Podrobný minimální sylabus

přednášek Lineární algebra I a II pro informatiky

připraveno ve spolupráci
s Jiřím Rohnem, Jiřím Tůmou, Jiřím Fialou a
Petrem Kolmanem

Verze: srpen 2006

Úvod

Lineární algebra je jedním ze základních kamenů pro jakékoli vážně míněné studium matematiky, informatiky, fyziky i inženýrských oborů. Pro většinu lidí, kteří ji začínají studovat, je to také vůbec první axiomaticky budovaná teorie, s níž se setkávají.

Základní objekt studia lineární algebry, tzv. vektorový prostor, je definován několika vlastnostmi (axiomy), z nichž se logicky odvozuje vše ostatní. Trochu podobně, jako se v pravidlech šachu neříká, jak má vypadat figurka jezdce, ale jenom jak smí tahat, v definici vektorového prostoru se neříká, co je to vektor či jak vypadá, nýbrž jenom podle jakých pravidel se s vektory počítá. Vybudovanou teorii můžeme pak použít na řadu konkrétních objektů, zdánlivě navzájem velmi odlišných.

Takto jsou vystavěna i jiná odvětví matematiky, ale lineární algebra je poměrně jednoduchá a rozvíjení matematické teorie se na ní dá zvlášť dobře ilustrovat. Časem lze ocenit i sílu této teorie: otázky o lineárních rovnicích, které jsou na první pohled zapeklité a bez přípravy těžko řešitelné i pro lidi matematicky velmi talentované, bude po zvládnutí základů lineární algebry snadné zodpovědět.

Tento text má sloužit jako kostra či podrobný sylabus přednášek Lineární algebra I a Lineární algebra II pro první ročník bakalářského studia informatiky na MFF UK Praha[1]. Každý přednášející má k látce samozřejmě svůj vlastní přístup a může ji podle úvahy obohatit a pozměnit. Tento sylabus tedy není nijak závazný (při zkoušce se požaduje látka z přednášky v té formě a s tím značením, jak byla přednesena), má však napomoct tomu, aby se látka či značení v jednotlivých bězích přednášky nelišily příliš zásadně a všichni studenti měli možnost získat srovnatelné základní znalosti.

Na studium lineární algebry je tento text příliš stručný. Určitě sám o sobě **nestačí na přípravu ke zkoušce**, už proto, že důkazy zde jsou jen v náznaku nebo chybí. Může být ale užitečný pro zopakování látky a kontrolu, že jste při přípravě nic důležitého nepřeskočili.

[1] Přednáška Lineární algebra II byla nedávno rozšířena o téma lineární programování. Tuto část sylabus záměrně nezahrnuje, protože koncepce její výuky zatím není ustálena.

1 Soustavy lineárních rovnic

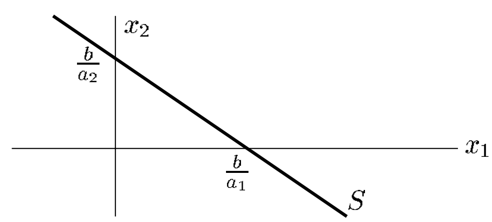
1. Příklady úloh, které vedou k soustavám lineárních rovnic (třeba proložení grafu kvadratické funkce tvaru $y = ax^2 + bx + c$ danými třemi body).

2. Rovnice $a_1x_1 + a_2x_2 = b$ (1 rovnice, 2 neznámé): množina řešení

$$S = \{(x_1, x_2) \in \mathbb{R}^2 : a_1x_1 + a_2x_2 = b\}.$$

   Zde $\mathbb{R}^2$ je množina všech uspořádaných dvojic (x, y), kde x, y jsou reálná čísla. Uspořádané dvojice, trojice, n-tice reálných čísel budeme nazývat **vektory**. (Obšírněji se někdy říká *aritmetické vektory*, protože se uvažují i jiné druhy vektorů.)

