Skończone rozszerzenia ciał

Notkę tę rozpoczniemy od definicji i prostych własności wielomianu minimalnego, następnie wprowadzimy pojecie rozszerzenia pojedynczego o element algebraiczny, udowodnimy twierdzenie Abela o elemencie prowotnym, wprowadzimy pojęcie stopnia rozszerzenia oraz przedstawimy dowód faktu, że wszystkie elementy algebraiczne tworzą ciało.

Wpierw zauważmy, że dla ciał zachodzi analogiczny fakt jak dla grup.

Twierdzenie 0.1 *Niech $\mathbb{L}$ będzie ustalonym ciałem, to dla dowolnej niepustej rodziny podciał $\emptyset \neq \mathscr{F} \subseteq \{\mathbb{M} \subseteq \mathbb{L} : \mathbb{M} \leq \mathbb{L}\}$ mamy $\bigcap \mathscr{F} \leq \mathbb{L}$.*

Powyższe twierdzenie pozwala nam na wprowadzenie pojęcia ciała generowanego przez zbiór.

Definicja 0.1 *Niech $\mathbb{L}$ będzie ciałem oraz $\emptyset \neq A \subseteq \mathbb{L}$, to zbiór*

$$\langle A \rangle = \bigcap \{\mathbb{M} : A \subseteq \mathbb{M} \wedge \mathbb{M} \leq \mathbb{L}\}.$$

nazywamy podciałem ciała $\mathbb{L}$ generowanym przez A. Ponadto jesli $\mathbb{K} \subseteq \mathbb{L}$ jest podciałem ciała $\mathbb{L}$, to

$$\mathbb{K}(A) = \langle \mathbb{K} \cup A \rangle$$

nazywać będziemy najmniejszym rozszerzeniem ciała $\mathbb{K}$ w ciele $\mathbb{L}$ zawierającym zbiór A lub krócej najmniejsze rozszerzenie ciała $\mathbb{K}$ o zbiór A. W przypadku gdy $A = \{a\}$ jest singletonem elementu a, to $\mathbb{K}(\{a\}) = \mathbb{K}(a)$ nazywać będziemy rozszerzeniem ciała $\mathbb{K}$ o element $a \in \mathbb{L}$.

Wielomian minimalny

Definicja 0.2 (wielomian minimalny) *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem ciała $\mathbb{K}$ oraz niech $a \in \mathbb{L}$, to $f \in \mathbb{K}[x]$ jest wielomianem minimalnym elementu a wtedy i tylko wtedy gdy:*

1. $f(a) = 0$,
2. $f \neq 0$,
3. $\forall g \in \mathbb{K}[x] \;\; g(a) = 0 \longrightarrow st\ f \leq st\ g$.

Definicja 0.3 (element algebraiczny) *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem ciała $\mathbb{K}$, to $a \in \mathbb{L}$ jest algebraiczny nad $\mathbb{K}$ wtedy i tylko wtedy gdy istnieje $f \in \mathbb{K}[x]$ dla którego $f(a) = 0$.*

Fakt 0.1 *Jeśli $a \in \mathbb{L}$ jest elementem algebraicznym nad $\mathbb{K} \subset \mathbb{L}$, to istnieje wielomian minimalny elementu a.*

Dowód. *Niech a jest elementem algebraicznym nad $\mathbb{K}$, to $Z = \{n \in \mathbb{N} : \exists f \in \mathbb{K}[x] \quad f(a) = 0 \wedge n = st\ f\} \neq \emptyset$ a więc istnieje $n_0 = \min Z \in Z$. Wtedy istnieje $f \in \mathbb{K}[x]$ że $f(a) = 0$ i $st\ f = n_0$. oczywiście f jest wielomianem minimalnym elementu a.* ■

Fakt 0.2 *Niech $\mathbb{K} \subset \mathbb{L}$ będzie rozszerzeniem ciała $\mathbb{K}$ i $a \in \mathbb{L}$, to*
$f \in \mathbb{K}[x]$ *– wielomian minimalny* $\longleftrightarrow f(a) = 0$ *oraz f nie jest rozkładalny nad $\mathbb{K}$.*

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.* ■

Fakt 0.3 *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 0.4 *Jeśli $f, g \in \mathbb{K}[x]$ są wielomianami minimalnymi elementu $a \in \mathbb{L}$, gdzie $\mathbb{K} \subset \mathbb{L}$ jest rozszeżeniem, to te wielomiany są stowarzyszone $f \sim g$.*

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

Przykład 0.1 *Niech $\mathbb{K} = \mathbb{Q}$ i $a := \sqrt[n]{p} \in \mathbb{R}$ 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 $f(a = \sqrt[n]{p}) = 0$ więc f jest wielomianem minimalnym elementu a.*

Fakt 0.5 *Niech $\mathbb{K} \subset \mathbb{L}$ jest rozszerzenie ciała $\mathbb{K}$ oraz $f \in \mathbb{K}[x]$ jest wielomianem minimalnym elemntu a, to*

$$\forall g \in \mathbb{K}[x] \quad 0 \leq st\ g < st\ f \longrightarrow NWD(f, g) = 1.$$

