

Konečná tělesa jsou jenom řádu mocniny prvočísla (15 bodů)

Řád tělesa je počet jeho prvků. Dokážeme si společně slavnou větu, která dává kompletní charakterizaci konečných těles:

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

Dokonce platí, že konečné těleso daného řádu je určeno jednoznačně (až na isomorfismus, který si lze představit jako přejmenování prvků). Překvapivé na důkazu této věty bude, že se v ní dokonce objeví vektorové prostory a jejich báze, přestože v definici tělesa se vůbec nevyskytují a naopak vektorové prostory se definují pomocí těles.

Nejprve ukážeme, že neexistuje konečné těleso, jehož řád by nebyl mocninou prvočísla!

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.

Kromě axiomů však známe i další věci o tělesech. Na cvičeních jsme ukázali, že operace v tělese splňují následující užitečné vlastnosti:

- Neutrální prvky 0 a 1 a inverze pro obě operace jsou určeny jednoznačně (protože jsou to grupy!).
- Libovolný násobek 0 je zase nula: $a \cdot 0 = 0$.
- Pokud $a + b = a + c$, potom $b = c$.
- Podobně pro násobení a $a \neq 0$: $a \cdot b = a \cdot c$, potom $b = c$.
- Neexistují dvě nenulová čísla a a b , že $a \cdot b = 0$.

$\mathbb{Z}_p$ je těleso (3 body)

Na rozjezd vyřešíme tělesa s prvočíselnou velikostí. Uvažujme strukturu $\mathbb{Z}_k$ tvořenou čísly $0, \dots, k-1$ a operacemi sčítání a násobení definovanými jako zbytek při 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. Dokážte, že $\mathbb{Z}_p$ je těleso, právě když p je prvočíslu.

Hint. Pokud p není prvočíslu, dokázali jsme si již na cvičení, že těleso nedostaneme, připomeňte si. Pro prvočísla: se sčítáním to bude docela jednoduché. Naopak je 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 a podtěleso $\mathbb{Z}_p$ (6 bodů)

Charakteristika je nejmenší přirozené číslo k takové, že součet k jedniček $1 + 1 + \dots + 1 = 0$, případně 0, pokud takové k neexistuje (třeba reálná čísla). Ukažte překvapivou vlastnost charakteristiky konečných těles.

Úloha. Dokážte, že pro každé konečné těleso $\mathbb{F}$ je jeho charakteristika nějaké prvočíslu p .

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

Označme součet k jedniček pomocí k . V tělese tedy máme prvky $0, \dots, p-1$.

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

Hint. Ověřte, že také násobení je v tělese $\mathbb{F}$ definované totožně jako v tělese $\mathbb{Z}_p$.

Cože? Těleso je vektorový prostor? (6 bodů)

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

Úloha. 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 takhle udělat).

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

Víme, že vektorové prostory tvoří silně předurčenou strukturu, pojďme toho tedy využít.

Úloha. Vektorový prostor $\mathbb{V}$ má konečnou dimenzi k , dokažte.

Podle Steinitzovy věty víme, že existuje nějaká báze B velikosti k . Sice vůbec netušíme, jak vypadá, ale to nebudeme potřebovat – stačí vědět, že existuje.

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

Úloha. Nechť B je báze vektorového prostoru, potom jednotlivé lineární kombinace vektorů báze definují po dvou různé vektory. Tedy formálně:

$$\sum_{i=1}^k \alpha_i b_i = \sum_{i=1}^k \bar{\alpha}_i b_i \implies \forall i : \alpha_i = \bar{\alpha}_i.$$

Dokažte.

Hint. Co by jinak bylo špatné? Opravdu by B byla báze, kdyby to neplatilo?

A na závěr složme oba poznatky dohromady.

Úloha. Konečné těleso $\mathbb{F}$ má p^k prvků.

Hint. Kolik rozdílných lineárních kombinací vektorů z B existuje? Proč z toho plyne, že těleso $\mathbb{F}$ má přesně p^k prvků?

Tím jsme ukázali neexistenci konečného tělesa velikosti, která není mocnina prvočísla. Pokud jste se dostali až sem (a případně všechna tvrzení po cestě dokázali), máte můj obdiv. Zbytek zase někdy příště (až to sám pochopím).

Determinant je multilineární alternující forma (15 bodů)

Těmito slovy by vám algebraik pravděpodobně popsal, co je to determinant. Na jednu stranu je to definice krátká a jednoduchá, na druhou stranu člověku neznalému těchto pojmů neřekne absolutně nic. Pojďme si na chvilku pohrát s vlastnostmi determinantu.

Na přednášce se determinant definoval jako nicneříkající suma:

$$(\clubsuit) \quad \det \mathbf{A} = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i \in [n]} a_{i, \pi(i)}.$$

Pro matici 2×2 dostáváme následující vzoreček:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$$

Jednotlivé vlastnosti si proto budeme ilustrativně ukazovat na maticích 2×2 . Můžeme na nich snadno zkontrolovat, že determinant definovaný $(\clubsuit)$ je splňuje.

