $\text{Aut}_{\mathbb{C}} E$ taka, że $[\text{Aut}_{\mathbb{C}} E : H] = 2$. Niech

$$L := \{u \in E : \sigma(u) = u \text{ dla wszystkich } \sigma \in H\}.$$

Wtedy $[L : \mathbb{C}] = [\text{Aut}_{\mathbb{C}} E : H] = 2$ na mocy na mocy Twierdzenia 2.17(1), co jest niemożliwe na mocy Lematu B.2. Stąd $l = 0$, a więc $\text{Aut}_{\mathbb{C}} E = \{\text{Id}_E\}$. Zauważmy, że ciało E jest rozszerzeniem Galois ciała $\mathbb{C}$ na mocy Twierdzenia 2.17(2), więc oznacza to, że $E = \mathbb{C}$, a co z tym idzie $F = \mathbb{C}$. W szczególności, $u \in \mathbb{C}$ oraz $f(u) = 0$. $\square$

4. GRUPA GALOIS WIELOMIANU

DEFINICJA.

Niech K będzie ciałem. GRUPĄ GALOIS wielomianu $f \in K[x]$ nazywamy grupę $\text{Aut}_K F$, gdzie F jest ciałem rozkładu wielomianu f nad ciałem K .

OZNACZENIE.

Jeśli K jest ciałem i $f \in K[x]$, to grupą Galois wielomianu f nad ciałem K oznaczamy $\text{Gal}_K f$.

TWIERDZENIE 4.1.

Niech K będzie ciałem i $f \in K[x]$ wielomianem stopnia n .

- (1) Jeśli X jest zbiorem pierwiastków wielomianu f w jego ciele rozkładu nad ciałem K , to funkcja

$$\varphi: \text{Gal}_K f \rightarrow \mathfrak{S}_X, \sigma \mapsto (x \mapsto \sigma(x)),$$

jest dobrze zdefiniowanym monomorfizmem grup.

W szczególności, grupa $\text{Gal}_K f$ jest izomorficzna z podgrupą grupy $\mathfrak{S}_X$.

- (2) Jeśli wielomian f jest rozdzielnym, to n dzieli $|\text{Gal}_K f|$ oraz grupa $\text{Im } \varphi$ jest podgrupą przechodnią grupy $\mathfrak{S}_X \simeq \mathfrak{S}_n$.

DOWÓD.

- (1) Poprawność definicji funkcji φ wynika z Twierdzenia 2.2. Łatwo też sprawdzić, że φ jest homomorfizmem grup. Jeśli F jest ciałem rozkładu wielomianu f nad ciałem K , to z definicji $F = K(X)$ i $\text{Gal}_K f = \text{Aut}_K F$, więc φ jest monomorfizmem.
- (2) Załóżmy teraz, że wielomian f jest rozdzielnym. Wtedy w szczególności $|X| = n$, więc $\mathfrak{S}_X \simeq \mathfrak{S}_n$. Wybierzmy pierwiastek $u \in X$. Wtedy $[K(u) : K] = n$ na mocy Twierdzenia 1.4. Ponieważ F jest rozszerzeniem Galois ciała K na mocy Twierdzenia 3.9, więc Twierdzenie 2.17(1) implikuje, że

$$[\text{Gal}_K f : \text{Aut}_{K(u)} K] = [\text{Aut}_K F : \text{Aut}_{K(u)} K] = [K(u) : K] = n.$$

W szczególności, n dzieli $|\text{Gal}_K f|$.

Dla dowodu przechodniości podgrupy $\text{Im } \varphi$ ustalmy pierwiastki $u, v \in X$. Na mocy Wniosku 1.6 istnieje K -izomorfizm $\tau: K(u) \rightarrow K(v)$ taki, że $\tau(u) = v$. Korzystając z Twierdzenia 3.7, wiemy, że istnieje izomorfizm $\sigma: F \rightarrow F$ taki, że $\sigma|_{K(u)} = \tau$. Wtedy $\sigma \in \text{Gal}_K f$ i $\sigma(u) = v$, co kończy dowód. $\square$

TWIERDZENIE 4.2.

Niech p będzie liczbą pierwszą i $f \in \mathbb{Q}[x]$ wielomianem nierozkładalnym

TEORIA GALOIS

stopnia p . Jeśli f ma dokładnie dwa nierzeczywiste pierwiastki zespolone, to $\text{Gal}_K f \simeq \mathfrak{S}_p$.

Dowód.

Niech X będzie zbiorem pierwiastków (zespolonych) wielomianu f . Na mocy Twierdzenia 4.1(1) możemy utożsamić grupę $\text{Gal}_K f$ z podgrupą grupy $\mathfrak{S}_X$. Ponieważ $\text{char } \mathbb{Q} = 0$, więc wielomian f jest rozdzielczy, zatem $|X| = p$, a więc $\mathfrak{S}_X \simeq \mathfrak{S}_p$. Wystarczy zatem pokazać, że $\text{Gal}_K f = \mathfrak{S}_X$.

Korzystając z Twierdzenia 4.1(2), wiemy, że p dzieli $|\text{Gal}_K f|$. Z Twierdzenia Cauchy'ego wynika zatem, że istnieje permutacja $\sigma \in \text{Gal}_K f$ rzędu p . Bez straty ogólności możemy założyć, że $\sigma(a) = b$, gdzie a i b są nierzeczywistymi pierwiastkami zespolonymi wielomianu f .

Niech $\tau \in \text{Gal}_K f$ będzie permutacją zbioru X indukowaną przez sprzężenie zespolone. Wtedy τ jest transpozycją elementów a i b oraz permutacje τ i σ generują grupę $\mathfrak{S}_X$. Ponieważ $\tau, \sigma \in \text{Gal}_K f$, więc mamy ciąg inkluzji

$$\mathfrak{S}_X = \langle \tau, \sigma \rangle \subseteq \text{Gal}_K f \subseteq \mathfrak{S}_X,$$

z którego wynika, że $\text{Gal}_K f = \mathfrak{S}_X$. □

5. CIAŁA SKOŃCZONE

TWIERDZENIE 5.1.

Niech P będzie najmniejszym podciałem ciała F .

- (1) Jeśli $\text{char } F > 0$, to $P \simeq \mathbb{F}_p$, gdzie $p := \text{char } F$.
- (2) Jeśli $\text{char } F = 0$, to $P \simeq \mathbb{Q}$.

DOWÓD.

Ponieważ P jest podciałem ciała F , więc funkcja $\varphi: \mathbb{Z} \rightarrow P$ zdefiniowana wzorem

$$\varphi(m) := m \cdot 1 \quad (m \in \mathbb{Z}),$$

jest dobrze określonym homomorfizmem. Wtedy $\text{Ker } \varphi = (p)$, gdzie $p := \text{char } F$.

- (1) Załóżmy, że $p > 0$. Niech $\psi: \mathbb{Z}/\text{Ker } \varphi \rightarrow P$ będzie monomorfizmem indukowanym przez φ . Wtedy $\mathbb{Z}/\text{Ker } \varphi \simeq \text{Im } \varphi$ jest dziedziną. Ponieważ każda skończona dziedzina jest ciałem, więc $\text{Im } \varphi$ jest ciałem i ψ jest monomorfizmem ciał. Z minimalności podciała P wynika, że $P = \text{Im } \varphi \simeq \mathbb{F}_p$.
- (2) Załóżmy, że $\text{char } F = 0$. Wtedy $\text{Ker } \varphi = \{0\}$ i $\varphi(m)$ jest elementem odwracalnym dla każdej liczby $m \in S := \mathbb{Z} \setminus \{0\}$. Stąd mamy indukowany homomorfizm ciał $\psi: \mathbb{Q} = S^{-1}\mathbb{Z} \rightarrow P$, który musi być monomorfizmem. Z minimalności podciała P wynika, że $P = \text{Im } \psi \simeq \mathbb{Q}$. $\square$

WNIOSEK 5.2.

Jeśli F jest ciałem skończonym, to istnieje liczba pierwsza p taka, że $\text{char } F = p$ i $|F| = p^n$ dla pewnej liczby $n \in \mathbb{N}_+$.

DOWÓD.

Niech P będzie najmniejszym podciałem ciała F . Ponieważ ciało F jest skończone, więc z Twierdzenia 5.1 wynika, że $p := \text{char } F > 0$ i $P \simeq \mathbb{Z}_p$. W szczególności, $p \in \mathbb{P}$, gdyż $\mathbb{Z}_p \simeq P$ jest ciałem. Zauważmy, że ciało F jest przestrzenią liniową nad ciałem P . Jeśli $n := \dim_P F$, to $|F| = |P|^n = p^n$ i $n \in \mathbb{N}_+$, gdyż $P \neq \{0\}$. $\square$

TWIERDZENIE 5.3.

Jeśli F jest ciałem i G jest podgrupą skończoną grupy $F^\times$, to grupa G jest cykliczna. W szczególności, jeśli F jest ciałem skończonym, to grupa $F^\times$ jest cykliczna.

DOWÓD.

Ponieważ G jest skończoną grupą abelową, więc istnieją liczby $m_1, \dots, m_n \in$

TEORIA GALOIS

$\mathbb{N}_+$ takie, że $m_1 \mid m_2 \mid \cdots \mid m_n$ i

$$G \simeq \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_n}.$$

W szczególności, $\text{ord}_G u \mid m_n$ dla każdego elementu $u \in G$. Innymi słowy, każdy element grupy G jest pierwiastkiem wielomianu $x^{m_n} - 1$. Ponieważ wielomian $x^{m_n} - 1$ ma co najwyżej m_n pierwiastków w ciele F , więc

$$m_1 \cdots m_n = |G| \leq m_n.$$

Stąd $m_1 = \cdots = m_{n-1} = 1$, a więc $G \simeq \mathbb{Z}_{m_n}$. □

6. ROZDZIELCZOŚĆ

DEFINICJA.

Niech F będzie rozszerzeniem ciała K .

- (1) Element $u \in F$ nazywamy CZYSTO NIEROZDZIELCZYM nad K , jeśli jest algebraiczny i istnieje $m \in \mathbb{N}_+$ takie, że $f = (x - u)^m$, gdzie $f \in K[x]$ jest wielomianem minimalnym elementu u .
- (2) Rozszerzenie F nazywamy CZYSTO NIEROZDZIELCZYM, jeśli każdy element ciała F jest czysto nierozdzielczy nad ciałem K .

TWIERDZENIE 6.1.

Niech F będzie rozszerzeniem ciała K . Element $u \in F$ jest rozdzielczy i czysto nierozdzielczy nad ciałem K wtedy i tylko wtedy, gdy $u \in K$.

DOWÓD.

Niech f będzie wielomianem minimalnym ciała elementu $u \in F$. Wtedy element jest rozdzielczy i czysto nierozdzielczy wtedy i tylko wtedy, gdy $\gcd(f, f') = 1$ oraz istnieje $m \in \mathbb{N}_+$ takie, że $f = (x - u)^m$. Ponieważ $f' = m \cdot (x - u)^{m-1}$, więc

$$\gcd(f, f') = \begin{cases} (x - u)^{m-1} & \text{gdy } \text{char } F \nmid m, \\ 0 & \text{gdy } \text{char } F \mid m, \end{cases}$$

więc powyższe warunki mogą być spełnione wtedy i tylko wtedy, gdy $m = 1$, a więc $u \in K$. $\square$

LEMAT 6.2.

