Wykład 15
Rozszerzenia ciał

1 Podciała generowane przez podzbiory ciała

Stwierdzenie 15.1. *Niech K będzie podciałem ciała L i niech $X \subseteq L$. Wówczas istnieje najmniejsze (w sensie inkluzji) podciało $K(X)$ ciała L zawierające $K \cup X$.*

Dowód. Niech T będzie rodziną wszystkich podciał ciała L, które zawierają $K \cup X$. Wtedy rodzina T jest niepusta, bo $L \in T$. Zatem ze Stwierdzenia 14.8, $M = \bigcap_{S \in T} S$ jest podciałem ciała L. Ale $K \cup X \subseteq S$ dla każdego $S \in T$, więc $K \cup X \subseteq M$. Ponadto $M \subseteq S$ dla każdego $S \in T$, czyli M jest najmniejszym w sensie inkluzji podciałem ciała L zawierającym $K \cup X$, czyli $M = K(X)$. $\square$

Stwierdzenie 15.2. *Niech K będzie podciałem ciała L i niech $X, Y \subseteq L$. Wówczas:*
(a) $K(X) \subseteq K(Y) \Leftrightarrow X \subseteq K(Y)$,
(b) $K(X) = K(Y) \Leftrightarrow [X \subseteq K(Y)$ oraz $Y \subseteq K(X)]$,
(c) $K(X \cup Y) = (K(X))(Y)$.

Dowód. (a). Niech $K(X) \subseteq K(Y)$. Ponieważ $X \subseteq K(X)$, więc $X \subseteq K(Y)$. Na odwrót, niech $X \subseteq K(Y)$. Wtedy $K(Y)$ jest jakimś podciałem ciała L zawierającym K i zawierającym X. Wobec tego $K(Y)$ musi zawierać najmniejsze podciało ciała L zawierające $K \cup X$, czyli $K(X) \subseteq K(Y)$.

(b). Wynika od razu z (a).

(c). Ponieważ $K \cup X \subseteq K(X)$ i $K(X) \cup Y \subseteq (K(X))(Y)$, więc $K \cup (X \cup Y) \subseteq (K(X))(Y)$, skąd $K(X \cup Y) \subseteq (K(X))(Y)$. Dalej, $X \subseteq X \cup Y$, więc z (a) mamy, że $K(X) \subseteq K(X \cup Y)$ oraz $Y \subseteq K(X \cup Y)$. Zatem $K(X \cup Y)$ jest jakimś podciałem ciała L zawierającym $K(X) \cup Y$, więc $(K(X))(Y) \subseteq K(X \cup Y)$ i ostatecznie $K(X \cup Y) = (K(X))(Y)$. $\square$

Uwaga 15.3. Jeśli K jest podciałem ciała L i $X = \{a_1, \ldots, a_n\} \subseteq L$, to zamiast $K(\{a_1, \ldots, a_n\})$ będziemy pisali $K(a_1, \ldots, a_n)$. Ze Stwierdzenia 15.2 mamy zatem, że dla $a, b \in L$: $K(a, b) = (K(a))(b) = (K(b))(a)$. Ponadto, dla dowolnego $n \in \mathbb{N}$ i dla dowolnych $a_1, \ldots, a_n, a_{n+1} \in L$ mamy, że $K(a_1, \ldots, a_n, a_{n+1}) = (K(a_1, \ldots, a_n))(a_{n+1})$.

