ELEMENTY TEORII GALOIS

ROBERT RAŁOWSKI

Spis treści

1. Zamiast wstępu 2
2. Elementy teorii grup 3
3. Teoria ciał w skrócie 15
4. Rozszerzenia Galois 26
5. Twierdzenia Galois 34
6. Rozszerzenia pierwiastnikowe 37
7. Grupy rozwiązalne oraz przykłady rozszerzeń, które nie są pierwiastnikowe 40
Literatura 42
Appendix A. Zasadnicze twierdzenie algebry 43
Appendix B. Twierdzenie o algebraicznym domknięciu ciała 46
Appendix C. Kryterium Eisensteina 47
Appendix D. Twierdzenie o wielomianie pierwotnym 47
Appendix E. Liniowa niezależność automorfizmów 48

Date: **Wersja z dnia:** 8 4 2023 roku.

1. Zamiast wstępu

Skrypt ten jest poświęcony teorii, której podstawy dał wybitny francuski matematyk Evariste Galois. Teoria ta jest poświęcona zagadnieniom związanych z istnieniem rozwiązań równań wielomianowych jednej zmiennej. Jak powszechnie wiadomo, znane są wzory na pierwiastki wiolomianów pierwszego i drugiego stopnia. Ponadto, w XVI wieku, Tartaglia i Cardano podali wzory na pierwiastki wielomianu trzeciego i czwartego stopnia. Historia odkrycia tych wzorów jest nico zawiła patrz [4]. Mianowicie, włoski matematyk Ferro odkrył wzór na pierwiastki dowolnego wielomianu trzeciego stopnia ale ich nie ujawnił. Niezależnie od Ferro ale nieco później, Cardano również znalazł formułe na pierwiastki wielomianu trzeciego stopnia. Również i Tartaglia nie chciał ujawnić tych wzorów ale Cardano wydobył od Tartaglii te wzory ale pod warunkiem, że Cardano utrzyma je w tajemnicy. W tym czasie, asystent Cardano Ferrari znalazł redukcję wielomianów czwartego topnia do wielomianów sześciennych i oznajmił to Cardano. Cardano i Ferrari spotkali się z zięciem Ferro, który poinformował ich, że to Ferro jest odkrywcą wzorów na pierwiastki wielomianów trzeciego stopnia. W tym momecie, Cardano był zwolniony z przyięgi danej Tartaglii i opublikował wzory na pierwiastki trzeciego i czwartego stopnia. Ogólne wzory na pierwiastki równania wyższych stopni przez około trzy stulecia nadal nie były znane. Pierwszym matematykiem, który udowodnił że analogicznych wzorów do formuł na pierwiastki wielomianów niższych stopni od pięciu nie można podać był Ruffini. Jego dowód zawierał luke, którą się dało usunąć. Abel podał w pełni zadawalający dowód, że nie ma ogólnych wzorów na pierwiastki wielomianów stopnia wyższego niż cztery, które wrażane są przez działania arytmetyczne i pierwiastkowanie (rozwiązania przez pierwiastniki). Jednak to Galois podał warunki konieczne i dostateczne aby wzory na pierwiastki dowolnego wielomianu wyrażały się przez pierwiastniki.

2. Elementy teorii grup

Teria grup odgrywa fundamentalną rolę w całej matematyce i opisuje symetrie w rozważanych objektach matematycznych. Przykładem takich objektów są naprzykład figury na płaszczyźnie, czy też wielosciany w euklidesowych przestrzeniach. Jednak pierwszymi objektami dla których rozważano grupy symetrri były właśnie równania algebraiczne a w szczególności równania wiolomianowe o jednej zmiennej. Pojęcie grupa w tym znaczeniu właśnie pochodzi od Evarysta Galois. Teoria grup jest jak wszystkie teorie matematyczne teorią aksjomatyczną, tak więc podamy aksjomaty tej teorii.

Definicja 2.1 (Grupa)**.** *Powiemy, że $(G, \cdot, e)$ jest grupą, jeżeli G jest niepustym zbiorem do którego należy e. Natomiast $\cdot$ jest dwuargumentowym działaniem na G (t.zn. $\cdot : G \times G \to G$ jest funkcją), spełniającym własności:*

1. $(\forall x, y, z \in G)\ ((x \cdot y) \cdot z = x \cdot (y \cdot z))$, *łączność działania* $\cdot$,
2. $(\forall x \in G)\ (x \cdot e = x = e \cdot x)$, *$e$ jest elementem neutralnym działania* $\cdot$,
3. $(\forall x \in G)(\exists y \in G)\ (x \cdot y = e = y \cdot x)$.

Jeżeli grupa $(G, \cdot)$ spełnia dodadkowo warunek przemienności $(\forall x, y \in G); x \cdot y = y \cdot x$, to grupę tę nazywamy grupą abelową albo przemienną. Tutaj wspomnijmy, że $\cdot$ jest funkccją, więc formalnie powinniśmy pisać $\cdot(x, y) = z$, czy nawet tak $((x, y), z) \in \cdot$, zamiast $x \cdot y = z$. Niemniej, klasyczna notacja jest o wiele bardziej czytelna niż wspomniana przed chwilą formalna. Najprosztszą grupą jest grupa składająca się z jednego elementu $G = \{e\}$, tutaj mamy $e \cdot e = e$. Łatwo sprawdzić, że $(\{e\}, \cdot)$ spełnia wszystkie aksjomaty grupy (nawet abelowej). Często będziemy pomijać znak działania $\cdot$ i zamiast $x \cdot y$ pisać będziemy xy dla dowolnych $x, y \in G$. Nim przejdziemy do następnych przykładów odnotujemy prosty ale użyteczny fakt.

Fakt 2.1. *Niech $(G, \cdot)$ będzie grupą, to wtedy:*

1. *istnieje dokkładnie jeden element neutralny,*
2. *dla dowolnego $x \in G$ istniej dokładnie jeden element $y \in G$, taki że $x \cdot y = e = y \cdot x$, taki element oznaczamy przez x^{-1},*
3. *dla dowolnego $x, y \in G$ zachodzą $(xy)^{-1} = y^{-1}x^{-1}$ oraz $(x^{-1})^{-1} = x$,*
4. *zachodzi prawo skracania, tzn. dla dowolnych $x, y, y' \in G$, jeżeli $x \cdot y = x \cdot y'$, to $y = y'$, podobnie zachodzi implikacja jeśli $y \cdot x = y' \cdot x$.*

Dowód. *Załóżmy, że są dwa elementy neutralne $e_1, e_2 \in G$, to wtedy $e_1 = e_1 \cdot e_2 = e_2$. By udowodnić drugą własność, zauważmy że jeśli $xy = eyx$ i $xy' = e = y'x$, to wtedy korzystając z prawa łączności działania $\cdot$, mamy*

$$y = ey = (y'x)y = y'(xy) = y'e = y'.$$

Kolejną własność dowodzimy następująco: $(xy)(xy)^{-1} = e = (xy)^{-1}(xy)$, z drugiej strony mamy

$$(xy)(y^{-1}x^{-1}) = x(y(y^{-1}x^{-1})) = x((yy^{-1})x^{-1}) = x(ex^{-1}) = xx^{-1} = e.$$

Więc $y^{-1}x^{-1}$ jest również elementem odwrotnym do xy, więc z jedyności elementu odwrotnego mamy żądaną równość $(xy)^{-1} = y^{-1}x^{-1}$. Udowodnimy prawo skracania, gdy x stoi

po prawej stronie iloczynu. Podobnie dowodzi się w drugim przypadku. Niech $xy = xy'$, to wtedy

$$y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}(xy') = (x^{-1}x)y' = ey' = y'.$$

■

Działanie $\cdot$ grupy o niewielu elementach możemy zapisywać w postaci tabelki. Tak więc wypiszemy tutaj przykłady grup $C_1 = (\{e\}, \cdot)$, $C_2 = (\{e, a\}, \cdot)$, $C_3 = (\{e, a, b\}, \cdot)$:

$\cdot$	e
e	e

$\cdot$	e	a
e	e	a
a	a	e

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Na mocy prawa skreśleń w grupie, w każdej kolumnie i każdym wierszu takiej tabelki nie powtarzają się żadne elemnty. Tak więc nie musimy wykonywać n^2 działań w grupie n-elementowej. Zauważmy, że innych tabelek dla tych grup z dokładnością do zamiany symboli e, a, b nie możemy napisać, to zostawiamy czytelnikowi. Natomiast w przypadku grup o czterech elementach $\{e, a, b, c\}$, możemy stworzyć zasadniczo różne dwa działania (co też zostawimy czytelnikowi), natomisat dla grupy 5-cio elementowej istotne działanie grupowe jest jedno:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$\cdot$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

Wszystkie wypisane powyżej tabelki są symetryczne względem diagonali, więc nasze grupy są abelowe. Sytuacja się zmienia w przypadku gdy grupa ma 6 elementów. Wtedy istnieje nieprzemienne działanie w tej grupie. Przykładem takiej grupy jest tzw. grupa S_3 tj. grupa wszystkich możliwych przestawień zbioru 3 elementowego $\{1, 2, 3\}$. Ta grupa jest również grupą izometrii trójkąta równobocznego o wierzchołkachs ponumerowanych zbiorem $\{1, 2, 3\}$. Działaniem w tej grupie jest składanie przestawień (zwanych też permutacji). Dowolna permutację $\sigma \in S_3$ możemy zapisać następująco:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \sigma_1 & \sigma_2 & \sigma_3 \end{pmatrix},$$

natomiast składanie zapiszemy tak:

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \sigma(\tau(3)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \sigma_{\tau_1} & \sigma_{\tau_2} & \sigma_{\tau_3} \end{pmatrix}.$$

Tak więc, jeśli $\{a, b, c\} = \{1, 2, 3\}$, to definiujemy przestawienia w sposób następujący:

$$e = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 2\ 3 \end{pmatrix}, \quad \tau_1 = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix},$$

$$\sigma_1 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix}.$$

Obliczmy dla przykładu $\tau_1 \cdot \sigma_2$:

$$\tau_1\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \tau_3.$$

Dalej mamy:

$$\sigma_1 \cdot \tau_1 = \tau_3,\ \tau_1 \cdot \sigma_1 = \tau_2,\ \sigma_2 \cdot \tau_1 = \tau_2,\ \tau_1 \cdot \tau_2 = \sigma_1,\ \tau_2 \cdot \tau_1 = \sigma_2.$$

Zauważmy, że $\sigma_2 = \sigma_1 \cdot \sigma_1 = \sigma_1^2$, $\sigma_1\sigma_2 = \sigma_1\sigma_1^2 = \sigma_1^3 = e$, $\tau_i^2 = e$ dla $i \in \{1, 2, 3\}$. Postępując podobnie z pozostałymi parami oraz korzystając z prawa skracania, otrzymujemy następującą tabelkę:

$\cdot$	e	σ_1	σ_2	τ_1	τ_2	τ_3
e	e	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	e	τ_3	τ_1	τ_2
σ_2	σ_2	e	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	e	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	e	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	e

Ogólnie, dla dowolnego niepustego zbioru X, para $(Sym(X), \circ)$ stanowi grupę symetryczną zbioru X. Tutaj $Sym(X) = \{f \in X^X :\ f \text{ jest bijekcją na } X\}$, natomiast $\circ$ jest superpozycją dowolnych funkcji $f, g \in Sym(X)$, tzn. $f \circ g$ jest zdefiniowane następująco:

$$(\forall x \in X)\ (f \circ g(x) = f(g(x))\ ).$$

Oczywiście trzeba sprawdzić, że $f \circ g$ jest funkcją na zbiorze X o wartościach w X, która jest "na" i różnowartociowa. Tutaj dle dowolnego $f \in Sym(X)$ definiujemy funkcję g następująco:

$$(\forall x, y \in X)\ g(x) = y \longleftrightarrow f(y) = x.$$

Łatwo sprawdzić, że $g \in Sym(X)$ jest funkcją odwrotną do f, tzn. dla dowolnego $x \in X$ mamy $f \circ (x) = x$ oraz $g \circ f(x) = x$. Funkcja $e(x) = x$ dla dowolnego $x \in X$ jest elementem neutralnym w $(Sym(X), \cdot)$. Szczegóły pozostawiamy czytelnikowi.

Jeżeli $n \in \mathbb{N}$ jest dodatnią liczbą naturalna, to wtedy definiujemy $S_n = Sym(\{1, \ldots, n\})$ i grupę tę nazywamy grupą permutacji zbioru $\{1, \ldots, n\}$. Grupa S_n jest $n!$ elementowa. We wcześniejszym przypadku dowolny element grupy s_3 był definiowany na $\{1, 2, 3\}$ w ten sposób, że określone było na co przechodzi 1, 2 czy 3. Na przykład $\tau_2(1, 2, 3) = (3, 2, 1)$. oznacz że $\tau_2(1) = 3$, $\tau_2(2) = 2$ oraz $\tau_2(3) = 1$. Element τ_2 możemy zapisać też tak

$$\tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Ogólnie $\sigma \in S_n$ zapiszemy tak:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma_1 & \sigma_2 & \ldots & \sigma_n \end{pmatrix},$$

gdzie $\sigma_i = \sigma(i)$ dla dowolnego $i \in \{1, \ldots, n\}$. Wtedy składanie dwóch permutacji $\sigma, \tau \in S_n$ zapiszemy następująco:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma_{\tau_1} \sigma_{\tau 2} \ldots \sigma_{\tau_n} \end{pmatrix}.$$

Na przykład

$$\begin{pmatrix} 1\,2\,3\,4 \\ 4\,2\,3\,1 \end{pmatrix} \circ \begin{pmatrix} 1\,2\,3\,4 \\ 3\,1\,2\,4 \end{pmatrix} = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,4\,2\,1 \end{pmatrix}.$$

Obliczmy teraz element odwrotny zo zadanej permutacji:

$$\begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}^{-1} = \begin{pmatrix} 1\,2\,3\,4 \\ 4\,3\,2\,1 \end{pmatrix}$$

Dla ustalonej permutacji σ_n, w zbiorze $[n] := \{1, \ldots, n\}$ zdefiniujemy relację w sposób

$$(\forall i, j \in [n])\ i \sim j \longleftrightarrow (\exists k \in \mathbb{Z})\ \sigma^k(i) = j.$$

Przekonujemy sie, że nasza relacja jest relacją równoważności (tzn. jest zwrotna, symetryczna i przechodnia). W takim razie klasy abstrakcji stanowią rodzinę niepustych posdziorów $[n]$ parami rozłącznych, której suma jest całym zbiorem $[n]$. Tutaj klasami jest rodzina $\{[i]_\sim : i \in [n]\} \subset P([n])$ oraz $[i]_\sim = \{j \in [n] :\ i \sim j\}$. Zbiór klas abstrakcji relacji $\sim$ dla zadanej permutacji σ oznaczymy przez $\sigma/_\sim$.

Niech $\sigma \in S_n$ będzie ustaloną permutacją. Ponieważ relacja $\sim$ jest relacją równoważności, to cykle które są klasami abstrakcji $\sim$ są rozłączne oraz dla dowolnych i, j takich że $i \in [j]_\sim$ mamy $\sigma(i) \in [j]_\sim$. Dla dowolnego $u \in \sigma/_\sim$ zdefiniujemy permutację cykliczną $c_u \in S_n$ w sposób następujący:

$$c_u(i) = \begin{cases} \sigma(i) & i \in u \\ i & i \in [n] \setminus u. \end{cases}$$

Niech $u, v \in \sigma/_\sim$ będą dwoma cyklami, to ponieważ $u \cap v = \emptyset$ i $\sigma[u] = u = c_u[u]$ i $\sigma[v] = v = c_v[v]$ i definicji c_u, c_v mamy przemienność permutacji cyklicznych $c_u c_v = c_v c_u$. Permutację σ możemy zapisać jako iloczyn permutacji cyklicznych $\prod_{u \in \sigma/_\sim} c_u$.

Przyklad 2.1. *Rozważmy nastepującą permutację zbioru 7-mio elementowego* $\sigma = \left(\begin{smallmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 4\,5\,6\,1\,2\,7\,3 \end{smallmatrix}\right)$. *Wówczas zbiór klas abstrakcji naszej relacji jest następujący: dla dowolnego* $i \in [n]$ *mamy*

$$P([7])/_\sim = \{[i]_\sim : i \in [7]\} = \{\{1, 4\}, \{2, 5\}, \{3, 6, 7\}\}.$$

Poszczególne klasy w tej relacji nazywamy cyklami w permutacji σ*, tutaj mamy* $i \to \sigma(i) = 4 \to \sigma(4) = 1$*, więc jest to cykl* $(1, 4)$*,* $2 \to \sigma(2) = 5 \to \sigma(5) = 2$*, co jest cyklem* $(2, 5)$ *i wreszcie* $3 \to \sigma(3) = 6 \to \sigma(6) = 7 \to \sigma(7) = 3$*, więc mamy do czynienia z cyklem* $(3, 6, 7)$*. W zapisie konkretnego cyklu, pominiemy przecinki. Wtedy, nasza permutacja rozbija się na następujące cykle:* $\sigma = (1\ 4)\ (2\ 5)\ (3\ 6\ 7)$.

Standardowymi przykładami grup przemiennych są $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $\mathbb{C} \setminus \{0\}, \cdot)$. Ponadto grupa reszt modulo $n \in \mathbb{N} \setminus \{0\|\}$ $(\mathbb{Z}_{st(f)}, +_n)$, gdzie $\mathbb{Z}_n$ jest postaci $\{0, 1, \ldots, n-1\}$ oraz $+_n$ jest dodawaniem modulo n, które jest resztą z dzielenia przez n sumy dwóch liczb całkowitych ze zbioru $\mathbb{Z}_n$. Grupa $(C_n, \cdot)$ wszystkich

pierwiastków zespolonych z jedności stopnia n jest również grupą abelową. Natomiast grupa $(GL(n), \cdot)$ odwracalnych macierzy kwadratowych stopnia n z mnożeniem macierzowym jest grupą nieprzemienną o ile $n > 1$.

Rzędem skończonej grupy G jest mocą G, tzn. $rank(G) = |G|$.

Mając zadaną grupę, możemy się zapytać o istnienie w niej zawartych innych grup. W takim razie podamy pojecie podgrup danej grupy.

Definicja 2.2 (Podgrupa)**.** *Niech $(G, \cdot)$ będzie grupą i $H \subseteq G$ będzie jej niepustym podzbiorem, Powiemy, że H jest podgrupą grupy G, co zapiszemy jako $H \leq G$, jeżeli $(H, \cdot \restriction_{(H\times H)})$ jest grupą.*[1]

Podamy, warunek konieczny i dostateczny na to aby niepusty $H \subseteq G$ był podgrupą grupy G.

Twierdzenie 2.1. *Niech $(G, \cdot)$ będzie grupą i $\emptyset \neq H \subseteq G$, to wtedy następujące trzy warunki są równoważne:*

(1) $H \leq G$,
(2) $(\forall x, y \in H)\ (xy^{-1} \in H)$,
(3) $(\forall x \in H)(x^{-1} \in H) \wedge (\forall x, y \in H)\ (xy \in H)$.

Dowód. *Zauważmy, że dla dowolnych $x, y \in H$ mamy równość $x\cdot \restriction_{H\times H} y = x \cdot y$. Tak więc z (1) wynika (2) i (3). Czytelnik sprawdzi, że (2) i (3) są równoważne. Pokażemy, że z (3) wynika (1). Niech $x, y, z \in H$, to wtedy $x\cdot \restriction_{H\times H} y = x \cdot y \in H$. Wiemy, że $z \in H$, to wtedy $(x\cdot \restriction_{(H\times H)} y)\cdot \restriction_{(H\times H)} z = (x \cdot y) \cdot z = x \cdot (y \cdot z)$. Ponieważ $y, z \in H$, to wtedy z 3 mamy $yz \in H$ więc $x(yz) \in H$. Stąd*

$$(x\cdot \restriction_{H\times H})\cdot \restriction_{(H\times H)} z = (x \cdot y) \cdot z = x \cdot (y \cdot z) = x\cdot \restriction_{(H\times H)} (y \cdot z) = x\cdot \restriction_{(H\times H)} (y\cdot \restriction_{(H\times H)} z).$$

Łączność w $(H, \cdot \restriction_{(H\times H)})$ została więc wykazana. Ponieważ H jest niepusty, to jest x taki że $x \in H$. Wtedy $x^{-1} \in H$ a więc $e = x \cdot x^{-1} \in H$. Ze względu na uwagę, że dla dowolnych $u, v \in H$ mamy $u\cdot \restriction_{(H\times H)} v = u \cdot v$, widzimy że dla dowolnego $y \in H$ mamy $y\cdot \restriction_{(H\times H)} e = y \cdot e = y = e \cdot y = e\cdot \restriction_{(H\times H)} y$. Pozostał więc do udowodnienia ostatni aksjomat grupy. Niech $x \in H$, to z (3) mamy pewien $y \in G$, taki że $y = x^{-1} \in H$. Oczywiście $y \in H$. Jeszcze raz korzystając z powyższej uwagi mamy:

$$x \cdot \restriction_{(H\times H)} y = x \cdot y = x \cdot x^{-1} = e = x^{-1} \cdot x = y \cdot x = y \cdot \restriction_{(H\times H)} x.$$

Dowód implikacji (3) $\rightarrow$ (1) został zakończony. ■

Przyklad 2.2. *Wyznaczmy wszystkie podgrupy grupy permutacji S_3. Są to*

$$\{e\},\ S_3, \{e, \tau_1\}, \{e, \tau_2\}, \{e, \tau_3\} \text{ oraz grupa } \{e, \sigma_1, \sigma_2\}.$$

Widzimy, że rzędy podgrup grupy S_3 są w zbiorze $\{1, 2, 3, 6\}$.

Jak się okazuje, to dla dowolnej grupy skończonego rzędu G, rzędy jej podgrup są dzielnikami $rank(G)$. W tym celu wprowadzimy pojęcie warstwy elementu grupy G względem jej podgrupy $H \leq G$.

[1] Jeżeli $f : X \rightarrow Y$ jest funkcją i $A \subseteq X$, to wtedy $f \restriction A = \{(x, y) \in f :\ x \in A\}$.

Definicja 2.3 (Warstwa w grupie)**.** *Niech $(G,\cdot)$ będzie ustaloną grupą i $H \leq G$ będzie jej podgrupą. Niech $a \in G$, to definiujemy warstwę lewostronną elementu a następująco $aH = \{a\cdot h :\ h \in H\}$. Analogicznie definiujemy warstwę prawostronną eleemntu $a \in G$ jako $Ha = \{ha :\ h \in H\}$. Zbiór warstw lewostronnych oznaczamy przez G/H_l a prawostronnych przez G/H_R. Jeżeli będzie jasne że mamy do czynienia z wastwami lewostronnyi, to będziemy pisać prościej, mianowicie $P(G)/H$. Powyższy zbiór nazywamy też przestrzenią warstw (lewo albo prawostronnych) względem grupy H. Jeśli $H = \{e\}$ w grupie G, to wtedy*

$$G/H_L = \{aH :\ a \in G\} = \{\{a \cdot h : h \in H\} : a \in G\} = \{\{a\} : a \in G\} = \ldots = P(G)/H_R.$$

Każdej warstwie lewostronnej można w jednoznaczny sposób określić warstwę prawostronną. Mianowicie prawdziwy jest następujący Fakt.