Niech F będzie rozszerzeniem ciała K charakterystyki $p > 0$. Jeśli element $u \in F$ jest algebraiczny nad ciałem K , to istnieje $n \in \mathbb{N}$ takie, że element u^{p^n} jest rozdzielczy nad ciałem K .

DOWÓD.

Jeśli element u jest rozdzielczy nad ciałem K (w szczególności, jeśli $u \in K$), to teza jest oczywista. Załóżmy zatem, że element u nie jest rozdzielczy i niech f będzie wielomianem minimalnym elementu u . Ponieważ element u nie jest rozdzielczy, więc $f' = 0$, zatem istnieje wielomian $g \in K[x]$ taki, że $f = g(x^p)$. Ponieważ $g(u^p) = 0$ oraz $\deg g < \deg f$, więc z założenia indukcyjnego istnieje $n \in \mathbb{N}$ takie, że element $(u^p)^{p^n} = u^{p^{n+1}}$ jest rozdzielczy nad ciałem K . $\square$

LEMAT 6.3.

Niech F będzie rozszerzeniem ciała K oraz $F = K(X)$ dla pewnego podzbioru X ciała F . Jeśli każdy element zbioru X jest rozdzielczy nad ciałem K , to F jest rozszerzeniem rozdzielczym ciała K .

Dowód.

Ustalmy element $v \in F$. Z Twierdzenia 1.2 wiemy, że istnieją elementy $u_1, \dots, u_n \in X$ takie, że $v \in K(u_1, \dots, u_n)$. Dla każdego $i \in [1, n]$ niech f_i będzie wielomianem minimalnym elementu u_i nad ciałem K . Wtedy wielomiany $f_1, \dots, f_n$ są rozdzielcze nad ciałem K . Niech E będzie ciałem rozkładu zbioru $\{f_1, \dots, f_n\}$ nad ciałem $K(u_1, \dots, u_n)$. Wtedy E jest również ciałem rozkładu zbioru $\{f_1, \dots, f_n\}$ nad ciałem K , zatem E jest rozszerzeniem rozdzielczym ciała K na mocy Twierdzenia 3.9. W szczególności element v jest rozdzielczy nad ciałem K , gdyż $v \in K(u_1, \dots, u_n) \subseteq E$. $\square$

Twierdzenie 6.4.

Niech F będzie rozszerzeniem algebraicznym ciała K . Jeśli S jest zbiorem wszystkich elementów ciała F , które są rozdzielcze nad ciałem K , to S jest podciałem ciała F , które jest rozszerzeniem rozdzielczym ciała K .

Dowód.

Musimy pokazać, że S jest podciałem ciała F , równoważnie $S = K(S)$. Z Lematu 6.3 wiemy jednak, że $K(S) \subseteq S$. Ponieważ inkluzja $S \subseteq K(S)$ jest oczywista, więc to kończy dowód. $\square$

Definicja.

Niech F będzie rozszerzeniem algebraicznym ciała K . Jeśli S jest podciałem ciała F złożonym ze wszystkich elementów, które są rozdzielcze nad ciałem K , to definiujemy stopień rozdzielczy $[F : K]_s$ ciała F nad ciałem K wzorem $[F : K]_s := [S : K]$ oraz stopień nierozdzielczy $[F : K]_i$ ciała F nad ciałem K wzorem $[F : K]_i := [F : S]$.

Uwaga.

Jeśli F jest rozszerzeniem algebraicznym ciała K , to $[F : K] = [F : K]_s \cdot [F : K]_i$.

Dowód.

Bezpośrednio z definicji oraz Twierdzenia 1.1. $\square$

Oznaczenie.

Jeśli F i E są rozszerzeniami ciała K , to przez $\text{Mor}_K(F, E)$ oznaczamy zbiór wszystkich K -homomorfizmów $F \rightarrow E$.

Uwaga.

Niech F będzie skończenie wymiarowym rozszerzeniem ciała K . Jeśli E jest rozszerzeniem ciała K , to zbiór $\text{Mor}_K(F, E)$ jest skończony.

Dowód.

Korzystając z założenia $[F : K] < \infty$ i Twierdzenia 1.8 wiemy, że F jest skończenie generowanym rozszerzeniem algebraicznym ciała K . Wybierzmy

TEORIA GALOIS

zatem skończony podzbiór $X \subseteq F$ taki, że $F = K(X)$, oraz dla każdego $u \in X$ niech f_u będzie wielomianem minimalnym elementu u . Niech Y zbiorem pierwiastków wielomianu $\prod_{u \in X} f_u$ w ciele E . Korzystając z Twierdzenia 2.2, wiemy, że jeśli $\sigma \in \text{Mor}_K(F, E)$, to $\sigma(X) \subseteq Y$. Ponadto, jeśli $\sigma, \tau \in \text{Mor}_K(F, E)$, to $\sigma = \tau$, o ile $\sigma(u) = \tau(u)$ dla każdego elementu $u \in X$, więc

$$|\text{Mor}_K(F, E)| \leq |Y^X| < \infty,$$

gdzie druga z nierówności wynika z faktu, że zbiór Y jest skończony. $\square$

LEMAT 6.5.

Niech F będzie rozszerzeniem ciała K , E podciałem ciała F zawierającym ciało K oraz N jest rozszerzeniem normalnym ciała K zawierającym ciało F . Niech $\Psi: \text{Aut}_K N \rightarrow \text{Mor}_K(E, N)$ i $\Phi: \text{Mor}_E(F, N) \times \text{Aut}_K N \rightarrow \text{Mor}_K(F, N)$ będą funkcjami danymi wzorami

$$\Psi(\sigma) := \sigma \circ \mu \quad (\sigma \in \text{Aut}_K N)$$

i

$$\Phi(\tau, \sigma) := \sigma \circ \tau \quad (\tau \in \text{Mor}_E(F, N), \sigma \in \text{Aut}_K N),$$

gdzie $\mu: E \rightarrow N$ jest naturalnym włożeniem. Wtedy

- (1) Funkcja Ψ jest surjekcją.
- (2) Jeśli X jest zbiorem reprezentantów włókien funkcji Ψ , to funkcja $\Phi|_{\text{Mor}_E(F, N) \times X}$ jest bijekcją.
- (3) $|\text{Mor}_K(F, N)| = |\text{Mor}_E(F, N)| \cdot |\text{Mor}_K(E, N)|$.

Dowód.

- (1) Z Twierdzenia 3.11 wiemy, że ciało N jest ciałem rozkładu pewnego zbioru $S \subseteq K[x] \setminus \{0\}$ nad ciałem K . Wtedy N jest również ciałem rozkładu zbioru S nad ciałem E . Ustalmy $\sigma \in \text{Mor}_K(E, N)$. Ponieważ $S \subseteq K[x]$, więc N jest ciałem rozkładu zbioru S nad ciałem $\sigma(E)$. Stąd na mocy Twierdzenia 3.7 istnieje automorfizm $\bar{\sigma} \in \text{Aut}_K N$ taki, że $\sigma = \bar{\sigma} \circ \mu$.
- (2) Pokażemy najpierw, że $\Phi|_{\text{Mor}_E(F, N) \times X}$ jest surjekcją. Dla $\phi \in \text{Mor}_K(F, N)$ definiujemy $\sigma \in \text{Mor}_K(E, N)$ wzorem $\sigma := \phi \circ \iota$, gdzie $\iota: E \rightarrow F$ jest naturalnym włożeniem. Z punktu (1) wiemy, że istnieje automorfizm $\bar{\sigma} \in X$ taki, że $\Psi(\bar{\sigma}) = \sigma$. Jeśli $\tau := \bar{\sigma}^{-1} \circ \phi$, to $(\tau, \bar{\sigma}) \in \text{Mor}_E(F, N) \times X$ i $\phi = \Phi(\tau, \bar{\sigma})$.

TEORIA GALOIS

Założmy teraz, że $\tau_1, \tau_2 \in \text{Mor}_E(F, N)$, $\sigma_1, \sigma_2 \in X$ oraz $\Phi(\tau_1, \sigma_1) = \Phi(\tau_2, \sigma_2)$. Wtedy $\tau_1 \circ \iota = \mu = \tau_2 \circ \iota$, gdyż $\tau_1, \tau_2 \in \text{Mor}_E(F, N)$. Stąd

$$\Psi(\sigma_1) = \sigma_1 \circ \mu = \sigma_1 \circ \tau_1 \circ \iota = \sigma_2 \circ \tau_2 \circ \iota = \sigma_2 \circ \mu = \Psi(\sigma_2),$$

Ponieważ $\sigma_1, \sigma_2 \in X$, więc $\sigma_1 = \sigma_2$, a więc również

$$\tau_1 = \sigma_1^{-1} \circ (\sigma_1 \circ \tau_1) = \sigma_2^{-1} \circ (\sigma_2 \circ \tau_2) = \tau_2.$$

- (3) Z punktu (2) wiemy, że $|\text{Mor}_K(F, N)| = |\text{Mor}_E(F, N)| \cdot |X|$, gdzie X jest zbiorem reprezentantów włókien funkcji Ψ . Ponadto z punktu (1) wynika, że $|X| = |\text{Mor}_K(E, N)|$, co kończy dowód. $\square$

STWIERDZENIE 6.6.

Niech F będzie skończenie wymiarowym rozszerzeniem ciała K . Jeśli N jest rozszerzeniem normalnym ciała K zawierającym ciało F , to

$$|\text{Mor}_K(F, N)| = [F : K]_s.$$

Dowód.

Założmy najpierw, że F jest rozszerzeniem rozdzielczym ciała K , a więc w szczególności $[F : K]_s = [F : K]$. Gdy $[F : K] = 1$, to $F = K$ i

$$|\text{Mor}_K(F, N)| = |\text{Mor}_K(K, N)| = 1 = [F : K].$$

Założmy więc, że $[F : K] > 1$ i wybierzmy element $u \in F \setminus K$. Jeśli $[K(u) : K] < [F : K]$, to z założenia indukcyjnego wiemy, że

$$|\text{Mor}_K(K(u), N)| = [K(u) : K] \quad \text{ i } \quad |\text{Mor}_{K(u)}(F, N)| = [F : K(u)].$$

Zatem korzystając z Lematu 6.5(3), otrzymujemy

$$\begin{aligned} |\text{Mor}_K(F, N)| &= |\text{Mor}_{K(u)}(F, N)| \cdot |\text{Mor}_K(K(u), N)| \\ &= [F : K(u)] \cdot [K(u) : K] = [F : K], \end{aligned}$$

gdzie ostatnia równość wynika z Twierdzenia 1.1.

Założmy zatem, że $K(u) = F$. Wtedy $[F : K] = \deg f$, gdzie f jest wielomianem minimalnym elementu u nad ciałem K (na mocy Twierdzenia 1.4(3)). Stwierdzenie 2.1, Twierdzenie 2.2 i Wniosek 1.6 implikują, że K -morfizmów z $F = K(u)$ do N jest dokładnie tyle co pierwiastków wielomianu f w ciele N . Ponieważ rozszerzenie F jest rozdzielcze, a rozszerzenie N jest normalne, więc tych pierwiastków jest dokładnie $\deg f = [F : K]$, co kończy dowód równości $|\text{Mor}_K(F, N)| = [F : K]$ w tym przypadku.

