- ORGANIZAČNÍ POZN.: KVÍZY PROSÍM ODESÍLAT, NEJEN UKLÁDAT!

TĚLESA

- OTÁZKA: V JAKÝCH ČÍSELNÝCH OBORECH MŮŽEME ŘEŠIT SOUSTAVY LIN. ROVNIC

NAPŘ.: $2x = 3 \quad (\rightsquigarrow x = \frac{3}{2})$

$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, JINÉ ČÍSELNÉ OBORY?

- UVAŽUJME MNOŽINU „ČÍSEL" T S BINÁRNÍMI OPERACEMI $+, \cdot$

$$+ : T \times T \longrightarrow T$$
$$(a, b) \longmapsto a + b \quad \text{(MÍSTO } +(a, b)\text{)}$$
$$\cdot : (a, b) \longmapsto a \cdot b$$

- NAPŘ. $a \cdot b + c \cdot (d + e)$
- $(T, +, \cdot)$ MUSÍ SPLŇOVAT AXIOMY, NAPŘ. $(a + b) + c = a + (b + c) \quad \forall a, b, c \in T$

PŘ. AXIOMY

- UVAŽUJME MNOŽINU T S JEDNOU BIN. OPERACÍ $\star : T \times T \longrightarrow T$
$(a, b) \longmapsto a \star b$

- PŘ: $T = \{\alpha, \beta, \gamma\}$

$\star$	α	β	γ
α	β	β	α
β	.....		
γ	.....		

← $\alpha \star \alpha = \beta$, $\alpha \star \beta = \beta$, $\alpha \star \gamma = \alpha$

$(T, \star)$

- BUDEME POŽADOVAT TYTO VLASTNOSTI $(T, \star)$ (TO BUDOU AXIOMY):

(H1) $\forall a, b, c \in T : (a \star b) \star c = a \star (b \star c)$ (ASOCIATIVITA)

(H2) $\exists 0 \in T \quad \forall a \in T : \quad 0 \star a = a = a \star 0$ (EXISTENCE NEUTRÁLNÍHO PRVKU)

- PŘ: 1) $(\mathbb{R}, +)$, $(\mathbb{N}_0, +)$, $(\mathbb{Z}, +)$, ...

2) $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}_{\geq 0}, \cdot)$, ...

3) X LIB. MNOŽINA, $S_X = \{f : X \to X : f$ BIJEKCE$\}$, MNOŽINA PERMUTACÍ NA X
$\rightsquigarrow (S_X, \circ)$, $\circ : (f, g) \longmapsto f \circ g$, NEUTRÁLNÍ PRVEK $id_X : X \to X$

POZN: SPECIÁLNĚ $0 \star 0 = 0$

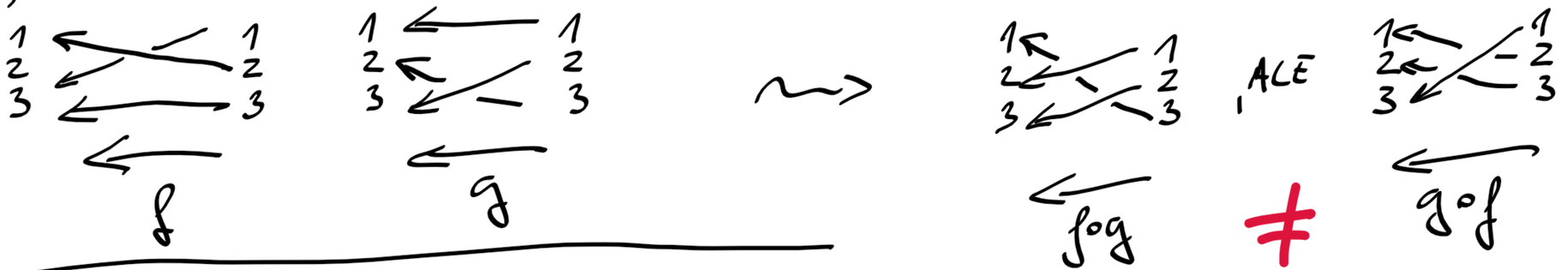
- BUDEME POŽADOVAT TYTO VLASTNOSTI $(T, *)$

(H1) $\forall a, b, c \in T : (a * b) * c = a * (b * c)$

(H2) $\exists 0 \in T \quad \forall a \in T : \quad 0 * a = a = a * 0$

- V $(S_X, \circ)$ POZOR: OBECNĚ NEPLATÍ $f \circ g = g \circ f$!