Fakt 2.2. *Niech $(G,\cdot)$ będzie grupą i H jej podgrupą. Wtedy istnieje bijekcja*

$$G/H_L \ni aH \mapsto F(aH) = Ha \in G/H_R.$$

Dowód. *Niech $F(aH) = F(bH)$, to wtedy $Ha = Hb$. Stąd $b \in Hb = Ha$ a więc dla pewnego $h \in H$ zachodzi $b = ha$* ■

Wprowadźmy relację w grupię G w sposób następujący: niech $H \leq G$, to wtedy

$$(\forall x, y \in G)\ x \sim_H y \longleftrightarrow x^{-1} \cdot y \in H.$$

Oczywiście relacja ta jest zwrotna: dla dowolnego $x \in G$ mamy $x^{-1} \cdot x = e \in H$,, więc $x \sim_H x$. Symetrię sprawdzamy następująco: niech $x \sim_H y$, to wtedy $x^{-1}y \in H$, stąd mamy $H \ni (x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x$ więc $y \sim_H x$. Pozostała przechodniość: niech $x \sim_H y$ i $y \sim_H z$, wtedy $x^{-1}y \in H$ oraz $y^{-1}z \in H$. Wtedy $H \ni (x^{-1}y)\cdot(y^{-1}z) = x^{-1}(yy^{-1})z = x^{-1}z$, więc $x \sim_H z$. Pokażamy równość pomiędzy klasami abstrakcji relacji $\sim_H$ a warstwami lewostronnymi: dla dowolnego $a \in G$ mamy

$$\begin{aligned}[a]_{\sim_H} =& \{y \in G :\ a \sim_H y\} = \{y \in G :\ a^{-1}y \in H\} = \{y \in G :\ (\exists h \in H) a^{-1}y = h\} \\ =& \{y \in G :\ (\exists h \in H) y = ah\} = aH.\end{aligned}$$

Ponieważ nasza relacja $\sim_H$ jest relacją równoważności na grupie G. Więc każde dwie różne klasy abstrakcji tej relacji są rozłączne i niepuste, Co więcej ich suma mnogościowa jest równa całej grupie G. ?ja zauważylismy wcześniej, każda klasa jest warstwą lewostronną i na odwrót. Więc

$$G = \bigcup_{\sigma \in G/\sim_H} \sigma = \bigcup_{\sigma \in G/H} \sigma,$$

zauważmy, że dla dowolnych $a, b \in G$ mamy $|aH = |bH|$ oraz $eH = H$. Stąd, dla skończonej grupy G mamy

$$rank(G) = |G| = |\bigcup_{\sigma \in G/H} \sigma| = \sum_{\sigma \in G/H} |\sigma| = \sum_{\sigma \in G/H} |H| = |H| \cdot |G/H|.$$

Indeksem grupy G względem jej podgrupy nazywamy moc przestrzeni ilorazowej G/H i oznaczamy przez $[G : H]$. Wprost z definicji indeksu i poprzedniego paragrafu mamy twierdzenie Lagrange'a.

Twierdzenie 2.2 (Lagrange'a)**.** *Jeżeli grupa G jest skończonego rzędu i H jest podgrupą grupy G, to wtedy*

$$rank(G) = [G : H] \cdot rank(H).$$

Wnosimy stąd, że rząd dowolnej podgrupy grupy skończonej jest dzielnikiem rzędu grupy. Nasuwa się pytanie, czy w przestrzeni ilorazowej G/H można wrpowadzić działanie grupowe w sposób naturalny: mając warstwy lewostronne $aH, b, H \in G/H$ definiujemy warstwę $(ab)H$. Oczywiście należy sprawdzić, czy w ten sposób określone działanie nie zależy od wyboru reprezentantów. To znaczy, mając dowolne $a' \in aH$ i $b' \in bH$, czy zachodzi równość $(a'b')H = (ab)H$.

Kluczowym pojęciem, dzięki któremu powyżej określone działanie jest poprawnie zdefiniowane jest podgrupa normalna, inaczej zwana dzielnikiem normalnym.

Definicja 2.4 (Dzielnik normalny)**.** *Niech $(G, \cdot)$ będzie grupą i $H \leq G$ będzie jej podgrupą. Powiemy, że H jest podgrupą normalną (czy też dzielnikiem normalnym) grupy G jeżeli*

$$(\forall a \in G)\ \ aH = Ha.$$

Warunek na bycie podgrupą normalną grupy G oznaczamy przez $H \trianglelefteq G$.

Zobaczymy, jak przedstawia się sytuacja w przypadku grupy S_3 i jej podgrupy $H = \{e, \tau_1\}$. Wyznaczmy wpierw przestrzeń ilorazową G/H_L. Mianowicie, na mocy twierdzenia Lagrange'a indeks $[G : H]$ jest równy 3 (więc są trzy warstwy): H, $\tau_2 H = \{\tau_2, \tau_2\tau_1\} = \{\tau_2, \sigma_2\}$, oraz $\sigma_1 H = \{\sigma_1, \sigma_{\tau 2}\tau_1\} = \{\sigma_1, \tau_3\}$. Więc $G/H_L = \{\{e, \tau_1\}, \{\tau_2, \sigma_2\}, \{\sigma_1, \tau_3\}\}$. Teraz zbadamy warunek na bycie grupą normalną, Oczywiście $eH = H = He$, dalej $\tau_1 H = H = H\tau_1$. Jednak, jak już wiemy $\tau_2 H = \{\tau_2, \sigma_2\}$ ale $H\tau_2 = \{\tau_2, \tau_1\tau_2\} = \{\tau_2, \sigma_1\}$, więc nie zachodzi równość $\tau_2 H = H\tau_2$. Wnosimy więc, że H nie jest podgrupą normalną grupy S_3.

Podamy warunek konieczny i dostateczny na bycie podgrupą normalną w G.

Twierdzenie 2.3. *Niech $H \leq G$ będzie podgrupą grupy $(G, \cdot)$. Następujące warunki są równoważne:*

(1) $H \trianglelefteq G$,
(2) $(\forall a \in G)\ (a^{-1}Ha \subseteq H)$,
(3) $(\forall a \in G)\ (aHa^{-1} \subseteq H)$.

Dowód. *Załóżmy* (1)*. wtedy dla dowolnego $b \in G$ mamy $bH = Hb$. Niech $a \in G$ i $x \in a^{-1}Ha$ będą dowolnie wybranymi elementami, to wtedy jest $h \in H$ takie, że $x = a^{-1}ha$. Wtedy $a^{-1}h \in a^{-1}H = Ha^{-1}$, to wtedy dla pewnego $h' \in H$ $a^{-1}h = h'a^{-1}$ i wtedy $x = a^{-1}ha = h'a^{-1}a = h'e = h' \in H$. Wobec dowolności a i x mamy* (2)*. Teaz zajmiemy się implikacją w drugą stronę. Zakładamy, że dla dowolnego $b \in G$ zachodzi $b^{-1}Hb \subseteq H$. Niech $a \in G$ i $x \in aH$ będą dowolne. Wtedy jest $h \in H$ takie że $x = ah = aha^{-1}a$. Biorąc $b = a^{-1}$ mamy $aha^{-1} = b^{-1}hb \in b^{-1}Hb \subseteq H$ a stąd dla pewnego $h \in H$ mamy $aha^{-1} = h'$. Więc $x = h'a \in Ha$. Ponieważ x było dowolnie wybrane, to mamy $aH \subseteq Ha$. Teraz niech $x \in Ha$, to $x = ha$ dla jakiegoś $h \in H$. Więc $x = aa^{-1}ha$. Ponieważ mamy $a^{-1}ha \in a^{-1}Ha \subseteq H$, to dla pewnego $h' \in H$ mamy równość $a^{-1}ha = h'$ a stąd $x = aa^{-1}h = ah' \in aH$. Wobec*

dowolności wyboru x mamy $Ha \subseteq aH$. Tak więc dla dowolnego $a \in G$ mamy $aH = Ha$, co należało dowieść. Czytelnik bez trudu sprawdzi równoważność (2) *z* (3). ■

W teorii grup jednym z głównych celów jest klasyfikacja grup istotnie różnych. Dwie grupy nie są istotnie rózne, jeśli mają identyczne własności algebraiczne i ich różnica polega na innych nazwach danym elementom tych grup. Ta zmiana nazwy przy zachowaniu własności algebraicznych obydwu grup prowadzi do pojęcia izomorfizmu

Definicja 2.5 (Izomorfizm grup)**.** *Niech będą dwie grupy $(G, \cdot)$ oraz $(H, \bullet)$), to powiemy że funkcja $f : G \to H$ jest izomorfizmem pomiędzy grupami, jeżeli*

(1) *f jest bijekcją,*
(2) $(\forall x, y \in G)\ (f(x \cdot y) = f(x) \bullet f(y))$.

Jeżeli taki izomorfizm istnieje pomiędzy grupami, to one są wtedy izomorficzne. Piszemy wtedy $(G, \cdot) \cong (H, \bullet)$, lub prościej $G \cong H$.

. Relacja binarna $\cong$ jest relacją równoważności w klasie wszystkich grup. Oczywiście identyczność na zadanej grupie G jest izomorfizmem z z nią samą. NIech f będzie izomorfizmem pomiędzy G i H. Pokażemy, że $g = f^{-1}$ ustala izomorfizm pomiedzy H i G. Niech $u, v \in H$, to wtedy są $x, y \in G$, takie że $u = f(x)$ i $v = f(y)$. Wtedy oczywiście $g(u) = x$ i $g(v) = y$. Wtedy

$$g(u \bullet v) = g(f(x) \bullet f(y)) = g(f(x \cdot y)) = x \cdot y = g(u) \cdot g(v).$$

Przechodniość relacji $\cong$ jest równie łatwa do udowodnienia jak zwrotność, czy symetria.

Niech f, g będą izomorfizmami pomiedzy grupami G, H, F, takimi że $f : G \to H$ i $g : H \to F$. Niech $x, y \in G$ będą dowolne w G. Tuaj działanie w grupie F oznaczamy przez $\diamond$. Wtedy

$$(g \circ f)(x \cdot y) = g(f(x \cdot y)) = g(f(x) \bullet f(y)) = g(f(x)) \diamond g(f(y)) = x \diamond y.$$

Oczywiście złożenie bijejkcji jest bijekcją. Pokazaliśmy więc, że $g \circ f : G \to F$ jest izomorfizmem pomiędzy G a F. Tak więc klasą abstrakcji relacji $\cong$ jest klasa wszystkich grup parami izomorficznych.

Grupy $(\mathbb{Z}_n, +_n)$, $(C_n, \cdot)$ są izomorficzne:

$$\mathbb{Z}_n \ni k \mapsto f(k) = e^{ik/2\pi n} \in C_n$$

Oczywiście funkcja jest "na" i $\mathbb{Z}_n$ i C_n sa równoliczne, więc f też jest różnowartościowa. Pokażemy, że f zachowuje działanie. Niech $x, y \in \mathbb{Z}_n$, wtedy dla pewnego $q \in \mathbb{Z}$ zachodzi $x + y = qn + (x +_n y)$ a stąd

$$\begin{aligned} f(x +_n y) =& e^{2\pi i(x+_n y)/n} = e^{2\pi i(x+y-nq)/n} = e^{2\pi i(x+y)/n - 2\pi q} \\ =& e^{2\pi(x+y)/n} = e^{2\pi x/n} \cdot e^{2\pi i y/n} = f(x) \cdot f(y). \end{aligned}$$

Szczególnym przypadkiem izomorfizmu jest automorfizm grupy, tzn. taka funkcja $f : G \to G$, że f jest izomorfizmem. Dla zadanej grupy $(G, \cdot)$ przez $Aut(G)$ oznaczymy zbiór wszystkich automorfizmów drupy G. Zauważmy, że $(Aut(G), \circ)$ stanowi grupę, w której $\circ$ jest składaniem funkcji. Co więcej, mamy $Aut(G) \leq Sym(G)$. Trywialnym przykładem

automorfizmu grupy G jest identyczność $id(x) = x$ dla dowolnego $x \in G$. W poniższym przykładzie podamy całą rodzinę automorfizmów mocy równej rzędowi grupy G.

Przyklad 2.3 (Automorfizmy wewnętrzne)**.** *Niech $(G, \cdot)$ będzie ustaloną grupą, z każdym elementem $a \in G$ związemy autmomorfizm σ_a zwany automorfizmem wewnętrznym. Mianowicie, dla dowolnego $x \in G$ $\sigma_a(x) = axa^{-1}$. Pokażmy wpierw, że σ_a jest bijekcją na grupie G.. Niech $y \in G$ będzie dowolne, to kładąc $x = a^{-1}ya$ mamy*

$$\sigma_a(x) = axa^{-1} = a(a^{-1}ya)a^{-1} = (aa^{-1})y(aa^{-1}) = y.$$

Niech $x, y \in G$ będa takie, że $\sigma_a(x) = \sigma_a(y)$, to wtedy $axa^{-1} = aya^{-1}$ i korzystając z prawa skracania w G otrzymujemy $x = y$. Więc $\sigma_a : G \to G$ jest bijekcją dla dowolnie wybranego $a \in G$. Pozostało wykazać, że σ_a zachowuje działanie. W tym celu wybierzmy dowolne elementy $x, y \in G$, to wtedy

$$\sigma_a(xy) = a(xy)a^{-1} = a(x(a^{-1}a)y)a^{-1} = (axa^{-1})(aya^{-1}) = \sigma_a(x) \cdot \sigma_a(y).$$

Oznaczmy przez $Inn(G)$ zbiór wszystkich automorfizmów wewnętrznych. Pokażemy, że $Inn(G) \leq Aut(G)$. Niech $a, b \in G$ oraz $x \in G$ będą dowolne, to wtedy

$$\sigma_{ab}(x) = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = \sigma_a(bxb^{-1}) = \sigma_a(\sigma_b(x)) = (\sigma_a \circ \sigma_b)(x).$$

Wobec dowolności $x \in G$ mamy $\sigma_a \circ \sigma_b = \sigma(ab) \in Inn(G)$. Zauważmy, że $\sigma_a \circ \sigma_{a^{-1}} = id = \sigma_{a^{-1}} \circ \sigma_a$. Niech $x \in G$ będzie dowolne, to $\sigma_e(x) = exe^{-1} = exe = x = id(x)$, więc

$$\sigma_a \circ \sigma_{a^{-1}} = \sigma_{a \cdot a^{-1}} = \sigma_e = id = \sigma_e = \sigma_{a^{-1}a} = \sigma_{a^{-1}} \circ \sigma_a.$$

Wykazaliśmy więc, że $Inn(G)$ jest podgrupą grupy $Aut(G)$.

Wiemy już że izomorfizmy a w szczególności automorfizmy zachowują odpowiednie działania. Ogólnie, dla dowolych grup $(G, \cdot)$, $(H, \bullet)$ funkcja $f : G \to H$ jest homomorfizmem jeżeli f zachowuje działania tj.:

$$(\forall x, y \in G)(f(x \cdot y) = f(x) \bullet f(y)).$$

Jeżeli f jest "na", to f jest wtedy epimorfizmem pomiędzy grupami G i H, natomiast jeżeli f jest "1-1", to f nazywamy monomorfizmem pomiędzy G a H. Zauważmy że jeżeli $f : G \to H$ jest homomorfizmem, to $f(e_G) = f(e_G e_G) = f(e_G) \bullet f(e_G)$ a stąd $e_H = f(e_g)$. Dalej, dla dowolnego $x \in G$ mamy $f(x^{-1}) = (f(x))^{-1}$. Aby się o tym przekonać, zauważmy że

$$e_H = f(e_G) = f(xx^{-1}) = f(x) \bullet f(x^{-1}).$$

Podobnie mamy $e_H = f(x^{-1}) \bullet f(x)$, więc z jedyności elementu odwrotnego do $f(x)$ mamy $(f(x))^{-1} = f(x^{-1})$.

Zachodzi ważne twierdzenie Caley'a.

Twierdzenie 2.4 (Caley'a)**.** *Jeżeli $(G, \cdot)$ jest grupą, to istnieje monomorfizm $f : G \to Sym(G)$.*

Dowód. *Zdefiniujemy odwzorowanie $f : G \to Sym(G)$ w taki sposób, że dla dowolnego $a \in G$ $f(a)$ jest dane wzorem:*

$$(\forall x \in G)\ (f(a)(x) = a \cdot x).$$

Niech $a, b \in G$ będa takie, że $f(a) = f(b)$, wtedy $a = ae = f(a)(e) = f(b)(e) = be = b$, skąd wynika różnowartościowość f. Sprawdzimy teraz, że dla dowolnego $a \in G$ $f(a)$ jest bijekcją na G (tzn. $f(a) \in Sym(G)$). Niech $x, y \in G$ będa dowolne, to wtedy

$$f(a)(x) = f(a)(y) \longleftrightarrow ax = ay \to x = y.$$

Niech teraz $y \in G$ będzie dowolne, to kładąc $x = a^{-1}y$ mamy

$$f(a)(x) = ax = a(a^{-1}y) = (aa^{-1})y = ey = y.$$

Więc $f : G \to Sym(G)$ jest funkcją różnowartościową o wartościach w zbiorze $Sym(G)$ i dziedzinie równej grupie G. Sprawdzimy, że f zachowuje działania co wynika z łączności mnożenia w grupie G. Dla dowolnych $a, b \in G$ i dowolnego $x \in G$ mamy

$$f(ab)(x) = (ab)x = a(bx) = f(a)(bx) = f(a)(f(b)(x) = f(a) \circ f(b)(x).$$

Wobec dowolności wyboru $x \in G$ mamy $f(ab) = f(a) \circ f(b)$. Ponieważ $a, b \in G$ są dowolne, to f zachowuje działania. Stąd f jest monomorfizmem pomiędzy $(G, \cdot)$ a $(Sym(G), \circ)$. ■

Bezpośrednim wnioskiem z twierdzenia Caley'a jest fakt, że jeśli dla pwenej liczby naturalnej n $rank(G) = n$ to G ma izomorficzną kopię w grupie S_n.

Przydatne okaże się twierdzenie o homomorfiźmie pomiędzy grupami.

Twierdzenie 2.5 (O homomorfiźmie grup)**.** *Niech $f : G \to H$ będzie homomorfizmem, to wtedy*

1. $ker(f) := f^{-1}[\{e_H\}] = \{x \in G :\ f(x) = e_H\} \trianglelefteq G$,
2. $Im(f) := f[G] = \{f(x) \in H :\ x \in G\} \leq H$.
3. $Im(f) \cong G/ker(f)_L$ *i* $Im(f) \cong G/ker(f)_R$.

Dowód. *Niech $x, y \in ker(f)$, to wtedy $f(x \cdot y) = f(x) \bullet f(y) = e_H \bullet e_H = e_H$. Więc $x \cdot y \in ker(f)$. Dalej, dla dowolnego $x \in ker(f)$ mamy $e_H = f(e_G) = f(x \cdot x^{-1}) = f(x) \bullet f(x^{-1}) = e_H \bullet f(x^{-1}) = f(x^{-1})$. Więc $x^{-1} \in ker(f)$. co ostatecznie dowodzi, że $ker(f) \leq G$. Teraz pokażemy, że dla dowolnego $a \in G$ zachodzi $a \cdot ker(f)a^{-1} \subseteq ker(f)$. Z tej inkluzji dostaniemy tezę (1). Niech $y \in a \cdot ker(f) \cdot a^{-1}$, to jest $h \in ker(f)$ takie, że $y = a \cdot h \cdot a^{-1}$. Wtedy*

$$\begin{aligned} f(y) =& f(aha^{-1}) = f(a) \bullet f(h) \bullet f(a^{-1}) = f(a) \bullet e_H \bullet f(a^{-1}) \\ =& f(a) \bullet f(a^{-1}) = f(aa^{-1}) = f(e_G) = e_H, \end{aligned}$$

więc $y \in ker(f)$ (tutaj wykorzystaliśmy fakt, że $f(e_G) = e_H$).

Dowód (2) pozostawimy czytelnikowi. Przejdziemy do dowodu (3). Zdefiniujemy odwzorowanie $\kappa : G/H_L \to Im(f)$ w sposób następujący, dla dowolnej warstwy $aH \in G/H_L$ $\kappa(aH) = f(a) \in Im(f)$. Odwzorowanie to nie zależy od wyboru reprezentanta warstwy aH. By to pokazać, niech $b \in aH$, to wtedy $b = ah$ dla pewnego $h \in ker(f)$. Więc $f(b) = f(ah) = f(a) \bullet f(h) = f(a) \bullet e_H = f(a)$, oczywiście $aH = bH$ ponieważ $b \in aH \cap bH$. Stąd

κ nie zależy od wyboru reprezentanta danej warstwy. Odwzorowanie $\kappa : G/H_L \to Im(f)$ jest homomorfizmem: niech $a, b \in G$ dowolne, to

$$\kappa(aH \cdot bH) = \kappa((ab)H) = f(ab) = f(a) \bullet f(b) = \kappa(aH) \bullet \kappa(bH).$$

Aby pokazać, że κ jest "na", niech $y \in Im(f)$, to jest $x \in G$ takie że $y = f(x) = \kappa(xH)$. Różnowartościowość wykażemy następująco: niech $\kappa(aH) = \kappa(bH)$, gdzie $a, b \in G$. Wtedy $f(a) = f(b)$ a stąd

$$e_H = f(a)^{-1} \bullet f(b) = f(a^{-1}) \bullet f(b) = f(a^{-1}b).$$

Stąd $a^{-1}b \in ker(f)$, więc jest $h \in ker(f)$ takie że $a^{-1}b = h$ co daje nam $b = ah \in aH$. Widzimy, że $b \in aH \cap bH$, co daje nam żądaną równość $aH = bH$. Dowód faktu, że $G/ker(f)_R \cong Im(f)$ jest analogiczny. ■

Powyższe twierdzenie wykorzystamy na potrzeby grupy permutacji S_n.

Przyklad 2.4 (Znak permutacji)**.** *Każdy element $\sigma \in S_n$ jest przestawieniem elementów zbioru $\{1, \ldots, n\}$. W takim razie permutacja σ przestawia kolumny macierzy jednostkowej I w sposób następujący:*

$$[A_\sigma]_{ij} = \begin{cases} 1 & \sigma(j) = i \\ 0 & \sigma(j) \neq i. \end{cases}$$

Zdefiniujmy odwzorowanie $F : S_n \to GL_n$ w sposób następujący $F(\sigma) = A_\sigma$. Zbadamy, czy F jest homomorfizmem. Niech $\sigma, \tau \in S_n$, wtedy dla dowolnych $i, j \in [n] = \{1, \ldots, n\}$ zachodzi

$$[A_\sigma \cdot A_\tau]_{ij} = 1 \longleftrightarrow \sum_{k=1}^{n} [A_\sigma]_{ik}[A_\tau]_{kj} = 1 \longleftrightarrow [A_\sigma]_{i\tau(j)}[A_\tau]_{\tau(j)j} = 1 \longleftrightarrow [A_\sigma]_{i\tau(j)} = 1$$
$$\longleftrightarrow i = \sigma(\tau(j)) \longleftrightarrow \sigma\tau(j) = i \longleftrightarrow [A_{\sigma\eta}]_{ij} = 1$$

Druga równoważność zachodzi bo jeżeli $k \neq \sigma(j)$, to $[A_\tau]_{kj} = 0$. Podobnie, dla dowolonych $i, j \in [n]$ mamy $[A_\sigma \cdot A_\tau]_{ij} = 0 \longleftrightarrow [A_{\sigma\eta}]_{ij} = 0$. Zauważmy, ze dla transpozycji $\tau_{kl} = \binom{1\ldots k\ldots l\ldots n}{1\ldots l\ldots k\ldots n}$ mamy macierz $A_{\tau_{kl}}$:

$$[A_{\tau_{kl}}]_{ij} = \begin{cases} 1 & (i,j) = (k,l) \\ 1 & (i,j) = (l,k) \\ 1 & i = j \wedge i \neq k \wedge i \neq l \\ 0 & \textit{other case} \end{cases}$$

Dla grupy S_3 odpowiadające macierze wyglądają następująco:

$$A_e = Id = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, A_{\tau_1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, A_{\tau_2} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, A_{\tau_3} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$A_{\sigma_1} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, A_{\sigma_2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Teraz jesteśmy gotowi zdefiniować znak permutacji jako funkcję $sign : S_n \to C_2$. *Mianowicie, dla dowolnego* $\sigma \in S_n$ *niech* $sign(\sigma) = det(F(\sigma)) = det(A_\sigma)$. *Korzystając z twierdzenia Cauchyego mamy*

$$sign(\sigma\tau) = det(F(\sigma\tau)) = det(F(\sigma)F(\tau)) = det(F(\sigma))det(F(\tau)) = sign(\sigma)sign(\tau).$$

Zauważmy, że dla $n > 1$ $F(e) = Id$, *więc* $sign(e) = 1$, *natomiast* $sign(\tau_{kl}) = -1$ *dla dowolnych parami różnych* $k, l \in [n]$. *W takim razie dla* $n \geq 2$ *mamy* $im(sign) = \{-1, 2\}$ *oraz*

$$A_n = ker(sign) \trianglelefteq S_n.$$

W takim razie na mocy powyższego twierdzenia mamy$S_n/A_n \cong C_2$. *Powiemy, że permutacja* σ *jest parzysta wtedy i tylko wtedy gdy* $\sigma \in A_n$. *W pozostałym przypadku mamy z permutacją nieparzystą. Dzielnik normalny* A_n *nazywamy też grupą alternującą.*

I jeszcze jeden przykład zastosowania twierdzenia o homomorfiźmie.

