

$\mathbb{C} \supseteq \mathbb{Q}$
 $\mathbb{Q}(a) \supseteq \mathbb{Q}$ skalarów $K \rightarrow \alpha_i$
 wektorów $L \rightarrow w_i, \alpha w_i$

DEF. Dwa ciała $L \supseteq K$, wtedy: K podciało L lub L rozszerzenie K
 $\alpha_1 w_1 + \dots + \alpha_n w_n$
 baza, komb. liniowa

■ L można traktować jako przestrzeń liniową nad K — $\dim_K L = [L : K]$ stopień rozszerzenia

PRZYKŁADY:

✓ $[\mathbb{C} : \mathbb{R}] = 2$, baza $\{1, i\} \Rightarrow \underline{a+bi}, a, b \in \mathbb{R}$

lin. niezal. $a+bi=0 \Rightarrow a=b=0$

$$\mathbb{Q}(i) = \{a+bi : a, b \in \mathbb{Q}\}$$

$$[\mathbb{Q}(i) : \mathbb{Q}] = 2$$

✓ $[\mathbb{R} : \mathbb{Q}] = \infty$ nie ma skończonego zbioru generatorów

$$a = \alpha_1 g_1 + \dots + \alpha_r g_r$$

✓ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ baza $\{1, \sqrt{2}\}$

$$\{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$$

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

$$a = -b\sqrt{2}, a^2 = b^2 \cdot 2$$

lin. niezal.

■ $L \supseteq M \supseteq K$ ciała, to $[L : K] = [L : M][M : K]$.

$$\underline{D-4} \quad [L : M] = r, [M : K] = s$$

baza: $a_1, \dots, a_r$

$b_1, \dots, b_s$

(?) $\sqrt{2}, \sqrt[3]{2}, \sqrt[5]{2}, \sqrt[7]{2}, \dots$
 $\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots$

$$a \in L \Leftrightarrow \alpha_1 a_1 + \dots + \alpha_r a_r, \quad \alpha_i = \beta_1^i b_1 + \dots + \beta_s^i b_s$$

$$a = \sum_i \alpha_i a_i$$

$$\alpha_i \in M, a_i \in L$$

$$\alpha_i = \sum_j \beta_j^i b_j$$

$$\beta_j^i \in K, b_j \in M$$

generatory r.s

$$a = \sum_i \left(\sum_j \beta_j^i b_j \right) a_i = \sum_{(i,j) \in K \times L} \beta_j^i (b_j a_i)$$

liniowa niezależność $b_j a_i$ — podanie $\triangleright$

$$\{b_j a_i\} \text{ — baza } \Rightarrow \text{ wzór}$$

$\mathbb{C} \supseteq \mathbb{Q}$ liczba algebraiczna

$f \neq 0$

DEF. $a \in L \supseteq K$ **element algebraiczny** nad K , jeśli istn. $f \in K[x] : f(a) = 0$. (a jest pierwiastkiem)

DEF. f - wielomian **minimalny** elementu algebraicznego a , jeśli najniższego stopnia, unormowany $a_n = 1$

FAKT: f minimalny $\Rightarrow$ nierozkładalny, wyznaczony jednoznacznie, $m_a(x)$, dzieli wszystkie inne. $\therefore f(a) = 0$

$$f(a) = g(a) \cdot h(a) = 0 \xRightarrow{\text{bez d.}} g(a) = 0 \vee h(a) = 0 \quad f(x) : m_a(x) =$$

DEF. w przeciwnym razie a **transcendentny** (lub przestępny)

$$f(x) = m_a(x) \cdot s(x) + r(x)$$

$$\Rightarrow r(a) = 0 \quad r(x) = 0$$

■ $[L : K] < \infty$, to każdy element L algebraiczny nad K

daw $a \in L$

Dł $[L : K] = n \quad 1, a, a^2, \dots, a^n \leftarrow$ liniowo zależne
 $\Rightarrow \exists \alpha_i \in K \quad \alpha_0 + \alpha_1 a + \dots + \alpha_n a^n = 0$ bo $|1, \dots, a^n| = n+1$
 $\Rightarrow a$ - algebraiczny.