TEORIA GALOIS

Niech teraz F będzie dowolnym ciałem i oznaczmy przez S podciało ciała F złożone ze wszystkich elementów, które są rozdzielcze nad K . Z części pierwszej dowodu wiemy, że

$$|\operatorname{Mor}_K(S, N)| = [S : K] = [F : K]_s.$$

Dla zakończenia dowodu wystarczy zatem pokazać że funkcja $\Phi: \operatorname{Mor}_K(F, N) \rightarrow \operatorname{Mor}_K(S, N)$ dana wzorem

$$\Phi(\sigma) := \sigma \circ \mu_S^F \quad (\sigma \in \operatorname{Mor}_K(F, N)),$$

gdzie $\mu_S^F: S \rightarrow F$ jest naturalnym włożeniem, jest bijekcją. Teza jest oczywista, gdy $\operatorname{char} K = 0$, gdyż wtedy $S = F$. Załóżmy zatem, że $p := \operatorname{char} K \neq 0$.

Pokażemy najpierw, że funkcja Φ jest surjekcją. W tym celu ustalmy homomorfizm $\tau \in \operatorname{Mor}_K(S, N)$. Ponieważ N jest rozszerzeniem normalnym ciała K , więc N jest ciałem rozkładu nad ciałem K pewnego zbioru T wielomianów z $K[x] \setminus \{0\}$ na mocy Twierdzenia 3.11. W konsekwencji N jest ciałem rozkładu zbioru T nad ciałami S i $\tau(S)$. Korzystając z Twierdzenia 3.7, otrzymujemy, że istnieje automorfizm $\bar{\tau} \in \operatorname{Aut}_K(N)$ taki, że $\bar{\tau} \circ \mu_S^N = \tau$, gdzie $\mu_S^N: S \rightarrow N$ jest naturalnym włożeniem. Wtedy $\tau = \Phi(\bar{\tau} \circ \mu_F^N)$, gdzie ponownie $\mu_F^N: F \rightarrow N$ jest naturalnym włożeniem.

Założmy teraz, że $\sigma_1, \sigma_2 \in \operatorname{Mor}_K(F, N)$ są homomorfizmami takimi, że $\Phi(\sigma_1) = \Phi(\sigma_2)$. Jeśli $u \in F$, to istnieje $n \in \mathbb{N}$ takie, że $u^{p^n} \in S$ na mocy Lematu 6.2. Wtedy

$$(\sigma_1(u))^{p^n} = \sigma_1(u^{p^n}) = \sigma_2(u^{p^n}) = (\sigma_2(u))^{p^n},$$

więc $\sigma_1(u) = \sigma_2(u)$. Z dowolności elementu u wynika, że $\sigma_1 = \sigma_2$, a więc Φ jest injekcją, co kończy dowód. $\square$

WNIOSEK 6.7.

Jeśli F jest skończone wymiarowym rozszerzeniem ciała K oraz E jest podciałem ciała F zawierającym ciało K , to

$$[F : K]_s = [F : E]_s \cdot [E : K]_s \quad \text{ i } \quad [F : K]_i = [F : E]_i \cdot [E : K]_i.$$

Dowód.

Niech $\overline{K}$ będzie domknięciem algebraicznym ciała K zawierającym ciało F . Wtedy z Twierdzeń 3.3(2) i 3.11 wynika, że $\overline{K}$ jest rozszerzeniem normalnym ciała K i E . Korzystając ze Stwierdzenia 6.6, wiemy zatem, że

$$[F : K]_s = |\operatorname{Mor}_K(F, \overline{K})|, \quad [F : E]_s = |\operatorname{Mor}_E(F, \overline{K})|$$

i

$$[E : K]_s = |\text{Mor}_K(E, \overline{K})|.$$

Lemat 6.5 implikuje zatem, że

$$\begin{aligned} [F : K]_s &= |\text{Mor}_K(F, \overline{K})| \\ &= |\text{Mor}_E(F, \overline{K})| \cdot |\text{Mor}_K(E, \overline{K})| = [F : E]_s \cdot [E : K]_s. \end{aligned}$$

Mamy ponadto

$$[F : K]_i = \frac{[F:K]}{[F:K]_s} = \frac{[F:E] \cdot [E:K]}{[F:E]_s \cdot [E:K]_s} = [F : E]_s \cdot [E : K]_i,$$

gdzie druga równość jest konsekwencją części pierwszej oraz Twierdzenia 1.1. $\square$

WNIOSEK 6.8.

Niech $f \in K[x]$ będzie unormowanym wielomianem nierozkładalnym, F ciałem rozkładu wielomianu f oraz $u \in F$ pierwiastkiem wielomianu f . Jeśli $u_1, \dots, u_n \in F$ są parami różnymi pierwiastkami wielomianu f w ciele F , to $n = [K(u) : K]_s$ oraz

$$f = ((x - u_1) \cdots (x - u_n))^{[K(u):K]_i}.$$

DOWÓD.

Teza jest oczywista, gdy $\text{char } K = 0$, zatem załóżmy, że $p := \text{char } K \neq 0$.

Niech $r_1, \dots, r_n$ będą krotnościami elementów $u_1, \dots, u_n$ jako pierwiastków wielomianu f . Ustalmy $i \in [1, n]$. Wniosek 1.6 implikuje, że istnieje K -izomorfizm $\sigma: K(u) \rightarrow K(u_i)$ taki, że $\sigma_i(u) = u_i$. Korzystając z Twierdzenia 3.7, otrzymujemy istnienie K -izomorfizmu $\bar{\sigma}_i: F \rightarrow F$ takiego, że $\bar{\sigma}_i|_{K(u)} = \sigma_i$. Ponieważ $f \in K[x]$, więc z Twierdzenia 2.2 wynika, że

$$(x - u_1)^{r_1} \cdots (x - u_n)^{r_n} = f = \bar{\sigma}_i f = (x - \bar{\sigma}_i(u_1))^{r_1} \cdots (x - \bar{\sigma}_i(u_n))^{r_n}.$$

Ponieważ pierścień $F[x]$ jest dziedziną z jednoznacznością rozkładu, więc $r_i = r$, gdzie r jest krotnością elementu u jako pierwiastku wielomianu f . Stąd

$$f = ((x - u_1) \cdots (x - u_n))^r \quad \text{ i } \quad \deg f = n \cdot r.$$

Zauważmy, że $n = |\text{Mor}_K(K(u), F)|$. Istotnie, jeśli $\sigma \in \text{Mor}_K(K(u), F)$, to $\sigma(u) = u_i$ dla pewnego $i \in [1, n]$ na mocy Twierdzenia 2.2, więc $|\text{Mor}_K(K(u), F)| \leq$

TEORIA GALOIS

n na mocy Stwierdzenia 2.1. Z drugiej strony, homomorfizmy $\sigma_1, \dots, \sigma_n$ konstruowane powyżej są parami różne, co dowodzi przeciwnej nierówności.

Ponieważ F jest rozszerzeniem normalnym ciała $K(u)$ na mocy Twierdzenia 3.11, więc powyższe obserwacja oznacza wobec Stwierdzenia 6.6, że $n = [K(u) : K]_s$. Na zakończenie dowodu pierwszej części zauważmy jeszcze, że

$$[K(u) : K]_i = \frac{[K(u):K]}{[K(u):K]_s} = \frac{\deg f}{n} = \frac{n \cdot r}{n} = r.$$

TEORIA GALOIS

7. ROZSZERZENIA CYKLICZNE

DEFINICJA.

Niech F będzie skończenie wymiarowym rozszerzeniem ciała K oraz $\overline{K}$ domknięciem algebraicznym ciała K zawierającym ciało F . Jeśli $u \in F$, to NORMĄ elementu u (względem F i K) nazywamy

$$N_K^F(u) := \prod_{\sigma \in \text{Mor}_K(F, \overline{K})} (\sigma(u))^{[F:K]_i}.$$

Podobnie, ŚLADEM elementu u (względem F i K) nazywamy

$$T_K^F(u) := [F : K]_i \cdot \sum_{\sigma \in \text{Mor}_K(F, \overline{K})} \sigma(u).$$

OZNACZENIE.

Jeśli ciała K i F wynikają z kontekstu, to piszemy N i T zamiast N_K^F i T_K^F .

PRZYKŁAD.

Jeśli $K = \mathbb{R}$ i $F = \mathbb{C}$, to

$$\text{Mor}_{\mathbb{R}}(\mathbb{C}, \mathbb{C}) = \{\text{Id}_{\mathbb{C}}, \tau\},$$

gdzie $\tau: \mathbb{C} \rightarrow \mathbb{C}$ jest dane wzorem:

$$\tau(z) := \bar{z} \quad (z \in \mathbb{C}).$$

Zatem

$$N(z) = z^1 \cdot \bar{z}^1 = |z|^2 \quad \text{i} \quad T(z) = 1 \cdot (z + \bar{z}) = 2 \operatorname{re} z$$

dla każdej liczby $z \in \mathbb{C}$.

TWIERDZENIE 7.1.

Niech F będzie skończenie wymiarowym rozszerzeniem Galois ciała K . Jeśli $u \in F$, to

$$N_K^F(u) := \prod_{\sigma \in \text{Aut}_K F} \sigma(u) \quad \text{i} \quad T_K^F(u) := \sum_{\sigma \in \text{Aut}_K F} \sigma(u).$$

DOWÓD.

Niech $\overline{K}$ będzie domknięciem algebraicznym ciała K zawierającym ciało F . Ponieważ F jest rozszerzeniem normalnym ciała K na mocy Wniosku 3.12(1), więc z Twierdzenia 3.11 wynika, że $\text{Mor}_K(F, \overline{K}) = \text{Aut}_K(F)$. Korzystając ponownie z Wniosku 3.12(1), wiemy, że F jest rozszerzeniem rozdzielczym ciała K , zatem $[F : K]_i = 1$ i teza wynika wprost z definicji. $\square$

TEORIA GALOIS

Twierdzenie 7.2.

Niech F będzie skończeniem wymiarowym rozszerzeniem ciała K .

(1) Jeśli $u, v \in F$, to

$$N_K^F(u \cdot v) = N_K^F(u) \cdot N_K^F(v) \quad \text{ i } \quad T_K^F(u + v) = T_K^F(u) + T_K^F(v).$$

(2) Jeśli $u \in K$, to

$$N_K^F(u) = u^{[F:K]} \quad \text{ i } \quad T_K^F(u) = [F : K] \cdot u.$$

(3) Jeśli $u \in F$ i $f = x^n + a_{n-1}x^{n-1} + \dots + a_0$ jest wielomianem minimalnym elementu u nad ciałem K , to

$$N_K^F(u) = ((-1)^n \cdot a_0)^{[F:K(u)]} \quad \text{ i } \quad T_K^F(u) = -[F : K(u)] \cdot a_{n-1}.$$

W szczególności, $N_K^F(u), T_K^F(u) \in K$.

(4) Jeśli E jest podciałem ciała F zawierającym ciało K oraz $u \in F$, to

$$N_K^F(u) = N_K^E(N_E^F(u)) \quad \text{ i } \quad T_K^F(u) = T_K^E(T_E^F(u)).$$

Uwaga.

Z punktu (3) wynika, że jeśli $u \in F$, to elementy $N_K^F(u)$ i $T_K^F(u)$ nie zależą od wyboru domknięcia algebraicznego $\overline{K}$ ciała K .

Dowód.

(1) Bezpośrednio z definicji.