Przyklad 2.5. *Niech* $(G, \cdot)$, *będzie grupą. Zdefiniujemy homomorfizm pomiędzy grupą* G *a* $Inn(G)$ *w sposób następujący:*

$$G \ni a \mapsto f(a) = \sigma_a \in Inn(G).$$

Zauważmy że f *jest homomorfizmem. Nich* $a, b \in G$ *będą dowolne, to wtedy:*

$$f(ab) = \sigma_{ab} = \sigma_a \circ \sigma_b = f(a) \circ f(b).$$

Oczywiście, f *jest odwzorowaniem "na"* $Inn(G)$. *Wyznaczmy* $ker(f)$, *dla dowolnego* $a \in G$ *mamy:*

$$a \in ker(f) \longleftrightarrow f(a) = id \longleftrightarrow (\forall x \in G)\ (axa^{-1} = x) \longleftrightarrow (\forall x \in G)\ (ax = xa) \longleftrightarrow a \in Z(G),$$

gdzie zbiór $Z(G) = \{a \in G : \ (\forall x \in G)\ (ax = xa)\}$ *nazywany jest centrum grupy* G. *Wykazaliśmy, że* $ker(f) = Z(G)$. *Z twierdzenia o homomorfiźmie wynika, że* $Z(G)$ *jest dzielnikiem normalnym grupy* G *oraz że zachodzi*

$$Inn(G) \cong G/Z(G).$$

3. Teoria ciał w skrócie

Zakładamy, że czytelnik zna podstawy teorii przestrzeni liniowych oraz podstawy teorii grup o których to będzie mowa w tych notatkach. Tutaj, nieco dokładniej przyjrzymy się elementom teorii ciał.

Rozdział ten rozpoczniemy od wprowadzenia definicji ciała.

Definicja 3.1 (Ciało)**.** *Czwórka* $(\mathbb{K}, +, \cdot, 0, 1)$ *jest ciałem jeżeli*

(1) $\mathbb{K}$ *ma przynajmniej dwa elementy,*
(2) $(\mathbb{K}, +, 0)$ *jest grupą abelową,*
(3) $(\mathbb{K} \setminus \{0\}, \cdot, 1)$ *jest grupą abelową,*
(4) $(\forall x, y, z \in \mathbb{K})\ ((x + y) \cdot z = x \cdot z + y \cdot z)$.

Przykładami ciał są zbiór liczb wymiernych $\mathbb{Q}$, zbiór liczb rzeczywistych $\mathbb{R}$ z naturalnymi działaniami dodawania i mnożenia, również ciałem jest zbiór liczb zespolonych $\mathbb{C}$.

W tym i następnych rozdziałach będziemy rozpatrywać jedynie ciała liczbowe tj takie $\mathbb{K}$, że $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{C}$.

Teraz wprowadzimy wazne pojęcie w teorii ciał jakim jest rozszerzenie skończone. Jak wiemy z elementarnego kursu algebry, jesli mamy dwa ciała $\mathbb{K} \subset \mathbb{L}$ to mozemy wprowadzić strukturę przestrzeni liniowej gdzie wektorami są elementy z ciała $\mathbb{L}$ nad ciałem $\mathbb{K}$.

Definicja 3.2. *Załózmy, że mamy następujący ciąg ciał* $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{L} \subset \mathbb{C}$*, to rozszerzenie* $\mathbb{K} \subset \mathbb{L}$ *nazywamy skończonym jeśli przestrzeń* $(\mathbb{L}, \mathbb{K}, +, \cdot)$ *jest skończenie wymiarowa.*

Definicja 3.3. *Niech* $a \notin \mathbb{K}$*-ciało to najmniejsze ciało zawierające ciało* $\mathbb{K}$ *i element* a *nazywamy rozszerzeniem ciała* $\mathbb{K}$ *o element* a *i oznaczamy* $\mathbb{K}(a)$*.*

Przyklad 3.1. *Przykład* $\mathbb{Q}(\sqrt{2})$*Niech* $\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$*, to najmniejsze ciało zawierające* $\mathbb{Q}$ *i* $\sqrt{2}$ *jednocześnie jest następującym zbiórem z działaniami z ciała* $\mathbb{R}$*:*

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \in \mathbb{R} : \ a, b \in \mathbb{Q}\}.$$

Nietrudno się przekonać, że zbiór ten zawiera oba elementy wspomniane wyżej oraz spełnia wszystkie aksjomaty ciała. Pokażemy jedynie, że istnieje element odwrotny oraz, że bazą tego rozszerzenia jest $1, \sqrt{2}$*. Niech* $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ *będzie niezerowym elementem, to*

$$\begin{aligned} \frac{1}{a + b\sqrt{2}} &= \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} \\ &= \frac{a}{a^2 - 2b^2} + \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}(\sqrt{2}). \end{aligned}$$

By zakończyc te rozwazania pokazemy, że jeśli

$$a + b\sqrt{2} = 0 \to a = b = 0.$$

Jeśli tak jest to albo $b = 0$ *i wtedy* $a = 0$ *albo* $b \neq 0$ *i mamy*

$$\sqrt{2} = -\frac{a}{b} \in \mathbb{Q},$$

co jak wiemy jest nieprawdą i to kończy dowód że $1, \sqrt{2}$ *jest baze rozszerzenia* $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. *Więc w szczególności jesli* $a + b\sqrt{2}$ *jest niezerowy, to i równiez* $a - b\sqrt{2}$ *jest niezerowym elementem* $\mathbb{Q}(\sqrt{2})$. ■

Ten przykład da się nieco uogólnić co można wyrazić w następującym

Twierdzenie 3.1. *Nich* $\mathbb{K} \subset \mathbb{L}$ *będzie dowolnym ciałem. Załóżmy, że istnieje taki element* $a \in \mathbb{L} \setminus \mathbb{K}$, *że* $a^2 \in \mathbb{K}$, *to zbiór*

$$\mathbb{K}(a) = \{x + y\, a \in \mathbb{L} : \, x, y \in \mathbb{K}\}$$

jest najmniejszym ciałem generowanym przez a *i zawierające ciało* $\mathbb{K}$.

Dowód. *Oczywiście zbiór* $\mathbb{K}(a)$ *jest zamknięty na mnożenie i dodawanie, oczywiście element przeciwny każdego elementu z* $\mathbb{K}(a)$ *należy do* $\mathbb{K}(a)$. */Łączność i przemienność jest dziedziczona z ciała* $\mathbb{L}$. *Pokażemy, że element odwrotny również jest w* $\mathbb{K}(a)$. *Nim to pokażemy, udowodnimy że*

$$x + y\, a = 0 \ \textit{o ile}\ x, y \in \mathbb{K} \to x = y = 0.$$

Załóżmy, że tak nie jest to znaczy $x \neq 0$ *lub* $y \neq 0$, *to w przypadku gdy* $x = 0$ *mamy* $y\, a = a$ *stąd* $y = 0$, *gdyby natomiast* $y \neq 0$ *to*

$$x + y\, a = 0 \to a = -\frac{x}{y} \in \mathbb{K},$$

wbrew założeniu, że $a \notin \mathbb{K}$. *Zauważmy, że:*

$$(x + y\, a)\frac{x - y\, a}{x^2 - y^2\, a^2} = \frac{x^2 - y^2\, a^2}{x^2 + y^2\, a^2} = 1,$$

o ile $x^2 - y^2\, a^2 \neq 0$. *Gdyby* $x^2 - y^2 a^2 = 0$ *to*

$$a^2 = \frac{x^2}{y^2} = \left(\frac{x}{y}\right)^2,$$

więc

$$a = \frac{x}{y} \in \mathbb{K} \ \textit{lub}\ a = -\frac{x}{y} \in \mathbb{K}$$

co jest sprzeczne z założeniem. ■

Przyklad 3.2. *Przykład* $\mathbb{Q}(\sqrt[3]{2})$ *W tym przykładzie pokażemy, że elementy odwrotne do liczb występujących w zbiorze*

$$\mathbb{Q}(\sqrt[3]{2}) \equiv \{x + y\sqrt[3]{2} + \sqrt[3]{4} \in \mathbb{R} : \, x, y, z \in \mathbb{Q}\}$$

istnieją (oczywiście poza zerem) i leża również w nim. Pozostałe aksjomaty ciała łatwo się pokazuje.

Skorzystamy z prostej własności algebraicznej, mianowicie:

$$x^3 + y^3 + z^3 - 3\, xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - xz - yz).$$

Lewa strona równości jest zerem wtedy gdy $x+y+z=0$ *lub* $x^2+y^2+z^2-xy-xz-yz=0$. *Gdyby*

$$x^2+y^2+z^2-xy-xz-yz=0$$

to wtedy:

$$\begin{aligned}2x^2+2y^2+2z^2-2xy-2xz-2yz&=0\\&=x^2-2xy+y^2+x^2-2xz-z^2+y^2-2yz+z^2\\&=(x-y)^2+(x-z)^2+(y-z)^2\end{aligned}$$

więc

$$\begin{cases}x-y=0\\y-z=0\\z-x=0\end{cases}$$

stąd dostajemy

$$x=y=z$$

Podstawiając w naszej tożsamości $y:=y\sqrt[3]{2}$ $z:=z\sqrt[3]{4}$ *mamy:*

$$\frac{1}{x+y\sqrt[3]{2}+\sqrt[3]{4}}=\frac{x^2+y^2\sqrt[3]{4}+2z^2\sqrt[3]{2}-xy\sqrt[3]{2}-xz\sqrt[3]{4}-2yz}{x^3+2y^3+4z^3-6xyz}.$$

Mianownik jest równy zero wtedy i tylko wtedy gdy $x=y\sqrt[3]{2}$ *oraz* $x=z\sqrt[3]{4}$, *co jest możliwe tylko w przypadku gdy* $x=y=z=0$ *ponieważ* $\sqrt[3]{2}$ *oraz* $\sqrt[3]{4}$ *są liczbami niewymiernymi. Oczywiście licznik jest elementem* $\mathbb{Q}(\sqrt[3]{2})$ *a mianownik jest liczbą wymierną.* ■

Zajmiemy sie teraz jedynie skończonymi rozszerzeniami ciał. Niech $\mathbb{L}=\mathbb{L}$ będzie takim rozszerzeniem ciała $\mathbb{K}$ i niech $a\in\mathbb{L}$. Wtedy istnieje skończona nietrywialna kombinacja liniowa równa zero:

$$\sum_{i=0}^{n}\alpha_i\,a^i=0 \text{ gdzie } \alpha_i\in\mathbb{K} \text{ dla } i\in\{0,\dots,n\}.$$

Czyli istnieje niezerowy wielomian $f\in\mathbb{K}[x]$ taki, że $f(a)=0$. W tym momencie możemy wprowadzić pojęcie wielomianu minimalnego.

Definicja 3.4. *Niech* $\mathbb{K}\subset\mathbb{L}$ *będzie skończonym rozszerzeniem,* $a\in\mathbb{L}$, *to wielomian* $f\in\mathbb{K}[x]$ *jest* **wielomianem minimalnym** *elementu* a *nad ciałem* $\mathbb{K}$ *jeżeli*

- $f\neq 0$ *i* $f(a)=0$
- $(\forall g\in\mathbb{K}[x])(stg<stf\wedge g(a)=0\to g=0)$.

Przyklad 3.3. *Wielomian* $f(x)=x^2-2$ *jest wielomianem minimalnym* $\sqrt{2}$ *nad ciałem liczb wymiernych* $\mathbb{Q}$.

Fakt 3.1. *Niech* $\mathbb{K}\subset\mathbb{L}$ *będzie rozszerzeniem ciał. Jeżeli* $f,g\in\mathbb{K}[x]$ *są wielomianami minimalnymi elementu* $a\in\mathbb{L}$, *to są one sprzężone tzn. istnieje element* $c\in\mathbb{K}\setminus\{0\}$ *taki że* $g(x)=c\cdot f(x)$.

Czasami rozważa się jedynie wielomian unormowany jako wielomian minimalny. Wtedy, takie wielomiany są jedyne.

Fakt 3.2. *Niech $\mathbb{K} \subseteq \mathbb{L}$ będzie rozszerzeniam ciał i $a \in \mathbb{L}$. Wtedy $f \in \mathbb{K}[x]$ jest wielomianem minimalnym elementu a wtedy i tylko wtedy gdy $f(a) = 0$ i f nie jest wielomianem rozkładalnym nad ciałem $\mathbb{K}$.*

Dowód. $\rightarrow$ *Jeśli $f \in \mathbb{K}[x]$ jest minimalny dla $a \in \mathbb{L}$ i f jest rozkładalny nad $\mathbb{K}$, to istnieją $f_1, f_2 \in \mathbb{K}[x]$ takie że $st\ f_1 < st\ f$, $st\ f_2 < st\ f$ i $f = f_1 f_2$. Wtedy $0 = f(a) = f_1(a)f_2(a)$ to $f_1(a) = 0$ lub $f_2(a) = 0$, co jest niemożliwe wobec minimalności f.*

$\leftarrow$ *Niech $f \in \mathbb{K}[x]$ nie jest wielomianem minimalnym i $f(a) = 0$. To wtedy istnieje niezerowy wielomian $g \in \mathbb{K}[x]$ taki że $g(a) = 0$ i stg, stf. Niech $n = \min\{stg : g \in \mathbb{K}[x] \wedge g(a) = 0 \wedge g \neq 0\}$ i $stg = n$. Wtedy, $g|f$ bo w przeciwnym wypadku, istniałby niezerowy wielomian $r \in \mathbb{K}[x]$ $q \in \mathbb{K}[x]$ takie że $f = q \cdot g + r$ i $st\ r < st\ g$ i oczywiście $r(a) = 0$ bo $f(g) = g(a) = 0$. To jest niemożliwe wobec minimalności n i faktu, że $st\ g = n$. Ponieważ $g|f$ i $st\ g < st\ f$, to wtedy f nie jest wielomianem nierozkładalnym nad ciałem $\mathbb{K}$.* ■

Fakt 3.3. *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem ciała $\mathbb{K}$ i $f \in \mathbb{K}[x]$ jest wielomianem minimalnym $a \in \mathbb{L}$ i $g \in \mathbb{K}[x]$ że $g(a) = 0$ to $f|g$.*

Dowód. *Jeśli $\neg f|g$ to istnieje $h, r \in \mathbb{K}[x]$ że $0 \leq st\ r < st\ f$ i $g = hf + r$ a wtedy $r(a) = g(a) - h(a)f(a) = 0$ co jest niemożliwe wobec minimalności f (st $r < st\ f$).* ■

Fakt 3.4. *Jeśli $f, g \in \mathbb{K}[x]$ są wielomianami minimalnymi elementu $a \in \mathbb{L}$, gdzie $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem, to te wielomiany są stowarzyszone $f \sim g$.*

Dowód. *Na mocy poprzedniego faktu $f|g$ i jednocześnie $g|f$ a więc otrzymujemy tezę $f \sim g$.* ■

W ogólności, nie jest sprawą łatwą rozstrzygnęcie faktu, ze dany wielomian $f \in \mathbb{K}[x]$ jest nierozkładalny nad $\mathbb{K}$. Pewnym rozwiązaniem tego problemu jest kryterium Eisensteina o nierozkładalności wielomianów o wsppółczynnikach całkowitych nad pierścieniem $\mathbb{Z}$. Ponadto, twierdzenie Gaussa pozwala przenieść nierozkładalność takich wielomianów nad $\mathbb{Z}$ na nierozkładalność nad ciałem $\mathbb{Q}$. Dowody tych twierdzedzeń znajdują się w Appendixach 7 i 7.

Twierdzenie 3.2 (Kryterium Eisensteina)**.** *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem o współczynnikach całkowitych $f(x) = \sum_{k=0}^{n} a_k x^k$ o takiej własności, że istnieje liczba pierwsza $p \in \mathbb{N}$ taka że*

$$\neg p|a_n \wedge p|a_{n-1} \wedge \ldots \wedge p|a_0 \wedge \neg p^2|a_0,$$

to f nie jest rozkładalny nad $\mathbb{Z}$.

Twierdzenie 3.3 (Gauss)**.** *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem o współczynnikach całkowitych $f(x) = \sum_{k=0}^{n} a_k x^k$, to f jest nierozkładalny nad $\mathbb{Q}$ wtedy i tylko wtedy gdy f jest nierozkładalny nad $\mathbb{Z}$.*

Jako zastostosowanie kryterium Eisensteina, mamy następujące twierdzenie:

Twierdzenie 3.4. *Niech $p \in \mathbb{N}$ będzie liczbą pierwszą, to wielomian $f(x) = \sum_{k=0}^{p-1} x^k \in \mathbb{Z}[x]$ jest nierozkładalny nad $\mathbb{Z}$.*

Dowód. *Oczywiście nie możemy zastosować wprost wspomnianego wyżej kryterium, więc zastosujmy podstawienie $x = y + 1$, to wtedy:*

$$f(x) = \sum_{k=0}^{p-1} x^k = \frac{x^p - 1}{x - 1} = \frac{(y+1)^p - 1}{y} = \frac{1}{y}\left(\sum_{k=0}^{p} \binom{p}{k} y^k - 1 \right) =$$

$$= \frac{1}{y}\left(1 + \sum_{k=1}^{p} -1 \binom{p}{k} y^k \right) = \sum_{k=1}^{p} \binom{p}{k} y^{k-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} y^k.$$

Zauważmy, że dla $k \in \{0, \ldots, p-1\}$ mamy $a_k = \binom{p}{k+1}$, co daje fakt że dla $k < p-1$ współczynnik $a_k = \frac{p!}{(k+1)!(p-(k+1))!}$ jest liczbą całkowitą podzielną przez liczbę pierwszą p, natomiast dla $k = p-1$ $a_k = \binom{p}{p} = 1$. Mamy ponadto, że $a_0 = \binom{p}{1} = p$, tak więc liczba pierwsza p dzieli a_0 ale p^2 nie dzieli a_0. Więc założenia kryterium Eisensteina są spełnione dla wielomianu $h(y) = f(y+1)$. Kryterium te daje nierozkładalność wielomianu h nad $\mathbb{Z}$ a więc w resultacie sam wielomian f jest nierozkładalny nad pierścieniem $\mathbb{Z}$. ■

W szczególności $1 + x + x^2$ jest wielomianem minimalnym liczby $e^{\frac{2}{3}\pi i}$.

Przyklad 3.4. *Niech $\mathbb{K} = \mathbb{Q}$ i $a := \sqrt[p]{p} \in \mathbb{R}$ dla pewnej liczby pierwszej $p \in \mathbb{N}$ i $n \in \mathbb{N} \setminus \{0, 1\}$, to z twierdzenia Eisensteina-Schonemanna wielomian $f(x) = x^n - p \in \mathbb{K}[x]$ jest nierozkładalny nad $\mathbb{K} = \mathbb{Q}$ i oczywiście $f(a = \sqrt[p]{p}) = 0$ więc f jest wielomianem minimalnym elementu a.*

Wielomian ten zalezy zarówno od elementu a jak i od ciała $\mathbb{K}$. Zauwazamy tez że kazdy element z ciała $\mathbb{L} = \mathbb{K}(a) \ni x$ da się przedstawić jako wartość pewnwgo wielomianu $g \in \mathbb{K}[x]$ w elemencie a tj.

$$\mathbb{K}(a) \ni x = g(a) \text{ gdzie } g \in \mathbb{K}[x].$$

Oczywiscie wystarczy brać wielomiany o stopniu mniejszym od stopnia wielomianu minimalnego elementu a poniewaz

$$g = q \cdot f + r \text{ oraz } g(a) = q(a)f(a) + r(a) = r(a) \text{ gdzie } g, f, q, r \in \mathbb{K}[x].$$

Twierdzenie 3.5. *Jeżeli $\mathbb{K} \subseteq \mathbb{L}$ jest skończonym rozszerzeniem o element $a \in \mathbb{L}$ oraz $f \in \mathbb{K}[x]$ jest wielomianem minimalnym a, to*

$$\mathbb{L} = \mathbb{K}(a) = \{g(a) : \ g \in \mathbb{K}[x] \wedge stg < stf\}.$$

Dowód. *Z definicji ciała $\mathbb{K}(a)$ mamy że $\mathbb{K} \cup \{a\} \subseteq \mathbb{K}(a)$, wiec $a^k \in \mathbb{K}(a)$ dla dowolnego $k \in \mathbb{N}$ oraz $b_k \cdot a^k \in \mathbb{K}(a)$ dla dowolnego $k \in \mathbb{N}$ i $b_k \in \mathbb{K}$ ze względu na fakt że każde ciało*

jest zamkniete na mnożenie, dalej $b_0+b_1a+\ldots+b_na^n=g(a)\in\mathbb{K}(a)$ *dla* $g\in\mathbb{K}[x]$ *z uwagi na to że każde ciało jest zamknięte na skończone sumy swoich elementów. Tak więc mamy*

$$\{g(a)\in\mathbb{L}:\ g\in\mathbb{K}[x]\}\subseteq\mathbb{K}(a).$$

Wystarczy zauważyć, że jeśli $g\in\mathbb{K}[x]$ *i* $g=qf+r$ *dla pewnych* $q,r\in\mathbb{K}[x]$ *oraz st* $r<st\ f$ *to wtedy*

$$g(g)=q(a)f(a)+r(a)=q(a)\cdot 0+r(a)=r(a)$$

więc mamy

$$\{g(a)\in\mathbb{L}:\ g\in\mathbb{K}[x]\wedge st(g)<st(f)\}=\{g(a)\in\mathbb{L}:\ g\in\mathbb{K}[x]\}\subseteq\mathbb{K}(a).$$

Jedyną nietrywialną własnością jaką należy sprawdzić, jest istnienie elementu odwrotnego do dowolnego $y\in\mathbb{K}(a)\setminus\{0\}$ *oraz że element odwrotny* $y^{-1}\in\mathbb{K}(a)$.

Tak więc załóżmy, że $y\in\mathbb{K}(a)\setminus\{0\}$, *to istnieje* $g\in\mathbb{K}[x]$ *dla którego* $y=g(a)$ *i* $st\ g<st\ f$, *gdzie* $f\in\mathbb{K}[x]$ *jest wielomianem minimalnym dla* a.

Zauważmy, że jeśli $r\in\mathbb{K}[x]$ *jest taki że* $r|g$ *i* $r|f$, *to ponieważ* f *jest nierozkładalny nad* $\mathbb{K}$ *i* $str\leq stg<stf$ *wnosimy, że* $r=c$ *dla pewnego* $c\in\mathbb{K}\setminus\{0\}$. *Więc,* $NWD(f,g)=1$ *a stąd istnieją* $u,v\in\mathbb{K}[x]$ *dla których zachodzi równość*

$$u\cdot f+v\cdot g=1\ \text{ a stąd }1=u(a)f(a)+v(a)g(a)=v(a)g(a)=v(a)y\ \ (f(a)=0),$$

stąd kładąc za $y^{-1}v(a)$ *mamy* $b^{-1}b=1$ *i* $b^{-1}\in\mathbb{K}(a)$ *o ile* $b\in\mathbb{K}(a)\setminus\{0\}$. ■

Przyklad 3.5. *Opisać ciało* $\mathbb{Q}(\sqrt[3]{2})$. *Niech* $f=x^3-2\in\mathbb{Z}[x]$ *i* $a=\sqrt[3]{2}$, *to oczywiście* $f(a)=0$. *Pokażemy, że* f *jest nierozkładalny nad* $\mathbb{Z}$ *a więc z Twierdzenia Gaussa,* f *jest również wielomianem nierozkładalnym nad* $\mathbb{Q}$. *Wykonajmy podstawienie* $x=y-1$, *to wtedy mamy*

$$h(y)=f(y-1)=(y-1)^3-2=y^3-3y^2+3y-1-2=y^3-3y^2+3y-3\in\mathbb{Z}[x].$$

Stosując Kryterium Eisensteina dla liczby pierwszej $p=3$ *otrzymujemy nierozkladalność wielomiany* h. *Gdyby wielomian* f *byłby rozkładalny nad* $\mathbb{Z}$, *to wtedy*

$$f(x)=f_1(x)\cdot f_2(x)\ \text{ dla }f_1,f_2\in\mathbb{Z}[x]\wedge st(f_1),st(f_2)<st(f)$$

a wtedy

$$h(y)=f(y-1)=f_1(y-1)\cdot f_2(y-1)=g_1(y)\cdot g_2(y)$$

oraz $g_i(y)=f_i(y-1)\in\mathbb{Z}[x]$ *a także* $st(g_i)=st(f_i)<st(f)$ *dla* $i\in\{1,2\}$ *a więc wielomian* h *byłby rozkładalny nad* $\mathbb{Z}$, *co jest niemożliwe.*

Na mocy powyższego twierdzenia 3.5, mamy

$$\begin{aligned}\mathbb{Q}(\sqrt[3]{2})=&\{g(\sqrt[3]{2}):\ g\in\mathbb{Q}\wedge st(g)<st(f)=3\}=\\=&\{x+y\sqrt[3]{2}+z\sqrt[3]{4}:\ x,y,z\in\mathbb{Q}\}.\end{aligned}$$

Przyklad 3.6. *Obliczyć* $(1+\sqrt[3]{3}+2\sqrt[3]{4})^{-1}$ *w* $\mathbb{Q}(\sqrt[3]{2})$.