PRZYKŁADY: $2+i, \sqrt{1+\sqrt[3]{2}}$ nad $\mathbb{Q}$

$$z = 2+i \quad z^2 = (2+i)^2 = 4+2i-1$$

$$z-2=i \quad (z-2)^2 = -1 \quad z^2 - 2z + 4 = -1 \Rightarrow z - \text{algebraiczny nad } \mathbb{Q}$$

$$a = \sqrt{1+\sqrt[3]{2}} \quad a^2 = 1+\sqrt[3]{2} \quad a^2 - 1 = \sqrt[3]{2}$$

$$(a^2 - 1)^3 = 2 \Rightarrow a \text{ algebraiczny nad } \mathbb{Q}$$



■ $\bigcap$ przekrój dowolnej rodziny podciał (podpierścieni) jest podciałem (podpierścieniem),

▣ $\cap L_i$ – jest podzbiorem

$\bigcap_{i=1}^n L_i = \{x, y\}$ (nonempty)
 $x, y \in \bigcap_{i=1}^n L_i \Leftrightarrow \forall i (x, y \in L_i) \Leftrightarrow \forall i (x, y \in L_i) \Leftrightarrow x, y \in \bigcap_{i=1}^n L_i$

zamen
na odjman.
i murtel

Dzi

(1) $K[a] = \{c_0 + c_1 a + \dots + c_m a^m : m \in \mathbb{N}, c_i \in K\}$ ma odzwierciedlenie i mnożenie

można wziąć $m = n-1$ s.t. $f(a) \in K[a]$

$f(x) = w_a(x) \cdot s(x) + r(x) \Rightarrow f(a) = 0 + r(a)$ OK
 ? st < n $\underbrace{c_0 + \dots + c_{n-1} a^{n-1}}$

$$(2) f(a) \in K[a] \stackrel{?}{=} \frac{1}{f(a)} \stackrel{\text{stz n}}{\in} K[a]$$

$\Rightarrow f(a) \in K[a] \Rightarrow f(a) \in K$
 ist zureichend: $f(x), m_a(x)$, dann $NWD(f(x), m_a(x)) \sim 1$
 $\Rightarrow \exists d(x), p(x)$ | $\text{ggT} \neq 1$, $\text{to } m_a(x)$
 $p(x) \cdot p(x) = 1$ | ggT nicht ~ 1

$$\Rightarrow \exists \alpha(x), \beta(x)$$

$$\alpha(x)f(x) + \beta(x)m_a(x) = 1$$

$$\alpha(a)f(a) + \frac{\beta(a)m_a(a)}{0} = 1$$

$$\alpha(a) \cdot f(a) = 1$$

$$d(a) = \frac{1}{f(a)}$$

WNIOSEK: Jeśli a jest elementem algebraicznym nad K , to $[K(a) : K] = \deg(m_a(x))$.
stopień rozszerzenia = stopień wielomianu minimalnego = (def) stopień elementu a

$$\begin{aligned} & [K(a) : K] < \infty \\ & \Leftrightarrow a\text{-algebraiczny} \end{aligned}$$

$$L \supseteq K$$

■ $L \not\subseteq K$. Zbiór $\text{alg}_K(L)$ elementów L algebraicznych nad K jest ciałem $L \not\subseteq \text{alg}_K(L) \not\subseteq K$.

$$\text{Dł. } a, b \in \text{alg}_K(L) \Rightarrow \frac{a-b}{\frac{a}{b}} \quad h(a-b) \stackrel{?}{=} 0 \quad ?$$

$$\begin{aligned} & \left. \begin{array}{l} f(a)=0 \\ g(b)=0 \end{array} \right\} \Rightarrow b \text{ jest algebraiczny nad } K(a), \quad (K(a))(b) = K(a, b) \\ & \text{obn składowe} \Rightarrow [K(a, b) : K] \text{-składowe} \end{aligned}$$

każdy $c \in K[a, b]$ algebr. nad K , w szczególności $a-b, \frac{a}{b} \in K[a, b]$

■ Ciała $\text{alg}_{\mathbb{Q}}(\mathbb{C}), \text{alg}_{\mathbb{Q}}(\mathbb{R})$ są przeliczalne ($\aleph_0$).

Ciągi $(a_0, a_1, \dots, a_n)$ $a_i \in \mathbb{Q}$

$$\text{stop.} \quad \min \frac{a(x)}{b} \in \mathbb{N}$$

■ Liczb przestępnych w $\mathbb{R}$ jest nieprzeliczalnie wiele (continuum). (WNIOSEK: $[\mathbb{R} : \mathbb{Q}] = \infty$).

