ALGEBRAICKÁ TĚLESA:

- ZOBECNĚNÍ ČÍSELNÝCH OBORŮ JAKO JE NAPŘÍKLAD $\mathbb{R}$
- TĚLESO $\mathbb{T}$ JE MNOŽINA SPOLU SE DVĚMA KOMUTATIVNÍMI BINÁRNÍMI OPERACEMI $+$ A $\cdot$ SPLŇUJÍCÍMI:
  1) $(\mathbb{T}, +)$ JE ABELOVA GRUPA (NEUTRÁLNÍ PRVEK JE 0, INVERZNÍ K a JE $-a$)
  2) $(\mathbb{T}\setminus\{0\}, \cdot)$ JE ABELOVA GRUPA (NEUTRÁLNÍ PRVEK JE 1, INVERZNÍ K a JE a^{-1})
  3) $\forall a,b,c \in \mathbb{T}: a(b+c) = a\cdot b + a\cdot c$ (DISTRIBUTIVITA)
- $+, \cdot$ NEMUSÍ BÝT KLASICKÉ SČÍTÁNÍ A NÁSOBENÍ
- PÍŠEME ab MÍSTO $a\cdot b$
- KAŽDÉ TĚLESO MÁ ALESPOŇ 2 PRVKY, PROTOŽE $0 \neq 1$
- ZAVEDENÍ OPERACÍ $a-b := a+(-b)$, $a/b := a\cdot b^{-1}$

PŘÍKLADY (VÍCE V PREZENTACI):

- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ S KLASICKÝM SČÍTÁNÍM A NÁSOBENÍM
- $\{0\}$ S NÁSOBENÍM A SČÍTÁNÍM NEMOHLO Z TOHO NEJMENŠÍ TĚLESO
- PODTĚLESO JE PODMNOŽINA TĚLESA, KTERÁ SE STEJNĚ DEFINOVANÝMI OPERACEMI TVOŘÍ TĚLESO

TVRZENÍ 6.1 (ZÁKLADNÍ VLASTNOSTI TĚLES):

PRVKY TĚLESA $\mathbb{T}$ SPLŇUJÍ NÁSLEDUJÍCÍ VLASTNOSTI:

1) $0a = 0$ PRO KAŽDÉ $a \in \mathbb{T}$
2) $ab = 0 \Rightarrow a = 0$ NEBO $b = 0$ PRO KAŽDÉ $a, b \in \mathbb{T}$
3) $-a = (-1)a$ PRO KAŽDÉ $a \in \mathbb{T}$

DŮKAZ:

1) $0a \overset{\text{NEUTRÁLNÍ PRVEK}}{=} (0+0)a \overset{\text{DISTRIBUTIVITA}}{=} 0a + 0a$

$-0a + 0a = -0a + 0a + 0a$ (PŘIČTENÍ $-0a$)

$0 = 0 + 0a$ (INVERZ K $+$)

$0 = 0a$ (NEUTRALITA 0)

2) PRO $a = 0$ PLATÍ. PRO $a \neq 0$ VYNÁSOBENÍM ZLEVA PRVKEM a^{-1} MÁME $a^{-1}ab = a^{-1}0$ A PODLE 1) TEDY $1b = 0$

3) $0 \overset{1)}{=} 0a = (1-1)a \overset{\text{INVERZNÍ PRVEK}}{=} 1a + (-1)a \overset{\text{DISTRIBUTIVITA}}{=} a + (-1)a \overset{\text{NEUTRALITA 1}}{=} a + (-1)a \overset{\text{ODEČTENÍ } a}{\Rightarrow} \underline{-a = (-1)a}$

⊠

KONEČNÁ TĚLESA:

- NA MNOŽINĚ $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ UVAŽTE OPERACE $+$ A $\cdot$ MODULO m
  - PAK $\mathbb{Z}_2$ A $\mathbb{Z}_3$ JSOU TĚLESA, ALE $\mathbb{Z}_4$ NE (2 NEMÁ V $\mathbb{Z}_4$ INVERZ)