Niech $a := \sqrt[3]{2}$ *i* $y = 1 + \sqrt[3]{3} + 2\sqrt[3]{4}$, *to wtedy* $y = g(a)$ *dla* $g(x) = 1 + x + x^2 \in \mathbb{Q}[x]$, *ponadto wiemy że* $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ *jest wielomianem mimimalnym elemntu* a. *Stosując algorytm Euklidesa, znajdujemy* $u, v \in \mathbb{Q}[x]$ *dla których spełnione jest równanie*

$$uf + vg = 1.$$

W naszym przypadku mamy $u(x) = ...$ *i* $v(x) = ...$ *a stąd* $y^{-1} = v(a) = ...$ □

Definicja 3.5 (stopień rozszerzenia)**.** *Niech* $\mathbb{K} \subset \mathbb{L}$ *jest rozszerzeniem ciała* $\mathbb{K}$, *to wtedy* $[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{L}$ *jest stopniem rozszerzenia* $\mathbb{K} \subseteq \mathbb{L}$, *o ile przestrzeń liniowa* $\mathbb{L}$ *nad ciałem* $\mathbb{K}$ *jest przestrzenią skończenie wymiarową, w przeciwnym wypadku stopień rozszerzenia jest nieskończony.*

Podamy dwa przydatne twierdzenie o stopniu rozszerzenia ciał.

Twierdzenie 3.6. *Jeżeli dany ciąg ciał* $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$ *jest taki, że* $\mathbb{K} \subseteq \mathbb{L}$ *jest skończone, to wtedy* $\mathbb{K} \subseteq \mathbb{M}$ *i* $\mathbb{M} \subseteq \mathbb{L}$ *są również skońzone i jednocześnie zachodzi*

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}] \cdot [\mathbb{M} : \mathbb{K}].$$

Na odwrót, jeżeli $\mathbb{K} \subseteq \mathbb{M}$ *i* $\mathbb{M} \subseteq \mathbb{L}$ *są rozszerzeniami skończonymi, to rozszerzenie* $\mathbb{K} \subseteq \mathbb{L}$ *jest również skończone.*

Dowód. *Załóżmy, że stopień rozszerzenia* $\mathbb{K} \subseteq \mathbb{L}$ *jest skończony. Wtedy istnieje* $\mathfrak{B} \subseteq \mathbb{L}$ *skończona baza* $\mathbb{L}$ *nad ciałem* $\mathbb{K}$. *Zauważmy, że z definicji bazy oraz faktu że* $\mathbb{M} \subseteq \mathbb{L}$, *mamy* $\mathbb{L} = span_{\mathbb{K}}\mathfrak{B} \subseteq span_{\mathbb{M}}\mathfrak{B} \subseteq \mathbb{L}$. *Więc jeśli* $\mathfrak{B}_0 \subseteq \mathbb{L}$ *jest bazą* $\mathbb{L}$ *nad ciałem* $\mathbb{M}$, *to wtedy* $|\mathfrak{B}_0| \leq |\mathfrak{B}| < \infty$. *Stąd* $\mathbb{M} \subseteq \mathbb{L}$ *jest rozszerzeniem skończonym. Zauważmy, że* $\mathbb{M}$ *jest podprzestrzenią liniową przestrzeni* $\mathbb{L}$ *nad ciałem* $\mathbb{K}$, *więc rozszerzenie* $\mathbb{K} \subseteq \mathbb{L}$ *jest również rozszerzeniem skończonym.*

Nech $\mathfrak{B}_0$ *będzie skończoną baza przestrzeni* $\mathbb{L}$ *nad ciałem* $\mathbb{M}$ *i* $\mathfrak{B}_1$ *bazą skończenie wymiarowej przestrzeni* $\mathbb{M}$ *nad* $\mathbb{K}$. *Wtedy każdy element* $z \in \mathbb{L}$ *jest pewną skończoną kombinacją liniową elementów* $\mathfrak{B}_0$ *o współczynnikach z ciała* $\mathbb{M}$*:*

$$z = \sum_{e \in \mathfrak{B}_0} a_e \cdot e.$$

Natomiast każdy element ciała $\mathbb{M}$ a *w szczególności* $a_e \in \mathbb{M}$ *dla dowolnego* $e \in \mathfrak{B}_0$ *jest skończona kombinacją elementów bazy* $\mathfrak{B}_1$ $a_e = \sum_{f \in \mathfrak{B}_1} b_{a_e,f} f$ *o współczynnikach z ciała* $\mathbb{K}$.. *Więc*

$$z = \sum_{e \in \mathfrak{B}_0} a_e \cdot e = \sum_{e \in \mathfrak{B}_0} (\sum_{f \in \mathfrak{B}_1} b_{a_e,f} f)e = \sum_{e \in \mathfrak{B}_0} \sum_{f \in \mathfrak{B}_1} b_{a_e,f} e \cdot f.$$

Wobec dowolności elementu $z \in \mathbb{L}$ *mamy* $\mathbb{L} = span_{\mathbb{K}}\{e \cdot f : \ (e, f) \in \mathfrak{B}_0 \times \mathfrak{B}_1\}$. *Pokażemy że* $\mathfrak{B} = \{e \cdot f : \ (e, f) \in \mathfrak{B}_0 \times \mathfrak{B}_1\} \subseteq \mathbb{L}$ *jest liniowo niezależnym układem nad ciałem* $\mathbb{K}$. *Nech* $\{\alpha_{e,f} \in \mathbb{K} : \ (e, f) \in \mathfrak{B}_0 \times \mathfrak{B}_1\}$ *będzie dowolnym zbiorem liczb z ciała* $\mathbb{K}$, *takim że* $\sum_{(e,f) \in \mathfrak{B}_0 \times \mathfrak{B}_1} \alpha_{e,f} e \cdot f = 0$. *Wtedy mamy*

$$0 = \sum_{(e,f) \in \mathfrak{B}_0 \times \mathfrak{B}_1} \alpha_{e,f} e \cdot f = \sum_{e \in \mathfrak{B}_0} (\sum_{f \in \mathfrak{B}_1} \alpha_{e,f} f)e.$$

Ponieważ $\mathfrak{B}_0$ jest liniowo niezależny nad $\mathbb{M}$, to dla dowolnego $e \in \mathfrak{B}_0$ mamy $\sum_{f\in\mathfrak{B}_1} \alpha_{e,f} f = 0$. Ponieważ $\mathfrak{B}_1$ jest liniowo niezależny nad $\mathbb{K}$ to wtedy dla każdego $e \in \mathfrak{B}_0$ i każdego $f \in \mathfrak{B}_1$ $\alpha_{e,f} = 0$. Pokazaliśmy więc, że $\mathfrak{B}$ jest baza przestrzni $\mathbb{L}$ nad cilem $\mathbb{K}$.. Zauważmy że $|\mathfrak{B}| = |\mathfrak{B}_0 \times \mathfrak{B}_1| = |\mathfrak{B}_0| \cdot |\mathfrak{B}_1|$. Stąd wynika żądana równość i fakt, że $\mathbb{K} \subseteq \mathbb{L}$ jest rozszerzeniem skończonym. ■

Fakt 3.5 (O stopniu rozszerzenia o element pierwotny)**.** *Jezeli $\mathbb{K}(a)$ jest rozszerzeniem skończonym ciała $\mathbb{K}$ a wielomian $f \in \mathbb{K}[x]$ jest wielomianem minimalnym elementu $a \in \mathbb{K}(a)$, to stopień rozszerzenia jest równy stopniowi wielomianu f, czyli $[\mathbb{K}(a) : \mathbb{K}] = st\, f$.*

Dowód. *Ponieważ $f = c_0 + c_1 x + c_2 x^2 + \ldots + c_n x^n$ (gdzie $c_n \neq 0$) jest wielomianem minimalnym elementu a, to $\mathfrak{B} = \{1, \ldots, a^{n-1}\}$ jest liniowo niezależnym zbiorem w przestrzeni $\mathbb{K}(a)$ nad ciałem $\mathbb{K}$. Z drugiej strony każdemu elementowi b ciała $\mathbb{K}(a)$ odpowiada wielomian $g \in \mathbb{K}[x]$ taki że $stg < stf$ oraz $b = g(a)$. Stąd $span_{\mathbb{K}}\mathfrak{B} = \mathbb{K}(a)$, więc $\mathfrak{B}$ jest bazą tej przestrzeni mocy $n = stf$.* ■

Przyklad 3.7. *Wykorzystując twierdzenie o stopniu rozszerzenia dla trzech ciał, pokażemy, że $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{3})(\sqrt{2})$. Zauważmy, że $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2})(\sqrt{3})$, więc $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2})(\sqrt{3})$. Ponieważ $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = 2$ oraz $(\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})) \leq 2$, więc $(\mathbb{Q}(\sqrt{2}(\sqrt{3}) : \mathbb{Q})) = (\mathbb{Q}(\sqrt{2})(\sqrt{3}) : \mathbb{Q}(\sqrt{2})) \cdot (\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) \leq 4$. Z drugiej strony, jeśli $x = \sqrt{2}+\sqrt{3}$, to $x^2 = 2 + 2\sqrt{6} + 3$ a więc $(x^2-5)^2 = 4 \cdot 6$. Niech $f(x) = (x^2-5)^2 - 24 = x^4 - 10x^2 + 25 - 24 = x^4 - 10x^2 + 1$. Ponieważ wielomian ten nie ma pierwiastków wymiernych, więc co najwyżej rozkłada się na iloczyn dwóch wielomianów z $\mathbb{Q}[x]$ o stopniu równym 2. W takim razie wystarczy zbadać, czy nasz wielomian da się rozłożyć na iloczyn dwóch wielomianów o współczynnikach z $\mathbb{Z}$ i o stopniach równych dwa. Można sprawdzić bespośrednom rachunkiem, że taki rozkład nie istnieje. Więc wielomian $x^4 - 10x^2 + 1$ jest nierozkładalny nad $\mathbb{Z}$ więc też nad $\mathbb{Q}$ na mocy twierdzenia Gaussa. W takim razie $(\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}) = 4$, co daje nam równość rozszerzeń $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$. Analogiczną równość mamy pomiędzy ciałami $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ i $\mathbb{Q}(\sqrt{3})(\sqrt{2})$.*

Definicja 3.6 (Ciało rozkładu wielomianu)**.** *Rozważmy rozszerzenie $\mathbb{K} \subseteq \mathbb{L}$ i wielomian $f \in \mathbb{K}[x]$, to $\mathbb{L}$ jest ciałem rozkładu wielomianu f jeżeli jest generowane przez wszystkie pierwiastki f, które są w algebraicznym domknięciu ciała $\mathbb{K}$.*

Przyklad 3.8. *Ciało $\mathbb{Q}(\sqrt{2})$ jest ciałem rozkładu wielomianu $f(x) = x^2 - 2$, natomiast $\mathbb{L} = \mathbb{Q}(\sqrt[3]{2})$ nie jest ciałem rozkładu wielomianu $f(x) = x^3 - 2$ bo nie zawiera pierwiastków zespolonych wielomianu f ($\mathbb{L}$ zawiera dokładnie jeden pierwiastek wielomianu f). Łatwo sprawdzić, że ciało $\mathbb{Q}(\sqrt[3]{2}, \epsilon\sqrt[3]{2})$ jest już ciałem rozkładu wielomianu $x^3 - 2$, gdzie $\epsilon = e^{i\frac{2}{3}\pi}$ jest pierwotnym pierwiastkiem z jedności stopnia trzeciego.*

Definicja 3.7 (Rozszerzenie rozdzielcze)**.** *$\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem rozdzielczym ciała $\mathbb{K}$, jeśli dla każdego elementu algebraicznego z ciała $\mathbb{L}$, wielomian minimalny tego elementu, ma parami różne pierwiastki w jego algebraicznym domknięciu.*

Fakt 3.6. *Jeśli $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{C}$, to $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem rozdzielczym.*

Dowód. *Niech $a \in \mathbb{L}$ będzie elementem algebraicznym nad ciałem $\mathbb{K}$, załóżmy że $f = a_0 + \ldots + a_n x^n \in \mathbb{K}[x]$ będzie wielomianem minimalnym elementu a, takim że $x_0 \in \mathbb{C}$ jest pierwiaskiem k krotnym spełniającym warunek $k \geq 2$. Więc istnieje wielomian $g \in \mathbb{C}[x]$ taki że*

$$f(x) = (x - x_0)^k g(x).$$

Załóżmy, że $a = x_0$. Ponieważ $2 \leq k$, więc x_0 jest również pierwiastkiem pochodnej wielomianu f:

$$f'(x) = k(x - x_0)^{k-1} g(x) + (x - x_0)^k g'(x) = (x - x_0)^{k-1}(kg(x) + (x - x_0)g'(x)).$$

Z drugiej strony mamy

$$f'(x) = a_1 + 2a_2 x + \ldots + na_n x^{n-1} \in \mathbb{K}[x],$$

tak więc istnieje wielomian f' o współczynnikach z ciała $\mathbb{K}$ zerujący x_0, takim że $stf' < stf$, sprzeczność wobec minimalności wielomianu f elementu x_0 który jest równy a.

Załóżmy teraz, że $a \neq x_0$. Na podstawie powyższego paragrafu, wielomian f nie jest wielomianem minimalnym elementu x_0. Niech $h \in \mathbb{K}[x]$ będzie wielomianem minimalnym x_0, Mając na uwadze, że $f(x_0) = 0$ i $f \in \mathbb{K}[x]$ dochodzimy do wnoisku, że h dzieli wielomian f i $st(h) < st(f)$. Wówczas istnieje $v \in \mathbb{K}[x]$ stopnia przynajmniej równego 1 taki, że

$$f = h \cdot v.$$

Ponieważ $f(a) = 0$, to $v(a) = 0$ lub $h(a) = 0$ oraz $st(v) < st(f)$, $st(h) < st(f)$, co jest niemożliwe wobec minimalności stopnia wielomianu f, dla którego a jest pierwiastkiem. ■

Zachodzi bardzo wazne twierdzenie o elemencie pierwotnym pochodzące od N. Abela:

Twierdzenie 3.7 (Abela o elemencie pierwotnym)**.** *Niech $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem rozdzielczym ciała $\mathbb{K}$ i niech $a, b \in \mathbb{L}$ bądą elementami algebraiczymi nad $\mathbb{K}$, to wtedy istnieje $c \in \mathbb{L}$ algebraiczny element nad $\mathbb{K}$ dla którego $\mathbb{K}(a, b) = \mathbb{K}(c)$ (rozszerzenie jest pierwotne i c jest elementem pierwotnym rozszerzenia).*

Dowód. *Przypadek gdy $\mathbb{K}$ jest nieskończone. Niech $f, g \in \mathbb{K}[x]$ będą wielomianami minimalnymi dla $a, b \in \mathbb{L}$ odpowiednio. Niech $\hat{\mathbb{K}}$ będzie algebraicznym domknięciem ciala $\mathbb{K}$ zawierającym ciało $\mathbb{L}$. Niech ponadto*

$$\mathscr{F} = \{a = a_1, \ldots, a_n\}, \;\; \mathscr{G} = \{b = b_1, \ldots, b_m\},$$

będą zbiorami wszystkich pierwiastków dla wielomianów $f, g \in \mathbb{K}[x]$ odpowiednio. Niech $d \in \mathbb{K}$ będzie elementem ciała $\mathbb{K}$ i $c \in \mathbb{L}$, takim że $c = a + db$ oraz

$$c - db_j \neq a_i \;\; dla \; j \in \{2, \ldots, m\}, \; i \in \{1, \ldots, n\},$$

co jest możliwe z uwagi na to że $\mathbb{K}$ ma nieskończenie wiele elementów. Oczywiście $\mathbb{K}(c) \subset \mathbb{K}(a, b)$. Niech

$$h(x) = f(c - dx), \;\; tutaj \; mamy \; h \in \mathbb{K}(c)[x]!$$

To wtedy, $h(b) = f(c - db) = f(a) = 0$ oraz $h(b_j) = f(c - db_j) \neq 0$ dla $j \in \{2, \ldots, m\}$, bo wtedy $c - db_j \neq a_i$ dla $i \in \{1, \ldots, n\}$. Tak więc $g, h \in \mathbb{K}(c)[x]$ mają dokładnie jeden wspólny pierwiastek w algebraicznym domknięciu ciała $\mathbb{K}$. Gdyby $NWD(g, h)$ miałby stopień większy od 1, to wspólny pierwiastek wielomianów f, g byłby przynajmniej podwójny, natomiast

f, g są wielomianami minimalnymi elementów a i b odpowiednio, więc rozszerzenie $K \subseteq \mathbb{L}$ nie byłyby rozdzielcze, sprzeczność. Stąd $st(NWD(f,g)) = 1$, więc dla pewnego b mamy

$$x - b = NWD(g,h) \in \mathbb{K}(c)[x],$$

co pociąga za sobą warunek $b \in \mathbb{K}(c)$ i dalej

$$a = c - db \in \mathbb{K}(c) \to \mathbb{K}(a,b) \subset \mathbb{K}(c).$$

Ostatecznie mamy równość ciał $\mathbb{K}(a,b) = \mathbb{K}(c)$, co kończy dowód w przypadku nieskończonego ciała $\mathbb{K}$.

Jeśli natomiast $\mathbb{K}$ jest skończone, to $\mathbb{K}(a,b)$ jest ciałem skończonym, to wtedy z twierdzenia o grupie multiplikatywnej ciała, wynika że $(\mathbb{K}(a,b) \setminus \{0\}, \cdot)$ jest grupą cykliczną a stąd istnieje $c \in \mathbb{K}(a,b) \setminus \{0\}$ i $n \in \mathbb{N}$, dla których $c^n = 1$ i

$$\mathbb{K}(a,b) \setminus \{0\} = \{c^k : \ k \in \{0, \ldots, n-1\}\}.$$

Z powyższej tożsamości dostajemy tezę. ■

Z tego waznego twierdzenia wypływa w sposób naturalny następujący wniosek:

Twierdzenie 3.8. *Wniosek Niech $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{L} \equiv \mathbb{K}(a_1, \ldots, a_n) \subset \mathbb{C}$ będzie skończonym rozszerzeniem, to istnieje $c \in \mathbb{L}$ taki, że $\mathbb{L} = \mathbb{K}(c)$.*

Dowód. *Dowód Dla $n = 1$ teza jest oczywista, dla $n = 2$ twierdzenie Abela daje pozytywną odpowiedź. Załózmy, że teza jest prawdziwa dla pewnego $n \in \mathbb{N}$. Wiec na mocy założenia indukcyjnego oraz twierdzeniu Abela mamy:*

$$\mathbb{K}(a_1, \ldots, a_n, a_{n+1}) = \mathbb{K}(a_1, \ldots, a_n)(a_{n+1}) = \mathbb{K}(b)(a_{n+1}) = \mathbb{K}(c),$$

dla pewnego $b \in \mathbb{K}(a_1, \ldots, a_n)$ i $c \in \mathbb{K}(b, a_{n+1})$. ■

Twierdzenie 3.9 (O podniesieniu)**.** *Niech $\mathbb{K}$ bedzie ustalonym ciałem, niech $f \in \mathbb{K}[x]$ będzie nierozkładalnym wielomianem o współczynnikach z ciała $\mathbb{K}$ oraz $a, b \in \hat{\mathbb{K}}$ będą pierwiastkami w pewnym algebraicznym domknięciu ciała $\mathbb{K}$. To wtedy istnieje jedyne odwzorowanie $\sigma : \mathbb{K}(a) \to \mathbb{K}(b)$ pomiędzy ciałami $\mathbb{K}(a)$ a $\mathbb{K}(b)$ spełniające warunki:*

1. *$\sigma(a) = b$,*
2. *$x \in \mathbb{K}$ to $\sigma(x) = x$,*
3. *$\sigma(x + y) = \sigma(x) + \sigma(y)$ oraz $\sigma(xy) = \sigma(x)\sigma(y)$ dla dowolnych $x, y \in \mathbb{K}(a)$*
4. *σ jest różnowartościowe i na.*

Dowód. *Każdy element ciała $\mathbb{K}(a)$ daje się jednoznacznie przedstawić jako wartość wielomianu $h \in \mathbb{K}[x]$ w punkcie a, którego stopnień jest mniejszy niż $st(f)$. Jeśli σ byłoby izomorfizmem o własnościach wymienionych w treści tego twierdzenia, to $\sigma(a) = b$, $\sigma(a^2) = \sigma(a)\sigma(a) = b^2$ oraz $\sigma(a^k) = \sigma(a)^k = b^k$ o ile $k \in \mathbb{Z}_{st(f)}$.*

Niech $n = st(f)$, to w takim razie jeśli $y = \sum_{k=0}^{n-1} c_k a^k \in \mathbb{K}(a)$, wtedy odwzorowanie σ definiujemy następująco:

$$\sigma(y) = \sum_{k=0}^{n-1} c_k b^k \in \mathbb{K}(b).$$

Niech $\eta : \mathbb{K}(a) \to \mathbb{K}(b)$ *będzie dowolną funkcją spełniająca warunki naszego twierdzenia. Wtedy* $\eta(a^k) = b^k$ *dla* $k \in \mathbb{Z}_{st(f)}$ *i* $\eta(d) = d$ *dla dowolnego* $d \in \mathbb{K}$*. Więc dla dowolnego* $y \in \mathbb{K}(a)$ *istnieją* $c_0, \ldots, c_{st(f)}$ *takie że* $y = \sum_{k=0}^{st(f)-1} c_k a^k$*. Wówczas mamy*

$$\eta(y) = \eta(\sum_{k=0}^{st(f)-1} c_k a^k) = \sum_{k=0}^{st(f)-1} \eta(c)_k \eta(a)^k = \sum_{k=0}^{st(f)-1} c_k b^k = \sigma(y).$$

Stąd takie odwzorowanie (które spełnia założenia $(1)-(4)$*) jest co najwyżej jedno. Oczywiście* $\sigma(a) = b$*, odwzorowanie* σ *jest "na" oraz jest identycznością na ciele* $\mathbb{K}$*.*

Pokażemy teraz, że zachodzi $\sigma(uv) = \sigma(u)\sigma(v)$*. Niech* $h_1, h_2 \in \mathbb{K}[x]$ *takie, że* $u = h_1(a)$ *oraz* $v = h_2(a)$*. Istnieją jedyne takie wielomiany* $q, r \in \mathbb{K}[x]$ *które spełniają:*

$$h_1 \cdot h_2 = q \cdot f + r \quad \wedge \quad st(r) < st(f).$$

Wtedy mamy:

$$\begin{aligned}\sigma(uv) =& \sigma(h_1(a)h_2(a)) = \sigma((h_1h_2)(a)) = \sigma((qf+r)(a)) = \sigma(q(a)f(a) + r(a)) = \sigma(r(a)) \\ =& r(b) = (h_1h_2 - qf)(b) = h_1(b)h_2(b) - q(b)f(b) = h_1(b)h_2(b) - q(b) \cdot 0 \\ =& h_1(b)h_2(b) = \sigma(h_1(a))\sigma(h_2(a)) = \sigma(u)\sigma(v).\end{aligned}$$

Analogiczne rozumowanie dowodzi $\sigma(u+v) = \sigma(u) + \sigma(v)$*. Pokazaliśmy więc, że* σ *jest epimowrfizmem ciała* $\mathbb{K}(a)$ *na ciało* $\mathbb{K}(b)$*.*

Pokażemy, że σ *jest odwzorowaniem różnowartościowym. Jeśli jest niezerowe* $x \in \mathbb{K}(a)$ *takie, że* $\sigma(x) = 0$*, to wtedy mamy*

$$1 = \sigma(1) = \sigma(xx^{-1}) = \sigma(x)\sigma(x^{-1}) = 0 \cdot \sigma(x^{-1}) = 0,$$

co jest niemożliwe. Jeżeli $\sigma(u) = \sigma(v)$*, to* $\sigma(u - v) = 0$ *a stąd* $u - v = 0$ *czyli* $u = v$*. Więc* σ *jest różnowartościowe.*

Dowód twierdzenia jest zakończony. ■

Kluczową rolę w teorii Galois odgrywają tak zwane rozszerzenia normalne. Wtedy dla rozszerzeń normalnych $\mathbb{K} \subseteq \mathbb{L}$ grupy automorfizmów stałych na $\mathbb{K}$, są normalne. To jest integralną częścią zasadniczego twierdzenia teorii Galois o którym będzie mowa później.

