Dvě roviny v $\mathbb{R}^4$ (1 bod)

Rovina je podmnožina $\mathbb{R}^4$ určená různoběžnými vektory u a v (tedy $su \neq tv$ pro $s, t \neq 0$) a vektorem w (bod, kterým rovina prochází) a jsou to všechny vektory

$$\{w + su + tv \mid s, t \in \mathbb{R}\}.$$

Úloha. Rozhodněte, zda existují dvě roviny v $\mathbb{R}^4$, jejichž průnikem je právě jeden bod.

Matice pro výpočet Fibonnaciho čísel (3 body)

Nechť F_n je n-té Fibbonaciho číslo. Ta definujeme následovně:

$$F_0 = 0, \qquad F_1 = 1, \qquad F_{n+2} = F_{n+1} + F_n.$$

Uvažme dvou složkový vektor tvořený dvěma po sobě jdoucími Fibonnaciho čísly: (F_k, F_{k+1}). Uvažme matici M definovanou následovně:

$$M = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Součin vektoru s maticí M je následující:

$$(F_k, F_{k+1}) \cdot \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = (F_{k+1}, F_k + F_{k+1}) = (F_{k+1}, F_{k+2}),$$

tedy dostáváme následující Fibbonaciho číslo. Násobit maticí M zprava můžeme znovu a znovu a jelikož násobení matic je asociativní, dostáváme následující postup pro výpočet F_n:

$$(F_n, F_{n+1}) = (F_0, F_1) \cdot M \cdot M \cdots M = (F_0, F_1) \cdot M^n.$$

Přitom M^n umíme spočítat v čase $\mathcal{O}(\log N)$.

Úloha. Zkuste výše uvedený postup zobecnit a tím i pochopit, jak jsme výše uvedenou matici M získali. Máme nějakou obecnou rekurzivně zadanou posloupnost. Několik prvních členů A_0 až A_{k-1} je pevně určeno. Každý další člen je tvořen lineární kombinací k předcházejících členů, tedy platí

$$A_{n+k} = a_{k-1}A_{n+k-1} + a_{k-2}A_{n+k-2} + \cdots + a_1 A_{n+1} + a_0 A_n$$

pro pevná čísla a_0 až a_{k-1}.

Příklad. Posloupnost může mít třeba určené první tři členy: $A_0 = 1$, $A_1 = 2$, $A_2 = 3$ a další členy jsou určeny předpisem $A_{n+3} = A_{n+2} - A_{n+1} + 3A_n$. Začátek posloupnosti je:

$$(1, 2, 3, 4, 7, 12, 17, 26, 45, \ldots).$$

Zobecněte násobící postup uvedený výše, tedy popište konstrukci podobné matice pro obecnou posloupnost a pochopitelně dokažte, že má požadované vlastnosti.

Hint. Zkuste nejprve uvažovat posloupnosti pro $k = 2$, tedy posloupnosti závislé jenom na dvou předcházejících členech. I za takové řešení lze získat alespoň jeden bod.

Permutační matice (3 body)

Permutace určitě znáte z diskrétní matematiky, je to bijektivní zobrazení $\pi : X \to X$. Bijektivní znamená, že pro každé $x, y \in X$, pokud $\pi(x) = \pi(y)$, potom $x = y$. Intuitivně, permutace je nějaké uspořádání prvku v X. Dále nás budou zajímat permutace množiny $X = \{1, 2, \ldots, n\}$.

Pro permutaci π je permutační matice P_π čtvercová matice $n \times n$ daná předpisem:

$$(P_\pi)_{ij} = \begin{cases} 1 & \text{pro } \pi(i) = j, \\ 0 & \text{jinak,} \end{cases}$$

tedy je to nula-jedničková matice, která má v i-tém řádku jsou skoro samé nuly a jediná jednička je na pozici $\pi(i)$.

Příklad. Ukážeme si dva příklady. Pro $n = 5$ mějme permutace π a σ dané následujícím předpisem:

$$\pi(1) = 2, \qquad \pi(2) = 3, \qquad \pi(3) = 1, \qquad \pi(4) = 5, \qquad \pi(5) = 4,$$

$$\sigma(1) = 3, \qquad \sigma(2) = 1, \qquad \sigma(3) = 2, \qquad \sigma(4) = 5, \qquad \sigma(5) = 4.$$

Tyto permutace mají permutační matice P_π a P_σ:

$$P_\pi = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \quad \text{a} \quad P_\sigma = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Úloha. Pro permutační matice vyřešte následující:

a) Nalezněte inverzní matice P_π a P_σ z příkladu.

b) Proč se permutačním maticím říká permutační? Pokud vám taková otázka připadá příliš obecná: Uvažte, co permutační matice provádí s maticí A (pochopitelně správné velikosti), pokud ji násobí zleva či zprava.

c) Permutační matice lze spolu násobit, tedy pro libovolné permutace π a σ má $P_\pi P_\sigma$ smysl. Ukažte, že součin permutačních matic je opět permutační matice a že tato permutace je v určitém vztahu k těmto dvěma permutacím. Tedy dokažte, že existuje permutace τ, že $P_\tau = P_\pi P_\sigma$ a popište vztah τ s π a σ.

d) Pro každou permutační matici existuje inverzní matice, neboť permutační matice mají plnou hodnost, $\operatorname{rank}(P_\pi) = n$. Pro libovolnou permutaci π ukažte, že $P_\pi^{-1} = P_\pi^T$ a že P_π^{-1} je opět permutační matice nějaké permutace σ a popište vztah σ a π.

Binární čísla a grupy (2 body)

Uvažme všechna k-bitová binární čísla, to jsou vlastně posloupnosti prvků $\{0, 1\}$ délky k. Pro dvě taková čísla budeme uvažovat několik bitových operací. To jsou operace, které se aplikují vždy na dvojice bitů na stejné pozici a výsledkem je jeden bit výsledku, tedy operace $f : \{0, 1\} \times \{0, 1\} \to \{0, 1\}$. Konkrétně budeme uvažovat čtyři operace `AND` ($\&$), `OR` ($\vee$), `XOR` ($\oplus$) a `EKV` ($\Leftrightarrow$), které jsou definované následujícími tabulkami:

$\&$	0	1
0	0	0
1	0	1

$\vee$	0	1
0	0	1
1	1	1

$\oplus$	0	1
0	0	1
1	1	0

$\Leftrightarrow$	0	1
0	1	0
1	0	1

Příklad. Možná následující příklad lépe osvětlí, jak tyto operace přesně fungují. Uvažme 6-bitová čísla $a = 011010$ a $b = 110110$, dostáváme $a \,\&\, b = 010010$, $a \vee b = 111110$, $a \oplus b = 101100$ a $a \Leftrightarrow b = 010011$.

Úloha. Uvažme všechna k-bitová čísla. Se kterou z těchto čtyř operací tvoří grupu a se kterou naopak grupu nedostaneme? Pokud grupu tvoří, nalezněte navíc její neutrální prvek a inverzní prvky.

Konečná tělesa jsou jenom řádu mocniny prvočísla (zatím 5 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 konečně 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 (1 bod)

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

Hint. Pokud p není prvočíslo, 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 $\mathbb{Z}_p$ (2 body)

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

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

Hint. 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 $0, \ldots, p-1$.

Úloha. Ukažte, že prvky $0, \ldots, p-1$ 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? (2 body)

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. Neplyne 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 špatně? 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).