Těleso Z2

- $Z_2 = \{0, 1\}$ se sčítáním „modulo“ a obvyklým násobením
- Uspořádané n-tice prvků ze Z_2 tvoří lineární prostor

Těleso

- je možina T prvků, na které jsou definovány operace + a $\cdot$, které splňují obvyklé vlastnosti, jako operace + a $\cdot$ s reálnými čísly.
- Jmenovitě pro všechna $a, b, c \in T$ platí:
- Asociativní zákon: $(a + b) + c = a + (b + c)$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Existence „neutrálního prvku“: $a + 0 = a$, $a \cdot 1 = 1 \cdot a = a$.
- Pro všechna $a \in T$ existuje $b \in T$ tak, že $a + b = 0$ (opačný prvek).
- Pro všechna $a \in T \setminus \{0\}$ ex. $b \in T$ tak, že $a \cdot b = 1$ (inverzní prvek).
- Komutativní zákon pro operaci +: $a + b = b + a$.
- Platí-li navíc komutativní zákon pro operaci $\cdot$: $a \cdot b = b \cdot a$, říkáme množině T *komutativní těleso*.

Z2

Množina $\mathbf{Z}_2 = \{0, 1\}$ s operacemi + a $\cdot$:

- $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 0$,
- $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, $1 \cdot 1 = 1$

tvoří těleso.

- Operace $\cdot$ je obvyklá a v operaci + je jedna výjimka. Nebo jiný pohled: + pracuje jako XOR, $\cdot$ jako AND, nebo jiný pohled: výsledek operace je potřeba upravit „modulo dvěma“, nebo jiný pohled: 0 značí sudá čísla a 1 lichá čísla a operace pracují s těmito množinami.

Lineární prostor „nad tělesem“

Nahradíme-li v definici lineárního prostoru množinu $\mathbf{R}$ reálných čísel množinou T, která je libovolným tělesem, dostáváme *lineární prostor nad tělesem T*.

Veškeré pojmy lineární algebry (lineární závislost, báze, lineární obaly, podprostory) „fungují“ stejně v lineárním prostoru nad tělesem T.

Příklad: Množina uspořádaných n-tic prvků z T s operacemi:

- $(a_1, a_2, \cdots, a_n) + (b_1, b_2, \cdots, b_n) \;=\; (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$
- $\alpha \cdot (a_1, a_2, \cdots, a_n) \;=\; (\alpha \cdot a_1, \alpha \cdot a_2, \cdots, \alpha \cdot a_n)$

kde $a_i \in T$, $b_i \in T$, $\alpha \in T$, je lineární prostor nad T. Tento lineární prostor značíme T^n.

Lineární prostor n-tic z tělesa Z2

Je konkretizací předchozího příkladu pro $T = \mathbf{Z}_2$, Tento lineární prostor značíme symbolem $\mathbf{Z}_2^n$.

Příklad: Nechť $\overrightarrow{x} = (0, 1, 1, 0, 0)$, $\overrightarrow{y} = (1, 1, 0, 1, 0)$ jsou dva vektory lineárního prostoru Z_2^5. Pak

- $\overrightarrow{x} + \overrightarrow{y} = (0, 1, 1, 0, 0) + (1, 1, 0, 1, 0) = (1, 0, 1, 1, 0)$
- $\langle \overrightarrow{x}, \overrightarrow{y} \rangle = \{0\overrightarrow{x} + 0\overrightarrow{y},\ 1\overrightarrow{x} + 0\overrightarrow{y},\ 0\overrightarrow{x} + 1\overrightarrow{y},\ 1\overrightarrow{x} + 1\overrightarrow{y}\} =$
  $= \{\overrightarrow{o}, \overrightarrow{x}, \overrightarrow{y}, \overrightarrow{x} + \overrightarrow{y}\} =$
  $= \{(0, 0, 0, 0, 0),\ (0, 1, 1, 0, 0),\ (1, 1, 0, 1, 0),\ (1, 0, 1, 1, 0)\}.$

Značení: Vektory z lineárního prostoru $\mathbf{Z}_2^n$ píšeme často zkráceně bez čárek mezi složkami a bez závorek. Takže lineární obal z předchozího příkladu zapíšeme:

$\langle 01100, 11010 \rangle = \{00000, 01100, 11010, 10110\}$

Základní vlastnosti lineárního prostoru $\mathbf{Z}_2^n$

- Pro $\overrightarrow{x} \in \mathbf{Z}_2$ je $1 \cdot \overrightarrow{x} = \overrightarrow{x}$, $0 \cdot \overrightarrow{x} = \overrightarrow{o}$. $\overrightarrow{x} + \overrightarrow{x} = \overrightarrow{o}$, $\overrightarrow{x} = -\overrightarrow{x}$.
- Celkový počet prvků v lineármím prostoru $\mathbf{Z}_2^n$ je 2^n a jeho dimenze je n.
- Lineární podprostor dimenze k má 2^k prvků.

Příklad: soustava lineárních rovnic v Z2

Vyřešíme soustavu lineárních rovnic v $\mathbf{Z}_2$ s maticí:

$$\left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 \end{array}\right) \sim \left(\begin{array}{cccccc|c} 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{array}\right)$$

Báze množiny řešení přidružené homogenní soustavy je:

$$B = \{011110, 010001\}$$

Partikulární řešení je: 111100 a všechna řešení soustavy zapíšeme ve tvaru

$$M \;=\; 111100 + \langle B \rangle \;=\; \{111100, 100010, 101101, 110011\}$$