- **LEMMA 6.2:**
  PRO PRVOČÍSLO m A NENULOVÉ $a \in \mathbb{Z}_m$ PŘI NÁSOBENÍ MODULO m PLATÍ $\{0, 1, \dots, m-1\} = \{0a, 1a, \dots, (m-1)a\}$

- DŮKAZ:
  - SPOREM - NECHŤ $\exists k, l \in \mathbb{Z}_m, k > l : ka = la \pmod m$
  - PAK $ka - la \equiv (k-l)a \equiv 0 \pmod m$ (DISTRIBUTIVITA)
  - m JE PRVOČÍSLO $\Rightarrow m$ DĚLÍ a NEBO $k-l$
  - ALE $m > a$ A $m > k-l$ ($a \in \mathbb{Z}_m$, $k, l \in \mathbb{Z}_m$) $\Rightarrow a = 0$ NEBO $k-l = 0 \Rightarrow$ SPOR ($k \neq l, a \neq 0$) ⊠

- **VĚTA 6.3:**
  $\mathbb{Z}_m$ JE TĚLESEM PRÁVĚ TEHDY, KDYŽ JE m PRVOČÍSLO

- DŮKAZ (NÁČRT):
  i) $\Rightarrow$: POKUD $m = pq$ PRO $1 < p, q < m$, POK JELI $\mathbb{Z}_m$ TĚLESEM, PAK $p \cdot q \equiv 0 \pmod m$, IMPLIKUJE $p \equiv 0$ NEBO $q \equiv 0 \pmod m$, SPOR ČÁSTI 2) CVIČENÍ 6.1, KTERÁ NEPLATÍ → $1 < p, q < m$
  ii) $\Leftarrow$: PRO PRVOČÍSELNÉ m STAČÍ UVĚŘIT AXIOMY TĚLESA EXISTENCE INVERZU a^{-1} PRO NENULOVÉ $a \in \mathbb{Z}_m$ PLYNE Z LEMMA 6.2 (MEZI NÁSOBKY a MUSÍ BÝT 1) ⊠

- EXISTUJÍ KONEČNÁ TĚLESA NEPRVOČÍSELNÝCH VELIKOSTÍ?

- **VĚTA 6.4** (O VELIKOSTI KONEČNÝCH TĚLES):
  KONEČNÁ TĚLESA EXISTUJÍ PRÁVĚ O VELIKOSTECH p^n, KDE p JE PRVOČÍSLO A $n \geq 1$

- BEZ DŮKAZU (GALOISOVA TĚLESA $GF(p^n)$)

- **CHARAKTERISTIKA TĚLESA:**
  - JE NEJMENŠÍ $n \in \mathbb{N}$ TAKOVÉ, ŽE $\underbrace{1+\dots+1}_{n} = 0$. POKUD TAKOVÉ n NEEXISTUJE, PAK JI DEFINUJEME JAKO 0

- **PŘÍKLADY:**
  - $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ MAJÍ CHARAKTERISTIKU 0, $\mathbb{Z}_n$ MÁ CHARAKTERISTIKU n
  - EXISTUJÍ NEKONEČNÁ TĚLESA S NENULOVOU CHARAKTERISTIKOU (TĚŽKÉ)
  - KONEČNÁ TĚLESA MAJÍ NENULOVOU CHARAKTERISTIKU (SNADNÉ CVIČENÍ)

- **TVRZENÍ 6.5:**
  CHARAKTERISTIKA KAŽDÉHO TĚLESA JE BUĎ 0 NEBO PRVOČÍSLO

  - **DŮKAZ:**
    - PROTOŽE $0 \neq 1$, TAK CHARAKTERISTIKA NEMŮŽE BÝT 1
    - SPOREM – POKUD BY CHARAKTERISTIKA BYLA SLOŽENÉ ČÍSLO