Definicja 3.8 (Rozszerzenie normalne)**.** *Powiemy, że algebraiczne rozszerzenie* $\mathbb{K} \subseteq \mathbb{L}$ *jest normalne wtedy gdy dla dowolnego* $a \in \mathbb{L}$ *i dla dowolnego* $f \in \mathbb{K}[x]$ *nierozkładalnego nad ciałem* $\mathbb{K}$*, jeżeli* $f(a) = 0$ *to dla każdego* $x \in \hat{\mathbb{K}}$ *takiego że* $f(x) = 0$ *wynika że* $x \in \mathbb{L}$*.*

Krócej, jeśli wielomian nierozkładalny $f \in \mathbb{K}[x]$ *nad ciałem* $\mathbb{K}$ *ma przynajmniej jeden pierwiastek w* $\mathbb{L}$*, to wszystkie pierwiastki* f *należą do ciała* $\mathbb{L}$*.*

Łatwo można zauważyć, że każdy wielomian nierozkładalny mający ustalony pierwiastek w ciele $\mathbb{L}$ jest wielomianem minimalnym tego elementu i na odwrót, każdy $f \in \mathbb{K}[x]$ będacy wielomianem minimalnym elementu $a \in \mathbb{L}$ jest nierozkładalny nad $\mathbb{K}$. Więc w powyższej definicji możemy zastąpić frazę wielomian nierozkładalny nad $\mathbb{K}$ mający pierwiastek w $\mathbb{L}$ przez frazę wielomian minimalny pewnego elementu ciała $\mathbb{L}$.

Ciałem rozkładu wielomianu $x^2 - 2$ jest $\mathbb{Q}(\sqrt{2})$. Niech $f \in \mathbb{Q}[x]$ będzie wielominem minimalnym ustalonego elementu $x = a + b\sqrt{2}$ $(b \neq 0)$, to wtedy $(x-a)^2 = 2b^2$ a stąd

$f(x) = c\cdot(x^2-2ax+a^2-2b^2)$ dla pewnej stałej $c \in \mathbb{Q}$. Wówczas $x-y\sqrt{2}$ jest pierwiastkiem tago wielomianu. Więc wszystkie pierwiastki f są w ciele $\mathbb{Q}(\sqrt{2})$, co dowodzi normalności rozszerzenia $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$.

Natomiast ciało $\mathbb{Q}(\sqrt[3]{2})$ nie jest rozszerzeniem normalnym ciała $\mathbb{Q}$, ponieważ wielomian $f(x) = x^3-2$ jest nierozkładalny nad $\mathbb{Q}$, którego jedynym pierwiastkiem w tym rozszerzeniu jest $\sqrt[3]{2}$ a pozostałe $\sqrt[3]{2}e^{2\pi i/3}$ oraz $\sqrt[3]{2}e^{4\pi i/3}$ są pierwiastakmi f spoza $\mathbb{Q}(\sqrt[3]{2})$. Okazuje się, że ciało $\mathbb{Q}(\sqrt[3]{2}, \xi)$, gdzie $\xi = e^{2\pi i/3}$ jest już rozszerzeniem normalnym ciała $\mathbb{Q}$.

4. Rozszerzenia Galois

W tym rozdziale poznamy ważne związki pomiędzy rozszerzeniami ciał $\mathbb{K} \subseteq \mathbb{L}$ a ich grupą symetrii, czyli grupami Galois $G(\mathbb{L}/\mathbb{K})$.

Wprowadzimy kluczową definicję w teorii rozszerzeń ciał jak i w samej teorii Galois.

Definicja 4.1. *Niech $\mathbb{K} \subset \mathbb{L}$ jest dowolnym rozszerzeniem ciała $\mathbb{K}$ do ciała $\mathbb{L}$. Grupę rozważanego rozszerzenia nazywamy podgrupę grupy automorfizmów ciała $\mathbb{L}$ będącą identycznością na ciele $\mathbb{K}$ i oznaczmy przez $G(\mathbb{L}/\mathbb{K})$, co można zapisać jako:*

$$G(\mathbb{L}/\mathbb{K}) = \{\sigma \in Aut(\mathbb{L}) : (\forall x \in \mathbb{K})\ \sigma(x) = x\}.$$

Jak łatwo się przekonać jest to rzeczywiście podgrupa grupy automorfizmów ciała $\mathbb{L}$. Grupa $G(\mathbb{L}/\mathbb{K})$ rozszerzenia $\mathbb{K} \subseteq \mathbb{L}$ nazywamy też grupą Galois tegoż rozszerzenia.

Podamy poniżej dwa proste ale użyteczne związki pomiędzy rozszerzeniami skończonymi ciał a ich grupami Galois.

Fakt 4.1. *Niech $\mathbb{K} \subset \mathbb{L}$ jest skończonym, rozdzielczym rozszerzeniem, to zachodzi następująca równość:*

$$|G(\mathbb{L}/\mathbb{K})| \leq [\mathbb{L} : \mathbb{K}].$$

Dowód. *Na mocy twierdzenia Abela $\mathbb{L} = \mathbb{K}(a)$ i niech $f \in \mathbb{K}[x]$ będzie jego wielomianem minimalnym. Oczywiście $0 = \sigma(f(a)) = f(\sigma(a))$ dla dowolnego $\sigma \in G(\mathbb{L}/\mathbb{K})$. Na mocy poprzedniego twierdzenia 3.9 jeżeli $\tau \in G(\mathbb{L}/\mathbb{K})$ i $\sigma(a) = \tau(a)$, to $\sigma = \tau$. Więc liczba automorfizmów nie przekracza liczby pierwiastków wielomianu f, które są parami rózne (rozdzielczość rozszerzenia $\mathbb{K} \subset \mathbb{L}$).* ■

Fakt 4.2. *Jeżeli dane są skończone rozszerzenia ciał $\mathbb{K} \subseteq \mathbb{M} \subseteq \mathbb{L}$, to wtedy $G(\mathbb{L}/\mathbb{M}) \subseteq G(\mathbb{L}/\mathbb{K})$.*

Definicja 4.2 (Ciało elementów stałych)**.** *Mając podgrupę $G \leq G(\mathbb{L}/\mathbb{K})$ możemy zdefiniować specjalny podzbiór ciała $\mathbb{L}$ a mianowicie*

$$G^{\#} = \{x \in \mathbb{L} : (\forall \sigma \in G)\ \ \sigma(x) = x\}$$

Zbiór ten jest podciałem ciała $\mathbb{L}$ oczym można się łatwo przekonać i nazywamy **ciałem elementów stałych** grupy automorfizmów rozszerzenia $\mathbb{K} \subset \mathbb{L}$ i oczywiscie zachodzi inkluzja

$$\mathbb{K} \subset G^{\#} \subset \mathbb{L}.$$

Ponieważ ciało $\mathbb{Q}$ ze zwykłymi działaniami dodawania i mnożenia jest ciałem prostym, to każdy automorfizm ciała $\mathbb{L}$ zawierającego $\mathbb{Q}$ jako podciało, jest identycznością na $\mathbb{Q}$. W takim razie $\mathbb{Q}$ zawiera się w grupie elementów stałych względem grupy automorfizmów ciała $\mathbb{L}$.

Przejdźmy do przykładów.

Przyklad 4.1. *Rozważmy rozszerzenie $\mathbb{K} = \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) = \mathbb{L}$. Każdy element tego rozszerzenia jest postaci $a+b\sqrt{2}$, dla pewnych liczb wymiernych a, b Weźmy dowolny automorfizm z $G(\mathbb{L}/\mathbb{K})$. Wtedy $\sigma(a) = a$ i $\sigma(b) = b$, dalej $2 = \sigma(2) = \sigma(\sqrt{2}\sqrt{2}) = \sigma(\sqrt{2})\sigma(\sqrt{2})$. Więc $\sigma(\sqrt{2}) = \sqrt{2}$ lub $\sigma(\sqrt{2}) = -\sqrt{2}$. Więc $G(\mathbb{L}/\mathbb{K})$ ma co najwyżej dwa elementy, mianowicie identyczność $e(a + b\sqrt{2}) = a + b\sqrt{2}$ i sprzężenie $\sigma(a + b\sqrt{2}) = a - b\sqrt{2}$. Łatwo się przekonać, że sprzężenie też jest automorfizmem ciała $\mathbb{Q}(\sqrt{2})$. Więc $G(\mathbb{L}/\mathbb{K}) = \{e, \sigma\}$. i jedynymi podgrupami są grupa identycznościowa $\{e\}$ oraz cała grupa $G(\mathbb{L}/\mathbb{K})$. Oczywiście stopień naszego rozszerzenia wynosi 2, więc nie ma ciał pośrednich pomiędzy $\mathbb{Q}$ a $\mathbb{Q}(\sqrt{2})$. Opisane rozszerzenie jest normalne (co widzieliśmy w poprzednim rozdziele). Policzmy teraz ciała elementów stałych względem podgrupy $\{e\}$ i grupy $G(\mathbb{L}/\mathbb{K})$. Mianowicie, każdy element naszego rozszerzenia jest punktem stałym względem identyczności, więc $\{e\}^{\#} = \mathbb{L} = \mathbb{Q}(\sqrt{2})$. Natomiast $G(\mathbb{L}/\mathbb{K})^{\#} = \{e, \sigma\}^{\#} = \mathbb{Q}$. W tym celu załóżmy że dla pewnych $a, b \in \mathbb{Q}$ mamy $\sigma(a + b\sqrt{2}) = a + b\sqrt{2}$. Więc $a - b\sqrt{2} = a + b\sqrt{2}$, stąd $2b\sqrt{2} = 0$ a co zatym idzie, $b = 0$. Więc nasz dowolnie wybrany element, który jest stały wzlędem $G(\mathbb{L}/\mathbb{K})$ jest liczbą wymierną. Graficznie opisaną zależność możemy przedstawić tak:*

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \longleftarrow & \{e\} \\ \uparrow 2 & & \uparrow 2 \\ \mathbb{Q} & \longleftarrow & G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}). \end{array}$$

Przyklad 4.2. *Niech $\mathbb{K} = \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{L}$. Wiemy, że rozszerzenie to jest równe $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2})(\sqrt{3})$ i stopień tego rozszerzenia wynosi 4. Jedynymi podciałami $\mathbb{L}$ są $\mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})$ i $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Wielomianem minimalnym elementu $\sqrt{2} + \sqrt{3}$ jest $x^4 - 10x^2 + 1$. Oprócz liczby $\sqrt{2} + \sqrt{3}$ pierwiastkami tego wielomianu są $-(\sqrt{2} + \sqrt{3})$, $\sqrt{2} - \sqrt{3}$, $-(\sqrt{2} - \sqrt{3})$, które nadal są elementami ciała $\mathbb{Q}(\sqrt{2} + \sqrt{3})$. Nasze ciało można zapisać następująco:*

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : \ a, b, c, d \in \mathbb{Q}\}.$$

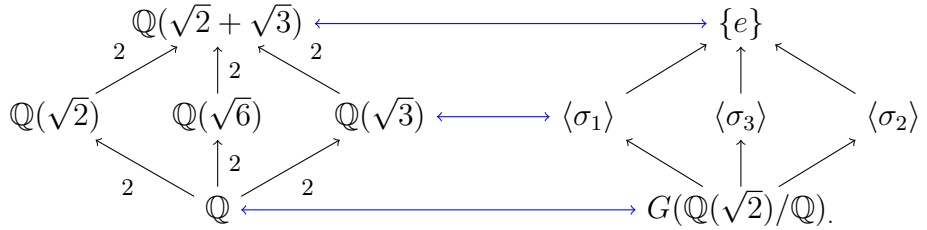
Każdy automorfizm σ ciała $\mathbb{L}$ jest taki, że $\sigma(\sqrt{2}) = \pm\sqrt{2}$ i $\sigma(\sqrt{3}) = \pm\sqrt{3}$. Pozostawiamy czytelnikowi do sprawdzenia, że $G(\mathbb{L}/\mathbb{K}) = \{e, \sigma_1, \sigma_2, \sigma_3\}$, gdzie:

$$\begin{aligned}
e(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6},\\
\sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6},\\
\sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6},\\
\sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.
\end{aligned}$$

Zauważmy, że dla $i \in \{1, 2, 3\}$ $\sigma_i^2 = e$, $\sigma_2\sigma_1 = \sigma_3 = \sigma_2\sigma_1$, $\sigma_1\sigma_3 = \sigma_2 = \sigma_3\sigma_1$ i analogicznie $\sigma_2\sigma_3 = \sigma_1 = \sigma_3\sigma_2$. Utwórzmy tabelkę działania w $G(\mathbb{L}/\mathbb{K})$.

$\cdot$	e	σ_1	σ_2	σ_3
e	e	σ_1	σ_2	σ_3
σ_1	σ_1	e	σ_3	σ_2
σ_2	σ_2	σ_3	e	σ_1
σ_3	σ_3	σ_2	σ_1	e

Patrząc na tabelkę działania tej grupy, widzimy, że jest taka sama ja tabelka czwórkowej grupy Kleina. Wiamy że czwórkowa grupa Kleina jest izomorficzna z iloczynem (sumą) prostą dwuelementowej grupy cyklicznej ze sobą: $G(\mathbb{L}/\mathbb{K}) \sim C_2 \oplus C_2$. Jedynymi podgrupami grupy $G(\mathbb{L}/\mathbb{K})$ są $\{e\}, \{e, \sigma_1\}, \{e, \sigma_2\}, \{e, \sigma_3\}$ oraz cała grupa $G(\mathbb{L}/\mathbb{K})$. Ciała elementów stałych względem tych podgrup są przedstawiają się następująco: $\{e\}^{\#} = \mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{L}$, $\{e, \sigma_1\}^{\#} = \mathbb{Q}(\sqrt{3})$, $\{e, \sigma_2\}^{\#} = \mathbb{Q}(\sqrt{2})$, $\{e, \sigma_3\}^{\#} = \mathbb{Q}(\sqrt{6})$, $G(\mathbb{L}/\mathbb{K})^{\#} = \mathbb{Q}$. Zależność pomiędzy ciałami i odpowiadającymi im podgrupami można przedstawić graficznie:



W obydwu przykładach rozważane rozszerzenia stanowiły ciało rozkładu wielomianu minimalnego elemntu generującego te ciało. Doszliśmy do wniosku, że rząd grupy $G(\mathbb{L}/\mathbb{K})$ jest równy $[\mathbb{L} : \mathbb{K}]$. W następnym przykładzie zobaczymy, jak przedstawia się sprawa w przypdaku rozszerzenia $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$.

Przyklad 4.3. *Rozszerzenie $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$, ma tę własność, że wielomian minimalny $f(x) = x^3 - 2$ elementu $\sqrt[3]{2}$ ma pierwiastki nie leżące w rozważanym ciele $\mathbb{Q}(\sqrt[3]{2})$. Oczywiście każdy automorfizm $\sigma \in G(\mathbb{Q}(\sqrt[3]{2}))/\mathbb{Q})$ przeprowadza pierwiastki (zawarte w ciele $\mathbb{Q}(\sqrt[3]{2})$) wiielomianu $f(x) = x^3 - 2$ na pierwiastki z tego ciała. Natomiast liczba $\sqrt[3]{2}$ jest jedynym pierwiastkie wielomianu f, który pochodzi z naszego ciała. Stąd wnosimy, że nasza grupa*

$G(\mathbb{Q}(\sqrt[3]{2}))/\mathbb{Q})$ jest trywialna. Stopień naszego rozszerzenia jest równy stopniowi wielomianu f i wynosi 3. mamy więc tutaj przypadek, w którym $|G(\mathbb{Q}(\sqrt[3]{2}))/\mathbb{Q})| < [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$.

W przypadku szczególnej klasy rozszerzeń ciał, taka sytuacja jak z powyższego przykładu nie zachodzi. Wtedy, jak się okaże, będziemy mieli jednoznaczną odpowiedniość pomiędzy podciałami naszego rozszerzenia a ich odpowiadającym podgrupom grupy automorfizmów rozważanego rozszerzenia.

Definicja 4.3 (Rozszerzenie Galois)**.** *Mówimy, że rozszerzenie $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem Galois wtedy i tylko wtedy gdy istnieje grupa $G \leq G(\mathbb{L}/\mathbb{K})$ tego rozszerzenia taka że ciało elementów stałych tej grupy jest ciało $\mathbb{K}$. Można to zapisać formułą:*

$$\mathbb{K} \subseteq \mathbb{L} \text{ jest rozszerzenie Galois} \longleftrightarrow (\exists G)\ (G \leq G(\mathbb{L}/\mathbb{K})\ \wedge\ G^{\#} = \mathbb{K}).$$

Twierdzenie 4.1. *Niech $\mathbb{K} \subset \mathbb{L}$ będzie skończonym rozszerzeniem rozdzielczym. Wtedy zachodzą następuujące warunki równoważne:*

1. *$\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem Galois,*
2. *Jeśli $f \in \mathbb{K}[x]$ jest wielomianem minimalnym pewnego elementu $a \in \mathbb{L}$, to wszystkie jego pierwiastki należą do $\mathbb{L}$, ($\mathbb{K} \subseteq \mathbb{L}$ jest rozszerzeniem normalnym),*
3. *Ciało $\mathbb{L}$ jest ciałem rozkładu pewnego wielomianu $f \in \mathbb{K}[x]$,*
4. *$[\mathbb{L} : \mathbb{K}] = |G(\mathbb{L}/\mathbb{K})|$,*
5. *$\mathbb{K} = (G(\mathbb{L}/\mathbb{K}))^{\#}$.*

Dowód. *($1 \to 2$). Niech $f \in \mathbb{K}[x]$ takim wielomianem minimalnym elementu $a \in \mathbb{L}$ stopnia n. Niech $k < n$ taka, że $a_1, \ldots, a_k \in \mathbb{L}$ są wszystkimi pierwiastkami wielomianu f z ciała $\mathbb{L}$. Ponieważ $\mathbb{K} \subseteq \mathbb{L}$ jest rozszerzeniem Galois, więc istnieje podgrupa $G \leq G(\mathbb{L}/\mathbb{K})$ taka, że $G^{\#} = \mathbb{K}$. Weźmy dowolny automorfizm $\sigma \in G$, to $\sigma(a_i) \in \mathbb{L}$ oraz pierwiastek przechodzi na pierwiastek wielomianu f. Niech $g(x) = (x - a_1) \ldots (x - a_k) = b_0 + b_1 x + b_2 x^2 + \ldots + b_{k-1} x^{k-1} + x^k$. Ponieważ wszystkie pierwiastki wielomianu g są w ciele $\mathbb{L}$, to wszystkie jego współczynniki również są elementami ciała $\mathbb{L}$ (więc $g \in \mathbb{L}[x]$). Pokażemy, że nasz wielomian g jest elementem $\mathbb{K}[x]$. Niech σ bedzie dowolnym elementem wspomnianej wyżej grupy G i niech $g_\sigma \in \mathbb{L}[x]$ będzie zdefiniowane następująco:*

$$g_\sigma(x) = \sigma(b_0) + \sigma(b_1)x + \ldots + \sigma(b_{k-1})x^{k-1} + x^k.$$

Jeżeli $x_i \in \mathbb{L}$ jest dowolnym pierwiaskiem wielomianu g, to wtedy istnieje jakiś pierwiastek x_j wielomianu g dl którego zachodzi $x_i = \sigma(x_j)$. Wtedy

$$\begin{aligned} g_\sigma(x_i) &= g_\sigma(\sigma(x_j)) = \sigma(b_0) + \sigma(b_1)\sigma(x_j) + \ldots + \sigma(b_{k-1})(\sigma(x_j))^{k-1} + (\sigma(x_j))^k \\ &= \sigma(g(x_j)) = \sigma(0) = 0. \end{aligned}$$

Ponieważ wielomian g_σ ma stopień k i $\{a_1, \ldots, a_k\}$ są jego pierwiastkami, to wtedy

$$g_\sigma(x) = (x - a_1) \ldots (x - a_k) = g(x).$$

Z równości wielomianów g i g_σ wynika, że mają one te same współczynniki[2] *tj. dla dowolnego $i \in \{0,\dots,k\}$ $\sigma(b_i) = b_i$ (tutaj $b_k = 1 = \sigma(1) = \sigma(b_k)$). Ponieważ $\sigma \in G$ było wybrane w sposób dowolny, to spółczynniki wielomianu nie ulegają zmianie pod działaniem dowolnego automorfizmu z G. Ponieważ $\mathbb{K} = G^\#$ jest ciałem elementów stałych względem grupy G, to wszystkie współczynniki wielomianu g są z ciała $\mathbb{K}$. Innymi słowy, $g \in \mathbb{K}[x]$ i oczywiście $stg = k < n = stf$, $g(a) = 0$, co prowadzi do sprzeczności, wobec minimalności wielomianu $f \in \mathbb{K}[x]$.* ■

Dowód. $2 \to 3$ *Ponieważ $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem skończonym, więc z twierdzenia Abela istnieje $a \in \mathbb{L}$ takie że $\mathbb{L} = \mathbb{K}(a)$. Wtedy, biorąc jego wielomian minimalny $f \in \mathbb{K}[x]$ ($f(a)=0$) z 2 wynika, że wszystkie jego pierwiastki są w $\mathbb{L}$ co dowodzi 3.* ■

Dowód. $3 \to 4$ *Na mocy wniosku 4.1 mamy $|G(\mathbb{L}/\mathbb{K})| \leq [\mathbb{L} : \mathbb{K}]$, więc wystarczy udowodnić nierówność w drugą stronę. Niech $\mathbb{L}$ będzie ciałem rozkładu wielomianu $f \in \mathbb{K}[x]$ stopnia n nad ciałem $\mathbb{K}$. Więc wszystkie pierwiastki sa w ciele $\mathbb{L}$ oraz je generują tzn. $\mathbb{L} = \mathbb{K}(a_1,\dots,a_n)$ i $f(a_i) = 0$. Na podstawie twierdzenia Abela, istnieje $c \in \mathbb{L}$ takie, że $\mathbb{L} = \mathbb{K}(c)$, weźmy jego wielomian minimalny $g \in \mathbb{K}[x]$ stopnia m. Niech $\{c_1, c_2, \dots, c_m\}$ będzie zbiorem wszystkich pierwiastków wielomianu g, należacymi do algebraicznego domkniecia ciała $\mathbb{K}$. Możemy założyć, że $c_1 = c$. Więc stopień rozszerzenia $\mathbb{K} \subset \mathbb{L}$ jest równy m. Z twierdzenia 3.9 o podniesieniu wynika, że każdy pierwiastek c_i generuje bijekcję $\sigma_i : \mathbb{K}(c) \mapsto \mathbb{K}(c_i)$, która $\sigma_i(c) = c_i$, zachowuje działania dodawania i mnożenia oraz jest identycznością na ciele $\mathbb{K}$. Pierwiastki są parami różne, bo to jest rozszerzenie rozdzielcze.*

A priori, nie wiemy czy wszystkie pierwiastki wielomianu g są w ciele $\mathbb{L}$. Pokażemy, że każde σ_i odwzorowuje ciało $\mathbb{L}$ na siebie (więc w szczególności rozważane pierwiastki są w $\mathbb{L}$). Wybierzmy dowolny pierwiastek a wielomianu f. Ponieważ $\mathbb{L}$ jest ciałem rozkładu f, to $a \in \mathbb{L}$. Widzimy że

$$0 = \sigma_i(0) = \sigma_i(f(a)) = f(\sigma_i(a)),$$

tak więc, skoro $\sigma_i(a)$ jest pierwiaskiem f, to $\sigma_i(a) \in \mathbb{L}$. Tak więc σ_i zadaje pewną permutację elementów zbioru wszystkich pierwiastków $a_1,\dots,a_n$ wielomianu f. Każdemu elementowi $y \in \mathbb{L} = \mathbb{K}(a_1,\dots,a_n)$ odpowiada funkcja wymierna h n zmiennych o współczynnikach z ciała $\mathbb{K}$, taki że $y = h(a_1,\dots,a_n)$. Wówczas

$$\sigma_i(y) = \sigma_i(h(a_1,\dots,a_n)) = h(\sigma_i(a_1),\dots,\sigma_i(a_n))$$

wówczas $\sigma_i(y) \in \mathbb{K}(a_1,\dots,a_n)$. W szczególności $c_i = \sigma_i(c) \in \mathbb{K}(a_1,\dots,a_n) = \mathbb{L}$. Więc wszystkie pierwiastki wielomianu g są w ciele $\mathbb{L}$. Zauważmy, że dowolnego $i \leq m$ mamy $\sigma_i[\mathbb{K}(c)] = \mathbb{K}(c_i) \subseteq \mathbb{L}$. Ponieważ $[\mathbb{L} : \mathbb{K}] = [\mathbb{K}(c) : \mathbb{K}] = m = [\mathbb{K}(c_i) : \mathbb{K}]$, więc $\mathbb{L} = \mathbb{K}(c) = \mathbb{K}(c_i)$ dla dowolnego $i \leq m$. Ostatecznie σ_i odwzorowuje $\mathbb{L}$ na siebie.