(2) Ponieważ $u \in K$, więc $\sigma(u) = u$ dla każdego homomorfizmu $\sigma \in \text{Mor}_K(F, \overline{K})$. Ponieważ ponadto $|\text{Mor}_K(F, \overline{K})| = [F : K]_s$ na mocy Stwierdzenia 6.6, więc

$$\begin{aligned} N_K^F(u) &= \prod_{\sigma \in \text{Mor}_K(F, \overline{K})} (\sigma(u))^{[F:K]_i} \\ &= \prod_{\sigma \in \text{Mor}_K(F, \overline{K})} u^{[F:K]_i} = u^{[F:K]_s \cdot [F:K]_i} = u^{[F:K]}. \end{aligned}$$

Analogicznie, $T_K^F(u) = [F : K] \cdot u$.

(0) Niech E będzie podciałem ciała F zawierającym ciało K . Z Lematu 6.5 wiemy, że zbiór $\text{Mor}_K(F, \overline{K})$ składa się z elementów postaci $\sigma_k \circ \tau_j$, $k \in [1, t], j \in [1, r]$, gdzie homomorfizmy $\tau_1, \dots, \tau_r$ są wszystkimi parami różnymi elementami zbioru $\text{Mor}_E(F, \overline{K})$, natomiast $\sigma_1, \dots, \sigma_t \in \text{Aut}_K \overline{K}$ są takimi automorfizmami, że homomorfizmy $\sigma_1 \circ \mu, \dots, \sigma_t \circ \mu$, gdzie

TEORIA GALOIS

$\mu: E \rightarrow \overline{K}$ jest naturalnym włożeniem, są wszystkimi parami różnymi elementami zbioru $\text{Mor}_K(E, \overline{K})$. Ponieważ $[F : K]_i = [F : E]_i \cdot [E : K]_i$ na mocy Wniosku 6.7, więc

$$\begin{aligned} N_K^F(u) &= \prod_{k=1}^t \prod_{j=1}^r (\sigma_k(\tau_j(u)))^{[F:K]_i} \\ &= \prod_{k=1}^t \left(\sigma_k \left(\prod_{j=1}^r (\tau_j(u))^{[F:E]_i} \right) \right)^{[E:K]_i} \\ &= \prod_{k=1}^t (\sigma_k(N_E^F(u)))^{[E:K]_i}. \end{aligned}$$

Analogicznie

$$T_K^F(u) = [E : K]_i \cdot \sum_{k=1}^t \sigma_k(T_E^F(u)).$$

- (3) Będziemy stosować notację i wzory z punktu (0) dla $E := K(u)$. Ponieważ $u \in K(u)$, więc $N_{K(u)}^F(u) = u^{[F:K(u)]}$ i $T_{K(u)}^F(u) = [F : K(u)] \cdot u$ na mocy punktu (2). Zatem, stosując wzory z części (0), otrzymujemy

$$N_K^F(u) = \prod_{k=1}^t (\sigma_k(u))^{[F:K(u)] \cdot [K(u):K]_i}$$

i

$$T_K^F(u) = [F : K(u)] \cdot [K(u) : K]_i \cdot \sum_{k=1}^t \sigma_k(u).$$

Zatem dla dowodu wystarczy pokazać, że

$$\prod_{k=1}^t (\sigma_k(u))^{[K(u):K]_i} = (-1)^n \cdot a_0 \quad \text{ i } \quad [K(u) : K]_i \cdot \sum_{k=1}^t \sigma_k(u) = -a_{n-1}.$$

Ponieważ $\sigma_1 \circ \mu, \dots, \sigma_t \circ \mu$ są wszystkimi parami różnymi elementami zbioru $\text{Mor}_K(K(u), \overline{K})$, więc $\sigma_1(u), \dots, \sigma_t(u)$ są wszystkimi parami różnymi pierwiastkami wielomianu f na mocy Wniosku 1.6, Stwierdzenia 2.1 oraz Twierdzenia 2.2. Korzystając z Wniosku 6.8, otrzymujemy

$$f = ((x - \sigma_1(u)) \cdots (x - \sigma_t(u)))^{[K(u):K]_i}.$$

TEORIA GALOIS

W szczególności $n = \deg f = t \cdot [K(u) : K]_i$. Ponadto

$$\begin{aligned} a_0 &= ((-1)^t \cdot \sigma_1(u) \cdots \sigma_t(u))^{[K(u):K]_i} \\ &= (-1)^{t \cdot [K(u):K]_i} \cdot (\sigma_1(u) \cdots \sigma_t(u))^{[K(u):K]_i} \\ &= (-1)^n \cdot \prod_{k=1}^t (\sigma_k(u))^{[K(u):K]_i}. \end{aligned}$$

Podobnie

$$a_{n-1} = -[K(u) : K]_i \cdot \sum_{k=1}^t \sigma_k(u),$$

co kończy dowód.

- (4) Ponownie będziemy stosować notację i wzory z punktu (0). Z części (3) wiemy, że $N_E^F(u), T_E^F(u) \in E$, więc $\sigma_k(N_E^F(u)) = (\sigma_k \circ \mu)(N_E^F(u))$ oraz $\sigma_i(T_E^F(u)) = (\sigma_k \circ \mu)(T_E^F(u))$ dla każdego $k \in [1, t]$. Ponieważ $\sigma_1 \circ \mu, \dots, \sigma_t \circ \mu$ są wszystkimi parami różnymi elementami zbioru $\text{Mor}_K(E, \overline{K})$, więc

$$\begin{aligned} N_K^F(u) &= \prod_{k=1}^t (\sigma_k(N_E^F(u)))^{[E:K]_i} = \prod_{k=1}^t ((\sigma_k \circ \mu)(N_E^F(u)))^{[E:K]_i} \\ &= \prod_{\sigma \in \text{Mor}_K(E, \overline{K})} (\sigma(N_E^F(u)))^{[E:K]_i} = N_K^E(N_E^F(u)). \end{aligned}$$

Analogicznie dowodzimy, że $T_K^F(u) = T_K^E(T_E^F(u))$. □

DEFINICJA.

Zbiór S automorfizmów ciała F nazywamy LINIOWO NIEZALEŻNYM, o ile spełniony jest warunek: jeśli $a_\sigma, \sigma \in S$, są elementami ciała F takimi, że $\#\{\sigma \in S : a_\sigma \neq 0\} < \infty$ i $\sum_{\sigma \in S} a_\sigma \cdot \sigma(u) = 0$ dla wszystkich elementów $u \in F$, to $a_\sigma = 0$ dla wszystkich automorfizmów $\sigma \in S$.

LEMAT 7.3.

Każdy zbiór automorfizmów ciała F jest liniowo niezależny.

DOWÓD.

Przypuśćmy, że istnieje zbiór automorfizmów ciała F , który nie jest liniowo niezależny, i ustalmy minimalny taki zbiór S . Wtedy $|S| < \infty$ oraz istnieją elementy $a_\sigma, \sigma \in S$, takie, że $a_\sigma \neq 0$ dla każdego automorfizmu $\sigma \in S$ oraz

$$(*) \quad \sum_{\sigma \in S} a_\sigma \cdot \sigma(u) = 0$$

TEORIA GALOIS

dla wszystkich elementów $u \in F$.

Zauważmy, że $|S| > 1$. Istotnie, gdyby $S = \{\sigma_1\}$, to $0 = \sum_{\sigma \in S} a_\sigma \cdot \sigma(1) = a_{\sigma_1}$, co byłoby sprzeczne z założeniami. Wybierzmy zatem automorfizmy $\sigma_1, \sigma_2 \in S$ oraz element $v \in F$ takie, że $\sigma_1(v) \neq \sigma_2(v)$. Z założenia (*) zastosowanego dla u równego $v \cdot u$ wynika, że

$$\sum_{\sigma \in S} a_\sigma \cdot \sigma(v) \cdot \sigma(u) = 0$$

dla wszystkich elementów $u \in F$. Odejmując od powyższej równości równość (*) pomnożoną przez $\sigma_1(v)$, otrzymujemy, że

$$\sum_{\sigma \in S'} a'_\sigma \cdot \sigma(u) = 0$$

dla wszystkich elementów $u \in F$, gdzie $S' := S \setminus \{\sigma_1\}$ oraz $a'_\sigma := (\sigma_1(v) - \sigma(v)) \cdot a_\sigma$ dla $\sigma \in S'$. Ponieważ $\sigma_2 \in S'$ i $a'_{\sigma_2} \neq 0$, więc zbiór S' nie jest liniowo niezależny, co przeczy minimalności zbioru S i kończy dowód. $\square$

DEFINICJA.

- (1) Rozszerzenie F ciała K nazywamy CYKLICZNYM, jeśli F jest algebraicznym rozszerzeniem Galois ciała K takim, że grupa $\text{Aut}_K F$ jest cykliczna.
- (2) Rozszerzenie F ciała K nazywamy ABELOWYM, jeśli F jest algebraicznym rozszerzeniem Galois ciała K takim, że grupa $\text{Aut}_K F$ jest abelowa.

TWIERDZENIE 7.4.

Niech F będzie skończenie wymiarowym rozszerzeniem cyklicznym ciała K . Jeśli σ jest generatorem grupy $\text{Aut}_K F$ oraz $u \in F$, to

- (1) $T_K^F(u) = 0$ wtedy i tylko wtedy, gdy istnieje element $v \in F$ taki, że $u = v - \sigma(v)$;
- (2) $N_K^F(u) = 1$ wtedy i tylko wtedy, gdy istnieje element $v \in F$ taki, że $u = v \cdot \sigma(v)^{-1}$.

UWAGA.

Twierdzenie 7.4(1) nosi nazwę Hilberts Satz 90.

DOWÓD.

Niech $n := [F : K]$. Ponieważ $n = |\text{Aut}_K F|$ na mocy Twierdzenia 2.17(1), więc Twierdzenie 7.1 implikuje, że

$$T(v) = v + \sigma(v) + \cdots + \sigma^{n-1}(v) \quad \text{ i } \quad N(v) := v \cdot \sigma(v) \cdots \sigma^{n-1}(v).$$

TEORIA GALOIS

- (1) Załóżmy najpierw, że $u = v - \sigma(v)$. Wtedy korzystając z pierwszego z powyższych wzorów oraz równości $\sigma^n = \text{Id}_F$, otrzymujemy łatwo $T(v) = 0$.

Założmy teraz, że $T(u) = 0$. Z Lematu 7.3 wiemy, że istnieje element $z \in F$ taki, że $T(z) \neq 0$. Ponieważ $T(z) \in K$ na mocy Twierdzenia 7.2(3), więc $\tau(T(z)^{-1} \cdot z) = T(z)^{-1} \cdot \tau(z)$ dla każdego automorfizmu $\tau \in \text{Aut}_K F$. W konsekwencji, jeśli $w := T(z)^{-1} \cdot z$, to $T(w) = T(z)^{-1} \cdot T(z) = 1$. Niech

$$v := \sum_{i=0}^{n-1} \sum_{j=0}^i \sigma^j(u) \cdot \sigma^i(w).$$

Ponieważ

$$u + \sigma(u) + \cdots + \sigma^{n-1}(u) = T(u) = 0$$

i

$$w + \sigma(w) + \cdots + \sigma^{n-1}(w) = T(w) = 1,$$

więc

$$\begin{aligned} v - \sigma(v) &= \sum_{i=0}^{n-1} \sum_{j=0}^i \sigma^j(u) \cdot \sigma^i(w) - \sum_{i=1}^n \sum_{j=1}^i \sigma^j(u) \cdot \sigma^i(w) \\ &= \sum_{i=0}^{n-1} u \cdot \sigma^i(w) - \sum_{j=1}^n \sigma^j(u) \cdot \sigma^n(w) = u \cdot 1 - 0 \cdot w = u. \end{aligned}$$

- (2) Podobnie jak w dowodzie punktu (1) łatwo pokazać, że jeśli $u = v \cdot \sigma(v)^{-1}$ dla pewnego elementu $v \in F$, to $N(u) = 1$.

