6 Konečná tělesa existují jen pro mocniny prvočísla (40 bodů)

V této úloze si ukážeme část z důkazu následující algebraické věty.

Věta. *Konečné těleso $\mathbb{F}$ řádu $\check{r}$ existuje, právě když $\check{r}$ je mocnina prvočísla p^k.*

Dokonce platí, že konečně těleso daného řádu je určeno jednoznačně (až na přejmenování prvků, kterému se odborně říká *isomorfismus*). Tato věta tedy opodstatňuje označení $\mathbb{GF}(p^k)$, neboť těleso řádu p^k je jednoznačně určené. V důkazu ukážeme, že každé takové těleso je vysoce symetrický objekt, který v sobě skrývá vektorový prostor. To je poměrně překvapivé, neboť v definici tělesa se vektorové prostory vůbec nevyskytují a naopak ty se definují pomocí těles.

Co o tělesech už známe ...

V samotném důkazu můžeme použít *pouze axiomy tělesa* a jejich důsledky! Připomeňme si, co říkají axiomy tělesa:

- Těleso je struktura s dvěma operacemi – sčítáním a násobením.
- Těleso obsahuje dva speciální prvky, neutrální prvek na sčítání (budeme značit 0) a neutrální prvek na násobení (značíme 1).
- Z hlediska sčítání se těleso chová jako grupa – máme inverzní prvky a neutrální prvek.
- Z hlediska násobení se těleso bez 0 chová jako grupa – opět máme inverze a neutrální prvek.
- Navíc operace sčítání a násobení jsou dohromady svázané distributivitou.

Z axiomů lze odvodit i další vlastnosti těles, některé jsme již viděli.

- Neutrální prvky 0 a 1 a inverze pro obě operace jsou určeny jednoznačně. Ostatně to platí obecně i v grupách.
- Libovolný násobek 0 je zase nula: $a \cdot 0 = 0$.
- Pokud $a + b = a + c$, potom $b = c$.
- Podobně pro násobení a $a \neq 0$, pokud $a \cdot b = a \cdot c$, potom $b = c$.
- Neexistují dvě nenulová čísla a a b, že $a \cdot b = 0$.

$\mathbb{Z}_p$ je podtěleso $\mathbb{F}$

Na rozjezd vyřešíme tělesa s prvočíselnou velikostí. Uvažujme strukturu $\mathbb{Z}_k$ tvořenou čísly $0, \ldots, k-1$ a operacemi sčítaní a násobení definovanými jako zbytek po celočíselném sčítání a násobení.

Příklad. Například pro $\mathbb{Z}_4$ a prvky $a = 2$ a $b = 3$ dostaneme, že $a + b = 1$ a $a \cdot b = 2$, neboť přesně takové zbytky mají čísla 5 a 6 po dělení 4.

Úloha 6.1. Dokažte, že $\mathbb{Z}_p$ je těleso, právě když p je prvočíslo.

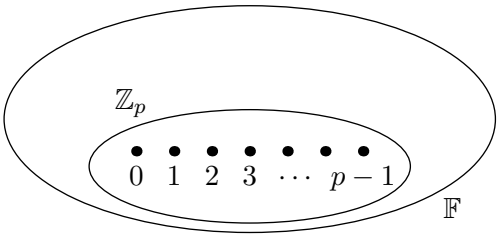
Nápověda. Pokud p není prvočíslo, není těžké nalézt dvojici, která porušuje poslední vlastnost. Pro prvočísla to se sčítáním bude docela jednoduché. Je však třeba pro každý prvek a ukázat, že násobení tímto prvkem je prosté, tedy že neexistuje dvě rozdílná čísla b a c, aby $a \cdot b = a \cdot c$.

Charakteristika tělesa je nejmenší přirozené číslo k takové, že součet k jedniček $1+1+\cdots+1 = 0$, případně 0, pokud takové k neexistuje (třeba reálná čísla).

Úloha 6.2. Dokažte, že pro každé konečné těleso $\mathbb{F}$ je jeho charakteristika nějaké prvočíslo p.

Nápověda. Ukažte nejprve, že charakteristika je nenulová. Poté zkuste dokazovat sporem. Kdyby charakteristika nebyla prvočíselná, co by bylo špatně?

Označme součet k jedniček pomocí k. V tělese tedy máme prvky $0, \ldots, p-1$. O dalších prvcích zatím nic nevíme.