Stwierdzenie 15.4. *Niech K będzie podciałem ciała L i $a \in L$. Wówczas:*

$$K(a) = \left\{ \frac{f(a)}{g(a)} : f, g \in K[x], g(a) \neq 0 \right\}.$$

Dowód. Oznaczmy $S = \left\{ \frac{f(a)}{g(a)} : f, g \in K[x], g(a) \neq 0 \right\}$. Dla $k \in K$ oraz $f = x$ i $g = 1$ mamy, że $k = \frac{f(k)}{g(k)}$, więc $K \subseteq S$; w szczególności $1 \in S$. Ponadto $a = \frac{f(a)}{g(a)} \in S$. Weźmy

dowolne $x, y \in S$. Wtedy istnieją $f, g, u, v \in K[x]$ takie, że $g(a), v(a) \neq 0$ oraz $x = \frac{f(a)}{g(a)}$ i $y = \frac{u(a)}{v(a)}$. Zatem $x - y = \frac{(fv-ug)(a)}{(gv)(a)} \in S$. Ponadto, jeśli $y \neq 0$, to $u(a) \neq 0$ i $\frac{x}{y} = \frac{(fv)(a)}{(gu)(a)} \in S$. Zatem ze Stwierdzenia 14.6, S jest podciałem ciała L. Ponadto $K \cup \{a\} \subseteq S$.

Niech teraz M będzie podciałem ciała L zawierającym $K \cup \{a\}$. Weźmy dowolne $f, g \in K[x]$ takie, że $g(a) \neq 0$. Wtedy $f = a_0 + a_1 x + \ldots + a_n x^n$ dla pewnych $a_0, a_1, \ldots, a_n \in K$, $n \in \mathbb{N}_0$ oraz $g = b_0 + b_1 x + \ldots + b_m x^m$ dla pewnych $b_0, b_1, \ldots, b_m \in K$, $m \in \mathbb{N}_0$. Stąd $f(a) = a_0 + a_1 \cdot a + \ldots + a_n \cdot a^n \in M$ oraz $0 \neq g(a) = b_0 + b_1 \cdot a + \ldots + b_m \cdot a^m \in M$, więc ze Stwierdzenia 14.6, $\frac{f(a)}{g(a)} \in M$. Wobec tego $S \subseteq M$ i S jest najmniejszym podciałem ciała L zawierającym $K \cup \{a\}$, czyli $S = K(a)$. $\square$

Przykład 15.5. Udowodnimy, że w ciele $\mathbb{R}$: $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Ponieważ $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, więc $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ i na mocy Stwierdzenia 15.2, $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Ponadto, $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, więc także $\frac{1}{\sqrt{3}+\sqrt{2}} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, skąd $\sqrt{3} - \sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Wobec tego $(\sqrt{3} + \sqrt{2}) + (\sqrt{3} - \sqrt{2}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ i $(\sqrt{3} + \sqrt{2}) - (\sqrt{3} - \sqrt{2}) \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, czyli $2\sqrt{3}, 2\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Ale $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$, więc $\frac{1}{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Zatem $\sqrt{3} = \frac{1}{2} \cdot 2\sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ i $\sqrt{2} = \frac{1}{2} \cdot 2\sqrt{2} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Wobec tego $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, więc na mocy Stwierdzenia 15.2, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$ i ostatecznie $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

2 Rozszerzenia algebraiczne ciał

Twierdzenie 15.6. *Niech ciało M będzie rozszerzeniem ciała L i niech ciało L będzie rozszerzeniem ciała K. Jeśli $(L:K) = r \in \mathbb{N}$ i $(M:L) = s \in \mathbb{N}$, to $(M:K) = r \cdot s$.*

Dowód. Niech $(a_1, \ldots, a_r)$ będzie uporządkowaną bazą L nad K oraz niech $(b_1, \ldots, b_s)$ będzie uporządkowaną bazą M nad L. Udowodnimy, że

$$(a_1 b_1, a_1 b_2, \ldots, a_1 b_s, \ldots, a_r b_1, a_r b_2, \ldots, a_r b_s)$$