Stąd $\sigma_i \in G(\mathbb{L}/\mathbb{K}))$ są automorfizmem rozszerzenia $\mathbb{K} \subset \mathbb{L}$ dla każdego $i \in \{1,\dots,m\}$. Więc rząd grupy $G(\mathbb{L}/\mathbb{K})$ jest taki sam jak stopień g a więc $|G(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$, co dowodzi powyższej inkluzji. ■

Dowód. $4 \to 5$ *Niech $\mathbb{M} = (G(\mathbb{L}/\mathbb{K}))^\#$. Wystarczy pokazać, że z warunku 4 wynika $\mathbb{K} = \mathbb{M}$. Oczywiście mamy $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, więc wystarczy dowieść $\mathbb{M} \subset \mathbb{K}$.*

[2]Można to również udowodnić, stosując wzory Viety, bo współczynniki wielomianu wyrażają się przez symetryczne wielomiany zależne od wszystkich pierwiastków tego wielomianu.

Wpierw udowodnimy, że $G(\mathbb{L}/\mathbb{K}) = G(\mathbb{L}/\mathbb{M})$. *Ponieważ zachodzi inkluzja* $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$, *to wtedy* $G(\mathbb{L}/\mathbb{M}) \subset G(\mathbb{L}/\mathbb{K})$. *Teraz inkluzja w drugą stronę. Niech* $\sigma \in G(\mathbb{L}/\mathbb{K})$ *będzie dowolnym automorfizmem rozszerzenia* $\mathbb{K} \subset \mathbb{L}$. *Ponieważ* $\mathbb{M}$ *jest ciałem elementów stałych względem grupy* $G(\mathbb{L}/\mathbb{K})$, *to dla dowolnego* $x \in M$ *mamy* $\sigma(x) = x$ *a stąd* $\sigma \in G(\mathbb{L}/\mathbb{M})$. *Ponieważ* $\sigma \in G(\mathbb{L}/\mathbb{K})$ *było dowolne, to wtedy* $G(\mathbb{L}/\mathbb{K}) \subset G(\mathbb{L}/\mathbb{M})$. *Tak więc mamy udowodniona równość* $G(\mathbb{L}/\mathbb{K}) = G(\mathbb{L}/\mathbb{M})$.

Korzystając z wniosku 4.1, który mówi, że zachodzi $|G(\mathbb{L}/\mathbb{M})| \leq [\mathbb{L} : \mathbb{M}]$ *i na mocy założenia* $|G(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}]$, *mamy następujące równości:*

$$|G(\mathbb{L}/\mathbb{K})| = [\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{M}][\mathbb{M} : \mathbb{K}] \geq |G(\mathbb{L}/\mathbb{M})|[\mathbb{M} : \mathbb{K}] = |G(\mathbb{L}/\mathbb{K})|[\mathbb{M} : \mathbb{K}].$$

Więc $[\mathbb{M} : \mathbb{K}] \leq 1$, *co razem z* $\mathbb{K} \subset \mathbb{M}$ *daje* $\mathbb{K} = \mathbb{M} = (G(\mathbb{L}/\mathbb{K}))^{\#}$. ■

Dowód. $5 \to 1$ *Ponieważ na podstwie* (5) *mamy* $\mathbb{K} = (G(\mathbb{L}/\mathbb{K}))^{\#}$, *to ciało* $\mathbb{K}$ *jest ciałem elementów stałych względem grupy* $G(\mathbb{L}/\mathbb{K})$ *co daje* (1) *i kończy dowód całego twierdzenia.* ■ ■

Wniosek 4.1. *Jeśli* $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$ *jest ciągiem ciał i jeśli* $\mathbb{K} \subset \mathbb{L}$ *jest rozszerzeniem Galois, to* $\mathbb{M} \subset \mathbb{L}$ *jest tez nim.*

Dowód. *Jeśli* $\mathbb{K} \subset \mathbb{L}$ *jest rozszerzeniem Galois, to* $\mathbb{L}$ *jest ciałem rozkładu pewnego wielomianu* $f \in \mathbb{K}[x]$ *o współczynnikach z* $\mathbb{K}$ *a więc tez o współczynnikach z* $\mathbb{M}$ *więc* $\mathbb{M} \subset \mathbb{L}$ *jest tez rozszerzeniem Galois.* ■

Na mocy twierdzenia 4.1 wnosimy, że rozszerzenia $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ oraz $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$ są rozszerzeniami Galois, ponieważ są ciałami rozkładu pewnych wielomianów o współczynnikach wymiernych (patrz przyklady 4.1. i 4.2 odpowiednio).

Fakt 4.3. *Niech* $\mathbb{K} \subset \mathbb{L}$ *będzie rozszerzeniem ciał, załóżmy, że istnieje* $n \in \mathbb{N}$ *takie, że stopień każdego elementu ciała* $\mathbb{L}$ *nie przekracza* n, *to stopień tego rozszerzenia nie przekracza* n *t.j.* $[\mathbb{L} : \mathbb{K}] \leq n$.

Twierdzenie 4.2. *Jeśli* $\mathbb{K} \subset \mathbb{L}$ *jest skończonym rozszerzeniem Galois oraz* $H < G(\mathbb{L}/\mathbb{K})$ *będzie podgrupą grupy wszystkich automorfizmów ciała* $\mathbb{L}$ *stałych na podciele* $\mathbb{K}$, *to* $[\mathbb{L} : H^{\#}] = |H|$.

Dowód. (Artina) *Wpierw zauważmy, że jeśli* $H < G(\mathbb{L}/\mathbb{K})$, *to* $\mathbb{K} \subset H^{\#} \subset \mathbb{L}$*: biorąc* $x \in \mathbb{K}$ *i* $\sigma \in H$ *to* $\sigma \in G(\mathbb{L}/\mathbb{K})$ *a więc*

$$\sigma x = x \to x \in H^{\#} = \{y \in \mathbb{L} : \ \forall \tau \in H \ \tau y = y\} \subset \mathbb{L}.$$

Wiemy że $\mathbb{K} \subset \mathbb{L}$ *jest rozszerzeniem Galois oraz* $\mathbb{K} \subset H^{\#} \subset \mathbb{L}$ *dostajemy, że* $H^{\#} \subset \mathbb{L}$ *jest rozszerzeniem Galois a więc*

$$[\mathbb{L} : H^{\#}] = |G(\mathbb{L}/H^{\#})|.$$

Wybierzmy dowolny element ciała $\mathbb{L}$, *niech to będzie* $y \in \mathbb{L}$. *Niech* $\{\sigma_1 y, \ldots, \sigma_k y\}$ *będzie maksymalnym ze względu na inkluzję, skończonym podzbiorem* $\mathbb{L}$, *to wtedy*

$$\forall \tau \in H \ \ \{\tau\sigma_1 y, \ldots, \tau\sigma_k y\} = \{\sigma_1 y, \ldots, \sigma_k y\} \wedge y \in \{\sigma_1 y, \ldots, \sigma_k y\}.$$

Niech $f_y(x) = \prod_{i=1}^{k}(x - \sigma_i y)$, *to współczynniki tego wielomianu nie ulegają zmianie pod działaniem elementów grupy* H *(korzystamy ze wzorów Viety). Wiec* $f_y \in H^{\#}[x]$, *ponadto* $f_y(y) = 0$ *bo* $y \in \{\sigma_1 y, \dots \sigma_k y\}$, *więc ostatecznie mamy:*

$$\forall y \in \mathbb{L} \;\; st\, y \leq st f_y \leq |H|.$$

Stosując powyższy fakt (zastepując w nim $\mathbb{K}$ *przez* $H^{\#}$*) otrzymujemy nierówność* $[\mathbb{L} : H^{\#}] \leq |H|$.

Zauważmy że $H \subset G(\mathbb{L}/H^{\#})$*:*

$$\sigma \in H \wedge x \in H^{\#} \to \sigma x = x \to \sigma \in G(\mathbb{L}/H^{\#}).$$

Więc

$$|H| \leq |G(\mathbb{L}/H^{\#})| = [\mathbb{L} : H^{\#}] \leq |H|,$$

co dowodzi żądaną równość. ■

Dowód. Inne rozumowanie - drobna modyfikacja. *Zauważmy że* $H \subset G(\mathbb{L}/H^{\#})$*:*

$$\sigma \in H \wedge x \in H^{\#} \to \sigma x = x \to \sigma \in G(\mathbb{L}/H^{\#}).$$

Stad mamy

$$|H| \leq |G(\mathbb{L}/H^{\#})| \leq [\mathbb{L} : H^{\#}].$$

Rozszerzenie $\mathbb{K} \subset \mathbb{L}$ *jest skończone, więc* $H^{\#} \subset \mathbb{L}$ *jest też rozszerzeniem skończonym. Istnieje więc element algebraiczny* $a \in \mathbb{L}$ *taki że* $\mathbb{L} = H^{\#}(a)$. *Niech więc* $f \in H^{\#}[x]$ *będzie wielomianem minimalnym elementu* a. *Stąd* $[\mathbb{L} : H^{\#}] = st(f)$. *Niech* $n = st(f)$ *i załóżmy że* $|H| = m < st(f) = n$ *oraz* $H = \{\sigma_1, \dots, \sigma_m\}$. *Ponumerujmy wszystkie pierwiastki* $a = x_1, x_2, \dots, x_n$ *wielomianu* f *w algebraicznym domknięciu zawierającym ciało* $\mathbb{L}$. *Oczywiście kazdy automorfizm z* H *przekształca* a *na jakiś pierwiastek wielomianu* f *należący do ciała* $\mathbb{L}$. *Wartość na* $a \in \mathbb{L}$ *każdego automorfizmu* $\sigma \in H$ *wyznacza dokładnie jeden taki automorfizm (patrz dowód twierdzenia o podniesieniu). Więc*

$$(\forall \sigma, \eta \in H) \;\; \sigma \neq \eta \to \sigma(a) \neq \eta(a).$$

Niech $g(x) = \prod_{\sigma \in H}(x - \sigma(a)) = (x - \sigma_1(a))(x - \sigma_2(a)) \dots (x - \sigma_m(a))$, *to stosując wzory Viety na współczynniki tego wielomianu mamy:*

$$\begin{aligned}
c_m &= 1 \\
(-1)c_{m-1} &= \sum_{\sigma \in H} \sigma(a) \\
&\vdots = \vdots \\
(-1)^k c_{m-k} &= \sum_{s \in [H]^k} \prod_{\sigma \in s} \sigma(a) \\
&\vdots = \vdots \\
(-1)^m c_0 &= \prod_{\sigma \in H} \sigma(a).
\end{aligned}$$

Tutaj mamy $[H]^k = \{s \in \mathscr{P}(H) : |s| = k\}$. *Niech* $\eta \in H$ *będzie dowolnym automorfizem z grupy* H, *to wtedy mamy:*

$$\begin{aligned}
\eta(c_m) =& \eta(1) = 1 \\
\eta((-1)c_{m-1}) =& \eta(\sum_{\sigma\in H} \sigma(a)) = \sum_{\sigma\in H} \eta\sigma(a) = \sum_{\sigma\in H} \sigma(a) = (-1)c_{m-1} \\
\vdots =& \vdots \\
\eta((-1)^k c_{m-k}) =& \eta(\sum_{s\in[H]^k} \prod_{\sigma\in s} \sigma(a)) = \sum_{s\in[H]^k} \prod_{\sigma\in s} \eta\sigma(a) = \sum_{s\in[H]^k} \prod_{\sigma\in s} \sigma(a) = (-1)^k c_{m-k} \\
\vdots =& \vdots \\
\eta((-1)^m c_0) =& \eta(\prod_{\sigma\in H} \sigma(a)) = \prod_{\sigma\in H} \eta\sigma(a) = \prod_{\sigma\in H} \sigma(a) = (-1)^m c_0.
\end{aligned}$$

Więc współczynniki wielomianu g *nie ulegają zmianie pod działaniem każdego automorfizmu z grupy* H, *stąd współczynniki te należą do ciała* $H^{\#}$ *a więc* $g \in H^{\#}[x]$. *Oczywiście* $id \in H$, *więc* $g(a) = 0$ *i* $st(g) = m < n = st(f)$, *co jest niemożliwe wobec minimalności wielomianu* f. *Więc* $[\mathbb{L} : H^{\#}] = n \leq |H|$ *a stąd mamy* $[\mathbb{L} : H^{\#}] = |H|$, *co kończy dowód naszego twierdzenia.* ■

5. Twierdzenia Galois

Jak wspomnieliśmy wcześniej, kazdemu podciału $\mathbb{M} \subset \mathbb{L}$ odpowiada grupa $G(\mathbb{L}/\mathbb{M})$ automorfizmów ciała $\mathbb{L}$, stałych na ciele $\mathbb{M}$ oraz kazdej grupie $G \subset G(\mathbb{L}/\mathbb{K})$ odpowiada ciało elementów stałych $G^{\#} \subset \mathbb{L}$ wzdlędem grupy G.

Związek pomiędzy grupami a ciałami wyjaśnia następujące

Twierdzenie 5.1 (I-Twierdzenie Galois)**.** *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem Galois, wtedy istnieje jeden jednoznaczna odpowiedniość pomiędzy ciałami $\mathbb{M}$, które są rozszerzeniami Galois $\mathbb{M} \subset \mathbb{L}$ a podgrupami $G \subset G(\mathbb{L}/\mathbb{K})$ automorfizmów ciała $\mathbb{L}$, stałych na $\mathbb{M}$.*

Neich będzie dane rozszerzenie ciał $\mathbb{K} \subset \mathbb{L}$, to wtedy definiujemy dwie rodziny w sposób następujący:

$$\mathscr{M} = \{\mathbb{M} \in \mathscr{P}(\mathbb{L}) : \ \mathbb{K} \subset \mathbb{M} \subset \mathbb{L}\} \text{ – wszystkie podciała pośrednie,}$$

$$\mathscr{G} = \{H \in \mathscr{P}(G(\mathbb{L}/\mathbb{K})) : \ H < G(\mathbb{L}/\mathbb{K})\} \text{ – wszystkie podgrupy.}$$

Powyższe twierdzenie wynika wprost z lematu:

Lemat 5.1. *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem Galois. Określmy odwzorowania:*

$$\mathscr{G} \ni G \mapsto h(G) = G^{\#} \in \mathscr{M}$$

$$\mathscr{M} \ni \mathbb{M} \mapsto f(\mathbb{M}) = G(\mathbb{L}/\mathbb{M}) \in \mathscr{G}.$$

to wtedy

$$f \circ h = \mathbf{I}d_{\mathscr{G}} \text{ oraz } h \circ f = \mathbf{I}d_{\mathscr{M}}.$$

Dowód. *Niech $G \in \mathscr{G}$, to wtedy $fh(G)$ jest grupą automorfizmów ciała $\mathbb{L}$ stałych na $h(G) = G^{\#}$ czyli*

$$fh(G) = G(\mathbb{L}/G^{\#})$$

Zauważmy że mamy $G \subset G(\mathbb{L}/G^{\#})$ a z drugiej strony:

$$|fh(G)| = |G(\mathbb{L}/G^{\#})| = [\mathbb{L} : G^{\#}] = |G|$$

pierwsza równość jest z definicji odwzorowań, druga wynika z faktu, że $G^{\#} \subset \mathbb{L}$ jest rozszerzeniem Galois a ostatnia jest prawdziwa na mocy twierdzenia4.2. Więc $fh = \mathbf{I}d_{\mathscr{G}}$.

Teraz pokazemy drugą identyczność. Niech $\mathbb{M} \in \mathscr{M}$, to $\mathbb{M} \subset hf(\mathbb{M}) = f(\mathbb{M})^{\#} = G(\mathbb{L}/\mathbb{M})^{\#}$ ale

$$[\mathbb{L} : G(\mathbb{L}/\mathbb{M})^{\#}][G(\mathbb{L}/\mathbb{M})^{\#} : \mathbb{M}] = [\mathbb{L} : \mathbb{M}] = |G(\mathbb{L}/\mathbb{M})| = [\mathbb{L} : G(\mathbb{L}/\mathbb{M})^{\#}],$$

ostatnia równość zachodzi na podstawie twierdzenia4.2, natomiast przedostatnia wynika z faktu, że $\mathbb{M} \subset \mathbb{L}$ jest rozszerzeniem Galois. Więc oczywiście mamy

$$[G(\mathbb{L}/\mathbb{M})^{\#} : \mathbb{M}] = 1$$

czyli $hf(\mathbb{M}) = G(\mathbb{L}/\mathbb{M})^{\#} = \mathbb{M}$ co kończy dowód lematu. ■

Twierdzenie 5.2 (II-Twierdzenie Galois)**.** *Jeśli $\mathbb{K} \subset \mathbb{M} \subset \mathbb{L}$ jest ciągiem ciał i niech $\mathbb{K} \subset \mathbb{M}$ jest rozszerzeniem Galois, to $\mathbb{K} \subset \mathbb{M}$ jest rozszerzeniem Galois wtedy i tylko wtedy gdy $G(\mathbb{L}/\mathbb{M})$ jest dzielnikiem normalnym $G(\mathbb{L}/\mathbb{K})$. Co więcej*

$$G(\mathbb{M}/\mathbb{K}) \equiv G(\mathbb{L}/\mathbb{K})/G(\mathbb{L}/\mathbb{M}).$$

Dowód. *Niech $\mathbb{K} \subset \mathbb{M}$ będzie rozszerzeniem Galois niech $\sigma \in G(\mathbb{L}/\mathbb{M})$ i $\tau \in G(\mathbb{L}/\mathbb{K})$ będą dowolnymi automorfizmami. Dowód zakończymy jeśli pokazemy $\tau^{-1}\sigma\tau \in G(\mathbb{L}/\mathbb{M})$. Na mocy twierdzenia Abela mamy $\mathbb{M} = \mathbb{K}(a)$ i jego wielomian minimalny $f \in \mathbb{K}[x]$. Wtedy na mocy twierdzenia wszystkie jego pierwiastki leżą w $\mathbb{M}$ więc $\tau(a) \in \mathbb{M}$. Stąd mamy:*

$$\tau^{-1}\sigma\tau(a) = \tau^{-1}\tau(a) = a \text{ poniewaz } \sigma \in G(\mathbb{L}/\mathbb{M}).$$

Więc, jeśli $x \in \mathbb{M}$ to $x = g(a)$ dla pewnego $g \in \mathbb{K}[x]$. Czyli

$$\begin{aligned}\tau^{-1}\sigma\tau(x) &= g(\tau^{-1}\sigma\tau(a)) \\ &= g(a) = x,\end{aligned}$$

czyli $\tau^{-1}\sigma\tau \in G(\mathbb{L}/\mathbb{M})$. Co dowodzi, że $G(\mathbb{L}/\mathbb{M})$ jest dzielnikiem normalnym grupy $G(\mathbb{L}/\mathbb{K})$.

Teraz udowodnimy wynikanie w drugą stronę. Załózmy, że $G(\mathbb{L}/\mathbb{M}) \triangleleft G(\mathbb{L}/\mathbb{K})$, to

$$\tau^{-1}\sigma\tau(a) = a \ \text{ a stąd } \sigma\tau(a) = \tau(a)$$

gdzie $\mathbb{M} = \mathbb{K}(a)$ na mocy twierdzenia Abela, więc jeśli $x \in \mathbb{M}$ to $x = g(a)$ oraz $g \in \mathbb{K}[x]$ to

$$\sigma\tau(x) = \tau(x) \text{ tutaj } \tau \in G(\mathbb{L}/\mathbb{K}) \text{ jest dowolne .}$$

Poniewaz $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem Galois, to równiez $\mathbb{M} \subset \mathbb{L}$ jest nim co pociąga za sobą $\tau(x) \in G(\mathbb{L}/\mathbb{M})^{\#} = \mathbb{M}$. Niech $f \in \mathbb{K}[x]$ st $f = n$ będzie wielomianem minimalnym $a \in \mathbb{M}$. Tak więc wszystkie pierwiastki $a = x_1, \ldots x_n$ wielomianu f są w ciele $\mathbb{L}$. Oczywiście

$$\mathbb{M} \ni a \to \tau_i(a) = x_i \in \mathbb{L}$$

rozszerza się do automorfizmu $\tau_i \in G(\mathbb{L}/\mathbb{K})$ na podstawie twierdzenia o podniesieniu do izomorfizmu. Ale pokazaliśmy wcześniej, że jeśli $\tau \in G(\mathbb{L}/\mathbb{K})$ to $\tau(\mathbb{M}) \subset \mathbb{M}$ więc $x_i = \tau_i(a) \in \mathbb{M}$ czyli ciało $\mathbb{M}$ jest ciałem rozkładu wielomianu $f \in \mathbb{K}[x]$ co dowodzi, że $\mathbb{K} \subset \mathbb{M}$ jest rozszerzeniem Galois.

Teraz pokazemy ostatnią równość. Tak jak pokazaliśmy $\tau(\mathbb{M}) \subset \mathbb{M}$ o ile $\tau \in G(\mathbb{L}/\mathbb{K})$ (istotne jest załozenie że $\mathbb{K} \subset \mathbb{M}$ oraz $\mathbb{K} \subset \mathbb{L}$ są rozszerzeniami Galois).

Skonstruujmy następujące odwzorowanie:

$$G(\mathbb{L}/\mathbb{K}) \ni \tau \to h(\tau) = \tau \restriction \mathbb{M} \in G(\mathbb{M}/\mathbb{K})$$

które jest hommomorfizmem oraz:

$$\begin{aligned}\ker h &= \{\tau \in G(\mathbb{L}/\mathbb{K}) : \ h(\tau) = e \in G(\mathbb{M}/\mathbb{K})\} \\ &= \{\tau \in G(\mathbb{L}/\mathbb{K}) : \ \tau|_{\mathbb{M}} = e \in G(\mathbb{M}/\mathbb{K})\} \\ &= \{\tau \in G(\mathbb{L}/\mathbb{K}) : \ \tau(x) = x \in \mathbb{M}\} \\ &= G(\mathbb{L}/\mathbb{M}).\end{aligned}$$

i oczywiście $Im\, h \subset G(\mathbb{M}/\mathbb{K})$

$$\begin{aligned} Im\, h &= |G(\mathbb{L}/\mathbb{K})||G(\mathbb{L}/\mathbb{M})|^{-1} = [\mathbb{L}:\mathbb{K}][\mathbb{L}:\mathbb{M}]^{-1} \\ &= [\mathbb{L}:\mathbb{M}][\mathbb{M}:\mathbb{K}][\mathbb{L}:\mathbb{M}]^{-1} = [\mathbb{M}:\mathbb{K}] = G(\mathbb{M}/\mathbb{K}). \end{aligned}$$

Stosując teraz dobrze znane twierdzenie o hommomorfiźmie grup mamy:

$$G(\mathbb{M}/\mathbb{K}) \sim G(\mathbb{L}/\mathbb{K})/\ker\, h \sim G(\mathbb{L}/\mathbb{K})/G(\mathbb{L}/\mathbb{M}),$$

co kończy dowód tego twierdzenia. ■

6. Rozszerzenia pierwiastnikowe

Rozdział ten zaczniemy od definicji rozszerzenia pierwiastnikowego. W całym rozdziale założymy, że ciało $\mathbb{K}$ zawiera wszystkie pierwiastki z jedności dowolnego naturalnego i niezerowego stopnia.