- NAPŘ $X = \{1,2,3\}$



- k čemu je (H1)?

$a * b * c$ NEZÁVISÍ NA UZÁVORKOVÁNÍ

- DÁ SE UKÁZAT: $\forall n \geq 3 \; \forall a_1, \ldots, a_n \in T$: $a_1 * a_2 * \ldots * a_n$ NEZÁVISÍ NA UZÁVORKOVÁNÍ!

(NAPŘ $(a * b) * (c * d) = ((a * b) * c) * d = \ldots$)

- **T**: UVAŽUJME $(T, \star)$ SPLŇUJÍCÍ (H2). PAK JE NEUTRÁLNÍ PRVEK URČEN JEDNOZNAČNĚ.

- **Dk**: - UVAŽUJME, ŽE MÁME PRVKY $0, 0' \in T$ SPLŇUJÍCÍ (H2)
- PAK:

$$0' \overset{(H2)}{=} 0 \star 0' \overset{(H2)}{=} 0$$

(H2) $\exists 0 \in T \quad \forall a \in T \qquad a \star 0 = a = 0 \star a$

- PŘIDÁME K (H1), (H2) DALŠÍ AXIOM:

(H3) $\forall a \in T \quad \exists (-a) \in T \quad : \quad a \star (-a) = 0 = (-a) \star a$

- **PŘ**: 1) $(\mathbb{Z}, +)$, ~~$(\mathbb{N}, +)$~~, $(\mathbb{R}, +)$, ...

2) $(\mathbb{R}_{>0}, \cdot)$ ... (H3) ŘÍKÁ, ŽE $\forall a \in \mathbb{R}_{>0} \; \exists b \in \mathbb{R}_{>0} : a \cdot b = 1 = b \cdot a$
~~$(\mathbb{R}, \cdot)$~~ (b TYPICKY ZNAČÍME $b = a^{-1}$)

3) $(S_X, \circ)$ ... (H3) $\forall f \in S_X \; \exists g \in S_X : f \circ g = id_X = g \circ f$ (ZASE: $g = f^{-1}$)

– **T:** AŤ $(T, \star)$ SPLŇUJE AXIOMY (H1), (H2), (H3).
PAK PRO KAŽDÉ $a \in T$ JE PRVEK $(-a)$ Z (H3) URČEN JEDNOZNAČNĚ.

– **Dk:** – PŘEDPOKLÁDEJME, ŽE PRO PRVEK $a \in T$ EXISTUJÍ $b, c \in T$ SPLŇUJÍCÍ:

$$a \star b = 0 = b \star a \quad \text{A} \quad a \star c = 0 = c \star a$$

– PAK:
$$c \overset{(H2)}{=} 0 \star c \overset{\text{PŘEDP.}}{=} (b \star a) \star c \overset{(H1)}{=} b \star (a \star c) \overset{\text{PŘEDP.}}{=} 0 \star 0 \overset{(H2)}{=} b$$

– TJ. $b = c$.

– TYPICKÝ V NAŠEM PŘÍPADĚ PŘIDÁME JEŠTĚ AXIOM KOMUTATIVITY:

(H4) $\forall a, b \in T$: $a \star b = b \star a$

AXIOMY TĚLES:

DEF: TĚLESEM (ANGL. FIELD) ROZUMÍME MNOŽINU T S BIN. OPERACEMI $+, \cdot : T \times T \to T$, KTERÉ SPLŇUJÍ TYTO AXIOMY

(S1) $\forall a,b,c \in T : (a+b)+c = a+(b+c)$

(S2) $\exists 0 \in T \ \forall a \in T : a+0 = a$

(S3) $\forall a \in T \ \exists (-a) \in T : a+(-a) = 0$

(S4) $\forall a,b \in T : a+b = b+a$

(N1) $\forall a,b,c \in T : (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(N2) $\exists 1 \in T : a \cdot 1 = a$

(N3) $\forall a \in T, a \neq 0 \ \exists a^{-1} \in T : a \cdot a^{-1} = 1$

(N4) $\forall a,b \in T : a \cdot b = b \cdot a$

(D) $\forall a,b,c \in T : (a+b) \cdot c = a \cdot c + b \cdot c$

($\neg$T) $|T| > 1$

POZN: $T = \{0\}$ S $+, \cdot$ SPLŇUJE VŠECHNO AŽ NA ($\neg$T)