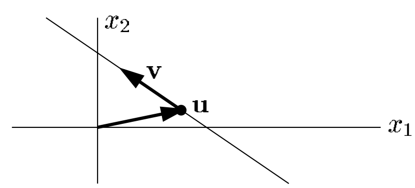
3. Geometricky odpovídá množina řešení přímce v rovině (pokud a_1 a a_2 nejsou obě rovna 0!):



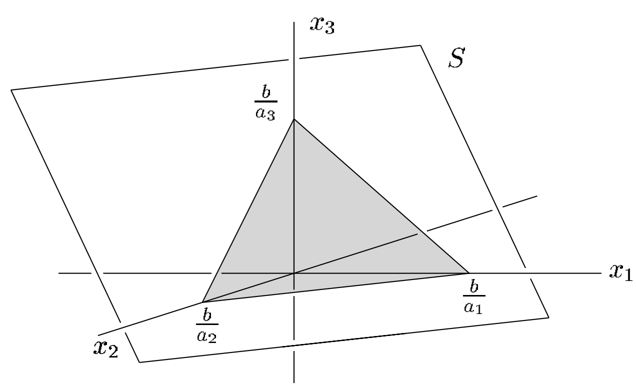
   Jiný způsob vyjádření téže množiny (parametrický zápis):

$$S = \{\mathbf{u} + t\mathbf{v} : t \in \mathbb{R}\},$$

   kde $\mathbf{u}$ a $\mathbf{v}$ jsou vhodné vektory z $\mathbb{R}^2$.



4. Podobně: množina řešení jedné lineární rovnice o 3 neznámých tvaru $a_1x_1 + a_2x_2 + a_3x_3 = b$ geometricky odpovídá rovině v $\mathbb{R}^3$ (pokud a_1, a_2, a_3 nejsou zároveň rovna 0).



Lze ji zapsat také v parametrickém tvaru

$$\{\mathbf{u} + s\mathbf{v} + t\mathbf{w} : s, t \in \mathbb{R}\}$$

pro vhodné vektory $\mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathbb{R}^3$ (ukážeme později). Řešíme-li soustavu k takových rovnic, hledáme průnik k rovin v $\mathbb{R}^3$.

5. Obecně uvažujeme soustavu m lineárních rovnic o n neznámých tvaru

$$\begin{array}{rcl} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = & b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = & b_2 \\ \vdots & & \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = & b_m \end{array}$$

(první index je vždy pro *řádek*!!). Přehlednější zápis téže soustavy:

$$A\mathbf{x} = \mathbf{b},$$

kde

- A je **matice soustavy** (matice s m řádky a n sloupci, neboli matice typu $m \times n$, kde v i-tém řádku a j-tém sloupci je a_{ij}),
- $\mathbf{b}$ je sloupcový vektor pravých stran, tj. matice typu $m \times 1$,
- $\mathbf{x}$ je sloupcový vektor neznámých, tj. matice typu $n \times 1$.

Zápis $A\mathbf{x}$ na levé straně je *součin matic*. Obecně bude součin matic definován později.

2 Řešení soustav: Gaussova eliminační metoda

6. **Elementární řádkové úpravy matice:**

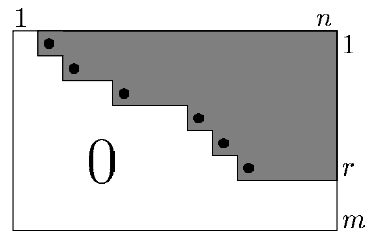
(a) vynásobení i-tého řádku nenulovým číslem t,
(b) přičtení j-tého řádku k i-tému řádku, $i \neq j$.

Pomocí operací (a) a (b) lze simulovat i operace

(b′) přičtení t-násobku j-tého řádku k i-tému řádku, $i \neq j$ a
(c) záměna dvou řádků.

