CIAŁA: $(K, +, \cdot)$ takie że

1. $(K, +)$ jest grupą przemienną
2. $(K \setminus \{0\}, \cdot)$ grupa przemienna
3. Rozdzielność mnożenia wzgl. dodawania

Przykłady: $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$.

Ciało $\mathbb{Z}_p = (\{0, 1, \dots, p-1\} +_p, \cdot_p)$ p liczba pierwsza.

Ciało $\mathbb{Z}_{11}$: $(\{0, 1, 2, \dots, 10\} +_{11}, \cdot_{11})$.

5^{-1}: $5^{-1} = x$ wtedy $5 \cdot_{11} x = 1$

$5 \cdot x \pmod{11} = 1$

$5 \cdot x = 11k + 1$ $\quad k \in \mathbb{Z}$.

$5 \cdot x + 11y = 1$ $\quad y = -1$

odpowiada: $5 \cdot (-2) + 11 \cdot 1$

$x = -2$

$(-2) \bmod 11 = 9$. $\quad 9 \in \{0, \dots 10\}$

Spr. $5 \cdot_{11} 9 = (5 \cdot 9) \bmod 11 = 45 \bmod 11 = 1$.

$5^{-1} = 9$

- Układ równań w $\mathbb{Z}_{11}$:

$$\begin{cases} x +_{11} 3 \cdot_{11} y = 1 & | \cdot_{11} 2 \\ 2 \cdot_{11} x +_{11} 5 \cdot_{11} y = 2 \end{cases} \sim \begin{cases} 2x +_{11} 6y = 2 \\ 2x +_{11} 5y = 2 \end{cases}$$

$$\sim \quad 1y = 0$$

$$y = 0$$

$6 -_{11} 5 =$
$6 +_{11} (-5) =$
$6 +_{11} 6 = 1$

Podst $y = 0$ do równania 1:

$x +_{11} 3y = 1$

$x +_{11} 3 \cdot 0 = 1$

$x + 0 = 1$

$x = 1$

$$\begin{cases} x = 1 \\ y = 0 \end{cases}$$

• Równanie kwadratowe w ciele $\mathbb{Z}_7 = (\{0,1,\dots,6\}, +_7, \cdot_7)$.

$x^2 + 2x + 6 = 0$. $\quad \left| \begin{array}{l} + = +_7 \\ 2x = 2 \cdot_7 x \end{array} \right. \quad x^2 = x \cdot_7 x$

$\Delta = b^2 - 4ac = 2^2 - 4 \cdot 1 \cdot 6 = 4 - 3 = 4 + (-3) = 4 + 4 = 1$

$\sqrt{\Delta} = \sqrt{1} : \sqrt{1} = 1 \ (6)$

$x_1 = \frac{-b + \sqrt{\Delta}}{2a} = \frac{-2+1}{2} = \frac{5+1}{2} = \frac{6}{2} = 6 \cdot 2^{-1} = 3(2 \cdot 2^{-1}) = 3 \cdot 1 = 3$ (3 nad równością)

$x_2 = \frac{-b - \sqrt{\Delta}}{2a} = \frac{-2-1}{2} = \frac{5+6}{2} = \frac{4}{2} = 2$

Spr: x_1: $x_1^2 + 2x_1 + 6 = 3^2 + 2 \cdot 3 + 6 = 2 + 6 + 6 = 0$. ok.

x_2 ...

CIAŁO $\mathbb{Q}[\sqrt{2}]$

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

• $\mathbb{Q} \subsetneq \mathbb{Q}[\sqrt{2}] \subsetneq \mathbb{R}$

$A \subsetneq B$ oznacza $A \subseteq B$ ale $A \neq B$ tzn A jest istotnie "mniejszy" zbiorem niż B ($A \subset B$)

Fakt $\mathbb{Q}[\sqrt{2}]$ jest ciałem.

Dowód:

• zauważmy $+, \cdot$ jest łączne i przemienne, oraz prawdziwe jest rozdzielność mnożenia względem dodawania.

• Element neutralny dodawania to $0 = 0 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

Element neutralny mnożenia to $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

• Element odwrotny do $a + b\sqrt{2}$ wzgl. dodawania to $-a - b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$

• Element odwrotny do $a + b\sqrt{2}$ względem mnożenia to

$$\frac{1}{a+b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \left(\frac{a}{a^2-2b^2}\right) + \left(\frac{-b}{a^2-2b^2}\right) \cdot \sqrt{2} \in \mathbb{Q}[\sqrt{2}]$$

□

Uwaga. $\mathbb{Q}[\sqrt{n}]$ jest ciałem, dla wszelkiej liczby $n \in \mathbb{N}$.

LICZBY NATURALNE.

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$

Zasada dobrego uporządkowania (WO).

- Każdy niepusty podzbiór zbioru $\mathbb{N}$ ma element najmniejszy.

$(\forall X \subseteq \mathbb{N} \quad \exists a \in X \quad \forall b \in X) \quad b \geq a$

Uwaga.
- Zasada WO nie jest prawdziwa w $\mathbb{Z}, \leq$
- Zasada WO nie jest prawdziwa $[0, \infty)$ bo $(0, 1)$ nie ma elementu najmniejszego.

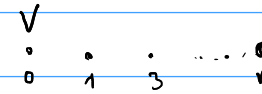
Zasada indukcji matematycznej IND.

$\forall A \subseteq \mathbb{N} \left[0 \in A \wedge \forall n \in \mathbb{N} \quad n \in A \to n+1 \in A \right] \to (\forall n \in \mathbb{N} \quad n \in A)$

TW. Zasada IND wynika z WO.

Dowód. Załóżmy WO oraz że IND jest nieprawdziwa:

$\exists A \subseteq \mathbb{N} \left[0 \in A \wedge \forall n \in \mathbb{N} \quad n \in A \to n+1 \in A \right] \wedge (\exists n \in \mathbb{N} \quad n \notin A)$

Rys 

Rozważmy zbiór $X = \{n \in \mathbb{N} : n \notin A\} = A^c$

Oblewo: $X \neq \emptyset$ oraz $0 \notin X$

Na mocy WO X ma element najmniejszy, oznaczmy go a.

Uwaga $a \neq 0$ zatem $a-1 \notin X$ więc $a-1 \in A$
zatem $a = (a-1)+1 \in A$, (ale $a \in X = A^C$)
$a \in A \wedge a \in A^C$, sprzeczność.
Zatem WO $\rightarrow$ IND $\square$.

Przykład.
Dowód faktu: $(\forall n \in \mathbb{N})\ 2 \mid n^2+n$.

Niech $A = \{n \in \mathbb{N} : 2 \mid n^2+n\}$
Zauważmy:
1. $0 \in A$ bo $2 \mid 0^2+0$
2. $(\forall n)\ n \in A \rightarrow n+1 \in A$, bo
$n \in A \rightarrow 2 \mid n^2+n \rightarrow 2 \mid n^2+n+2(n+1) \rightarrow$
$2 \mid n^2+2n+1+n+1 \rightarrow 2 \mid (n+1)^2+(n+1)$
$\rightarrow n+1 \in A$.

(1) i (2): $[0 \in A \wedge \forall n \in \mathbb{N}\ \ n \in A \rightarrow n+1 \in A] \xrightarrow{IND}$

$(\forall n)\ n \in A$
tzn $(\forall n)\ 2 \mid n^2+n$