PŘ: $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\{0,1\}, \text{XOR}, \text{AND})$

XOR	0	1
0	0	1
1	1	0

ZNAČENÍ: $(a \cdot b) + c =: a \cdot b + c$, $a - b := a + (-b)$ (S3), $\frac{a}{b} := a \cdot b^{-1}$

- DALŠÍ VLASTNOSTI TĚLES (PLATÍ PRO LIBOVOLNÉ TĚLESO $(T, +, \cdot)$):

(1) JE-LI $a, b \in T$, $a \neq 0$, PAK $a \cdot x + b = 0$ MÁ V T PRÁVĚ JEDNO ŘEŠENÍ

$\left(x = \frac{-b}{a} \right)$

---

(2) $\forall a \in T : \; a \cdot 0 = 0$

- Dk:

$$a \cdot 0 + a \cdot 0 \overset{(D)}{=} a \cdot (0 + 0) \overset{(S2)}{=} a \cdot 0$$

$$\Rightarrow \quad a \cdot 0 + a \cdot 0 = a \cdot 0$$

$$a \cdot 0 + a \cdot 0 + (-(a \cdot 0)) = a \cdot 0 + (-(a \cdot 0)) \quad \downarrow (S2)$$

$$a \cdot 0 + 0 = 0 \quad \downarrow (S2)$$

$$a \cdot 0 = 0$$

---

(3) $a \cdot b = 0 \Rightarrow a = 0$ NEBO $b = 0$

---

(4) $0 \neq 1$

- Dk: VEZMĚME LIBOVOLNÉ $a \in T$. KDYBY $0 = 1$, PAK: $0 \overset{(2) \text{ VÝŠE}}{=} 0 \cdot a = 1 \cdot a \overset{(N2)}{=} a$.

SPOR $\lightning$ $(\neg T)$.

- PŘ.: BUĎ $n \geq 2$ A $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$

UVAŽUJME $\oplus : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$(a, b) \longmapsto (a+b) \bmod n$

$\odot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$(a, b) \longmapsto (a \cdot b) \bmod n$

- V.: $(\mathbb{Z}_n, \oplus, \odot)$ SPLŇUJE PRO $n \geq 2$ VŠECHNY AXIOMY TĚLESA AŽ NA (A3)

(AŽ NA EXISTENCI INVERZNÍCH PRVKŮ).

$(\mathbb{Z}_n, \oplus, \odot)$ JE TĚLESO, PRÁVĚ KDYŽ n JE PRVOČÍSLO.

NAPŘ.: $(\mathbb{Z}_5, \oplus, \odot)$, $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ JE TĚLESO

$(3 \oplus 3 = 3 + 3 \bmod 5 = 1$, ATD.$)$

- PERMUTACE A AXIOMY:

- VEZMĚME MNOŽINU X, MNOŽINU $S_X = \{f : X \to X : \text{BIJEKCE}\}$ A OPERACI SKLÁDÁNÍ $\circ$

- PAK $(S_X, \circ)$ SPLŇUJE:

  - $\forall f, g, h \in S_X : (f \circ g) \circ h = f \circ (g \circ h)$ $\quad X \xleftarrow{h} X \xleftarrow{g} X \xleftarrow{f} X$

  - $\exists id_X \in S_X \quad \forall f \in S_X : f \circ id_X = f = id_X \circ f$

  - $\forall f \in S_X \; \exists f^{-1} \in S_X : f \circ f^{-1} = id_X = f^{-1} \circ f$

- POZN: $(\mathbb{Z}_4, \oplus, \odot)$ NENÍ TĚLESO, NAPŘ. $2 \odot 2 = 0$

- $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}$

- $1+1=0 \Rightarrow \forall x \in \mathbb{F}_4 : x + x = 0 \Rightarrow \forall x \in \mathbb{F}_4 : x = -x$

  ($1 = -1$ | $x + x = 1 \cdot x + 1 \cdot x = (1+1) \cdot x = 0 \cdot x = 0$)

  – TO URČUJE SČÍTÁNÍ, NAPŘ. $\alpha + (\alpha+1) = (\alpha+\alpha)+1 = 0+1 = 1$, ATD.

- NÁSOBENÍ: $\alpha^2 + \alpha + 1 = 0$, JINAK ŘEČENO $\alpha^2 = \alpha^2 + (\alpha+1) + (\alpha+1) = \alpha + 1$

  – TO URČUJE NÁSOBENÍ