jest uporządkowaną bazą M nad K. W tym celu weźmy dowolne $c_{ij} \in K, i = 1, \ldots, s, j = 1, \ldots, r$ takie, że $\sum_{i,j} c_{ij} a_i b_j = 0$. Wówczas $\sum_{j=1}^{s} \Big(\sum_{i=1}^{r} c_{ij} a_i \Big) b_j = 0$. Elementy stojące w nawiasach należą do ciała L, więc dla $j = 1, \ldots, s$ mamy, że $\sum_{i=1}^{r} c_{ij} a_i = 0$. Stąd z liniowej niezależności elementów $a_1, \ldots, a_r$ wynika, że $c_{ij} = 0$ dla $i = 1, \ldots, r$. Zatem $c_{ij} = 0$ dla wszystkich i, j, czyli elementy $a_1 b_1, a_1 b_2, \ldots, a_1 b_s, \ldots, a_r b_1, a_r b_2, \ldots, a_r b_s$ są liniowo niezależne nad K. Weźmy teraz dowolne $a \in M$. Wówczas istnieją $t_1, \ldots, t_s \in L$ takie, że $a = \sum_{i=1}^{s} t_j \cdot b_j$ oraz dla $j = 1, \ldots, s$ istnieją $c_{1j}, c_{2j}, \ldots, c_{rj} \in K$ takie, że $t_j = \sum_{i=1}^{r} c_{ij} \cdot a_i$.

Stąd $a = \sum_{i,j} c_{ij}(a_i \cdot b_j)$. Zatem elementy $a_1b_1, a_1b_2, \ldots, a_1b_s, \ldots, a_rb_1, a_rb_2, \ldots, a_rb_s$ generują M nad K. Stąd mamy tezę. $\square$

Definicja 15.7. Niech K będzie podciałem ciała L. Powiemy, że element $a \in L$ jest *algebraiczny* względem ciała K, jeżeli istnieje niezerowy wielomian $f \in K[x]$ taki, że $f(a) = 0$. W przeciwnym przypadku element $a \in L$ nazywamy *przestępnym* względem ciała K. Ciało L nazywamy *rozszerzeniem algebraicznym* ciała K, gdy każdy element $a \in L$ jest algebraiczny względem K.

Uwaga 15.8. Zauważmy, że dla dowolnego ciała K: $x \in K(x)$ jest elementem przestępnym nad K.

Uwaga 15.9. Liczby zespolone a, które są elementami algebraicznymi względem ciała $\mathbb{Q}$ nazywamy krótko *liczbami algebraicznymi*. Liczbę $a \in \mathbb{C}$ nazywamy *przestępną*, jeżeli a nie jest liczbą algebraiczną. Np. $a = e$ i $a = \pi$ są przestępne.

Lemat 15.10. *Niech K będzie ciałem i niech $f \in K[x]$ będzie wielomianem nierozkładalnym w $K[x]$. Wówczas dla dowolnego $g \in K[x]$ równoważne są warunki:*

(i) g nie jest podzielne przez f w $K[x]$,

(ii) $fu + gv = 1$ dla pewnych $u, v \in K[x]$.

Dowód. $(i) \Rightarrow (ii)$. Z Wniosku 13.16 wynika, że (f) jest ideałem maksymalnym pierścienia $K[x]$. Ponadto $(f) \subseteq (f, g)$ i $g \in (f, g)$. Ale g nie jest podzielne przez f, więc $g \notin (f)$. Zatem $(f) \subset (f, g)$ i z maksymalności ideału (f), $(f, g) = K[x]$. Stąd $1 \in (f, g)$, więc $fu + gv = 1$ dla pewnych $u, v \in K[x]$.