7. **Rozšířená matice soustavy** $A\mathbf{x} = \mathbf{b}$ je matice $(A\,|\,\mathbf{b})$, tj. matice A, k níž je zprava připsán sloupec $\mathbf{b}$. Tvrzení: Elementární řádkové úpravy rozšířené matice nemění množinu řešení soustavy.

8. **Matice v odstupňovaném tvaru**: existuje číslo r, $0 \leq r \leq m$, tak že řádky $1, 2, \ldots, r$ jsou nenulové, řádky $r+1, \ldots, m$ jsou nulové, a je-li $j(i) = \min\{j : a_{ij} \neq 0\}$, pak $j(1) < j(2) < \cdots < j(r)$. (Obšírněji by se mohlo říkat *řádkově odstupňovaný tvar matice*, poněvadž analogicky se dá definovat i *sloupcově odstupňovaný tvar*. My o něm ale mluvit nebudeme a spokojíme se tedy s kratším termínem.)



Na obrázku vyznačují puntíky nenulové prvky na místech $(i, j(i))$, $i = 1, 2, \ldots, r$; těm se někdy říká **pivoty**.

9. **Gaussova eliminace:** algoritmus pro úpravu dané matice na odstupňovaný tvar elementárními řádkovými úpravami.

10. *Řešení soustavy* $A\mathbf{x} = \mathbf{b}$ eliminací: matice A se převede na odstupňovaný tvar, přitom se všechny řádkové úpravy aplikují na celou rozšířenou matici. Jak vypadají řešení soustavy, jejíž matice A je v odstupňovaném tvaru? Jestliže $b_{r+1}, \ldots, b_m$ nejsou všechna 0, pak soustava nemá žádné řešení, jinak se všechna řešení dostanou tak, že se neznámé x_j ve sloupcích neobsahujících pivot (těch je $n - r$) zvolí libovolně, a zbývajících r neznámých se dopočítá (jednoznačně). Speciálně pro $r = n$ je právě jedno řešení.

11. Numerické záležitosti, špatně podmíněné matice (maličká změna matice způsobí obrovskou změnu řešení). Příklad $(2{\times}2)$, geometrická interpretace (skoro rovnoběžné přímky).

3 Operace s maticemi, speciální typy matic

12. Součet matic (stejného typu!) po složkách, násobení reálným číslem po složkách.

13. **Transponovaná matice** A^T: prvek a_{ij} přijde na pozici (j, i).

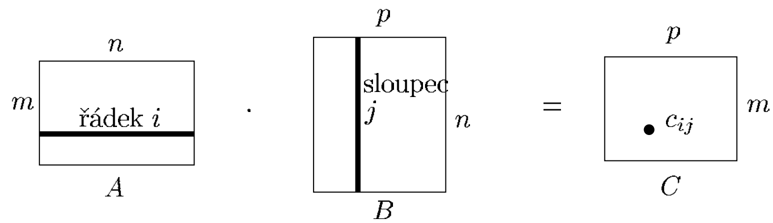
14. **Symetrická matice:** čtvercová, tj. $n \times n$, a $A^T = A$.

15. **Jednotková matice** I_n: typu $n \times n$, jedničky v pozicích (i, i), $i = 1, 2, \ldots, n$, nuly všude jinde.

16. **Diagonální matice**: má nenulové prvky pouze na hlavní diagonále, tj. $a_{ij} = 0$ pro všechna $i \neq j$.

17. **Násobení matic:** součin AB není definován pro libovolné dvě matice A a B, ale jen pokud počet sloupců A je roven počtu řádků B, tj. A je typu $m \times n$ a B je typu $n \times p$. Součin AB je pak matice C typu $m \times p$, kde

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$



Ověřit: $AI_n = I_m A = A$, pro libovolnou A typu $m \times n$.

18. Násobení a transpozice: $(AB)^T = B^T A^T$ (přesněji: součin AB je definován, právě když je definován součin $B^T A^T$, a v takovém případě platí uvedená rovnost – podobné poznámky se vztahují i k rovnostem mezi maticemi v dalším textu.)