Przypuśćmy teraz, że $N(u) = 1$. Oczywiście $u \neq 0$. Korzystając z Lematu 7.3, wiemy, że istnieje element $y \in F$ taki, że element v zdefiniowany wzorem

$$v := \sum_{i=0}^{n-1} \left(\prod_{j=0}^i \sigma^j(u) \right) \cdot \sigma^i(y)$$

jest niezerowy. Ponieważ

$$\sigma(u) \cdots \sigma^{n-1}(u) \cdot \sigma^n(u) = N(u) = 1,$$

więc

$$u^{-1} \cdot v = \sum_{i=0}^{n-1} \left(\prod_{j=1}^i \sigma^j(u) \right) \cdot \sigma^i(y) = 1 \cdot y + \sum_{i=1}^{n-1} \left(\prod_{j=1}^i \sigma^j(u) \right) \cdot \sigma^i(y)$$

TEORIA GALOIS

$$\begin{aligned}
 &= \left(\prod_{j=0}^{n-1} \sigma^{j+1}(u) \right) \cdot \sigma^n(y) + \sum_{i=0}^{n-2} \left(\prod_{j=0}^i \sigma^{j+1}(u) \right) \cdot \sigma^{i+1}(y) \\
 &= \sum_{i=0}^{n-1} \left(\prod_{j=0}^i \sigma^{j+1}(u) \right) \cdot \sigma^{i+1}(y) = \sigma(v).
 \end{aligned}$$

Stąd $u = v \cdot \sigma(v)^{-1}$, co kończy dowód. $\square$

STWIERDZENIE 7.5.

Niech F będzie rozszerzeniem cyklicznym ciała K oraz $[F : K] = m \cdot p^t$, gdzie $p := \text{char } K \neq 0$ i $p \nmid m$. Wtedy istnieje ciąg ciał

$$K = E_0 \subset E_1 \subset \cdots \subset E_t \subseteq F$$

taki, że F jest rozszerzeniem cyklicznym stopnia m ciała E_t oraz E_i jest rozszerzeniem cyklicznym ciała E_{i-1} stopnia p , dla $i \in [1, t]$.

DOWÓD.

Ponieważ $\text{Aut}_K F$ jest grupą cykliczną rzędu $m \cdot p^t$, więc istnieje ciąg podgrup

$$\{\text{Id}_F\} = G_{t+1} \leq G_t < \cdots < G_1 < G_0 = \text{Aut}_K F$$

taki, że G_t jest grupą cykliczną rzędu m oraz G_{i-1}/G_i jest grupą cykliczną rzędu p dla $i \in [0, t-1]$. Niech

$$E_i := G'_i := \{u \in F : \sigma(u) = u \text{ dla wszystkich } \sigma \in G_i\}$$

dla $i \in [0, t+1]$. Ponieważ F jest skończone wymiarowym rozszerzeniem Galois ciała K , więc z definicji $E_0 = K$, zaś z Lematu 2.10(3) wiemy, że $\text{Aut}_{E_i} F = G_i$ dla każdego $i \in [0, t+1]$. Zatem, korzystając z Twierdzenia 2.17(1), otrzymujemy

$$[F : E_t] = [G_t : G_{t+1}] = m \quad \text{oraz} \quad [E_i : E_{i-1}] = [G_{i-1} : G_i] = p$$

dla wszystkich $i \in [1, t]$.

Ustalmy teraz $i \in [1, t+1]$. Z Twierdzenia 2.17(2) wiemy, że F jest rozszerzeniem Galois ciała E_{i-1} . Ponieważ $\text{Aut}_{E_i} F = G_i$ jest dzielnikiem normalnym grupy $\text{Aut}_{E_{i-1}} F = G_{i-1}$, więc Twierdzenie 2.17(3) i (4) implikuje, że E_i jest rozszerzeniem Galois ciała E_{i-1} takim, że $\text{Aut}_{E_{i-1}} E_i = G_{i-1}/G_i$ dla każdego $i \in [1, t+1]$. $\square$

LEMAT 7.6.

Niech K będzie ciałem charakterystyki $p \neq 0$, $a \in K$ i $f := x^p - x - a$. Jeśli $f(u) = 0$ dla pewnego $u \in F$, gdzie F jest rozszerzeniem ciała K , to

$$f = (x - u) \cdots (x - (u + 1)) \cdots (x - (u + p - 1)).$$

W szczególności, jeśli F jest ciałem rozkładu wielomianu F , to $F = K(u)$.

TEORIA GALOIS

Dowód.

Przypomnijmy że $\mathbb{F}_p \subseteq K$ na mocy Twierdzenia 5.1. Dla każdego $i \in \mathbb{F}_p$ mamy $i^p = i$, więc

$$f(u+i) = (u+i)^p - (u+i) - a = u^p + i^p - u - i - a = f(u) = 0,$$

zatem $u, u+1, \dots, u+p-1$ są wszystkimi parami różnymi pierwiastkami wielomianu f , co kończy dowód pierwszej części. Ponieważ $1, \dots, p-1 \in K$, zatem jeśli F jest ciałem rozkładu wielomianu f , to

$$F = K(u, u+1, \dots, u+p-1) = K(u). \quad \square$$

LEMAT 7.7.

Niech K będzie ciałem charakterystyki $p \neq 0$, $a \in K$ i $f := x^p - x - a$. Jeśli F jest ciałem rozkładu wielomianu f oraz $u \in F$ jest pierwiastkiem wielomianu f , to funkcja $\Phi: \text{Aut}_K F \rightarrow \mathbb{F}_p$ dana wzorem

$$\Phi(\sigma) := \sigma(u) - u \quad (\sigma \in \text{Aut}_K F),$$

jest dobrze zdefiniowanym monomorfizmem grup.

Dowód.

Z Lematu 7.6 wiemy, że $F = K(u)$ oraz

$$f = (x-u) \cdot (x-(u+1)) \cdots (x-(u+p-1)).$$

W szczególności F jest ciałem rozkładu pewnego zbioru wielomianów rozdzielczych (czynniki nierozkładalnych wielomianu f nad ciałem K), więc F jest rozszerzeniem Galois ciała K na mocy Twierdzenia 3.9.

Korzystając ze Stwierdzenia 2.1 oraz Twierdzenia 2.2, wiemy, że funkcja Φ jest dobrze zdefiniowaną injekcją. Łatwo sprawdzić, że Φ jest również homomorfizmem grup. $\square$

STWIERDZENIE 7.8.

Niech K będzie ciałem charakterystyki $p \neq 0$. Ciało F jest rozszerzeniem cyklicznym ciała K stopnia p wtedy i tylko wtedy, gdy istnieje element $a \in K$ taki, że F wielomian $f := x^p - x - a$ jest nierozkładalny oraz F jest ciałem rozkładu wielomianu f .

Dowód.

$\Rightarrow$: Załóżmy, że F jest rozszerzeniem cyklicznym ciała K stopnia p , i niech σ będzie generatorem grupy $\text{Aut}_K F$. Z Twierdzenia 7.2(2) wiemy, że $T_K^F(1) = [F : K] \cdot 1 = 0$, więc istnieje element $v \in F$ taki, że $1 = v - \sigma(v)$ na mocy Twierdzenia 7.4(1). Niech $u := -v$. Wtedy $\sigma(u) = u+1 \neq u$, więc $u \in K$. Ponieważ stopień $[F : K]$ jest liczbą pierwszą, więc $F = K(u)$.

TEORIA GALOIS

Niech $a := u^p - u$. Wtedy

$$\sigma(a) = \sigma(u)^p - \sigma(u) = (u+1)^p - (u+1) = u^p + 1 - u - 1 = a,$$

zatem $a \in K$, gdyż F jest rozszerzeniem Galois ciała K i σ jest generatorem grupy $\text{Aut}_K F$. Oczywiście u jest pierwiastkiem wielomianu $f := x^p - x - a$. Ponieważ $\deg f = p = [F : K] = [K(u) : K]$, więc z Twierdzenia 1.7(2) wynika, że wielomian f jest nierozkładalny (nad ciałem K).

Z Lematu 7.6 wiemy, że

$$f = (x - u) \cdot (x - (u + 1)) \cdots (x - (u + p - 1)).$$

Ponieważ oczywiście $F = K(u) = K(u, u + 1, \dots, u + p - 1)$, więc F jest ciałem rozkładu wielomianu f .

$\Leftarrow$: Załóżmy, że $a \in K$, wielomian $f := x^p - x - a$ jest nierozkładalny oraz F jest ciałem rozkładu wielomianu f . Z Lematu 7.7 wiemy, że grupa $\text{Aut}_K F$ jest izomorficzna z podgrupą grupy addytywnej ciała $\mathbb{F}_p$, a więc jest cykliczna. Ponadto z Lematu 7.6 wynika, że jeśli $u \in F$ jest pierwiastkiem wielomianu f , to $F = K(u)$. Stąd

$$[F : K] = [K(u) : K] = \deg f = p$$

na mocy Twierdzenia 1.7(2). □

WNIOSEK 7.9.

Niech K będzie ciałem charakterystyki $p \neq 0$, $a \in K$ i $f := x^p - x - a$. Wtedy nad ciałem K wielomian f jest nierozkładalny albo jest iloczynem parami niestowarzyszonych wielomianów stopnia 1.

DOWÓD.

Niech F będzie ciałem rozkładu wielomianu f . Z Lematu 7.7 wiemy, że funkcja $\Phi: \text{Aut}_K F \rightarrow \mathbb{F}_p$ dana wzorem

$$\Phi(\sigma) := \sigma(u) - u \quad (\sigma \in \text{Aut}_K F),$$

jest dobrze zdefiniowanym monomorfizmem grup. W szczególności, $\text{Aut}_K F = \{\text{Id}_F\}$ lub Φ jest izomorfizmem. Z Lematu 7.6 wiemy, że wielomian f nad ciałem F wielomian f jest iloczynem parami niestowarzyszonych wielomianów stopnia 1. Stąd F jest rozszerzeniem Galois ciała K na mocy Twierdzenia 3.9. Zatem jeśli $\text{Aut}_K F = \{\text{Id}_F\}$, to $F = K$, a więc nad ciałem K wielomian f jest iloczynem parami niestowarzyszonych wielomianów stopnia 1.

Założmy zatem, że Φ jest izomorfizmem. Jeśli v jest pierwiastkiem wielomianu f , to z Lematu 7.6 wynika, że istnieje automorfizm $\sigma \in \text{Aut}_K F$ taki,

TEORIA GALOIS

że $\Phi(\sigma) = v - u$, tzn. $\sigma(v) = u$. Stąd wynika, że elementy u i v mają ten sam wielomian minimalny nad ciałem K . Ponieważ z Lematu 7.6 wynika, że nad ciałem K wielomian f jest iloczynem parami niestowarzyszonych wielomianów nierozkładalnych, więc dowolność pierwiastka v implikuje, że wielomian f jest nierozkładalny. $\square$

DEFINICJA.