■ *Konkretne liczby przestępne*: pewna klasa rozwinięć nieskończonych (Liouville 1844), liczba e (Hermite 1873), liczba π (Lindemann 1882), liczby postaci $a^b 2^{\sqrt{2}}$ (Gelfond 1934),

para klasa

Oznaczenia: $K[x], K(x)$ – ciało funkcji wymiernych nad K , rozszerzenia o element niealgebraiczny x
 $K(\pi) \cong K(x)$, $K[\pi] \cong K[x]$

$$\frac{w(x)}{u(x)} \in K(x)$$

■ Dla ciała K następujące warunki są równoważne:

- (i) każdy $f \in K[x]$ ma pierwiastek w K $\Leftrightarrow \Delta > 0$
- (ii) każdy $f \in K[x]$ rozkłada się w K na czynniki liniowe
- (iii) K nie ma rozszerzeń skończonych

$$(i) \Rightarrow (ii) \quad f(x) = (x-a) \underbrace{f_1(x)} \Rightarrow \dots (x-a)(x-a_1) \dots (x-a_r) a_{\text{res.}}$$

pierwiastki wielomianu(?)

$$(ii) \Rightarrow (iii) \quad \text{Nie wpł. } L \supseteq K, [L : K] < \infty$$

$$\exists a \in L/K, \text{ algebraiczny} \quad \exists f(x) \in K[x] \quad (sk \Rightarrow \text{algebr}) \quad f(a) = 0 \quad a_i \in K.$$

$$\Rightarrow a_i \in K \quad \hookrightarrow$$

$$f(x) = (x-a_1) \dots (x-a_n)$$

(iii) $\Rightarrow$ (i) – dalej $\downarrow$ $f(x)$ – wielomian, to ist. rozwiązanie z pierwiastkami

DEF. ↑ **ciało algebraicznie domknięte** (na przykład $\mathbb{C}$)

■ Ciało $\text{alg}_{\mathbb{Q}}(\mathbb{C})$ jest algebraicznie domknięte.

$$\mathbb{C} \supseteq \text{alg}_{\mathbb{Q}}(\mathbb{C}) \supseteq \mathbb{Q}$$

$$\rightarrow f(x) = a_0 + a_1x + \dots + a_nx^n, \quad a_i \in \mathbb{A} \quad f(a) = 0 \Rightarrow \exists g$$

$$g(x) = b_0 + b_1x + \dots + b_mx^m, \quad b_i \in \mathbb{Q} \quad g(a) = 0$$

$p_1, p_2, \dots, p_n \rightarrow$ pierw. wiel. $f(x)$

$$\mathbb{Q}(a_1, a_2, \dots, a_n) \supseteq \mathbb{Q}(a_1, \dots, a_{n-1}) \supseteq \dots \supseteq \mathbb{Q}(a_1)$$

składowe algebra

$$\Rightarrow [L : \mathbb{Q}] < \infty, \quad f(a) = 0, \quad a \in \mathbb{C} \quad [L(a) : \mathbb{Q}] < \infty \quad \overline{[L(a) : \mathbb{Q}]} < \infty$$

■ Każde ciało ma rozszerzenie do ciała algebraicznie domkniętego, i takie rozszerzenie jest wyznaczone jednoznacznie (z dokładnością do izomorfizmu).

algebraicznie domknięcie - ↑ a -ady $\text{alg}_{\mathbb{Q}}$

Najpierw:

DEF. Jeśli istn. ciało $L \supseteq K$, w którym $f \in K[x]$ ma rozkład na czynniki liniowe, to takie ciało z najmniejszym stopniem rozszerzenia $[L : K]$ nazywamy **ciałem rozkładu wielomianu** f ,

■ $f \in K[x], \deg(f) = n > 0$, to istn. rozszerzenie $L \supseteq K, [L : K] \leq n$, w którym f ma pierwiastek.

D-d Możemy złożyć f -niezmienny $K[x]$, ideał (f)

$$L = \frac{K[x]}{(f)} - \text{ciężko}, \quad \supseteq K$$

$$f(x) = a_0 + a_1x + \dots + a_nx^n = f(y)$$

elem $a = \underline{x + (f)} \in \frac{K[x]}{(f)}$

$$a + (f) = b + (f) \in \frac{K[x]}{(f)}$$

$$\stackrel{\text{st. 0}}{\Leftrightarrow} (a-b) + (f) = 0 (= (f))$$

$$\underline{a-b} \in (f) \stackrel{\text{st. 0}}{\Rightarrow} \underline{a-b} = \underline{f(y)}$$

$$a_0 + a_1(x + (f)) + \dots + a_n(x + (f))^n =$$

$$\stackrel{x + (f)}{=} \underline{x^n + (f)} = \underline{(a_0 + a_1x + \dots + a_nx^n) + (f)} =$$

$$= \underline{f(x) + (f)} = \underline{(f)} \text{ zerowa}$$

■ $f \in K[x]$, niezmienny, $f(a) = f(b) = 0$ (pierw). wtedy

||| $K(a) \cong K(b)$

$K \rightarrow K + \text{trimini}$
 $a \rightarrow b$

↑
sposób
(niezmienny)