$(ii) \Rightarrow (i)$. Jeśli $f|g$ w $K[x]$, to $g = fh$ dla pewnego $h \in K[x]$. Stąd $fu + fhv = 1$, czyli $f(u + hv) = 1$. Zatem $f \in (K[x])^*$, co przeczy nierozkładalności wielomianu f. Wobec tego g nie jest podzielne przez f w $K[x]$. $\square$

Twierdzenie 15.11. *Niech K będzie podciałem ciała L i $a \in L$. Wówczas a jest algebraiczny względem ciała K wtedy i tylko wtedy, gdy a jest pierwiastkiem pewnego wielomianu nierozkładalnego w $K[x]$.*

Ponadto, gdy a jest pierwiastkiem wielomianu f nierozkładalnego w $K[x]$, to dla dowolnego $g \in K[x]$: $g(a) = 0$ wtedy i tylko wtedy, gdy $f \mid g$ w $K[x]$.

Dowód. Jeśli $f(a) = 0$ dla pewnego wielomianu $f \in K[x]$ nierozkładalnego w $K[x]$, to $f \neq 0$, a więc element a jest algebraiczny nad K. Na odwrót, załóżmy, że $a \in L$ jest algebraiczny względem K. Wtedy istnieje niezerowy wielomian $h \in K[x]$ taki, że $h(a) = 0$. Stąd $st(h) \geq 1$, więc na mocy Wniosku 12.36, $h = h_1h_2 \ldots h_s$ dla pewnych wielomianów $h_1, h_2, \ldots, h_s$ nierozkładalnych w $K[x]$. Wobec tego w ciele K: $0 = h_1(a) \cdot h_2(a) \cdot \ldots \cdot h_s(a)$, skąd $h_i(a) = 0$ dla pewnego $i = 1, 2, \ldots, n$.

Niech teraz a będzie pierwiastkiem wielomianu f nierozkładalnego w $K[x]$ i niech $g \in K[x]$. Jeśli $f|g$ w $K[x]$, to $g = fw$ dla pewnego $w \in K[x]$, skąd $g(a) = f(a) \cdot w(a) =$

$0 \cdot w(a) = 0$, a więc $g(a) = 0$. Na odwrót, załóżmy, że $g(a) = 0$. Jeśli g nie jest podzielne przez f w $K[x]$, to z Lematu 15.10, $fu + gv = 1$ dla pewnych $u, v \in K[x]$, skąd $1 = f(a) \cdot u(a) + g(a) \cdot v(a) = 0 \cdot u(a) + 0 \cdot v(a) = 0$ i mamy sprzeczność. Wobec tego $f|g$ w $K[x]$. $\square$

Wniosek 15.12. *Jeśli element a ciała L jest algebraiczny względem podciała K, to wielomian nierozkładalny $f \in K[x]$, którego a jest pierwiastkiem, jest wyznaczony jednoznacznie z dokładnością do stałego czynnika.*

Dowód. Jeżeli $f_1, f_2 \in K[x]$ są wielomianami nierozkładalnymi w $K[x]$ takimi, że $f_1(a) = f_2(a) = 0$, to z Twierdzenia 15.11 mamy, że $f_1 \mid f_2$ i $f_2 \mid f_1$ w $K[x]$, więc $f_1 \sim f_2$. Stąd istnieje niezerowe $c \in K$ takie, że $f_2 = c \cdot f_1$. $\square$

Uwaga 15.13. Gdy element a ciała L jest algebraiczny względem podciała K, to stopień wielomianu f nierozkładalnego w $K[x]$, którego a jest pierwiastkiem nazywamy *stopniem elementu a względem ciała K*, zaś f nazywamy *wielomianem minimalnym dla a względem ciała K*. Określenie to jest poprawne na mocy Twierdzenia 15.11 i Wniosku 15.12. Zauważmy jeszcze, że jeśli $b \in L$ jest pierwiastkiem wielomianu $g \in K[x]$ nierozkładalnego w $K[x]$, to na mocy Twierdzenia 15.11 i Wniosku 15.12, g jest wielomianem minimalnym dla b i wobec tego $st(g)$ jest stopniem elementu b względem ciała K.