Jeśli K jest ciałem i $n \in \mathbb{N}_+$, to element $\zeta \in K$ jest nazywany **PIERWIASTKIEM (PIERWOTNYM) n -TEGO STOPNIA Z JEDYNKI**, jeśli $\zeta^n = 1$ (oraz $\zeta^m \neq 1$ dla $m \in [1, n-1]$).

UWAGI.

- (1) Jeśli K jest ciałem i $n \in \mathbb{N}_+$, to zbiór pierwiastków n -tego stopnia z jedynki z działaniem mnożenia tworzy grupę, która jest cykliczna (na mocy Twierdzenia 5.3) rzędu co najwyżej n . Jeśli ζ jest pierwiastkiem pierwotnym z jedynki, to ζ jest generatorem tej grupy.
- (2) Załóżmy, że K jest ciałem charakterystyki p . Jeśli $p \mid n$ (w szczególności $p \neq 0$), to $x^n - 1 = (x^m - 1)^p$, gdzie $m := \frac{n}{p}$. W szczególności każdy pierwiastek n -tego stopnia z 1 jest pierwiastkiem stopnia m . Ponieważ $m < n$, więc nie istnieją pierwiastki pierwotne n -tego stopnia z 1.
- (3) Załóżmy, że K jest ciałem charakterystyki p . Jeśli $p \nmid n$ i $f := x^n - 1$, to $\gcd(f, f') = 1$, więc wielomian f ma n parami różnych pierwiastków w ciele F rozkładu wielomianu f nad ciałem K . Zatem grupa pierwiastków n -tego stopnia z jedynki w ciele F , która jest cykliczna, ma rząd n , więc w ciele F istnieje pierwiastek pierwotny n -tego stopnia z 1. Ponadto, jeśli istnieje pierwiastek pierwotny n -tego stopnia z 1 w ciele K , to $F = K$.

PRZYKŁADY.

- (1) 1 jest pierwiastkiem n -tego stopnia z 1 dla każdej liczby $n \in \mathbb{N}_+$.
- (2) Jeśli K jest ciałem charakterystyki $p \neq 0$ i $n := p^k$ dla pewnej liczby $k \in \mathbb{N}$, to 1 jest jednym pierwiastkiem n -tego stopnia z 1.
- (3) W ciele $\mathbb{Q}(\iota)$ są cztery pierwiastki czwartego stopnia z 1 (w tym dwa pierwotne), ale tylko jeden (trywialny) pierwiastek trzeciego stopnia z 1.
- (4) Dla każdej liczby $n \in \mathbb{N}_+$ liczba $\cos \frac{2\pi}{n} + \iota \cdot \sin \frac{2\pi}{n}$ jest pierwiastkiem pierwotnym n -tego stopnia z 1.

LEMAT 7.10.

Niech $n \in \mathbb{N}_+$ i K będzie ciałem zawierającym pierwiastek pierwotny ζ n -tego stopnia z 1.

TEORIA GALOIS

- (1) Jeśli $d \mid n$, to $\eta := \zeta^{n/d}$ jest pierwiastkiem pierwotnym stopnia d z 1.
- (2) Jeśli $d \mid n$, $a \in K$ oraz u jest niezerowym pierwiastkiem wielomianu $f := x^d - a$ (w pewnym rozszerzeniu ciała K), to wielomian f na d różnych pierwiastków: $u, \eta \cdot u, \dots, \eta^{d-1} \cdot u$, gdzie η jest pierwiastkiem pierwotnym stopnia d z 1. Ponadto ciało $K(u)$ jest ciałem rozkładu wielomianu f i rozszerzeniem Galois ciała K .

Dowód.

- (1) Ćwiczenie.
- (2) Oczywiście $(\eta^i \cdot u)^d = 1$ dla każdego $i \in [0, d-1]$, gdyż η jest pierwiastkiem d -tego stopnia z 1. Ponadto pierwotność η implikuje, że elementy $u, \eta \cdot u, \dots, \eta^{d-1} \cdot u$ są parami różne. Stąd

$$f = (x - u) \cdot (x - \eta \cdot u) \cdots (x - \eta^{d-1} \cdot u).$$

Ponieważ $\eta \in K$, więc $K(u, \eta \cdot u, \dots, \eta^{d-1} \cdot u) = K(u)$, zatem ciało $K(u)$ jest ciałem rozkładu wielomianu f . Ponadto z powyższej równości wynika, że wielomian f jest iloczynem wielomianów rozdzielczych, zatem ciało $K(u)$ jest rozszerzeniem Galois ciała K na mocy Twierdzenia 3.9. $\square$

Twierdzenie 7.11.

Niech $n \in \mathbb{N}_+$ i K będzie ciałem zawierającym pierwiastek pierwotny ζ n -tego stopnia z 1. Jeśli F jest rozszerzeniem ciała K , to następujące warunki są równoważne.

- (1) F jest rozszerzeniem cyklicznym stopnia d takiego, że $d \mid n$.
- (2) F jest ciałem rozkładu nad ciałem K wielomianu postaci $x^n - a$.
- (3) F jest ciałem rozkładu nad ciałem K wielomianu nierozkładalnego postaci $x^d - b$, gdzie $d \mid n$.

Dowód.

(2) $\implies$ (1): Niech $u \in F$ będzie pierwiastkiem wielomianu $f := x^n - a$. Bez straty ogólności możemy założyć, że $a \neq 0$ i konsekwencji $u \neq 0$. Z Lematu 7.10(2) wiemy, że $F = K(u)$ oraz F jest rozszerzeniem Galois ciała K . Niech G będzie grupą pierwiastków n -tego stopnia z 1 w ciele K . Definiujemy funkcję $\Phi: \text{Aut}_K F \rightarrow G$ wzorem

$$\Phi(\sigma) := \frac{\sigma(u)}{u} \quad (\sigma \in \text{Aut}_K F).$$

Z Twierdzenia 2.2 i Lematu 7.10(2) wynika, że funkcja Φ jest dobrze określona. Ponadto Stwierdzenie 2.1 implikuje, że funkcja Φ jest różnowartościowa.

TEORIA GALOIS

Łatwo też sprawdzić, że funkcja Φ jest homomorfizmem. Z powyższych faktów wynika, że grupa $\text{Aut}_K F$ jest izomorficzna z podgrupą grupy G , która jest cykliczna rzędu n . Stąd grupa $\text{Aut}_K F$ jest cykliczna rzędu dzielącego n .

(1) $\implies$ (3): Z założenia grupa $\text{Aut}_K F$ jest cykliczna rzędu d oraz $d = [F : K]$. Niech σ będzie generatorem grupy $\text{Aut}_K F$. Jeśli $\eta := \zeta^{n/d}$, to η jest pierwiastkiem pierwotnym stopnia d z 1 na mocy Lematu 7.10(1). Korzystając z Twierdzenia 7.2(2), otrzymujemy

$$N_K^F(\eta) = \eta^{[F:K]} = \eta^d = 1.$$

Wobec Twierdzenia 7.4(2) oznacza to, że istnieje element $w \in F$ taki, że $\eta = w \cdot (\sigma(w))^{-1}$. Innymi słowy, jeśli $v := w^{-1}$, to $\sigma(v) = \eta \cdot v$, więc

$$\sigma(v^d) = \eta^d \cdot v^d = 1 \cdot v^d = v^d.$$

Ponieważ F jest rozszerzeniem Galois ciała K , więc powyższa równość oznacza, że $b := v^d \in K$, zatem element v jest pierwiastkiem wielomianu $f := x^d - b \in K[x]$. Z Lematu 7.10(2) wiemy, że ciało $K(v)$ jest ciałem rozkładu wielomianu f , a $v, \eta \cdot v, \dots, \eta^{d-1} \cdot v$ są wszystkimi parami różnymi pierwiastkami wielomianu f . Ponieważ $\sigma^i(v) = \eta^i \cdot v$, więc σ indukuje K -izomorfizm $K(v) \simeq K(\eta^i \cdot v)$ taki, że $\sigma(v) = \eta^i \cdot v$, a zatem elementy v i $\eta^i \cdot v$ mają ten sam wielomian minimalny nad ciałem K na mocy Wniosku 1.6, dla każdego $i \in [0, d-1]$. Stąd wynika, że wielomian f jest nierozkładalny. W szczególności,

$$[K(v) : K] = \deg f = d = [F : K]$$

na mocy Twierdzenia 1.7(2), zatem $F = K(v)$.

(3) $\implies$ (2): Jeśli v jest pierwiastkiem wielomianu $x^d - b$, to $F = K(v)$ na mocy Lematu 7.10(2). Niech $u := \zeta \cdot v$ i $a = b^{n/d}$. Wtedy

$$u^n = (\zeta \cdot v)^n = \zeta^n \cdot v^n = 1 \cdot (v^d)^{n/d} = b^{n/d} = a,$$

zatem u jest pierwiastkiem wielomianu $f := x^n - a$. Korzystając ponownie z Lematu 7.10(2), wiemy, że ciało $K(u)$ jest ciałem rozkładu wielomianu f . Ponadto

$$K(u) = K(\eta \cdot v) = K(v) = F,$$

gdyż $\eta \in K$, co kończy dowód. □

8. ROZSZERZENIA CYKLOTOMICZNE

DEFINICJA.

ROZSZERZENIEM CYKLOTOMICZNYM RZĘDU n ciała K nazywamy ciało rozkładu wielomianu $x^n - 1$.

UWAGA.

Jeśli K jest ciałem charakterystyki $p \neq 0$, to F jest rozszerzeniem cyklotomicznym rzędu n ciała K wtedy i tylko wtedy, gdy jest rozszerzeniem cyklotomicznym stopnia $p \cdot n$. W konsekwencji wystarczy badać rozszerzenia cyklotomiczne stopni niepodzielnych przez $\text{char } K$.

Twierdzenie 8.1.

Niech n będzie dodatnią liczbą całkowitą, K ciałem taki, że $\text{char } K \nmid n$ oraz F rozszerzeniem cyklotomicznym ciała K rzędu n .

- (1) $F = K(\xi)$, $\xi \in F$ jest pierwiastkiem pierwotnym stopnia n z 1.
- (2) Grupa $\text{Aut}_K F$ jest izomorficzna z podgrupą grupy $\mathbb{Z}_n^\times$.
- (3) Ciało F jest rozszerzeniem abelowym ciała K stopnia d takiego, że $d \mid \varphi(n)$. Jeśli n jest liczbą pierwszą, to ciało F jest rozszerzeniem cyklicznym ciała K .

Dowód.