Definice determinantu pomocí vlastností

Zkusíme *determinant definovat pomocí vlastností*, které splňuje. Determinant $\det$ je zobrazení, které přiřazuje čtvercovým maticím reálná čísla (nebo prvky jiného tělesa, i když zde je malý problém s tělesy charakteristiky dva) a které splňuje následující tři vlastnosti:

- (1) Determinant je lineárně závislý na prvním řádku matice. Tedy pokud první řádek lze zapsat jako $\mathbf{u} + \mathbf{v}$, potom determinant této matice získáme jako součet determinantů matic s prvním řádkem $\mathbf{u}$ a prvním řádkem $\mathbf{v}$ (ostatní řádky nemodifikujeme). Pokud první řádek je roven $\alpha\mathbf{u}$, potom determinant je roven α -násobku determinantu matice s prvním řádkem $\mathbf{v}$. To je ona lineárnost.

$$\begin{vmatrix} a+a' & b+b' \\ c & d \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} a' & b' \\ c & d \end{vmatrix}, \quad \begin{vmatrix} \alpha a & \alpha b \\ c & d \end{vmatrix} = \alpha \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

- (2) Prohození dvou řádků matice mění znaménko determinantu. Díky této vlastnosti se říká, že determinant je alternující.

$$\begin{vmatrix} c & d \\ a & b \end{vmatrix} = - \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

- (3) Determinant jednotkové matice $\det \mathbf{I}_n$ je roven jedné.

$$\begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1, \quad \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} = 1, \quad \dots$$

Není těžké nahlédnout, že definice ($\clubsuit$) vlastností (1) až (3) splňuje. Naopak může být překvapivé, že funkce $\det$ je určena těmito vlastnostmi jednoznačně – nic dalšího nepotřebujeme. To budeme chtít dokázat v tomto úkolu. Třetí pravidlo nám pouze fixuje determinant nějaké matice, jinak by zobrazení nebylo jednoznačně určené.

Odvození dalších vlastností

Začneme tím, že z vlastností (1) až (3) odvodíme základní vlastnosti determinantu. Nakonec z nich odvodíme přímo vzoreček ($\clubsuit$), čímž získáme jednoznačnost definice.

Úloha. Vaším úkolem bude pro jednotlivé vlastnosti dokázat, že jsou správně. V jejich důkazu však nemůžete používat nic jiného než vlastností (1) až (3) a důsledků, které z nich dokážete.

- (1') Na prvním řádku není nic speciálního, determinant je lineárně závislý na libovolném řádku matice. Této vlastnosti se říká multilineárnost.

$$\begin{vmatrix} a & b \\ c+c' & d+d' \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix} + \begin{vmatrix} a & b \\ c' & d' \end{vmatrix}, \quad \begin{vmatrix} a & b \\ \alpha c & \alpha d \end{vmatrix} = \alpha \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

- (4) Pokud má determinant nulový řádek, je roven nule.

$$\begin{vmatrix} 0 & 0 \\ c & d \end{vmatrix} = 0.$$

- (5) Pokud má determinant dva řádky stejné, je roven nule.

$$\begin{vmatrix} a & b \\ a & b \end{vmatrix} = 0.$$

- (6) Přičtení libovolného násobku jednoho řádku k jinému nemění determinant.

$$\begin{vmatrix} a+\alpha c & b+\alpha d \\ c & d \end{vmatrix} = \begin{vmatrix} a & b \\ c & d \end{vmatrix}.$$

- (7) Determinant trojúhelníkové matice (horní či dolní) je roven součinu prvků na hlavní diagonále – $\det \mathbf{A} = a_{1,1} \cdot a_{2,2} \cdots a_{n,n}$.

$$\begin{vmatrix} a & b \\ 0 & d \end{vmatrix} = ad.$$

- (8) Determinant každé singulární matice je nulový, naopak regulární (invertovatelná) matice má vždy nenulový determinant.

Hint. Použijte Gaussovu eliminaci. Jak dopadne, pokud je matice regulární? Jaký výsledek dostaneme pro singulární matici?

(9) Determinant součinu dvou matic je součin jejich determinantů – $\det \mathbf{AB} = \det \mathbf{A} \det \mathbf{B}$.

$$\begin{vmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{vmatrix} = (ae + bg)(cf + dh) - (af + bh)(ce + dg) = (ad - bc)(eh - fg) = \begin{vmatrix} a & b \\ c & d \end{vmatrix} \begin{vmatrix} e & f \\ g & h \end{vmatrix}.$$

Hint. Toto lze dokázat využitím Gaussovy eliminace nebo následujícím trikem. Singulární případy pro $\mathbf{A}$ a $\mathbf{B}$ vyřešíme zvlášť. Pokud jsou obě regulární, definujme zobrazení $d(\mathbf{A}) = \det \mathbf{AB} / \det \mathbf{B}$. Pro dokázání vlastnosti (9) potřebujeme ukázat, že zobrazení d je determinant. K tomu stačí ověřit, že splňuje vlastnosti (1) až (3).