Dowód. *Niech $0 < st\ NWD(f, g)$ i $d = NWD(f, g) \in \mathbb{K}[x]$, to wtedy $0 < st\ d \leq st\ g < st\ f$ i $d|f$, więc $f = qd$ dla pewnego $q \in \mathbb{K}[x]$. Zauważmy że*

$$st\ f = st\ q + st\ d > st\ q + 0 = st\ q,$$

tak więc $0 \leq st\ q < st\ f$ i $st\ d < st\ f$ a stąd $0 = f(a) = q(a)d(a)$ więc $d(a) = 0$ lub $q(a) = 0$, co jest niemożliwe wobec minimalności stopnia wielomianu f zerującego element a. ■

Rozszerzenia pojedyńcze

Niech $\mathbb{K} \subseteq \mathbb{L}$ i $a \in \mathbb{L}$, to ciało $\mathbb{K}(a)$ jest rozszerzeniem pojedyńczym ciała $\mathbb{K}$ o element a. Ponadto, jeśli a jest elementem algebraicznym nad $\mathbb{K}$, to takie rozszerzenie nazywamy pojedyńczym rozszerzeniem algebraicznym ciała $\mathbb{K}$ albo algebraicznym rozszerzeniem ciała $\mathbb{K}$ o element $a \in \mathbb{L}$.

Twierdzenie 0.2 *Niech $\mathbb{K} \subset \mathbb{L}$ i $a \in \mathbb{L}$ jest elementem algebraicznym w ciele $\mathbb{L}$ a $f \in \mathbb{K}[x]$ jest jego wielomianem minimalnym, to*

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

Dowòd. *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 $b_0 + b_1 a + \ldots + b_n a^n = g(a) \in \mathbb{K}(a)$ 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. Wtedy z faktu 0.5 wiemy że $NWD(f, g) = 1$ 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 $b \in \mathbb{K}(a) \setminus \{0\}$. ■

Przykład 0.2 *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

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

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 0.2, mamy

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

Przykład 0.3 *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 $y^{-1} = v(a) = ...$ $\square$

Definicja 0.4 (stopień rozszerzenia) *Niech $\mathbb{K} \subset \mathbb{L}$ jest rozszerzeniem ciała $\mathbb{K}$, to $[\mathbb{L} : \mathbb{K}] := \dim_{\mathbb{K}} \mathbb{L}$ 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.*

Twierdzenie 0.3 *Niech $\mathbb{K}(a)$ będzie rozszerzeniem elementu a algebraicznego nad $\mathbb{K}$ i niech $f \in \mathbb{K}[x]$ będzie jego wielomianem minimalnym stonia $n \in \mathbb{N}$, to*

1. *zbiór $\mathscr{B} := \{1, a, \ldots, a^{n-1}\}$ stanowi bazę przestrzeni $\mathbb{K}(a)$ nad ciałem $\mathbb{K}$,*

2. $[\mathbb{K}(a):\mathbb{K}] = n = st\ f$*,*

3. każdy element ciała $\mathbb{K}(a)$ *jest algebraiczny nad cialem* $\mathbb{K}$*.*

Dowòd. *Wystarczy udowodnić 1), natomiast* 2) *wynika z 1) natychmiast. Z faktu 0.2 wynika że* $\mathbb{K}(a) = lin_{\mathbb{K}}\mathscr{B}$*. Pozostało udowodnić liniową niezależnośc elementów ze zbioru* $\mathscr{B}$*. Gdyby zbiór* $\mathscr{B}$ *byłby liniowo niezależny, to istniałby ciąg* $(\alpha_i)_{i=0}^{n-1}$ *z* $\mathbb{K}$ *i pewne* $j \in \{0,\ldots,n-1\}$ *dla którego* $\alpha_j \neq 0$ *oraz* $\sum_{i=0}^{n-1} \alpha_i a^i = 0$ *a więc istniałby niezerowy wielomian* $g \in \mathbb{K}[x]$ *(*$g(x) = \sum_{i=0}^{n-1} \alpha_i x^i$*) dla którego* $st\ g < n$ *i* $g(a) = 0$*, co jest oczywiście niemożliwe wobec minimalności stopnia wielomianu (o współczynnikach z* $\mathbb{K}$*) zerującego element* a*.*