Twierdzenie 15.14. *Gdy element a ciała L jest algebraiczny stopnia $n \in \mathbb{N}$ względem podciała K, to $(1, a, a^2, \ldots, a^{n-1})$ jest bazą uporządkowaną $K(a)$ nad K. W szczególności $(K(a) : K) = n$, elementy $1, a, a^2, \ldots, a^{n-1}$ są liniowo niezależne nad K i każdy element ciała $K(a)$ można jednoznacznie zapisać w postaci $b_0 + b_1 \cdot a + \ldots + b_{n-1} \cdot a^{n-1}$ dla pewnych $b_0, b_1, \ldots, b_{n-1} \in K$.*

Dowód. Jeżeli $n = 1$, to $a \in K$ i $K(a) = K$, więc teza jest oczywista. Niech dalej $n > 1$. Wystarczy wykazać, że $(1, a, a^2, \ldots, a^{n-1})$ jest bazą uporządkowaną $K(a)$ nad K. Na mocy Twierdzenia 15.11 i Wniosku 15.12 istnieje wielomian f stopnia n nierozkładalny w $K[x]$ i taki, że $f(a) = 0$. Jeżeli $b_0, b_1, \ldots, b_{n-1} \in K$ są takie, że $b_0 + b_1 \cdot a + \ldots + b_{n-1} \cdot a^{n-1} = 0$, to $g(a) = 0$ dla $g = b_0 + b_1 \cdot x + \ldots + b_{n-1} \cdot x^{n-1} \in K[x]$. Zatem z Twierdzenia 15.11, $f|g$. Ale $st(f) = n$, więc $g = 0$ i $b_0 = b_1 = \ldots = b_{n-1} = 0$. Wobec tego elementy $1, a, a^2, \ldots, a^{n-1}$ są liniowo niezależne nad K.

Niech

$$M = \{b_0 + b_1 \cdot a + \ldots + b_{n-1} \cdot a^{n-1} : b_0, b_1, \ldots, b_{n-1} \in K\}.$$

Wówczas $K \subseteq M$ i $a \in M$. Jeśli $h \in K[x]$, to z Twierdzenia 12.3 istnieją $q, r \in K[x]$ takie, że $h = q \cdot f + r$ i $st(r) < n$, więc $h(a) = q(a)f(a) + r(a) = r(a) \in M$. Zatem $M = \{h(a) : h \in K[x]\}$. Stąd od razu mamy, że M jest podpierścieniem ciała L. Weźmy dowolne $b_0, b_1, \ldots, b_{n-1} \in K$ takie, że $b_0 + b_1 \cdot a + \ldots + b_{n-1} \cdot a^{n-1} \neq 0$. Wtedy, jak wiemy, $g = b_0 + b_1 \cdot x + \ldots + b_{n-1} \cdot x^{n-1} \neq 0$ oraz g nie dzieli się przez f w $K[x]$.

Zatem na mocy Lematu 15.10 istnieją $u, v \in K[x]$ takie, że $g \cdot u + f \cdot v = 1$. Stąd $g(a) \cdot u(a) + f(a) \cdot v(a) = 1$, czyli $\frac{1}{g(a)} = u(a) \in M$. Zatem na mocy Stwierdzenia 14.6, M jest podciałem ciała L zawierającym $K \cup \{a\}$. Niech N będzie dowolnym podciałem ciała L zawierającym $K \cup \{a\}$. Wtedy $1, a, a^2, \ldots, a^{n-1} \in N$ oraz dla dowolnych $b_0, b_1, \ldots, b_{n-1} \in K$, $b_0 + b_1 \cdot a + \ldots + b_{n-1} \cdot a^{n-1} \in N$. Stąd $M \subseteq N$. Zatem $M = K(a)$ i wobec powyższego $(1, a, a^2, \ldots, a^{n-1})$ jest uporządkowaną bazą $K(a)$ nad K. $\square$

Twierdzenie 15.15. *Element a ciała L jest algebraiczny względem podciała K wtedy i tylko wtedy, gdy $(K(a) : K) < \infty$.*