- (1) Ponieważ $\text{char } F = \text{char } K \nmid n$, więc istnieje $\xi \in F$ będące pierwiastkiem pierwotnym stopnia n z 1. Wtedy $1, \xi, \dots, \xi^{n-1}$ są wszystkimi pierwiastkami wielomianu $x^n - 1$, więc $F = K(\xi)$.
- (2) Jeśli $\sigma \in \text{Aut}_K F$, to $\sigma(\xi)$ jest pierwiastkiem pierwotnym wielomianu $x^n - 1$ na mocy Twierdzenia 2.2, zatem $\sigma(\xi) = \xi^i$ dla pewnego (jednoznacznie wyznaczonego) $i \in \mathbb{Z}_n^\times$. Oznaczając i przez $\Phi(\sigma)$, otrzymujemy funkcję $\Phi: \text{Aut}_K F \rightarrow \mathbb{Z}_n^\times$. Funkcja ta jest różnowartościowa na mocy Stwierdzenia 2.1 i punktu (1). Ponadto łatwo pokazać, że funkcja Φ jest homomorfizmem, co implikuje tezę.
- (3) Ponieważ pierwiastki wielomianu $x^n - 1$ są parami różne, więc wielomian $x^n - 1$ jest iloczynem wielomianów rozdzielczych, zatem ciało F jest rozszerzeniem Galois ciała K na mocy Twierdzenia 3.9. Ponieważ dodatkowo $|\mathbb{Z}_n^\times| = \varphi(n)$ oraz, gdy $n \in \mathbb{P}$, grupa $\mathbb{Z}_n^\times$ jest cykliczna na mocy Twierdzenia 5.3, więc teza wynika z punktu (2) (oraz Twierdzenia Lagrange'a). $\square$

9. ROZSZERZENIA PIERWIASTNIKOWE

DEFINICJA.

Rozszerzenie F ciała K nazywamy PIERWIASTNIKOWYM, jeśli istnieją elementy $u_1, \dots, u_n$ ciała F takie, że $F = K(u_1, \dots, u_n)$ oraz dla każdego $i \in [1, n]$ istnieje $m_i \in \mathbb{N}_+$ takie, że $u_i^{m_i} \in K(u_1, \dots, u_{i-1})$.

UWAGA.

Jeśli F jest rozszerzeniem pierwiastnikowym ciała K , to F jest skończenie wymiarowym rozszerzeniem algebraicznym ciała K .

DOWÓD.

Wybermy elementy $u_1, \dots, u_n$ ciała F takie, że $F = K(u_1, \dots, u_n)$ oraz dla każdego $i \in [1, n]$ istnieje $m_i \in \mathbb{N}_+$ takie, że $u_i^{m_i} \in K(u_1, \dots, u_{i-1})$. Wtedy na mocy Twierdzenia 1.9 dla każdego $i \in [1, n]$ $K(u_1, \dots, u_i)$ jest rozszerzeniem algebraicznym ciała $K(u_1, \dots, u_{i-1})$ oraz $[K(u_1, \dots, u_i) : K(u_1, \dots, u_{i-1})] < \infty$. Stąd $[K(u_1, \dots, u_n) : K] < \infty$ wobec Twierdzenia 1.1. W szczególności, Twierdzenie 1.8 implikuje, że $K(u_1, \dots, u_n)$ jest rozszerzeniem algebraicznym ciała K . $\square$

DEFINICJA.

Niech K będzie ciałem i $f \in K[x] \setminus \{0\}$. Mówmy, że równanie $f(x) = 0$ jest ROZWIĄZALNE PRZED PIERWIASTNIKI wtedy i tylko wtedy, gdy istnieje rozszerzenie pierwiastnikowe F ciała K i ciało rozkładu E wielomianu f nad ciałem K takie, że $E \subseteq F$.

LEMAT 9.1.

Jest F jest skończenie wymiarowym rozszerzeniem ciała K i N jest domknięciem normalnym ciała F , to istnieją podciała $E_1, \dots, E_r$ ciała N takie, że $E_i \simeq F$ dla każdego $i \in [1, r]$ oraz $N = E_1 \cdots E_r$.

DOWÓD.

Wybermy bazę $w_1, \dots, w_n$ ciała F nad ciałem K . Zauważmy, że elementy $w_1, \dots, w_n$ są algebraiczne nad ciałem K na mocy Twierdzenia 1.8. Dla każdego $i \in [1, n]$ niech $f_i \in K[x]$ będzie wielomianem minimalnym elementu w_i . Ze Stwierdzenia 3.13 i Twierdzenia 3.14 wynika, że N jest ciałem rozkładu zbioru $\{f_1, \dots, f_n\}$ nad ciałem K .

Ustalmy $i \in [1, n]$ oraz pierwiastek $v \in N$ wielomianu f_i . Z Twierdzenia 1.5 wiemy, że istnieje K -izomorfizm $\sigma: K(w_i) \rightarrow K(v)$ taki, że $\sigma(w_i) = v$. Twierdzenie 3.7 implikuje, że istnieje automorfizm $\tau \in \text{Aut}_K N$ taki, że $\tau|_{K(w_i)} = \sigma$. Zauważmy, że $E_{i,v} := \tau(F)$ jest podciałem ciała N zawierającym ciało K oraz element $\tau(w_i) = \sigma(w_i) = v$. Innymi słowy, dla każdego $i \in [1, n]$ oraz pierwiastka v wielomianu f_i istnieje podciało $E_{i,v}$ ciała N takie, że $v \in E_{i,v}$ oraz

TEORIA GALOIS

$E_{i,v} \simeq F$. Jeśli $E_1, \dots, E_r$ są wszystkimi ciałami otrzymanymi w ten sposób, to $N = E_1 \cdots E_r$, gdyż N jest ciałem rozkładu zbioru $\{f_1, \dots, f_n\}$ nad ciałem K . $\square$

WNIOSEK 9.2.

Jest F jest rozszerzeniem pierwiastnikowym ciała K i N jest domknięciem normalnym ciała F , to N jest rozszerzeniem pierwiastnikowym ciała K .

DOWÓD.

Z Lematu 9.1 wynika, że istnieją podciała $E_1, \dots, E_r$ ciała N takie, że $E_i \simeq F$ dla każdego $i \in [1, r]$ oraz $N = E_1 \cdots E_r$. Z izomorfizmu $E_i \simeq F$ wynika, że E_i jest rozszerzeniem pierwiastnikowym ciała K dla każdego $i \in [1, r]$, więc również $N = E_1 \cdots E_r$ jest rozszerzeniem pierwiastnikowym ciała K .

LEMAT 9.3.

Jeśli F jest rozszerzeniem Galois ciała E , E jest rozszerzeniem Galois ciała K oraz F jest ciałem rozkładu nad ciałem E pewnego zbioru wielomianów o współczynnikach w ciele K , wtedy ciało F jest rozszerzeniem Galois ciała K .

DOWÓD.

Ustalmy element u ciała F nienależący do K . Jeśli $u \notin E$, to istnieje automorfizm $\sigma \in \text{Aut}_E F \subseteq \text{Aut}_K F$ taki, że $\sigma(u) \neq u$, ponieważ F jest rozszerzeniem Galois ciała E . Załóżmy zatem, że $u \in E$. Ponieważ E jest rozszerzeniem Galois ciała K , więc istnieje automorfizm $\sigma \in \text{Aut}_K E$ taki, że $\sigma(u) \neq u$. Z Twierdzenia 3.7 wiemy, że istnieje automorfizm $\tau \in \text{Aut}_K F$ taki, że $\tau|_E = \sigma$. Wtedy $\tau(u) = \sigma(u) \neq u$, co kończy dowód. $\square$

TWIERDZENIE 9.4.

Jeśli F jest rozszerzeniem pierwiastnikowym ciała K i E jest podciałem ciała F zawierającym ciało K , to grupa $\text{Aut}_K E$ jest rozwiązalna.

DOWÓD.

Założmy najpierw, że $E = F$ oraz F jest rozszerzeniem Galois ciała K . Z definicji rozszerzenia pierwiastkowego wiemy, że istnieją elementy $u_1, \dots, u_n$ ciała F oraz liczby $m_1, \dots, m_n \in \mathbb{N}_+$ takie, że $F = K(u_1, \dots, u_n)$ oraz $u_i^{m_i} \in K(u_1, \dots, u_{i-1})$ dla każdego $i \in [1, n]$. Bez straty ogólności możemy założyć, że $u_i \neq 0$ oraz $\text{char } K \nmid m_i$ dla każdego $i \in [1, n]$. Istotnie, jeśli $\text{char } K \mid m_i$, to $p := \text{char } K \in \mathbb{P}$ oraz $m_i = r \cdot p^t$, gdzie $r, t \in \mathbb{N}_+$ oraz $p \nmid r$. Wtedy element u_i^r jest czysto nierozdzielczy nad ciałem $K(u_1, \dots, u_{i-1})$. Wiemy jednak z Twierdzenia 3.9, że ciało F , jako rozszerzenie Galois, jest rozdzielcze nad ciałem K , a więc również rozdzielcze nad ciałem $K(u_1, \dots, u_{i-1})$. To oznacza, że $u_i^r \in K(u_1, \dots, u_{i-1})$ na mocy Twierdzenia 6.1, zatem możemy zastąpić liczbę m_i liczbą r .

Niech $m := m_1 \cdots m_n$ oraz niech $F(\xi)$ będzie rozszerzeniem cyklotomicznym ciała F rzędu m , gdzie ξ jest pierwiastkiem pierwotnym stopnia m z 1. Pokażemy, że wystarczy pokazać, że grupa $\text{Aut}_{K(\xi)} F(\xi)$ jest rozwiązalna. Istotnie, $F(\xi)$ jest rozszerzeniem Galois ciała F (na mocy Twierdzenia 8.1(3)), więc również ciała K (na mocy Lematu 9.3). Z Twierdzenia 2.17(4) wiemy, że $\text{Aut}_K F \simeq \text{Aut}_K F(\xi) / \text{Aut}_F F(\xi)$. W szczególności, rozwiązalność grupy $\text{Aut}_K F$ jest równoważna rozwiązalności grupy $\text{Aut}_K F(\xi)$, gdyż na mocy Twierdzenia 8.1(2) grupa $\text{Aut}_F F(\xi)$ jest abelowa. Analogicznie $K(\xi)$ jest rozszerzeniem abelowym ciała K oraz $\text{Aut}_K K(\xi) \simeq \text{Aut}_K F(\xi) / \text{Aut}_{K(\xi)} F(\xi)$, więc rozwiązalność grupy $\text{Aut}_K F(\xi)$ jest równoważna rozwiązalności grupy $\text{Aut}_{K(\xi)} F(\xi)$.

Aby pokazać rozwiązalność grupy $\text{Aut}_{K(\xi)} F(\xi)$ oznaczmy dla $i \in [0, n]$ przez E_i ciało $K(\xi, u_1, \dots, u_i)$. W szczególności $E_0 = K(\xi)$ i $E_n = F(\xi)$. Niech $H_i := \text{Aut}_{E_i} F(\xi)$ dla $i \in [0, n]$. W szczególności $H_0 = \text{Aut}_{K(\xi)} F(\xi)$ oraz $H_n = \{\text{Id}_{F(\xi)}\}$. Na mocy Lematu 7.10(1) ciało $K(\xi)$ zawiera pierwiastek pierwotny stopnia m_i z jedynki. Ustalmy $i \in [1, n]$. Ponieważ $u_i^{m_i} \in E_{i-1}$, więc na mocy Lematu 7.10(2) ciało $E_i = E_{i-1}(u_i)$ jest ciałem rozkładu nad ciałem E_{i-1} wielomianu $x^{m_i} - u_i^{m_i}$ i rozszerzeniem Galois ciała E_{i-1} . Wobec Twierdzenia 2.17(3) oznacza to, że grupa H_i jest dzielnikiem normalnym grupy H_{i-1} , zaś Twierdzenie 2.17(4) implikuje, że $H_{i-1}/H_i \simeq \text{Aut}_{E_{i-1}} E_i$. Ponadto z Twierdzenia 7.11 wynika, że E_i jest rozszerzeniem cyklicznym ciała E_{i-1} , zatem grupa $\text{Aut}_{E_{i-1}} E_i$ jest cykliczna, a więc również abelowa. Innymi słowy ciąg

$$\{\text{Id}_{F(\xi)}\} = H_n \leq H_{n-1} \leq \cdots \leq H_1 \leq H_0 = \text{Aut}_{K(\xi)} F(\xi)$$

jest ciągiem oznaczającym rozwiązalność grupy $\text{Aut}_{K(\xi)} F(\xi)$.