$\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt[3]{2})$

niezmienny

$$\mathbb{Q}(1+i) \cong \mathbb{Q}(1-i) \quad - \quad (x-(1+i))(x-(1-i)) = (x^2-1)^2 + 1 = x^4 - 2x^2 + 2$$

■ WNIOSEK. ... istn. rozszerzenie $L \supseteq K$, $[L : K] < n!$, w którym f ma rozkład na czynniki liniowe.

$$d_m \leftarrow \text{pierwiastki} \leq L$$

■ Ciało rozkładu wielomianu $K(f) = K(a_1, \dots, a_m)$ jest wyznaczone jednoznacznie z dokładnością do izomorfizmu.

minimalne

$$\mathbb{R}(x^2+1) = \mathbb{R}(i) = \mathbb{C} \quad x^2+1 = (x-i)(x+i)$$

$$[\mathbb{C} : \mathbb{R}] = 2$$

$$\mathbb{Q}(x^2+1) = \{a+bi : a, b \in \mathbb{Q}\}$$

$$[\mathbb{Q}(x^2+1) : \mathbb{Q}] = 2.$$

ciała rozkładu wielomianu

$$\mathbb{R}(f)$$



PRZYKŁADY. $\mathbb{R}(x^2+1)$, $\mathbb{Q}(x^3-2)$, $\mathbb{Q}((x^2+1)(x^2-2))$

$$\mathbb{Q}(x^3-2) =$$

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$$

$$x^3-2 = (x-\sqrt[3]{2})(x-\epsilon\sqrt[3]{2})(x-\epsilon^2\sqrt[3]{2})$$

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$$

$$\mathbb{Q}(\sqrt[3]{2}, \epsilon\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \epsilon)$$

$$= (\mathbb{Q}(\sqrt[3]{2}))(\epsilon) \quad x^3-1 = (x-1)(x^2+x+1)$$

$$[\mathbb{Q}(x^3-2) : \mathbb{Q}] = 6$$

$$\epsilon = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$$

$$L = \mathbb{Q}((x^2+1)(x^2-2))$$

$$(x^2+1)(x^2-2) = (x-i)(x+i)(x-\sqrt{2})(x+\sqrt{2})$$

$$= \mathbb{Q}(i, \sqrt{2}) \quad \text{Jaki jest}$$

$$[L : \mathbb{Q}(i, \sqrt{2})] = 1 \quad (?)$$

$$= \mathbb{Q}(i+\sqrt{2}) \quad \geq \text{oczywiste.}$$

$$(\mathbb{Q} \subseteq \mathbb{Q}(i, \sqrt{2}) \supseteq \mathbb{Q}(i+\sqrt{2}))$$

$$a = i+\sqrt{2} \quad \text{wiel. minimalne?}$$

$$|i + \sqrt{2} \rightarrow i, \sqrt{2}|$$

$$(i + \sqrt{2})^2 = -1 + 2\sqrt{2}i + 2 = 2\sqrt{2}i + 1$$

$$8(1) +$$

$$\boxed{a = i + \sqrt{2}}$$

$$\bar{a} = \sqrt{2} - i$$

wird m.n. stop. 2. ? $\mathbb{Q}$

$$(x - (\sqrt{2} + i))(x - (\sqrt{2} - i)) = \underline{x^2 - 2\sqrt{2}x + 3}$$

$\Rightarrow$ st. 4

$$(a^2 + 3)^2 = (2a\sqrt{2})^2 = 8a^2 \quad \underline{f(x) = x^4 - 2x^2 + 9} > 0$$

$$a^2 = (i + \sqrt{2})^2 = 2\sqrt{2}i + 1 \quad -2(2\sqrt{2}i + 1) + 4 \quad (x^4 - 2x^2 + 9)$$

$$a^4 = -6 + 1 + 4\sqrt{2}i = \underline{-5 + 4\sqrt{2}i}$$

$$\boxed{i + \sqrt{2} \rightarrow i, \sqrt{2}}$$

$$\mathbb{Q}(x^4 - 2x^2 + 9)$$

$$\underline{a + b(i + \sqrt{2}) + c(i + \sqrt{2})^2 + d(i + \sqrt{2})^3 = i + \sqrt{2}}$$

$$\underline{(\mathbb{Q}(i))(\sqrt{2})}$$

$$a, b, c, d \in \mathbb{Q}$$

 2AD.