Dowód. $\Rightarrow$. Wynika z Twierdzenia 15.14. $\Leftarrow$. Załóżmy, że $(K(a) : K) = n \in \mathbb{N}$. Wówczas elementy $1, a, a^2, \ldots, a^n$ są liniowo zależne nad K oraz należą do $K(a)$, więc istnieją $b_0, b_1, \ldots, b_n \in K$ nie wszystkie równe 0 i takie, że $b_0 + b_1 \cdot a + \ldots + b_n \cdot a^n = 0$. Stąd $g(a) = 0$ dla $gb_0 + b_1 \cdot x + \ldots + b_n \cdot x^n \in K[x] \setminus \{0\}$. Zatem a jest elementem algebraicznym względem ciała K. $\square$

Wniosek 15.16. *Każde rozszerzenie skończone ciał jest algebraiczne.*

Dowód. Niech K będzie podciałem ciała L takim, że $(L : K) = n \in \mathbb{N}$. Wtedy dla dowolnego $a \in L$, $K(a) \subseteq L$, więc $(K(a) : K) \leq n$. Stąd wobec Twierdzenia 15.15, a jest elementem algebraicznym względem ciała K. $\square$

Wniosek 15.17. *Jeśli elementy $a_1, \ldots, a_n$ ciała L są algebraiczne względem podciała K, to $K(a_1, \ldots, a_n)$ jest rozszerzeniem algebraicznym i skończonym ciała K.*

Dowód. Indukcja względem n. Dla $n = 1$ teza wynika z Twierdzenia 15.14 i z Wniosku 15.16. Załóżmy, że teza zachodzi dla pewnego naturalnego n i niech $a_1, \ldots, a_n, a_{n+1} \in L$ będą elementami algebraicznymi względem K. Niech $f \in K[x]$ będzie wielomianem minimalnym dla a_{n+1} względem K. Wtedy $f \in K(a_1, \ldots, a_n)[x]$, więc $(K(a_1, \ldots, a_n)(a_{n+1}) : K(a_1, \ldots, a_n)) \leq (K(a_{n+1}) : K) < \infty$, czyli $(K(a_1, \ldots, a_n, a_{n+1}) : K(a_1, \ldots, a_n)) \in \mathbb{N}$. Ponadto z założenia indukcyjnego $(K(a_1, \ldots, a_n) : K) \in \mathbb{N}$, więc z Twierdzenia 15.6, $(K(a_1, \ldots, a_n, a_{n+1}) : K) < \infty$. Stąd i z Wniosku 15.16, $K(a_1, \ldots, a_{n+1})$ jest rozszerzeniem algebraicznym ciała K. $\square$

Wniosek 15.18. *Niech K będzie podciałem ciała L. Wówczas zbiór M wszystkich elementów ciała L algebraicznych względem K jest podciałem ciała L zawierającym K.*

Dowód. Ponieważ każde $a \in K$ jest pierwiastkiem wielomianu $x - a \in K[x]$, więc $K \subseteq M$. Niech $a, b \in M$. Wtedy z Wniosku 15.17 $K(a, b)$ jest rozszerzeniem algebraicznym ciała K, czyli $K(a, b) \subseteq M$. Zatem $a - b \in M$ i $\frac{a}{b} \in M$ dla $b \neq 0$. Stąd i ze Stwierdzenia 14.6, M jest podciałem ciała L. $\square$

Twierdzenie 15.19. *Jeżeli ciało L jest algebraicznym rozszerzeniem ciała K i ciało M jest algebraicznym rozszerzeniem ciała L, to ciało M jest algebraicznym rozszerzeniem ciała K.*

Dowód. Weźmy dowolne $a \in M$. Wówczas istnieje $0 \neq f \in L[x]$ takie, że $f(a) = 0$.