Matice je permutační, pokud v každém řádku a sloupci obsahuje právě jednu jedničku a na ostatních pozicích nuly (přesnější popis s příklady naleznete v úkolech z minulého semestru). Nalezněte souvislost mezi determinantem této matice a znaménkem permutace, kterou reprezentuje. Zkuste to dokázat jak pomocí vlastností (1) až (3), tak pomocí definice z přednášky.

Zbývá ukázat poslední vlastnost a tím bude náš seznam vlastností úplný, bohužel její důkaz bude nejobtížnější.

(10) Determinant matice i její transpozice je stejný – $\det \mathbf{A} = \det \mathbf{A}^T$.

Hint. Neznám žádný elegantní důkaz této vlastnosti, takže pokud nějaký objevíte, rád si ho přečtu a udělím bonusové body. Důkaz, který jsem viděl, využívá *LDU dekompozici*. Pokud je matice singulární, tvrzení vyřešíme zvlášť. Pokud je matice regulární, potom ji lze rozložit na součin tří matic $\mathbf{L}$ (dolní trojúhelníkové, od anglického lower), $\mathbf{D}$ (diagonální, od anglického diagonal) a $\mathbf{U}$ (horní trojúhelníková, od anglického upper), kde trojúhelníkové matice mají na diagonále jedničky. Platí tedy, že každou regulární matici $\mathbf{A}$ lze rozložit:

$$\mathbf{PA} = \mathbf{LDU},$$

kde $\mathbf{P}$ je permutační matice. Důkaz se potom provede porovnáním $\mathbf{A}$ a $\mathbf{A}^T$ s využitím vzorce $(\mathbf{XY})^T = \mathbf{Y}^T \mathbf{X}^T$ a vlastností (7) a (9).

Ještě pár slov k LDU dekompozici obecně: Funguje tak, že nejprve přeházíme řádky matice $\mathbf{A}$ a na výsledek provedeme Gaussovu eliminaci (bez prohazování řádků) a tím generujeme matice $\mathbf{L}$, $\mathbf{D}$ a $\mathbf{U}$. Pokud bychom řádky neproházeli, mohla by Gaussova eliminace selhat, třeba pokud by levý horní roh byl nulový. Na vzniklé matice LDU dekompozice se lze dívat jako na zápis jednotlivých operací, které s maticí provádíme. LDU dekompozice má spoustu hezkých vlastností, kdyby vás zajímali, můžete se mě třeba někdy zeptat na cvičení.

Poslední vlastnost (10) vlastně prakticky zdvojuje seznam vlastností, které o determinantu známe. Získáváme podobné vlastnosti o sloupečcích matice – determinant je lineárně závislý na libovolném sloupečku; pokud je libovolný sloupeček nulový nebo dva sloupečky jsou stejné, potom je i determinant nulový, ...

Jednoznačnost a ekvivalence s definicí (♣)

Nyní nám zbývá dokázat poslední věc – jednoznačnost determinantu definovaného vlastnostmi (1) až (3). To dokážeme tak, že je tato definice ekvivalentní se vzorcem (♣).

Úloha. Dokažte, že determinant definovaný vlastnostmi (1) až (3) je ekvivalentní s definicí (♣).

Hint. Rozdělíme výpočet jednoho determinantu na výpočet n^n determinantů. Podle vlastnosti (1) rozdělíme determinant na n determinantů, každý z nich obsahuje pouze jedno číslo z prvního řádku a na zbývajících pozicích nuly:

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \begin{vmatrix} a & 0 \\ c & d \end{vmatrix} + \begin{vmatrix} 0 & b \\ c & d \end{vmatrix}.$$

Stejně tak rozdělíme i ostatní řádky, každý na n dalších determinantů:

$$\begin{vmatrix} a & 0 \\ c & d \end{vmatrix} + \begin{vmatrix} 0 & b \\ c & d \end{vmatrix} = \begin{vmatrix} a & 0 \\ c & 0 \end{vmatrix} + \begin{vmatrix} a & 0 \\ 0 & d \end{vmatrix} + \begin{vmatrix} 0 & b \\ c & 0 \end{vmatrix} + \begin{vmatrix} 0 & b \\ 0 & d \end{vmatrix}.$$

Získáme tak triviální matice, pro které je snadné s využitím výše uvedených vlastností spočítat determinant. Například pro výše uvedený determinant dostáváme $0 + ad - bc + 0 = ad - bc$.