19. Distributivita: $A(B + C) = AB + AC$, a podobně zprava.

20. Násobení matic je asociativní, $(AB)C = A(BC)$.

21. Nechť A je matice typu $n \times n$. Matice B je **inverzní** k A, pokud $AB = I_n$. (Pozor, o inverzní matici mluvíme pouze u čtvercových matic!) Inverzní matici, pokud existuje, značíme A^{-1}.

22. Které matice mají inverzní matici? V odpovědi je potřeba následující pojem: Čtvercová matice A se nazývá **regulární**, pokud soustava $A\mathbf{x} = \mathbf{0}$ má jediné řešení (tj. $\mathbf{x} = \mathbf{0}$). Čtvercová matice, která není regulární, se jmenuje **singulární.**

23. Věta: Matice A typu $n \times n$ má inverzní matici, právě když je regulární. V takovém případě je inverzní matice určena jednoznačně, a platí $AA^{-1} = A^{-1}A = I_n$, tj. inverzní matice je inverzní zleva i zprava.

24. V důkazu i na jiné věci se hodí tvrzení:

    Čtvercová matice A je regulární

    $\Leftrightarrow$ v (nějakém) odstupňovaném tvaru platí $r = n$

    $\Leftrightarrow$ soustava $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení pro každé $\mathbf{b}$.

    Pak v důkazu věty využijeme: i-tý sloupec matice A^{-1} je řešení soustavy $A\mathbf{x} = \mathbf{e}_i$, kde $\mathbf{e}_i$ je i-tý sloupec jednotkové matice I_n.

25. Násobení a inverze: $(AB)^{-1} = B^{-1}A^{-1}$ (jako u transpozice).

26. Výpočet inverzní matice: Utvoříme matici $(A \,|\, I_n)$ a řádkovými úpravami ji převedeme na tvar $(I_n \,|\, B)$ (když to jde), pak $B = A^{-1}$. Když to nejde, je A singulární.

4 Tělesa (v algebře)

27. S racionálními, reálnými, komplexními čísly můžeme dělat „čtyři základní početní úkony“: máme operace sčítání a násobení a odvozené (inverzní) operace odčítání a dělení. Těleso je algebraická struktura, v níž jsou definovány operace s podobnými vlastnostmi a s jejímiž prvky tudíž můžeme „počítat“ podobně jako s reálnými čísly.

28. Těleso definujeme **axiomy**, tj. vlastnostmi, které musí příslušné operace splňovat.

29. Je-li X nějaká množina, **binární operace** na X je libovolné zobrazení $X \times X \to X$. Neformálně, binární operace přiřazuje každým dvěma prvkům $a, b \in X$ prvek z X, což je výsledek té operace provedené na a a b. Příklad: násobení reálných čísel je binární operace na $\mathbb{R}$; dělení není binární operace na $\mathbb{R}$, ale je to binární operace na $\mathbb{R} \setminus \{0\}$.

30. **Těleso** je množina $\mathbb{K}$ spolu se dvěma binárními operacemi $+$ (sčítání) a $\cdot$ (násobení), splňujícími následující axiomy:

(SK)	Sčítání je **komutativní**, tj. $a + b = b + a$ pro každé $a, b \in \mathbb{K}$.
(SA)	Sčítání je **asociativní**, tj. $a + (b + c) = (a + b) + c$ pro každé $a, b, c \in \mathbb{K}$.
(S0)	Existuje **nulový prvek** $0 \in \mathbb{K}$ neutrální vzhledem ke sčítání, tj. platí $a + 0 = a$ pro každé $a \in \mathbb{K}$.
(SI)	Pro každé $a \in \mathbb{K}$ existuje **opačný** prvek $b \in \mathbb{K}$, pro nějž $a+b = 0$. Takový prvek b (o němž se ukáže, že je určen jednoznačně) se zpravidla značí $-a$.
(NK)	Násobení je komutativní, tj. $a \cdot b = b \cdot a$ pro každé $a, b \in \mathbb{K}$.
(NA)	Násobení je asociativní, tj. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro každé $a, b, c \in \mathbb{K}$.
(N1)	Existuje **jednotkový prvek** $1 \in \mathbb{K}$ neutrální vzhledem k násobení, tj. $1 \cdot a = a$ pro každé $a \in \mathbb{K}$ *různé od* 0.
(NI)	Pro každé $a \in \mathbb{K}$ *různé od* 0 existuje **inverzní** prvek b, pro nějž $a \cdot b = 1$. Takový prvek b (o němž se ukáže, že je určen jednoznačně) se zpravidla značí a^{-1}.
(D)	Násobení je **distributivní** vzhledem ke sčítání, tj. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ pro všechna $a, b, c \in \mathbb{K}$.
(01)	$0 \neq 1$.

Pozor, definice tělesa v sobě skrývá též požadavek, že kdykoli $a, b \in \mathbb{K}$, pak také $a + b \in \mathbb{K}$ a $a \cdot b \in \mathbb{K}$.

Součin $a \cdot b$ zapisujeme většinou jen ab. Odčítání definujeme $a - b = a + (-b)$, a dělení $a/b = a \cdot b^{-1}$.

To, čemu zde říkáme těleso, se někdy obšírněji nazývá *komutativní těleso*, a uvažují se též tělesa nekomutativní, jež nemusí splňovat axiom (NK). Zde budeme tělesem rozumět jen komutativní těleso.

31. Tvrzení o násobení matic, inverzních maticích, řešení soustav lineárních rovnic platí, i když místo reálných čísel pracujeme s libovolným jiným tělesem. Vše je třeba řádně dokázat z axiomů (a ničeho jiného!!!). Pro představu několik jednoduchých tvrzeníček; např. jednoznačnost 0, 1; jednoznačnost $-a$, a^{-1}; $0 \cdot a = 0$; $(-1) \cdot a = -a$; „krácení“ (z $a + b = a + c$ plyne $b = c$, z $a \cdot b = a \cdot c$ plyne $b = c$ pro nenulové a).

32. Příklady těles: racionální čísla $\mathbb{Q}$, reálná čísla $\mathbb{R}$, komplexní čísla $\mathbb{C}$, dvouprvkové $\mathbb{Z}_2$. Exotičtější: $\mathbb{R}(x)$ – prvky jsou všechny racionální funkce $p(x)/q(x)$, kde $p(x)$ a $q(x)$ jsou mnohočleny s reálnými koeficienty.

33. Značení $\mathbb{Z}_n$ (čísla $0, 1, 2, \ldots, n - 1$ s operacemi sčítání a násobení modulo n, čili *zbytkové třídy* modulo n). $\mathbb{Z}_3$ je těleso, $\mathbb{Z}_4$ NENÍ!!!

34. Tvrzení: $\mathbb{Z}_n$ je těleso, právě když n je prvočíslo. Princip důkazu: Je-li n složené, tvaru $n = k\ell$, pak zbytkové třídy k a ℓ jsou *dělitelé nuly*, tj. jejich součin v $\mathbb{Z}_n$ je 0. Je-li n prvočíslo, stačí ukázat, že pro každé nenulové $\ell \in \mathbb{Z}_n$ je zobrazení „násobení ℓ“: $\mathbb{Z}_n \to \mathbb{Z}_n$ surjektivní (na). Trik: ověřit injektivitu (že je prosté).

35. Označení: GF(q) konečné těleso s q prvky (Galois Field) pokud existuje. Existuje právě když q je mocnina prvočísla, a pak existuje právě 1 (bez důkazu). Konečná tělesa jsou velmi významná pro informatiku (např. pro kódy, třeba na CD nebo DVD).