Ale $f = l_0 + l_1 x + \ldots + l_n x^n$ dla pewnych $l_0, \ldots, l_n \in L$ oraz z Wniosku 15.17 mamy, że $(K(l_0, \ldots, l_n) : K) < \infty$. Ponadto a jest algebraiczny względem ciała $K(l_0, \ldots, l_n)$, więc z Twierdzenia 15.15 mamy, że $\Big((K(l_0, \ldots, l_n))(a) : K(l_0, \ldots, l_n)\Big) < \infty$. Zatem z Twierdzenia 15.6 i z Wniosku 15.16, a jest algebraiczny względem ciała K. $\square$

Przykład 15.20. Udowodnimy, że zbiór $X = \{\sqrt[n]{12} : n = 2, 3, \ldots\}$ jest liniowo niezależny nad ciałem liczb wymiernych $\mathbb{Q}$. Z algebry liniowej I wystarczy udowodnić, że każdy niepusty skończony podzbór zbioru X jest liniowo niezależny nad ciałem $\mathbb{Q}$. Weźmy zatem dowolne liczby naturalne: s oraz $2 \leq n_1 < n_2 < \ldots < n_s$. Udowodnimy, że jest liniowo niezależny nad ciałem $\mathbb{Q}$ zbiór $A = \{\sqrt[n_1]{12}, \sqrt[n_2]{12}, \ldots, \sqrt[n_s]{12}\}$ i to zakończy rozwiązanie zadania. Niech $n = n_1 \cdot n_2 \cdot \ldots \cdot n_s$ oraz $m_i = \frac{n}{n_i}$ dla $i = 1, \ldots, s$. Wtedy dla każdego $i = 1, 2, \ldots, s$: $m_i \in \mathbb{N}$ oraz $\sqrt[n_i]{12} = (\sqrt[n]{12})^{m_i}$, przy czym $n > m_1 > m_2 > \ldots > m_s$, bo $n_1 \geq 2$ oraz $n_1 < n_2 < \ldots < n_s$. Stąd A jest podzbiorem s-elementowym zbioru $B = \{1, \sqrt[n]{12}, (\sqrt[n]{12})^2, \ldots, (\sqrt[n]{12})^{n-1}\}$ i wystarczy wykazać liniową niezależność nad $\mathbb{Q}$ zbioru B. Ale $\sqrt[n]{12}$ jest pierwiastkiem wielomianu $f = x^n - 12$, który jest nierozkładalny w $\mathbb{Q}[x]$ z kryterium Eisensteina przy $p = 3$, więc liniowa niezależność zbioru B wynika z Twierdzenia 15.14.

Przykład 15.21. Zilustrujemy udowodnione twierdzenia dla pewnych podciał ciała $\mathbb{R}$. Ponieważ $\sqrt{2}$ jest pierwiastkiem wielomianu $f = x^2 - 2$, który jest nierozkładalny w $\mathbb{Q}[x]$ z kryterium Eisensteina dla $p = 2$, więc na mocy Twierdzenia 15.14 bazą przestrzeni $\mathbb{Q}(\sqrt{2})$ nad $\mathbb{Q}$ jest $\{1, \sqrt{2}\}$, skąd $(\mathbb{Q}(\sqrt{2}) : \mathbb{Q}) = 2$ i $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