Úloha 6.3. Ukažte, že prvky $0, \ldots, p-1$ tvoří podtěleso totožné $\mathbb{Z}_p$.

Cože? Těleso je vektorový prostor?

Nyní využijeme získané znalosti o tělesech a dokončíme důkaz překvapivým úskokem, však posuďte sami.

Úloha 6.4. Dokažte, že každé konečné těleso $\mathbb{F}$ charakteristiky p je vektorový prostor $\mathbb{V}$ nad tělesem $\mathbb{Z}_p$. Operace $\mathbb{V}$ definujeme takto: sčítání vektorů odpovídá sčítání v tělese a skalární násobení násobením v tělese (protože $\mathbb{Z}_p$ je podtěleso $\mathbb{F}$, lze to takto definovat).

Nápověda. K tomu potřebujeme dokázat, že vzniklá struktura splňuje všechny axiomy vektorového prostoru. Neplyne to snadno z toho, že $\mathbb{F}$ je těleso?

Víme, že vektorové prostory tvoří silně předurčenou strukturu, pojďme toho tedy využít. Vektorový prostor $\mathbb{V}$ má totiž konečnou dimenzi k. Podle Steinitzovy věty víme, že existuje nějaká báze $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Sice vůbec netušíme, jak vypadá, ale to nebudeme potřebovat – stačí vědět, že existuje.

Bude se hodit ještě jedno obecné tvrzení o bázích a lineárních kombinacích.

Úloha 6.5. Dokažte, že pokud $\mathbf{b}_1, \ldots, \mathbf{b}_k$ je báze vektorového prostoru, potom její různé lineární kombinace definují různé vektory. Tedy dokažte, že $\sum_{i=1}^{k} \alpha_i \mathbf{b}_i = \sum_{i=1}^{k} \bar{\alpha}_i \mathbf{b}_i$ implikuje, že $\alpha_i = \bar{\alpha}_i$.

Dokončení důkazu

A na závěr složme oba poznatky dohromady.

Úloha 6.6. Dokažte, že každé konečné těleso $\mathbb{F}$ má p^k prvků.

Nápověda. Kolik rozdílných lineárních kombinací vektorů z $\mathbf{b}_1, \ldots, \mathbf{b}_k$ existuje?

Tím jsme ukázali neexistenci konečného tělesa velikosti, která není mocnina prvočísla. Také vám přijde trik hezký? Pokud jste se dostali až sem (a případně všechna tvrzení po cestě dokázali), máte můj obdiv (a zasloužíte si své body :)).

7 Svědci a světci (10 bodů)

Představme si, že po nás někdo chce vyřešit soustavu $A\mathbf{x} = \mathbf{b}$. To není nijak těžké, že? Ale co s tím, když takové řešení neexistuje? Na cvičeních jsme ukázali, jak za pomocí metody nejmenších čtverců soustavu co nejméně pozměnit, aby řešení existovalo. To je vhodné jen pro některé aplikace a pro jiné by se více hodilo mít *svědka* (neboli *certifikát*), pomocí kterého snadno dokážeme, že řešení neexistuje. Certifikáty hrají důležitou roli v teorii složitosti.

Zkusíme si vyrobit jeden takový certifikát pro to, že $A\mathbf{x} = \mathbf{b}$ nemá řešení. Stačí k tomu nalézt vektor $\mathbf{y}$ správných vlastností.

Úloha 7.1. Soustava $A\mathbf{x} = \mathbf{b}$ nemá řešení, právě když existuje $\mathbf{y}$, že $A^\mathsf{T}\mathbf{y} = \mathbf{0}$ a $\mathbf{y}^\mathsf{T}\mathbf{b} = -1$.

Nápověda. Zamyslete se nad tím, co úloha říká v řeči fundamentálních prostorů A. Rozmyslete si také, že bude platit i tvrzení, kde bychom nahradili -1 libovolnou jinou nenulovou konstantou.

Poznámka. V praxi se používají ještě o něco silnější tvrzení, tzv. *Farkašova lemmata*. Jsou to oddělovací lemmata pro systémy například $A\mathbf{x} \leq \mathbf{b}$ nebo dokonce $\max_{\mathbf{x}}\{\mathbf{c}^\mathsf{T}\mathbf{x} : A\mathbf{x} = \mathbf{b}\}$.