36. **Charakteristika** tělesa: nejmenší $n \geq 1$ takové, že

$$\underbrace{1 + 1 + \cdots + 1}_{n-\text{krát}} = 0,$$

nebo 0, pokud takové n není. Tvrzeníčko: charakteristika je vždy prvočíslo nebo 0.

5 Vektorové prostory

37. Zatím pro nás vektory byly uspořádané n-tice reálných čísel, tvaru $\mathbf{v} = (v_1, \ldots, v_n)$, žijící v $\mathbb{R}^n$ (kartézský součin n kopií $\mathbb{R}$, např. $\mathbb{R}^2$ popisuje rovinu). Můžeme je sčítat, a také násobit reálným číslem. Podobně jako jsme reálná čísla pomocí axiomů zobecnili na tělesa, zobecníme $\mathbb{R}^n$ pomocí axiomů na tzv. vektorový prostor.

38. Dá se říct, že lineární algebra je studium vektorových prostorů. Budeme-li mluvit o vektorových prostorech, můžete si vždy představovat $\mathbb{R}^2$, $\mathbb{R}^3$ a obecně $\mathbb{R}^n$ jako základní (a nejdůležitější) příklady.

39. **Vektorový prostor** nad tělesem $\mathbb{K}$ je množina V (prvky = **vektory**) s binární operací + (sčítání vektorů) a operací $\cdot$ (násobení vektoru skalárem z tělesa $\mathbb{K}$; je to zobrazení $\mathbb{K} \times V \to V$), splňující následující axiomy:

(SK)	Sčítání vektorů je komutativní, tj. $\mathbf{u} + \mathbf{v} = \mathbf{v} + \mathbf{u}$ pro každé $\mathbf{u}, \mathbf{v} \in V$.
(SA)	Sčítání vektorů je asociativní, tj. $\mathbf{u} + (\mathbf{v} + \mathbf{w}) = (\mathbf{u} + \mathbf{v}) + \mathbf{w}$ pro každé $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$.
(S0)	Existuje **nulový vektor** $\mathbf{0} \in V$ neutrální vzhledem ke sčítání vektorů, tj. $\mathbf{v} + \mathbf{0} = \mathbf{v}$ pro každé $\mathbf{v} \in V$. [Pozor, máme teď dvě (různé) 0 – jednu v $\mathbb{K}$ a jednu (tučnou) ve V!!!]
(SI)	Pro každé $\mathbf{v} \in V$ existuje opačný vektor $-\mathbf{v} \in V$, pro nějž $\mathbf{v} + (-\mathbf{v}) = \mathbf{0}$.
(NA)	Násobení vektoru skalárem je „asociativní", tj. $a \cdot (b \cdot \mathbf{v}) = (a \cdot b) \cdot \mathbf{v}$ pro každé $a, b \in \mathbb{K}$ a každé $\mathbf{v} \in V$.
(N1)	Platí $1 \cdot \mathbf{v} = \mathbf{v}$ pro každé nenulové $\mathbf{v} \in V$ (kde $1 \in \mathbb{K}$ je jednotkový prvek tělesa).
(D1)	Platí takováto distributivita: $(a + b) \cdot \mathbf{v} = (a \cdot \mathbf{v}) + (b \cdot \mathbf{v})$, pro každé $a, b \in \mathbb{K}$ a každé $\mathbf{v} \in V$,
(D2)	a taky takováhle distributivita: $a \cdot (\mathbf{u} + \mathbf{v}) = (a \cdot \mathbf{u}) + (a \cdot \mathbf{v})$, pro každé $a \in \mathbb{K}$ a každé $\mathbf{u}, \mathbf{v} \in V$.

Všimněte si, že kdykoli $\mathbf{u}, \mathbf{v} \in V$ a $a \in \mathbb{K}$, požadujeme též $\mathbf{u} + \mathbf{v} \in V$ a $a\mathbf{v} \in V$.