Załóżmy, że $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$. Wtedy $\sqrt{3} = a + b\sqrt{2}$ dla pewnych $a, b \in \mathbb{Q}$. Stąd po podniesieniu do kwadratu: $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ i z liniowej niezależności nad $\mathbb{Q}$ zbioru $\{1, \sqrt{2}\}$, $3 = a^2 + 2b^2$ i $2ab = 0$. Zatem $a = 0$ i $b^2 = \frac{3}{2}$, skąd $\sqrt{\frac{3}{2}} \in \mathbb{Q}$, co prowadzi do sprzeczności lub $b = 0$ i $a^2 = 3$, skąd $\sqrt{3} \in \mathbb{Q}$ i też mamy sprzeczność. Wobec tego $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Zatem wielomian $g = x^2 - 3$ ma stopień 2 i nie posiada pierwiastka w ciele $\mathbb{Q}(\sqrt{2})$. Ze Stwierdzenia 12.32 wynika więc, że wielomian g jest nierozkładalny w $(\mathbb{Q}(\sqrt{2}))[x]$ i $g(\sqrt{3}) = 0$. Wobec tego na mocy Twierdzenia 15.14 bazą przestrzeni $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ nad ciałem $\mathbb{Q}(\sqrt{2})$ jest zbiór $\{1, \sqrt{3}\}$ i $((\mathbb{Q}(\sqrt{2}))(\sqrt{3}) : \mathbb{Q}(\sqrt{2})) = 2$.

Ale $\mathbb{Q}$ jest podciałem ciała $\mathbb{Q}(\sqrt{2})$ i $\mathbb{Q}(\sqrt{2})$ jest podciałem ciała $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$, więc na mocy Twierdzenia 15.6, $((\mathbb{Q}(\sqrt{2}))(\sqrt{3}) : \mathbb{Q}) = 2 \cdot 2 = 4$. Ponadto z dowodu tego twierdzenia bazą przestrzeni $(\mathbb{Q}(\sqrt{2}))(\sqrt{3})$ nad ciałem $\mathbb{Q}$ jest zbiór $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2} \cdot \sqrt{3}\}$, więc

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

Ze Stwierdzenia 15.12 mamy, że $(\mathbb{Q}(\sqrt{2}))(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Zatem $(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) = 4$. Ale z Przykładu 15.5, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, więc także $(\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}) = 4$. Oznaczmy $a = \sqrt{2} + \sqrt{3}$. Wtedy $a^2 = 2 + 2\sqrt{6} + 3$, więc $(a^2 - 5)^2 = 24$, skąd $a^4 - 10a^2 + 1 = 0$. Wobec tego a jest pierwiastkiem wielomianu $f = x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ i $st(f) = 4$. Ale

$(\mathbb{Q}(a) : \mathbb{Q}) = 4$, więc wielomian minimalny h dla a nad ciałem $\mathbb{Q}$ ma stopień 4. Ponadto z Twierdzenia 15.11, $h|f$ w $\mathbb{Q}[x]$, więc $h \sim f$, czyli f jest wielomianem minimalnym dla a. W szczególności wielomian $f = x^4 - 10x^2 + 1$ jest nierozkładalny w $\mathbb{Q}[x]$.

Zagadka 1. W pierścieniu $\mathbb{Q}[x]$ dany jest ideał $I = (x^4 + 2x + 2)$. Udowodnij, że pierścień ilorazowy $\mathbb{Q}[x]/I$ jest ciałem i wyznacz element odwrotny do warstwy $\alpha = (x^6 + 2x^3 + 2x^2 + x + 1) + I$.

Zagadka 2. Udowodnij, że ciało L wszystkich zespolonych liczb algebraicznych jest przeliczalne i jest algebraicznie domknięte, tzn. każdy wielomian dodatniego stopnia z $L[x]$ ma pierwiastek w L.

Zagadka 3. Czy zbiór $\{\sqrt[n]{2} \ : \ n = 2, 3, \ldots\}$ jest liniowo niezależny nad $\mathbb{Q}$?

Zagadka 4. Czy jest prawdą, że $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$?

Zagadka 5. Wyznacz wielomian minimalny elementu $a = \sqrt{3} + \sqrt{5}$ ciała $\mathbb{R}$ nad ciałem $\mathbb{Q}$.

Zagadka 6. Czy $\sqrt{5} \in \mathbb{Q}(\sqrt{3})$?

Zagadka 7. Czy pierścień ilorazowy $\mathbb{Z}_3[x]/(x^4 + 1)$ jest ciałem?