CIAŁA.

Podstawowe własności.

- Obliczenia podobne jak w $(\mathbb{R}+,\cdot)$ — I semestr.
- W ciałach nie istnieją (nietrywialne) dzielniki zera
- Ideałami w ciele K są tylko K oraz $\{0\}$.

PODCIAŁA

Def. Niech $(K,+,\cdot)$ ciało. $A\subseteq K$ nazywamy podciałem gdy, $\forall a,b\in A$ $a+b, -a, a\cdot b, a^{-1}\in A$ $a\neq 0$.

Fakt Niech $(K+,\cdot)$ ciało $A\subseteq K$ podciało
Wtedy $(A+,\cdot)$ jest ciałem.

Lemat. Niech $\mathcal{K}$ rodzina podciał ciała K
Wtedy, $\bigcap\mathcal{K}$ jest podciałem K.

Def Niech K ciało, $A\subseteq K$.
Podciałem generowanym przez A nazywamy zbiór:

$$\langle A\rangle=\bigcap\{L\leqslant K:\ A\subseteq L\}$$

$L\leqslant K$ znaczy, że L jest podciałem K.

Przykłady. $K=\mathbb{R}$. $A=\mathbb{Q}\cup\{\sqrt{2}\}$.

$$\langle A\rangle=\{a+b\sqrt{2}:\ a,b\in\mathbb{Q}\}:=\mathbb{Q}(\sqrt{2})$$

$K=\mathbb{R}$ $A=\mathbb{Q}\cup\{\sqrt[3]{2}\}$
$\langle A\rangle=\mathbb{Q}(\sqrt[3]{2})=\{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2\ a,b,c\in\mathbb{Q}\}$

- PRODUKT

Przykład $\mathbb{R}\times\mathbb{R}$ nie jest ciałem bo $(1,0)$ jest różnym od zera elementem nieodwracalnym

Fakt Niech K, L ciała, wtedy $K\times L$ jest ciałem $\leftrightarrow$ $|K|=1 \vee |L|=1$

- HOMOMORFIZMY

Def. Niech K, L ciała, $f: K\to L$.
Wtedy f nazywamy homomorfizmem, gdy:

$$\forall_{a,b\in K} \quad f(a+b) = f(a)+f(b)$$
$$f(a\cdot b) = f(a)\cdot f(b).$$

Obserwacja. homomorfizm ciał jest homomorfizmem pierścieni

Przykład: $f(a+b\sqrt{2}) = a-b\sqrt{2} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ homomorfizm ciał.

Fakt. Niech K, L - ciała, $f: K\to L$ homomorfizm.
Wtedy albo
$$\forall_{a\in K} \quad f(a)=0$$
albo f jest różnowartościowy.

D-d. Funkcja $f: K\to L$ jest homomorf. pierścieni.
Rozważmy $\operatorname{Ker} f = \{a\in K : f(a)=0\}$
Wiemy, że
$$\operatorname{Ker} f \trianglelefteq K$$
K jest ciałem, więc albo $\operatorname{Ker} f = K$, albo $\operatorname{Ker} f = \{0\}$

Jeśli $\ker f = K$. Wtedy $\forall a \in K$ $a \in \ker f$, tzn $f(a) = 0$.

Jeśli $\ker f = \{0\}$. Wtedy f jest różnowartościowa. $\square$.

Wniosek. Nietrywialne homomorfizmy ciał są włożeniami.

Def. Funkcję $f: K \to L$ nazywamy izomorfizmem jeśli jest bijekcją i homomorfizmem.

Przykład $f(a+b\sqrt{2}) = a - b\sqrt{2} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ izomorfizm

$f(z) = \bar{z} : \mathbb{C} \to \mathbb{C}$ izomorfizm.

- Izomorfizm ciała K w ciało K nazywamy automorfizmem.

Fakt. Niech $K \leq L$ ciała. $f(x) \in K[x]$ wielomian nierozkładalny w $K[x]$. Niech $a, b \in L$, $f(a) = f(b) = 0$

Wtedy istnieje izomorfizm.

$$\varphi : K(a) \to K(b)$$

taki, że
- $\varphi(a) = b$.
- $\forall k \in K$ $\varphi(k) = k$.

- Rozszerzenia ciał, elementy algebraiczne.

Def Niech $K \leq L$ ciała. Element $a \in L$ nazywamy algebraicznym nad K gdy istnieje wielomian różny od zera $f(x) \in K[x]$ taki że $f(a) = 0$.

Przykłady - $\mathbb{Q} \leq \mathbb{R}$. $a = \sqrt{2} \in \mathbb{R}$

$\sqrt{2}$ jest algebraiczny bo jest pierwiastkiem wielomianu
$f(x) = x^2 - 2 \in \mathbb{Q}[x]$.

• π nie jest liczbą algebraiczną

Fakt. Niech $K \leq L$ ciała skończone, wtedy każdy element $a \in L$ jest algebraiczny nad K.