      $n = pq$, PAK:

      $0 = \underbrace{1+\dots+1}_{n=pq} = (\underbrace{1+\dots+1}_{p})(\underbrace{1+\dots+1}_{q})$ A DOSTÁVÁME

      ČÁSTI 2) **TVRZENÍ 6.1** JE $p = 0$ NEBO $q = 0$

      – TO JE SPOR S MINIMALITOU n ☒

- **MALÁ FERMATOVA VĚTA:**
  - PRO KAŽDÉ PRVOČÍSLO p A NENULOVÉ $a \in \mathbb{Z}$ PLATÍ $a^{p-1} \equiv 1 \pmod p$
    – POUŽÍVÁ SE NAPŘÍKLAD V PRAVDĚPODOBNOSTNÍCH TESTECH PRVOČÍSELNOSTI
  - FORMULACE V JAZYCE KONEČNÝCH TĚLES:
  - **VĚTA 6.6** (MALÁ FERMATOVA VĚTA):
    PRO KAŽDÉ PRVOČÍSLO p A NENULOVÉ $a \in \mathbb{Z}_p$ PLATÍ

    $$a^{p-1} = 1 \text{ V TĚLESE } \mathbb{Z}_p$$

    - **DŮKAZ:**
      - Z **LEMMA 6.2** PLATÍ $\{0, 1, \dots, p-1\} = \{0a, 1a, \dots, (p-1)a\}$
      - Z ČÁSTI 1) **TVRZENÍ 6.1** JE $0a = 0$, TAKŽE $\{1, \dots, p-1\} = \{1a, \dots, (p-1)a\}$
      - TEDY $1 \cdot 2 \cdots (p-1) = (1a)(2a) \cdots ((p-1)a)$ A Z VYKRÁCENÍ $1, \dots, p-1$ DOSTÁVÁME $1 = a \cdots a = a^{p-1}$ ☒

VEKTOROVÉ PROSTORY:

- ZOBECNĚNÝ POJMEM TOHO PROSTORU ARITMETICKÝCH VEKTORŮ Z $\mathbb{R}^n$
- BUĎ $\mathbb{T}$ TĚLESO S NEUTRÁLNÍMI PRVKY 0 A 1 PRO SČÍTÁNÍ A NÁSOBENÍ

VEKTOROVÝ PROSTOR NAD $\mathbb{T}$ JE MNOŽINA V S OPERACEMI SČÍTÁNÍ VEKTORŮ $+ : V \times V \to V$ A NÁSOBENÍ SKALÁREM $\cdot : \mathbb{T} \times V \to V$ SPLŇUJÍCÍ PRO KAŽDÉ $\alpha, \beta \in \mathbb{T}$ A $u, v \in V$:

1) $(V, +)$ JE ABELOVA GRUPA (NEUTRÁLNÍ PRVEK o, INVERZNÍ K u JE $-u$)
2) $\alpha(\beta v) = (\alpha\beta)v$, (ASOCIATIVITA)
3) $1v = v$,
4) $(\alpha + \beta)u = \alpha u + \beta u$ (DISTRIBUTIVITA)
5) $\alpha(u + v) = \alpha u + \alpha v$ (DISTRIBUTIVITA)

- PRVKY MNOŽINY V NAZÝVÁME **VEKTORY**
- PRVKY MNOŽINY $\mathbb{T}$ NAZÝVÁME **SKALÁRY**

- PŘÍKLADY (VÍCE V PREZENTACI):
  - ARITMETICKÉ PROSTORY $\mathbb{R}^n$, $\mathbb{T}^n$
  - PROSTOR MATIC $\mathbb{T}^{m \times n}$
  - PROSTOR REÁLNÝCH POSLOUPNOSTÍ P, PROSTOR REÁLNÝCH FUNKCÍ $\mathcal{F}$