Definicja 6.1 (Rozszerzenie pierwiastnikowe)**.** *Powiemy że rozszerzenie $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem pierwiastnikowym jeśli następujące warunki są spełnione:*

1. *Istnieje skończony rosnący względem inkluzji ciąg ciał $\mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \mathbb{K}_n$, taki że $\mathbb{K} = \mathbb{K}_0$ i $\mathbb{L} = \mathbb{K}_n$,*
2. *każde rozszerzenie $\mathbb{K}_{i-1} \subset \mathbb{K}_i$ jest cykliczne, to znaczy istnieje ciąg $\langle a_i \in \mathbb{K}_i : i \in \{1, \ldots, n\}\rangle$ taki że:*
   (a) $\forall i \in \{1, \ldots, n\}\ \mathbb{K}_i = \mathbb{K}_{i-1}(a_i)$,
   (b) $\forall i \in \{1, \ldots, n\} \exists n_i \in \mathbb{N} \setminus \{0\}\ a_i^{n_i} \in \mathbb{K}_{i-1}$.

Następujące lematy okazą ie użyteczne:

Lemat 6.1. *Jesli skończone rozszerzenie $\mathbb{K} \subset \mathbb{L}$ jest cykliczne, to grupa Galois tego rozszerzenia $G(\mathbb{L}/\mathbb{K})$ jest cykliczna.*

Dowód. *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem cyklicznym. Wtedy istnieją $n \in \mathbb{N}$ i $a \in \mathbb{L}$ takie że, $\mathbb{L} = \mathbb{K}(a)$ oraz $a^n \in \mathbb{K}$. Możemy założyć, że nasze n jest najmniejszą dodatnią liczbą naturalną, takż że $a^n \in \mathbb{K}$. Niech $b = a^n \in \mathbb{K}$, to wtedy $\mathbb{L}$ jest ciałem rozkładu wielomianu $f(x) = x^n - b \in \mathbb{K}[x]$. Zakładając fakt, że $\mathbb{L}$ zawiera wszystkie pierwiastki z jedności stopnia n $\{\xi_i : i \in \{0, \ldots, n-1\}\}$, $\{a\xi_i : 0 \leq i < n\} \subseteq \mathbb{L}$ jest zbiorem wszystkich pierwiatków wielomianu $x^n - b$. Na mocy założenia o liczbie n, wielomian f jest wielomianem minimalnym elementu a. Więc $G(\mathbb{L}/\mathbb{K})$ ma rząd co najwyżej n. Z drugiej strony, dla $\sigma \in G(\mathbb{L}/\mathbb{K})$ takiego że $\sigma(a) = a\xi_1$ mamy $\{\sigma^i : i < n\} \leq G(\mathbb{L}/\mathbb{K})$. Z minimalności liczby n, grupa $\{\sigma^i : i < n\}$ jest rzędu n, co w rezultacie daje równość $G(\mathbb{L}/\mathbb{K}) =< \sigma >= \{\sigma^i : i < n\}$.* ■

Kolejny lemat pochodzi od Lagrange'a.

Lemat 6.2 (Lagrange)**.** *Jeśli skończona grupa $G(\mathbb{L}/\mathbb{K})$ rozszerzenia Galois $\mathbb{K} \subset \mathbb{L}$ jest cykliczna, to te rozszerzenie jest cykliczne.*

Dowód. *Niech $\mathbb{K} \subseteq \mathbb{L}$ będzie skończonym rozszerzeniam Galois, takim że grupa $G(\mathbb{L}/\mathbb{K})$ jest cykliczna rzędu n. Niech $a \in \mathbb{L}$ będzie elementem pierwotnym naszego rozszerzenia ciał i $f \in \mathbb{K}[x]$ będzie jego wielomianem minimalnym takim że $f(x) = c_0 + c_1 x + \ldots + c_n x^n$. Wtedy $st(f) = [\mathbb{L} : \mathbb{K}] = |G(\mathbb{L}/\mathbb{K})| = n$ (rozszerzenie nasze jest rozszerzeniem Galois, więc $[\mathbb{L} : \mathbb{K}] = |G(\mathbb{L}/\mathbb{K})|$). Jeżeli pokażemy, że dla pewnego $m \in \mathbb{N}$ zachodzi $a^m \in \mathbb{K}$, to dowód będzie zakończony.*

Niech σ będzie generatorem grupy cyklicznej $G(\mathbb{L}/\mathbb{K})$ oraz $\xi = e^{2\pi i/n}$ będzie pierwotnym pierwiastkiem z 1 stopnia n. Definiujemy wielomian

$$g(x) = \sum_{k<n} \xi^k \sigma^k(x) = c_0 + \xi c_1 \sigma(x) + \ldots + \xi^{n-1} \sigma^{n-1}(x)$$

Wtedy

$$\begin{aligned}\sigma(g(x)) =&\sigma(\sum_{k<n}\xi^k\sigma^k(x)) = \sum_{k<n}\xi^k\sigma^{k+1}(x) = \xi^{-1}\sum_{k<n}\xi^{k+1}\sigma^{k+1}(x)\\ =&\xi^{-1}\sum_{k<n}\xi^k\sigma^k(x) = \xi^{-1}g(x).\end{aligned}$$

Więc dla dowolnego i mamy

$$\sigma^i(g(x)) = \xi^{-i}g(x).$$

Załóżmy, że jeżeli $g(x) \neq 0$, to zbiór $\{\sigma^i(g(x)) : i < n\}$ jest n-elementowy.

$$\sigma(g^n(x)) = (\sigma(g(x)))^n = (\xi^{-1}g(x))^n = g^n(x).$$

Więc dla każdego $i < n$ mamy $\sigma^i(g^n(x)) = g^n(x)$. Stąd mamy $g^n(x) \in \mathbb{K}$ (bo $G(\mathbb{L}/\mathbb{K}) = \{\sigma^i : i < n\}$). Pozostaje więc wykazać, że istnieje $x \in \mathbb{L} = \mathbb{K}(a)$ takie, że $g(x) \neq 0$. Skorzystamy z faktu o liniowej niezależności grupy $Aut(G)$ w przestrzeni wszystkich funkcji $\mathbb{L}^{\mathbb{L}}$ nad ciałem $\mathbb{K}$, twierdzenie 7.10 w Appendixie 7. o automorfizmach ciał.

Mianowicie, na mocy twierdzenia 7.10 , $G(\mathbb{L}/\mathbb{K})$ jest zbiorem liniowo niezależnym, więc jest $x \in \mathbb{L}$ takie, że dla $n = rz(G(\mathbb{L}/\mathbb{K}))$

$$\sum_{k<n}\xi_k\sigma^k(x) \neq 0.$$

Czyli jest $x \in \mathbb{L}$ takie, że $g(x) \neq 0$. ■

Twierdzenie 6.1 (Zasadnicze twierdzenie Galois)**.** *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem Galois, to na to aby $\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \ldots \subset \mathbb{K}_n = \mathbb{L}$ było rozszerzeniem pierwiastnikowym potrzeba i wystarcza aby istniał ciąg grup $\{e\} = G_n < \ldots < G_i < G_{i-1} < \ldots < G_0 = G(\mathbb{L}/\mathbb{K})$ o następujących własnościach:*

(1) $\forall i \in \{1, \ldots, n\}$ $G_{i-1} \lhd G_i$,
(2) $\forall i \in \{1, \ldots, n\}$ G_i/G_{i-1} *jest grupą cykliczną.*

Dowód. " $\rightarrow$ ". *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem Galois które jest pierwiastnikowe o takim ciągu podciał jak jest w twierdzeniu. Niech $G_i = G(\mathbb{L}/K_i)$, to wtedy mamy ciąg*

$$G(\mathbb{L}/\mathbb{K}) = G(\mathbb{L}/\mathbb{K}_0) = G_0 \supset G_1 \supset \ldots G_{n-1} \supset G_n = G(\mathbb{L}/\mathbb{K}_n) = G(\mathbb{L}/\mathbb{L}) = \{e\}$$

podgrup takich że $G_i < G_{i-1}$ dla $i \in \{1 \ldots, n\}$. Z założenia $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem Galois oraz $\mathbb{K} \subset \mathbb{K}_i \subset \mathbb{L}$, to $\mathbb{K}_i \subset \mathbb{L}$ jest rozszerzeniem Galois oraz $\mathbb{K}_{i-1} \subset \mathbb{K}_i \subset \mathbb{L}$ dla każdego $i \in \{1 \ldots, n\}$. $\mathbb{K}_{i-1} \subset \mathbb{K}_i \subset \mathbb{L}$ jest rozszrzeniem cyklcznym więc jest rozszerzeniem Galois oraz na mocy drugiego twierdzenia Galois $G_i \lhd G_{i-1}$ jest dzielnikiem normalnym dla $i \in \{1 \ldots, n\}$. Stosując jeszcze raz drugie twierdzenie Galois, mamy $G(\mathbb{K}_{i-1}/\mathbb{K}_i) = G_{i-1}/G_i$ ale $\mathbb{K}_{i-1} \subset \mathbb{K}_i$ jest rozszrzeniem cyklcznym dla $\mathbb{K}_{i-1} \subset \mathbb{K}_i$ jest rozszrzeniem cyklcznym Stąd ostatecznie na mocy lematu 6.1 G_{i-1}/G_i jest grupą cykliczna dla $i \in \{1, \ldots, n\}$.

" $\leftarrow$ ". *Nich będzie dany ciąg grup spełniający warunki naszego twierdzenia. Niech $\mathbb{K}_i = G_i^{\#}$ będzie ciałem elementów stałych względem grupy G_i. Teraz zastosujemy lemat*

5.1. Niech $\mathscr{G} \ni G \mapsto h(G) = G^{\#} \in \mathscr{M}$, $\mathscr{M} \ni M \mapsto f(M) = G(\mathbb{L}/M) \in \mathscr{G}$ *będą odwzorowaniami pomiędzy rodzinami* $\mathscr{G}$ *wszystkich podgrup grupy* $G(\mathbb{L}/\mathbb{K})$ *a* $\mathscr{M}$ *wszystkimi podciałami pośrednimi pomiędzy* $\mathbb{K} \subset \mathbb{L}$. *To z lematu 5.1 mamy*

$$G_i = id(G_i) = fh(G_i) = f(G_i^{\#}) = G(\mathbb{L}/G_i^{\#}) = G(\mathbb{L}/\mathbb{K}_i).$$

Więc mamy $\mathbb{K}_i = G_i^{\#} = (G(\mathbb{L}/\mathbb{K}_i))^{\#}$ *co dowodzi, że* $\mathbb{K}_i \subset \mathbb{L}$ *jest rozszerzeniem Galois dla* $i \in \{1, \ldots, n\}$. *Oczywiście mamy inkluzję* $\mathbb{K}_{i-1} \subset \mathbb{K}_i \subset \mathbb{L}$ *dla* $i \in \{1, \ldots, n\}$. *Wiemy, że* $G_i \lhd G_{i-1}$ *i* G_{i-1}/G_i *jest cykliczna, to na mocy II twierdzenia Galois mamy* $G(\mathbb{K}_i/\mathbb{K}_{i-1}) = G_{i-1}/G_i$ *jest grupą cykliczną, więc na mocy lematu 6.2 rozszerzenie* $\mathbb{K}_{i-1} \subset \mathbb{K}_i$ *jest cykliczne dla* $i \in \{1, \ldots, n\}$, *co dowodzi, że rozszerzenie* $\mathbb{K} \subset \mathbb{L}$ *jest rozszerzeniem pierwiastnikowym.* ■

7. Grupy rozwiązalne oraz przykłady rozszerzeń, które nie są pierwiastnikowe

Definicja 7.1 (Grupa rozwiązalna)**.** *$(G,\cdot)$ jest grupą rozwiązalną wtedy i tylko wtedy gdy istnieje skończony rosnący ciag podgrup grupy G:*

$$\{e\} = G_0 < G_1 < \ldots < G_i < \ldots < G_n = G,$$

taki że

(1) $\forall i \in \{1,\ldots,n\}\ \ G_{i-1} \lhd G_i$,
(2) $\forall i \in \{1,\ldots,n\}\ \ G_i/G_{i-1}$ *jest cykliczna.*

Fakt 7.1. *Jeśli G jest rozwiązalna a $H < G$, to H też jest rozwiązalna.*

Dowód. *Niech będzie dany ciąg $(G_i)_{i=0}^n$ świadczący, że G jest rozwiązalna. Niech $H_i = H \cap G_i$ będzie ciągiem podgrup grupy H. Pokażemy że nasz ciąg $(H_i)_{i=0}^n$ świadczy że H jest grupą rozwiązalną. Niech $\sigma \in H_{i-1}$ a $\tau \in H_i$, to $\tau^{-1}\sigma\tau \in G_{i-1}$ ale $H_{i-1} < H_i < H$ więc $\tau^{-1}\sigma\tau \in H$ więc $\tau^{-1}\sigma\tau \in G_{i-1} \cap H = H_{i-1}$. Więc mamy*

$$\{e\} = H_0 \lhd \ldots \lhd H_n = H.$$

Pokażemy że H_i/H_{i-1} jest grupą cykliczną. Niech $x \in H_i/H_{i-1}$ to jest $a \in H_i$, dla k/torego $x = [a]_H = \{b \in H_i :\ \exists h \in H_{i-1}\ \ b = ah\} \subset [a]_G = \{b \in G_i :\ \exists h \in G_{i-1}\ \ b = ah\} = \tau$, gdzie τ jest generatorem grupy G_i/G_{i-1} rzędu $n \in \mathbb{N}$.

$$\bigcup_{i=0}^{n-1}[a]_H = \bigcup_{i=0}^{n-1}\{ah \in H_i :\ h \in H_{i-1}\}$$

$$= \bigcup_{i=0}^{n-1}\{ah \in H_i :\ h \in G_{i-1} \cap H\}$$

■

Przyklad 7.1. *S_3 jest rozwiązalna. Grupa alternująca $A_3 = \{(123),(231),(312)\}$ jest dzielnikiem normalnym rzędu 3, więc z twierdzenia Lagrange'a o indeksie grup skończonych $rz(S_3/A_3) = [S_3 : A_3] = \frac{|S_3|}{|A_3|} = 6/3 = 2$. Więc S_3/A_3 jest grupą cykliczną rzędu 2, $S_3/\{e\} \approx A_3$ jest grupą cykliczną rzędu 3. Wtedy ciąg $\{e\} \lhd A_3 \lhd S_3$ świadczy o rozwiązalności grupy S_3.*

Przyklad 7.2. *A_5 nie jest rozwiązalna, więc S_5 nie jest rozwiązalna. Niech $\{e\} \neq H \subseteq A_5$ będzie dzienikiem normalnym grupu wszystkich permutacji parzystych w S_5. Pokażemy ze $H = A_5$, a więc $H/\{e\} \cong A_5$ nie jest abelowa a więc, nie jest grupą cykliczną. Niech $a \in A_5 \setminus \{e\}$. Rozważymy trzy przypadki, mianowicie gdy a jest cyklem długości 5 lub 4, oraz a ma najdłuższy cykl 3 i 2. W pierwszym przypadku bez straty ogólności możemy założyć, że $a = (12345)$ lub $a = (1234)$. Niech $b = (123) \in A_5$, wtedy*

$$H \ni a^{-1}b^{-1}ab = \begin{pmatrix}23451\\12345\end{pmatrix}\begin{pmatrix}23145\\12345\end{pmatrix}\begin{pmatrix}12345\\23451\end{pmatrix}\begin{pmatrix}12345\\23145\end{pmatrix} = \begin{pmatrix}12345\\13542\end{pmatrix} = (235)$$

Dla $a = (1234)$, $b = (123)$

$$H \ni a^{-1}b^{-1}ab = \begin{pmatrix} 23415 \\ 12345 \end{pmatrix}\begin{pmatrix} 23145 \\ 12345 \end{pmatrix}\begin{pmatrix} 12345 \\ 23415 \end{pmatrix}\begin{pmatrix} 12345 \\ 23415 \end{pmatrix} = \begin{pmatrix} 12345 \\ 13245 \end{pmatrix} = (235)$$

Twierdzenie 7.1. *Jeżeli* $n > 3$, $\mathbb{Q} \subset \mathbb{K} \subseteq \mathbb{C}$ *i dany wielomian* $f(x) = a_0 + a_1x + \ldots + a_{n-3}x^{n-3} + a_nx^n \in \mathbb{K}[x]$ *stopnia* n *ma jedynie pierwiaski rzeczywiste, to* $f(x) = a_nx^n$.

Dowód. *Stosując wzory Viety:*

$$0 = \frac{a_{n-1}}{a_n} = x_1 + \ldots + x_n \quad oraz \quad 0 = \frac{a_{n-2}}{a_n} = \sum_{1 \le i < j \le n} x_ix_j,$$

mamy

$$x_1^2 + \ldots + x_n^2 = (\sum_{i=1}^{n} x_i)^2 - 2\sum_{1 \le i < j \le n} x_ix_j = 0 - 0 = 0.$$

Więc mamy $x_1 = \ldots x_n = 0$, *co w rezultacie daje* $f(x) = a_nx^n$. ■

Twierdzenie 7.2. *Niech* $p \ge 5$ *będzie liczba pierwszą,* $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{R}$ *będzie ciałem liczbowym oraz* $f(x) = x^p + a_{p-3}x^{p-3} + \ldots + a_0 \in \mathbb{K}[x]$ *wielomianem nierozkładalnym nad ciałem* $\mathbb{K}$. *Niech* $\mathbb{L}$ *będzie ciałem rozkładu wielomianu* f. *Jeżeli* f *ma dokładnie* 2 *różne pierwiastki zespolone* $z, \bar{z}$, *to* $\mathbb{K} \subset \mathbb{L}$ *nie jest rozszerzeniem pierwiatnikowym.*

Dowód. *Zauważmy, że każdy automorfizm* $\sigma \in G(\mathbb{L}/\mathbb{K})$ *jest permutacją wszystkich pierwiastków wielomianu* f. *Niech* $z, \bar{z}$ *bedą różnymi pierwiastkimi wielomianu* f. *Wtedy istnieje* $\sigma_1 \in G(\mathbb{L}/\mathbb{K})$ *takie że,* $rz(\sigma_1) = 2$ *i* $\sigma(z) = \bar{z}$. *Z drugiej strony, jeśli liczba* $a \in \mathbb{L}$ *jest pierwiastkiem* f, *to z nierozkładalności* f *nad* $\mathbb{K}$ *wynika, że* f *jest wielomianem minimalnym* a. *Stąd mamy* $[\mathbb{K}(a) : \mathbb{K}] = p$ *a więc* $p|[\mathbb{L} : \mathbb{K}]$. *Ponieważ* $\mathbb{L}$ *jest ciałem rozkładu wielomianu* $f \in \mathbb{K}[x]$, *to* $\mathbb{K} \subset \mathbb{L}$ *jest rozserzeniem Galois, co daje* $p|[\mathbb{L} : \mathbb{K}] = rzG(\mathbb{L}/\mathbb{K})$. *Więc, na mocy twierdzenia Lagrange'a istnieje permutacja* $\sigma \in S_p$ *rzędu* p. *Ponieważ liczba* p *jest pierwsza, to* σ *jest permutacją cykliczną rzędu* p. *Bez straty ogólności,* $\sigma_1 = (1\ 2)$, *natomiast dla* σ *istnieje* $k \le n$, *takie że,* $\sigma^k = (1\ 2\ \ldots)$. *Po ewentualnym przenumerowaniu zbioru* $\{3, 4, \ldots, p\}$, *możemy przyjąć, że* $\sigma = (1\ 2\ 3\ \ldots\ n)$ *jest cyklem długości* p *kolejnych liczb naturalnych. Ponieważ dla dowolnej transpozycji* $(i\ i+1)$ *mamy* $(i\ i+1) = \sigma^{-(i-1)}(1\ 2)\sigma^{i-1}$ *i każda permutacja w* S_p *da się przedstawić jako iloczyn transpozycji dwóch elementów sąsiednich, to mamy* $G(\mathbb{L}/\mathbb{K}) = S_p$. *Ponieważ liczba pierwsza* p *jest nie mniejsza niż* 5, *to* S_p *a więc i* $G(\mathbb{L}/\mathbb{K})$ *nie jest grupą rozwiązalną. Ostateczmie na mocy zasadniczego twierdzenia 6.1 teorii Galois, rozszerzenie Galois* $\mathbb{K} \subseteq \mathbb{L}$ *nie jest pierwiastnikowe.* ■

Przyklad 7.3. *Niech* $f(x) = x^5 - 9x + 3$ *będzie wielomianem stopnia piątego o współczynnikach całkowitych. Zauważmy że dla liczby* $q = 3$ *możemy zastosować kryterium Eisensteina do wielomianu* f, *więc* f *nie jest rozkładalny nad* $\mathbb{Z}$ *a więc też nad ciałem* $\mathbb{Q}$. *Zauważmy, że*

$$f(-2) = -2^5 + 18 + 3 = -10 < 0 < 3 = f(0) \ oraz\ f(1) = -5 < 0 < 17 = f(2).$$

Na mocy twierdzenia 7.1 nasz wielomian ma dokładnie 3 *pierwiastki rzeczywiste i dwa różne pierwiastki zespolone sprzężone do siebie nawzajem. Na mocy ostatniego twierdzenia 7.2,*

ciało rozkładu wielomianu f jest niepierwiastnikowym rozszerzeniem Galois ciała $\mathbb{Q}$. Więc ostatecznie, pierwiastki wielomianu f nie dają się wyrazić wzorami przez pierwiastniki.

Literatura

[1] M. Bryński, Elementy teorii Galois, Wydawnictwo Alfa z serii Delta przedstawia, 1985.
[2] J. Browkin, Teoria ciał, Biblioteka matematyczna tom 49, Warszawa PWN, 1977.
[3] Serge Lang, Algebra, Warszawa PWN, 1973.
[4] Wikipedia, `https://en.wikipedia.org/wik/Cubic_function`.

Appendix A. Zasadnicze twierdzenie algebry

Do dowodu twierdzenia będącego tytułem niniejszego appendixu wykorzystamy następujące dwa twierdzenia

Twierdzenie 7.3. *Twierdzenie Niech $f \in \mathbb{K}[x]$ będzie wielomianem o współczynnikach z ciała $\mathbb{K}$, to istnieje ciało $\mathbb{L}$ takie, że jest ciałem rozkładu wielomianu f.*

Dowód. *Dowód przeprowadzimy przez indukcję względem stopnia wielomianu $f \in \mathbb{K}[x]$. Dla wielomianu stopnia pierwszego teza jest oczywista. Niech $f \in \mathbb{K}[x]$ będzie wielomianem nad ciałem $\mathbb{K}$, to albo on ma pierwiastek i stosujemy wtedy krok indukcyjny względem ilości pierwiastków albo nasz wielomian nie posiada pierwiasków w ciele $\mathbb{K}$. W tym drugim przypadku istnieje wielomian minimalny $f_0 \in \mathbb{K}[x]$ który dzieli nasz wielomian $f \in \mathbb{K}[x]$. Wówczas niech $\mathbb{L} \equiv \mathbb{K}[x]/f_0$ (tutaj $f_1 \sim f_2 \longleftrightarrow f_1 - f_2 \equiv 0 \mod f_0 \longleftrightarrow f_0 | f_1 - f_2$), który jest ciałem zawierającym wielomiany stałe $c \in \mathbb{K}$ stąd $\mathbb{K} \subset \mathbb{L}$. Oczywiście mamy $f \in \mathbb{L}[x]$, niech $x_0 \in \mathbb{L}$ będzie wielomianem identycznościowym tzn. $x_0(x) = x$, to wtedy mamy:*

$$f(x_0) = f(x) \equiv 0 \mod f_0 \in \mathbb{L},$$

więc istnieje ciało w którym wielomian posiada pierwiastek skąd

$$f(x) = (x - x_0)g(x), \qquad g \in \mathbb{L}[x]$$

i stosując założenie indukcyjne do wielomianu $g \in \mathbb{L}[x]$ mamy tyle pierwiastków co stopień wielomianu f w pewnym ciele $\mathbb{L}' \supset \mathbb{L} \supset \mathbb{K}$. ■

Twierdzenie 7.4. *Zasadnicze twierdzenie o wielomianach symetrycznych Jeśli $f \in \mathbb{R}[x_1, \ldots, x_n]$ jest wielomianem symetrycznym, to istnieje dokładnie jeden wielomian $h \in \mathbb{R}[x_1, \ldots, x_n]$ taki że:*

$$f(x_1, \ldots, x_n) = h(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n)),$$

gdzie $s_1, \ldots, s_n \in \mathbb{R}[x_1, \ldots, x_n]$ są elementarnymi wielomianami symetrycznymi (o grupie symetrii S_n).