D-d. L jest przestrzenią liniową nad K.
Niech $n = \dim(L/K)$.
Rozważmy zbiór $A = \{1, a, a^2, a^3, \dots, a^n\}$.
$|A| = n+1$ więc A jest liniowo zależny, tzn
$\exists k_0, k_1, k_2, \dots, k_n \in K$ takie, że

$1 \cdot k_0 + a \cdot k_1 + \dots k_n a^n = 0$
tzn, że a jest pierwiastkiem $f(x) = k_0 + k_1 x + \dots + k_n x^n \in K[x]$
$\square$

Fakt. Istnieją liczby rzeczywiste nie algebraiczne nad $\mathbb{Q}$
D-d.
Niech $\mathbb{R} \supseteq K \supseteq \mathbb{Q}$, $K = \{a \in \mathbb{R} : a \text{ - algebr nad } \mathbb{Q}\}$

$$K \subseteq \bigcup_{\substack{f \in \mathbb{Q}[x] \\ \neq 0}} \{a \in \mathbb{R} : f(a) = 0\}$$

• $(\forall f \in \mathbb{Q}[x]) \ |\{a \in \mathbb{R} : f(a) = 0\}| < \aleph_0$
• $|\{f \in \mathbb{Q}[x]\}| = \aleph_0$

$$|K| \leq \left|\bigcup_{\substack{f \in \mathbb{Q}[x] \\ \neq 0}} \{a \in \mathbb{R} : f(a) = 0\}\right| \leq \aleph_0 \cdot \aleph_0 = \aleph_0$$

Ale $|\mathbb{R}| = \mathfrak{c} > \aleph_0$ zatem istnieje liczba $t \in \mathbb{R} \setminus K$

Takie t jest liczbą niealgebraiczną. $\square$

Przykład • Liczby π, e, są niealgebraiczne.
• $0{,}\underset{1}{1}\underset{2}{1}0\underset{2^2}{1}000\underset{2^3}{1}0000000\underset{2^4}{1}00\ldots$ jest niealgebraiczna.

• Ciała algebraicznie domknięte.

Def Ciało K nazywamy algebraicznie domkniętym, gdy
$\forall_{\substack{f \in K[x] \\ st f > 0}} \; \exists a \in K \quad f(a) = 0$

Przykład. • $\mathbb{C}$ jest ciałem algebr. domkniętym.
• $\mathbb{R}$ NIE jest algebr. domknięte bo x^2+1 nie ma pierw. w $\mathbb{R}$.

Fakt. 1. Ciała skończone NIE są algebraicznie domknięte
2. Dla każdego ciała K istnieje ciało $L \supseteq K$ które jest algebraicznie domknięte.

D-d. 1. Niech $K = \{k_1, k_2, \ldots k_n\}$.
Wtedy $f = (x-k_1)(x-k_2)\ldots(x-k_n)+1 \in K[x]$
$\forall k \in K \quad f(k) = 1 \neq 0$.

2. Konstrukcja ciała L bazuje na obserwacji, że jeśli $f(x) \in K[x]$ nierozkładalny to

$f(x) = 0$ ma rozwiązanie w ciele $K[x]/\langle f \rangle \hookleftarrow K$

• Ciała skończone
Niech f wielomian stopnia n nierozkładalny nad $\mathbb{Z}_p$ $p \in \mathbb{P}$
Wtedy $\mathbb{Z}_p[x]/\langle f \rangle$ jest p^n-elementowym ciałem.

Tw. Każde ciało skończone ma moc p^n gdzie $p \in \mathbb{P}$ $n \in \mathbb{N}$.

\# Tw. Dla każdych $p \in \mathbb{P}$, $n \in \mathbb{N}$ istnieje ciało K. $|K| = p^n$.

Tw. Jeśli K, L ciała skończone. $|K| = |L| \Rightarrow K \cong L$

Komentarz do \#:

Niech L ciało algebraicznie domknięte $\mathbb{Z}_p \leq L$.

Niech $f(x) = x^{p^n} - x$

Wtedy $K = \{a \in L : f(a) = 0\}$ -

- $f(x)$ jest wielomianem stopnia p^n bez pierwiastków wielokrotnych:
  $NWD(f, f') = NWD(x^{p^n} - x, p^n x^{p^n - 1} - 1) = 1$.
  Zatem $|K| = p^n$.

- K jest podciałem L. W ciele charakt. p: $(x+y)^p = x^p + y^p$
  Niech $a, b \in K$, wtedy $f(a) = a^{p^n} - a = 0$, $f(b) = 0$. Więc
  $f(a+b) = (a+b)^{p^n} - (a+b) = a^{p^n} + b^{p^n} - a - b = (a^{p^n} - a) + (b^{p^n} - b) =$
  $= 0 + 0 = 0$
  Więc $a+b \in K$.
  Także $a \cdot b \in K$ ...
  Zatem $K \leq L$

Zatem K jest p^n elementowym ciałem.