By udowodnić punkt 3) naszego twierdzenia, niech

$$z \in span_{\mathbb{K}}\{a, a^2, \ldots, a^{k-1}\} = \mathbb{K}(a).$$

To faktu, że $[\mathbb{K}(a):\mathbb{K}] = dim_{\mathbb{K}}\mathbb{K}(a) = k$*, gdzie* k *jest stopniem wielomianu minimalnego* $f_a \in \mathbb{K}[x]$ *elementu* a*, zbiór*

$$\{1, z, \ldots, z^k\}$$

jest liniowo zależny nad $\mathbb{K}$*. Więc istnieją* $\{\alpha_0,\ldots,\alpha_k\} \subseteq \mathbb{K}$*, sposród których, przynajmniej jedna jest niezerowa, dla których mamy:*

$$\alpha_0 + \alpha_1 z + \ldots + \alpha_k z^k = 0.$$

Więc istnieje niezerowy wieloman $h = \alpha_0 + \alpha_1 x + \ldots \alpha_k x^k \in \mathbb{K}[x]$*, taki że* $z \in \mathbb{K}(a)$ *jest jego pierwiastkiem.* ■

Definicja 0.5 (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 0.6 *Jeśli* $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L} \subseteq \mathbb{C}$*, to* $\mathbb{K} \subset \mathbb{L}$ *jest rozszerzeniem rozdzielczym.*

Dowòd. *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*

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

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

$$f'(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1} \in \mathbb{K}[x],$$

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. ■

Twierdzenie 0.4 (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).*

Dowòd. *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*

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

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. ■

Przykład 0.4 *Niech* $\mathbb{L} = \mathbb{Q}(\sqrt{2},\sqrt{3})$ *będzie najmniejszym ciałem liczbowym, zawirającym liczby niewymierne* $\sqrt{2},\sqrt{3}$*. Postępujemy jak w dowodzi twierdzenia Abela,* $f(x) = x^2 - 2$ *jest wielomiane minimalnym dla* $a_1 = \sqrt{2}$ *i dla* $a_2 = -\sqrt{2}$ *oraz* $g(x) = x^2 - 3$ *jest wielomianem minimalnym dla* $b_1 = \sqrt{3}$ *jak i dla* $b_2 = -\sqrt{3}$*. Liczba* $c = a_1 + d \cdot b_1 = \sqrt{2} + 1 \cdot \sqrt{3}$ *(tutaj* $d = 1$*) ma tę własność że* $c - d \cdot b_j \neq a_2$ *dla* $j = 1, 2$*, więc* $\mathbb{L} = \mathbb{Q}(\sqrt{2} + \sqrt{3})$*.*

Wniosek 0.1 *Jeżeli rozszerzenie* $\mathbb{K} \subseteq \mathbb{L}$ *jest rozdzielcze oraz elementy*

$$a_1, \ldots, a_n \in \mathbb{L}$$

są algebraiczne nad ciałem $\mathbb{K}$*, to istnieje element algebraiczny* $c \in \mathbb{L}$ *nad ciałem* $\mathbb{K}$*, taki że*

$$\mathbb{K}(a_1, \ldots, a_n) = \mathbb{K}(c).$$

Twierdzenie 0.5 *Zbiór wszystkich liczb algebraicznych stanowi podciało ciała liczb zespolonych* $\mathbb{C}$*.*

Dowòd. *Niech* A *oznacza zbiór wszytkich liczb algebraicznych nad* $\mathbb{Q}$*. Aby* A *byłoby cialem, wystarczy pokazać, że* A *jest zamknięty na dodawanie, mnożenie i branie elementu odwrotnego do niezerowego elementu ze zbioru* A*. Niech* $a, b \in A$ *i* $f, g \in \mathbb{Z}[x]$ *będą wielomianami, dla których liczby* a, b *są pierwiastkami wielomianów* f, g *odpowiednio. Załóżmy że*

$$f = a_0 + a_1 x + \ldots + a_n x^n \ \text{ i } \ g = b_0 + b_1 x + \ldots + b_m x^m.$$

Jeżeli $a \neq 0$*, to wielomian* $h = a_n + a_{n-1}x + \ldots + a_0 x^n \in \mathbb{Z}[x]$ *zeruje liczbę* a^{-1}*, stąd mamy* $a^{-1} \in A \setminus \{0\}$*. Niech* $\{x_0, \ldots, x_n\}, \{y_0, \ldots, y_m\} \in P(\mathbb{C})$ *będą*

wszystkimi pierwiastkami wielomianów f, g oraz niech $x_0 = a$ i $y_0 = b$. To na mocy **Wniosku 0.1**, *istnieje element algebraiczny $c \in \mathbb{C}$ nad $\mathbb{Q}$, taki że*

$$\mathbb{Q}(x_0, \ldots, x_n, y_0, \ldots, y_m) = \mathbb{Q}(c).$$

Stąd mamy $ab, a + b \in \mathbb{Q}(c)$, natomiast na podstawie własności 3) w **Twierdzeniu 0.3**, *każdy element ciała $\mathbb{Q}(c)$ jest algebraiczny nad $\mathbb{Q}$. W szczególności elemnty $ab, a + b \in span_{\mathbb{Q}}\{c, c^2, \ldots, c^{k-1}\} = \mathbb{Q}(c)$ są algebraiczne nad $\mathbb{Q}$, gdzie k jest stopniem wielomianu minimalnego $f_c \in \mathbb{Q}[x]$ elementu c, co kończy dowód naszego twierdzenia.* ■

Robert Rałowski