Teraz możemy sformułować nasze tytułowe twierdzenie:

Twierdzenie 7.5. *Zasadnicze Twierdzenie Algebry Niech $f \in \mathbb{C}[x]$ będzie wielomianem o współczynnikach zespolonych, to istnieje taka liczba zespolona $c \in \mathbb{C}$, że $f(c) = 0$.*

Dowód. *Wpierw rozpatrzymy wielomiany $f \in \mathbb{R}[x]$*

$$f(x) = a_m x^m + \cdots + a_1 x + a_0,$$

których stopień jest parzysty $\operatorname{st} f = m = 2^n k$ (k jest nieparzyste) i udowodnimy te twierdzenie właśnie dla takich wielomianów przez indukcję względem n.

Z pierwszego twierdzenia istnieje ciało $\mathbb{L} \supset \mathbb{C}$ które jest ciałem rozkładu wielomianu

$$g(x) = (x^2 + 1)\, f(x) \text{ oczywiście } g \in \mathbb{C}[x].$$

Oznaczmy wszystkie jego pierwiastki przez $u_i \in \mathbb{L}$ $i = 1, \ldots, n$ (pomijamy pierwiastki i oraz $\bar{i}$). Teraz wybierzmy dowolną liczbę rzeczywistą $a \in \mathbb{R}$ i niech $v_{i,j} = u_i u_j + a(u_i + u_j) \in \mathbb{L}$ Wprowadźmy wielomian

$$f_a(x) = (x - v_{1,2}) \ldots (x - v_{m-1,m})$$

którego stopień jest równy

$$st\, f_a = \binom{m}{2} = \frac{2^n k(2^n k-1)}{2} = 2^{n-1}k(2^n k-1).$$

Przyjmując za b_i współczynniki wielomianu f_a tzn.

$$f_a(x) = b_{st\, f_a} x^{st\, f_a} + \ldots + b_1 x + b_0$$

i korzystając że wzorów Viet'y mamy:

$$(-1)^i\, b_i = s_i(v_{1,2}, \ldots, v_{m-1,m}) = h(u_1, \ldots, u_m)$$

Łatwo zauważyć, że $h \in \mathbb{R}[x_1, \ldots, x_m]$ jest równiez wielomianem symetrycznym ze względu na grupę S_m. Stosując więc zasadnicze twierdzenie o wielomianach symetrycznych mamy

$$(-1)^i\, b_i = g(s_1(u_1, \ldots, u_m), \ldots, s_m(u_1, \ldots, u_m)) = g(a_1, \ldots, a_m)$$

dla pewnego wielomianu $g \in \mathbb{R}[x_1, \ldots, x_m]$.

Więc stopień parzystości się zmniejszył o jeden i nasz wielomian $f_a \in \mathbb{R}[x]$ ma współczynniki rzeczywiste, wobec czego, możemy zastosować indukcję matematyczną z której wynika istnienie pary i, j takiej, że $u_{i,j} \in \mathbb{C}$.

Dla różnych a, a' istnieje taka para i, j, że $v_{i,j} \in \mathbb{R}$

$$c_i = u_i u_j + a(u_i + u_j) \quad oraz \quad c_i' = u_i u_j + a'(u_i + u_j).$$

stąd

$$u_i + u_j = \frac{c_i - c_i'}{a - a'} \in \mathbb{C} \quad oraz \quad u_i u_j = c_i - a\frac{c_i - c_i'}{a_i - a_i'} \in \mathbb{C}$$

Stąd wielomian zdefiniowany następująco

$$w(x) = (x - u_i)(x - u_j) = x^2 - (u_i + u_j)x + u_i\, u_j$$

ma współczynniki zespolone $w \in \mathbb{C}[x]$ i stosując wzory na pierwiastki trójmianu kwadratowego dochodzimy do wniosku, ze $w(u_i) = w(u_j) = 0$ i $u_i, u_j \in \mathbb{C}$. Stąd pokazaliśmy, że kazdy wielomian rzeczywisty o stopniu parzystym ma pewien pierwiastek zespolony.

Teraz możemy przejść do dowolnego wielomianu $f \in \mathbb{C}[x]$

$$f(x) = \sum_{i=0}^{n} a_i\, x^i \;\; gdzie\; a_i \in \mathbb{C}.$$

Wówczas biorąc za g wielomian

$$g(x) = f(x)\overline{f}(x) = \sum_{i=0}^{2n} b_i x^i$$

widzimy, że jego stopień jest parzysty oraz jego współczynniki są rzeczywiste $g \in \mathbb{R}[x]$ bo

$$\overline{b_i} = \overline{\sum_{k=0}^{i} a_k \overline{a_{i-k}}} = \sum_{k=0}^{i} \overline{a_k} a_{i-k} = b_i.$$

Więc istnieje $c \in \mathbb{C}$ która jest pierwiastkiem g ($g(c) = 0$). Stąd

$$g(c) = f(c)\overline{f}(c) = 0,$$

więc albo $f(c) = 0$ co kończy dowód albo

$$\overline{f}(c) = 0$$

stąd $f(\overline{c}) = 0$ co kończy dowód zasadniczego twierdzenia algebry. ■

Lemat 7.1. *Każdy wielomian $f \in \mathbb{C}[z]$, którego stopień jest większy bądź równy jedności jest nieograniczony w następującym sensie:*

$$\forall M \geq 0 \exists R > 0 \forall z \in \mathbb{C} \;\; R < |z| \to M < |f(z)|.$$

Dowód. *Lemat ten udowodnimy przez indukcję względem stopnia wielomianu f. Jeśli $st\ f = 1$ to tezę pozostwiamy do udowodnienia czytelnikowi. Załóżmy że teza lematu jest prawdziwa dla wszystkich wielomianów dodatniego stopnia mniejszego niż n. Niech $st\ f = n$, jeśli $f(z) = a_n \cdot z^n + a_0$ to warunek w tezie jest spełniony w niemal oczywisty sposób. W pozostałym przypadku, $f(z) = z \cdot h(z) + a_0$ i $1 \leq st\ h < n$. Korzystamy teraz z założenia indukcyjnego dla wielomianu h. Załóżmy że $M > 0$ i niech $R > 1$ będzie takie że dla każdego $z \in \mathbb{C}$ dla którego spełniony jest warunek $R < |z|$ zachodzi nierówność $M + |a_0| < |h(z)|$ to wtedy mamy:*

$$|f(z)| = |z \cdot h(z) + a_0| \geq |z \cdot h(z)| - |a_0| > |h(z)| - |a_0| > M + |a_0| - |a_0| = M,$$

dla $|z| > R$. Korzystając z zasady indukcji skończonej otrzymjemy tezę, co kończy dowód naszego lematu. ■

Twierdzenie 7.6 (Zasadnicze tw. algebry, Gauss (1799))**.** *Każdy wielomian zespolony $f \in \mathbb{C}[z]$, którego stopień jest nie mniejszy niż 1 ma pierwiastek.*

Dowód. *Niech $f \in \mathbb{C}[z]$ będzie wielomianem o następującej postaci $f(z) = \sum_{k=0}^{n} a_k z^k$. Stosując powyższy lemat, istnieje $R > 1$ dla którego zachodzi następująca inkluzja $D := \{z \in \mathbb{C} : \; |f(z)| \leq |a_0|\} \subset K_R := \{z \in \mathbb{C} : \; |z| \leq R\}$, gdzie D jest jest domknięty i ograniczony w $\mathbb{C}$. Wtedy na mocy twierdzenia Weierstrassa o osiąganiu kresów, istnieje $z_0 \in D \subset K_R$ takie że $|f(z_0)| = \min\{|f(z)| : \; z \in \mathbb{C}\}$ jest kresem dolnym wszystkich modułów wartości wielomianu f. Udowodnimy teraz że $f(z_0) = 0$. Jeśli nie, to $|f(z_0)| > 0$ i wtedy dla każdego $z = z_0 + r \cdot e^{i\phi}$ mamy*

$$f(z_0 + re^{i\phi}) = f(z_0) + \sum_{k=0}^{n} b_k r^k e^{ik\phi}.$$

Niech $k_0 = \min\{k < n : \ b_k \neq 0\}$, *to dla* $r \in (0,1)$ *i* $\phi = \frac{\pi - arg(b_{k_0})}{k_0}$ *mamy:*

$$|f(z_0 + re^{i\phi})| = |f(z_0) + \sum_{k=k_0}^{n} b_k r^k e^{ik\phi}| \leq |f(z_0) + b_{k_0} r^{k_0} e^{i\phi k_0}| + |\sum_{k=k_0+1}^{n} b_k r^k e^{ik\phi}|$$

$$\leq |f(z_0) + b_{k_0} r^{k_0} e^{i\phi k_0}| + \sum_{k=k_0+1}^{n} |b_k| r^k \leq |f(z_0) + b_{k_0} r^{k_0} e^{i\phi k_0}|$$

$$+ n \max\{|b_k| : \ k = 0, ..., n\} r^{k_0+1} = |f(z_0)| - |b_{k_0}| r^{k_0} + C r^{k_0+1} < |f(z_0)|,$$

gdzie $C = n \max\{|b_k| : \ k = 0, ..., n\}$ *i wystarczająco małego* r, *co prowadzi do sprzeczności. W ten sposób, dowód istnienia* $z_0 \in \mathbb{C}$ *dla którego* $f(z_0) = 0$ *został zakończony.* ■

Appendix B. Twierdzenie o algebraicznym domknięciu ciała

Twierdzenie 7.7. *Każde ciało zawarte jest w ciele algebraicznie domkniętym.*

Dowód. *Niech* $\mathbb{K}$ *będzie dowolnym ciałem. Zbudujemy ciąg ciał* $(\mathbb{K}_n)_{n\in\mathbb{N}}$ *o następujących własnościach:*

(1) $\mathbb{K}_0 = \mathbb{K}$,
(2) $(\forall n \in \mathbb{N})(\mathbb{K}_n \subseteq \mathbb{K}_{n+1})$,
(3) $(\forall n \in \mathbb{N})(\forall f \in \mathbb{K}_n[x])$ ($\mathbb{K}_{n+1}$ *zawiera ciało rozkładu wielomianu* f).

Wówczas, jak łatwo sprawdzić $\hat{\mathbb{K}} = \bigcup_{n\in\mathbb{N}} \mathbb{K}_n$ *jest ciałem. Niech* $f(x) = a_0 + \ldots + a_n x^n \in \hat{\mathbb{K}}$, *wtedy istnieje* $m \in \mathbb{N}$ *dla którego* $a_0, \ldots a_n \in \mathbb{K}_m$. *Więc* $f \in \mathbb{K}_m[x]$ *i korzystając z ostatniego punktu, istnieją elementy* $x_1, \ldots, x_n \in \mathbb{K}_{m+1}$ *takie, że* $f(x) = a_n(x - x_1) \ldots (x - x_n)$.

Załóżmy, że mamy ciąg $\mathbb{K}_0 \subset \ldots \subset \mathbb{K}_n$ *o własnościach* $(1) - (3)$. *Ponumerujmy* $\mathbb{K}_n[x] = \{f_\xi : \xi < \kappa\}$, *zbudujemy ciąg ciał* $(\mathbb{L}_\xi)_{\xi<\kappa}$ *taki że*

(1) $\mathbb{L}_0 = \mathbb{K}_n$,
(2) *dla dowolnych* $\alpha < \beta < \kappa$ *mamy* $\mathbb{L}_\alpha \subseteq \mathbb{L}_\beta$,
(3) *dla każdego* $\xi < \kappa$, *ciało* $\mathbb{L}_{\xi+1}$ *zawiera ciało rozkładu wielomianu* f_ξ.

Załóżmy, że dla $\xi < \kappa$ *mamy ciąg ciał* $(L_\eta)_{\eta<\xi}$ *mający wyżej wymienione własności. Jeżeli* ξ *jest graniczna, to rozważmy* $\mathbb{L}_\xi = \bigcup_{\eta<\xi} \mathbb{L}_\eta$ *które jest ciałem zawierającym każde* $\mathbb{L}_\eta$ *dla* $\eta < \xi$. *Oczywiscie* $f_\xi \in \mathbb{K}_n \subseteq \mathbb{L}_\xi$. *Na mocy lematu 7.3 istnieje rozszerzenie* $\mathbb{L}_\xi \subseteq \mathbb{L}$, *które zawiera ciało rozkładu wielomianu* f_ξ. *Za* $\mathbb{L}_{\xi+1}$ *możemy przyjąc właśnie ciało* $\mathbb{L}$ *tak więc warunki* $(1) - (3)$ *również są spełnione dla wielomianu* f_ξ. *Jeżeli* ξ *nie jest graniczną liczbą porządkową, to dla pewnego* $\beta < \xi$ *mamy* $\xi = \beta + 1$. *Stosując lemat 7.3 do wielomianu* f_β *otrzymujemy rozszerzenie* $\mathbb{L}_\beta \subset \mathbb{L}_{\beta+1} = \mathbb{L}_\xi$ *takie, że ciało* $\mathbb{L}_\xi$ *zawiera ciało rozkładu wielomianu* f_β. *Korzystając z twierdzenia o indukcji pozaskończonej otrzymujemy żądany ciąg ciał długości* κ *spełniający warunki* $(1) - (3)$. *Niech* $\mathbb{K}_{n+1} = \bigcup_{\xi<\kappa} \mathbb{L}_\xi$, *to wtedy* $\mathbb{K}_n \subset \mathbb{K}_{n+1}$ *jest rozszerzeniem takim, że dla dowolnego wielomianu* $f \in \mathbb{K}_n[x]$, $\mathbb{K}_{n+1}$ *zawiera ciało rozkładu wielomianu* f. *Tak więc na mocy zasady indukcji skończonej, konstrukcja ciagu ciał* $(\mathbb{K}_n)_{n\in\mathbb{N}}$ *spełniające własności* $(1) - (3)$ *jest zakończona. Dowód twierdzenia jest zakńczony.* ■

Appendix C. Kryterium Eisensteina

Twierdzenie 7.8 (Kryterium Eisensteina)**.** *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem o współczynnikach całkowitych $f(x) = \sum_{k=0}^{n} a_k x^k$ o takiej własności że istnieje liczba pierwsza $p \in \mathbb{N}$ taka że*

$$\neg p|a_n \wedge p|a_{n-1} \wedge \ldots \wedge p|a_0 \wedge \neg p^2|a_0,$$

to f nie jest rozkładalny nad $\mathbb{Z}$.

Dowód. *Przypuścmy że teza nie zachodzi dla pewnego $f \in \mathbb{Z}[x]$ przy prawdziwych założeniach. Niech więc $f = f_1 f_2$ dla pewnych $f_1, f_2 \in \mathbb{Z}[x]$ takich że $m := st\ f_1 < st\ f$ i $st\ f_2 < st\ f$. Niech ponadto $f_1(x) = \sum_{k=0}^{m} b_k x^k$ i $f_2(x) = \sum_{k=0}^{n-m} c_k x^k$. To wtedy $a_0 = b_0 c_0$, niech $p|b_0$ to $\neg p|c_0$, bo w przeciwnym przypadku $p^2|a_0$ wbrew założeniu. Niech $k \in \{1, \ldots, m\}$ będzie liczbą że dla każdego $i < k$ $p|b_i$, to wtedy mamy że $k \leq m = st\ f_1 < st\ f = n$ a stąd $p|a_k$ oraz:*

$$a_k = \sum_{i=0}^{k} b_i c_{k-i} = \sum_{i=0}^{k-1} b_i c_{k-i} + b_k c_0,$$

stąd $p|b_k c_0$ (bo $p|b_i$ dla $i < k$) a stąd $p|b_k$, więc dla każdego $i \in \{0, \ldots, m\}$ $p|b_i$. Z drugiej strony mamy z założenia $\neg p|a_n$ oraz:

$$a_n = \sum_{k=0}^{n} b_k c_{n-k} = \sum_{k=0}^{m} b_k c_{n-k}$$

a stąd wynikałoby że $p|a_n$, sprzeczność z założeniem. ■

Appendix D. Twierdzenie o wielomianie pierwotnym

Twierdzenie 7.9 (Gauss)**.** *Niech $f \in \mathbb{Z}[x]$ będzie wielomianem o współczynnikach całkowitych $f(x) = \sum_{k=0}^{n} a_k x^k$, to f jest nierozkładalny nad $\mathbb{Q}$ wtedy i tylko wtedy gdy f jest nierozkładalny nad $\mathbb{Z}$.*

Wprowadzimy pojęcie wielomianu pierwotnego.

Definicja 7.2. *Wielomian $f(x) = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ stopnia n jest wielomianem pierwotnym wtedy i tylko wtedy, gdy wszystkie jego współczynniki są względnie pierwsze ($NWD(a_0, \ldots, a_n) = 1$).*

Lemat 7.2. *Iloczyn dwóch wielomianów pierwotnych jest wielomianem pierwotnym.*

Dowód. *Dowód niewprost. Niech $f = a_0 + \ldots + a_n x^n$ i $g = b_0 + \ldots + b^m x^m$ bedą wielomianami pierwotnymi dla których iloczyn $c_0 + \ldots + c_{n+m} x^{n+m}$ nie jest wielomianem pierwotnym. Więc istnieje liczba pierwsza p która dzieli wszystkie współczynniki $c_0, \ldots, c_{n+m}$.*

Niech $n_0 \leq n$ i $m_0 \leq m$ będą najmniejszymi liczbami naturalnymi, dla których p nie dzieli a_{n_0} i b_{m_0}. Wyznaczmy współczynnik $c_{n_0+m_0}$

$$c_{n_0+m_0} = a_0 b_{n+m_0} + a_1 b_{n_0+m_0-1} + \ldots a_{n_0} b_{m_0} + a_{n_0+1} b_{m_0-1} + \ldots a_{n_0+m_0} b_0.$$

Zauważmy, że

$$p|c_{n_0+m_0} \wedge p|a_0 b_{n_0+m_0}, \ldots p|a_{n_0-1} b_{m_0+1}, p|a_{n_0+1} b_{m_0-1}, \ldots, p|a_{n_0+m_0} b_0,$$

więc również p dzieli $a_{n_0} b_{m_0}$, a stąd $p|a_{n_0}$ lub $p|b_{m_0}$, sprzeczność z definicją liczb n_0 i m_0. ■

Dowód. *Twierdzenia 3.3. Jezeli wielomian jest nierozkładalny nad $\mathbb{Q}$, to oczywiście jest nierozkładalny nad $\mathbb{Z}$. W drugą stronę, załóżmy że f jest nierozkladalny nad $\mathbb{Z}$ a jest rozkładalny nad $\mathbb{Q}$. Wtedy istnieją wielomiany $h, g \in \mathbb{Q}[x]$ dla których mamy $f = gh$. Wówczas istnieją wielomiany pierwotne $g_0, h_0 \in \mathbb{Z}[x]$ oraz liczby całkowite $a, b, a', b' \in \mathbb{Z}$ takie że*

$$h = \frac{a}{b} h_0 \wedge g = \frac{a'}{b'} g_0 \wedge NWD(a, b) = 1 \wedge NWD(a', b') = 1.$$

Zauważmy że z Lematu wielomian $h_0 g_0 = c_0 + \ldots + c_n x^n \in \mathbb{Z}[x]$ jest pierwotny. Przypuśćmy że b nie dzieli a'. Niech liczba p będzie dzielnikiem pierwszym liczby b, to istnieje liczba naturalna $k \leq n$ że p nie dzieli c_k. Ponieważ liczba $\frac{aa'}{bb'} c_k \in \mathbb{Z}$ jest liczbą całkowitą i m jest największą liczbą taką że $p^m|b$, stąd $p^m|a'$ (b i a są względnie pierwsze). Więc b dzieli a'. Analogicznie $b'|a$, więc $\frac{aa'}{bb'} \in \mathbb{Z}$ jest liczbą całkowitą, stąd ostatecznie

$$hg = (\frac{aa'}{bb'} h_0) g_0, \quad \frac{aa'}{bb'} h_0, g_0 \in \mathbb{Z}[x]$$

jest iloczynem wielomianów o współczynnikach całkowitych, sprzeczność z założeniem że f jest nierozkładalny nad $\mathbb{Z}$. ■

Appendix E. Liniowa niezależność automorfizmów

Zauważmy, że mając ustalone ciało $\mathbb{L}$ zbiór $\mathbb{L}^{\mathbb{L}}$ stanowi przestrzeń liniową wszystkich funkcji z $\mathbb{L}$ do $\mathbb{L}$ nad ciałem $\mathbb{L}$. Tutaj działaniami są dodawanie funkcji oraz mnożenie funkcji prze element ciała $\mathbb{L}$.

Przejdziemy do głownego rezultatu.

Twierdzenie 7.10. *Jeżeli $\mathbb{L}$ jest ciałem, to zbiór $Aut(\mathbb{L})$ jest liniowo niezależny w $\mathbb{L}^{\mathbb{L}}$.*

Dowód. Załóżmy, $Aut(\mathbb{L})$ nie jest liniowo niezależny w $\mathbb{L}^{\mathbb{L}}$. Wtedy istnieje skończony podzbiór $A \subseteq Aut(\mathbb{L})$, taki, że jest on liniowo zależny i każdy niepusty właściwy jego podzbiór jest liniowo niezależny. Po pierwsze A musi zawierać przynajmniej dwa elementy. W przeciwnym wypadku jesli $A = \{\sigma\}$, to jeżeli $\alpha \cdot \sigma = 0$, to $\alpha = \alpha \cdot 1 = \alpha \cdot \sigma(1) = 0$ a stąd $\alpha = 0$. Więc $A = \{\sigma\}$ jest liniowo niezależny w $\mathbb{L}^{\mathbb{L}}$.

Niech $A = \{f_0, \ldots, f_n\}$ oraz dla pewnych nie wszystkich równych zeru $\alpha_0, \ldots, \alpha_n \in \mathbb{L}$ zachodzi

$$\sum_{k \leq n} \alpha_k \cdot f_k = 0.$$

Wybierzmy dowolne $x, y \in \mathbb{L}$. Wtedy mamy

$$\sum_{k \leq n} \alpha_k \cdot f_k(x) = 0.$$

oraz

$$0 = \sum_{k \leq n} \alpha_k \cdot f_k(x \cdot y) = \sum_{k \leq n} \alpha_k \cdot f_k(y) \cdot f_k(x).$$

Mnożąc pierwszą równość przez $f_0(y)$ mamy

$$\sum_{k \leq n} \alpha_k \cdot f_0(y) \cdot f_k(x) = 0.$$

Odejmując osstatnią równość od jej poprzedniej dostajemy

$$\sum_{k=1}^{n} \alpha_k \cdot (f_k(y) - f_0(y)) \cdot f_k(x) = 0.$$

Ponieważ $|B = \{f_k : 0 < k \leq n\}| < |A|$ i $B \subseteq A$ widzimy, że B jest liniowo niezależny. Więc dla każdego $y \in \mathbb{L}$ i każdego $k \in \{1, \ldots, n\}$ mamy $\alpha_k \cdot (f_k(y) - f_0(y)) = 0$. Ponieważ wszystkie elementy A (a więc i B) są parami różne, to dla każdego $k \in \{1, \ldots, n\}$ jest $y \in \mathbb{L}$ takie, że $f_k(y) - f_0(y) \neq 0$. Więc dla każdego $k \in \{1, \ldots, n\}$ $\alpha_k = 0$.

W takim razie mamy

$$\sum_{k \leq n} \alpha_k \cdot f_k = 0 \longleftrightarrow \alpha_0 \cdot f_0 = 0.$$

Więc

$$\alpha_0 = \alpha_0 \cdot 1 = \alpha_0 \cdot f_0(1) = 0$$

a stąd $\alpha_0 = 0$. Pokazaliśmy więc, że

$$\forall k \in \{0, \ldots, n\}\ \alpha_0 = 0,$$

co jest sprzeczne z założeniem, że dla któregoś $k \in \{0, \ldots, n\}$ $\alpha_k \neq 0$. □

Robert Rałowski, Katedra Informatyki, Wydział Podstawowych Problemów Techniki, Politechnika Wrocławska.

Email address: ralowski@im.pwr.edu.pl