Rozważmy teraz sytuację ogólną. Niech

$$L := \{u \in E : \sigma(u) = u \text{ dla wszystkich } \sigma \in \text{Aut}_K E\}.$$

Wtedy $\text{Aut}_K E = \text{Aut}_L E$, ciało E jest rozszerzeniem Galois ciała L oraz ciało F jest rozszerzeniem pierwiastnikowym ciała L . Niech N będzie domknięciem normalnym ciała F nad ciałem L . Wtedy N jest rozszerzeniem pierwiastnikowym ciała L na mocy Wniosku 9.2 oraz E jest podciałem stabilnym ciała N względem podciała L na mocy Lematu 2.14. W szczególności otrzymujemy homomorfizm $\Phi: \text{Aut}_L N \rightarrow \text{Aut}_L E$ dany wzorem $\Phi(\sigma) := \sigma|_E$ dla $\sigma \in \text{Aut}_L N$. Ze Stwierdzenia 3.13 i Twierdzenia 3.14 wynika, że N jest ciałem rozkładu zbioru pewnego zbioru wielomianów nad ciałem L , więc Φ jest epimorfizmem na mocy Twierdzenia 3.7.

Niech

$$M := \{u \in N : \sigma(u) = u \text{ dla wszystkich } \sigma \in \text{Aut}_L N\}.$$

TEORIA GALOIS

Wtedy N jest pierwiastnikowym rozszerzeniem Galois ciała M , więc grupa $\text{Aut}_L N = \text{Aut}_M N$ jest rozwiązalna na mocy pierwszej części dowodu. Ponieważ $\text{Aut}_K E = \text{Aut}_L E = \text{Im } \Phi$ oraz obraz grupy rozwiązalnej jest rozwiązalny, to kończy dowód. $\square$

WNIOSEK 9.5.

Niech K będzie ciałem i $f \in K[x]$. Jeśli równanie $f(x) = 0$ jest rozwiązalne przez pierwiastniki, to grupa Galois wielomianu f jest rozwiązalna.

Dowód.

Natychmiast z definicji i Twierdzenia 9.4. $\square$

TEORIA GALOIS

C. OGÓLNE RÓWNANIE STOPNIA n

DEFINICJA.

Jeśli K jest ciałem i $n \in \mathbb{N}_+$, to OGÓLNYM RÓWNANIEM STOPNIA n NAD CIAŁEM K nazywamy równanie

$$x^n - t_1 \cdot x^{n-1} + \cdots + (-1)^{n-1} \cdot t_{n-1} \cdot x_1 + (-1)^n \cdot t_n = 0$$

o współczynnikach w ciele funkcji wymiernych $K(t_1, \dots, t_n)$.

OZNACZENIE.

Niech K będzie ciałem oraz $n \in \mathbb{N}_+$. Jeśli $\sigma \in \mathfrak{S}_n$ oraz $u \in K(x_1, \dots, x_n)$, to przez u^σ oznaczamy obraz funkcji u przy K -automorfizmie ciała $K(x_1, \dots, x_n)$ indukowanym przez przyporządkowanie $x_i \mapsto x_{\sigma(i)}$, $i \in [1, n]$.

DEFINICJA.

Jeśli K jest ciałem oraz $n \in \mathbb{N}_+$, to funkcję wymierną $u \in K(x_1, \dots, x_n)$ nazywamy SYMETRYCZNĄ, jeśli $u^\sigma = u$ dla wszystkich permutacji $\sigma \in \mathfrak{S}_n$.

LEMAT C.1.

Jeśli $n \in \mathbb{N}_+$ oraz E będzie ciałem symetrycznych funkcji wymiernych nad ciałem K od n zmiennych, to $\text{Aut}_E K(x_1, \dots, x_n) \simeq \mathfrak{S}_n$.

DOWÓD.

Mamy monomorfizm $\Phi: \mathfrak{S}_n \rightarrow \text{Aut}_K K(x_1, \dots, x_n)$ dany wzorem

$$(\Phi(\sigma))(u) := u^\sigma \quad (\sigma \in \mathfrak{S}_n, u \in K(x_1, \dots, x_n)).$$

Wtedy

$$E = \{u \in K(x_1, \dots, x_n) : \sigma(u) = u \text{ dla wszystkich } \sigma \in \text{Im } \Phi\}.$$

Z Twierdzenia 2.18 wynika, że $\text{Aut}_E K(x_1, \dots, x_n) \simeq \text{Im } \Phi \simeq \mathfrak{S}_n$. □

LEMAT C.2.

Jeśli K jest ciałem oraz $n \in \mathbb{N}_+$, to funkcja wymierna $f \in K(x_1, \dots, x_n)$ jest symetryczna wtedy i tylko wtedy, gdy istnieją wielomiany symetryczne $f, g \in K[x_1, \dots, x_n]$ takie, że $u = \frac{f}{g}$.

DOWÓD.

$\Leftarrow$: Oczywiście.

$\Rightarrow$: Wybierzmy wielomiany $a, b \in K[x_1, \dots, x_n]$ takie, że $u = \frac{a}{b}$. Wtedy $u = \frac{f}{g}$, gdzie $f := a \cdot \prod_{\sigma \in \mathfrak{S}_n \setminus \{\text{Id}\}} b^\sigma$ oraz $g := \prod_{\sigma \in \mathfrak{S}_n} b^\sigma$. Oczywiście wielomian g jest symetryczny. Ponadto $f = u \cdot g$, więc wielomian f też jest symetryczny. □

TEORIA GALOIS

DEFINICJA.

Jeśli K jest ciałem $n \in \mathbb{N}_+$, to ELEMENTARNYMI FUNKCJAMI SYMETRYCZNYMI nazywamy wielomiany $s_1, \dots, s_n \in K[x_1, \dots, x_n]$ zdefiniowane wzorami

$$s_i := \sum_{1 \leq j_1 < \dots < j_i \leq n} x_{j_1} \cdots x_{j_i} \quad (i \in [1, n]).$$

STWIERDZENIE C.3.

Jeśli $n \in \mathbb{N}_+$ oraz E jest ciałem symetrycznych funkcji wymiernych nad ciałem K od n zmiennych, to $E = K(s_1, \dots, s_n)$.

DOWÓD.

Korzystając z Lematu C.2, wiemy, że wystarczy pokazać, że jeśli wielomian $f \in K[x_1, \dots, x_n]$ jest symetryczny, to $f \in K[s_1, \dots, s_n]$.

Niech $\prec$ będzie porządkiem leksykograficznym na jednomianach, tj.

$$x_1^{p_1} \cdots x_n^{p_n} \prec x_1^{q_1} \cdots x_n^{q_n} : \Longleftrightarrow \exists l \in [1, n] : p_1 = q_1 \wedge \dots \wedge p_{l-1} = q_{l-1} \wedge p_l < q_l.$$

Zauważmy, że jednomianami wiodącymi (w powyższym porządku) wielomianów $s_1, \dots, s_n$ są wielomiany

$$h_i := x_1 \cdots x_i \quad (i \in [1, n]),$$

odpowiednio. Ponadto, jeśli jednomian $h = x_1^{p_1} \cdots x_n^{p_n}$ jest jednomianem wiodącym wielomianu symetrycznego f , to $p_1 \geq \dots \geq p_n$. W szczególności, istnieją wykładniki $m_1, \dots, m_n \in \mathbb{N}$ takie, że $h = h_1^{m_1} \cdots h_n^{m_n}$. Stąd istnieje $u \in K$ takie, że wielomian $f - u \cdot s_1^{m_1} \cdots s_n^{m_n}$ jest wielomianem symetrycznym z mniejszym (lub zerowym) jednomianem wiodącym, więc teza wynika przez prostą indukcję. $\square$

TWIERDZENIE C.4 (ABEL).

Niech K będzie ciałem i $n \in \mathbb{N}_+$. Jeśli ogólne równanie stopnia n nad ciałem K jest rozwiązywalne przez pierwiastniki, to $n \leq 4$.

DOWÓD.

Niech

$$p_n := x^n - t_1 \cdot x^{n-1} + \dots + (-1)^{n-1} \cdot t_{n-1} x + (-1)^n \cdot t_n$$

oraz F będzie ciałem rozkładu wielomianu p_n nad ciałem $K(t_1, \dots, t_n)$. Wtedy istnieją elementy $u_1, \dots, u_n \in F$ takie, że $F = K(t_1, \dots, t_n)(u_1, \dots, u_n)$ oraz

$$p_n = (x - u_1) \cdots (x - u_n).$$

TEORIA GALOIS

Stąd łatwo widać, że $t_i = s_i(u_1, \dots, u_n)$ dla każdego $i \in [1, n]$. W szczególności, $t_1, \dots, t_n \in K(u_1, \dots, u_n)$, a więc $F = K(u_1, \dots, u_n)$.

Rozważmy odwzorowanie $\Phi: K[t_1, \dots, t_n] \rightarrow K[x_1, \dots, x_n]$ dane wzorem

$$\Phi(g) := g(s_1, \dots, s_n).$$

Przypuśćmy, że $\Phi(g) = 0$. Wtedy

$$\begin{aligned} g = g(t_1, \dots, t_n) &= g(s_1(u_1, \dots, u_n), \dots, s_n(u_1, \dots, u_n)) \\ &= (\Phi(g))(u_1, \dots, u_n) = 0. \end{aligned}$$

Zatem Φ jest monomorfizmem oraz $\text{Im } \Phi = K[s_1, \dots, s_n]$. Stąd Φ indukuje izomorfizm $\Phi: K(t_1, \dots, t_n) \simeq K(s_1, \dots, s_n)$.

Zauważmy, że

$$\begin{aligned} \Phi(p_n) &= x^n - s_1 \cdot x^{n-1} + \dots + (-1)^{n-1} \cdot s_{n-1} \cdot x + (-1)^n \cdot s_n \\ &= (x - x_1) \cdots (x - x_n). \end{aligned}$$

W szczególności, ciało $K(x_1, \dots, x_n)$ jest ciałem rozkładu wielomianu $\Phi(p_n)$ nad ciałem $K(s_1, \dots, s_n)$. Twierdzenie 3.7 implikuje zatem, że

$$\text{Aut}_{K(t_1, \dots, t_n)} F \simeq \text{Aut}_{K(s_1, \dots, s_n)} K(x_1, \dots, x_n).$$

Ponieważ $K(s_1, \dots, s_n)$ jest ciałem symetrycznych funkcji wymiernych na mocy Stwierdzenia C.3, więc z Lematu C.1 wynika, że $\text{Aut}_{K(t_1, \dots, t_n)} F \simeq \mathfrak{S}_n$. Z Wniosku 9.5 wiemy, że jeśli równanie $p_n(x) = 0$ jest rozwiązywalne przez pierwiastniki, to grupa $\text{Aut}_{K(t_1, \dots, t_n)} F$ jest rozwiązalna. Ponieważ grupa $\mathfrak{S}_n$ jest rozwiązalna wtedy i tylko wtedy, gdy $n \leq 4$, więc otrzymujemy tezę. $\square$