40. Příklady:

- $\{\mathbf{0}\}$ (triviální vektorový prostor).
- $\mathbb{K}^n$ (**aritmetický vektorový prostor** dimenze n nad $\mathbb{K}$) pro libovolné těleso $\mathbb{K}$.
- Množina všech matic typu 7×11 s prvky z $\mathbb{K}$ (nebo nějakého jiného pevně zvoleného typu $m \times n$).
- $\mathbb{R}[x]$ (všechny polynomy s reálnými koeficienty).
- Polynomy stupně nejvýš 293 s reálnými koeficienty (nebo jiného daného maximálního stupně).
- Množina všech podmnožin množiny X jako vektorový prostor nad GF(2) (sčítání = symetrická diference množin).
- Množina všech funkcí $\mathbb{R} \to \mathbb{R}$ ($(f+g)(x) = f(x)+g(x)$ atd.), podobně množina všech *spojitých* funkcí $\mathbb{R} \to \mathbb{R}$ či všech *diferencovatelných* funkcí $\mathbb{R} \to \mathbb{R}$.
- Exotický příklad: $\mathbb{R}$ (reálná čísla) jako vektorový prostor nad $\mathbb{Q}$ (racionálními čísly).

41. Tvrzeníčka o vektorových prostorech: $0\mathbf{x} = \mathbf{0}$; $(-1)\mathbf{x} = -\mathbf{x}$; $a\mathbf{x} = \mathbf{0}$, právě když $a = 0$ nebo $\mathbf{x} = \mathbf{0}$.

42. **Podprostor** vektorového prostoru V je podmnožina $W \subseteq V$, která je vektorovým prostorem vzhledem k $\mathbf{0}$, „$+$" a „$\cdot$" zděděným z V. Tj. platí $\mathbf{0} \in W$, $\mathbf{u} + \mathbf{v} \in W$ pro libovolná $\mathbf{u}, \mathbf{v} \in W$, a také $a\mathbf{v} \in W$ pro libovolné $a \in \mathbb{K}$ a libovolné $\mathbf{v} \in W$.

43. Příklad: vektorové podprostory $\mathbb{R}^2$ jsou (geometricky) počátek, celé $\mathbb{R}^2$, a každá přímka procházející počátkem (ověříme později).

44. Pozorování: průnik libovolného souboru podprostorů vektorového prostoru V je opět podprostor. Definice: Je-li X podmnožina vektorového prostoru V, **podprostor generovaný $\boldsymbol{X}$** je průnik všech těch podprostorů W, které X obsahují. Označení: $\mathrm{span}(X)$ (v literatuře též $\langle X \rangle$, $\mathcal{L}(X)$, $[X]$, název též **lineární obal $\boldsymbol{X}$**).

45. Jsou-li $\mathbf{v}_1, \ldots, \mathbf{v}_n \in V$ vektory, každý výraz $a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$, kde $a_i \in \mathbb{K}$, se nazývá **lineární kombinace** $\mathbf{v}_1, \ldots, \mathbf{v}_n$ (v lineární kombinaci máme vždy *konečný* počet vektorů!). Vektor $\mathbf{0}$ považujeme za lineární kombinaci prázdného souboru vektorů. Tvrzení (explicitní popis podprostoru generovaného X): $\mathrm{span}(X)$ je množina všech lineárních kombinací vektorů z X.

46. Buď A matice typu $m \times n$. Vektorové prostory s ní spojené:

    - **řádkový prostor** (= podprostor $\mathbb{K}^n$ generovaný řádky A),
    - **sloupcový prostor** (= podprostor $\mathbb{K}^m$ generovaný sloupci A),
    - **jádro** (= podprostor $\mathbb{K}^n$ tvořený všemi řešeními soustavy $A\mathbf{x} = \mathbf{0}$), označení: $\mathrm{Ker}\, A$ (kernel).

    Pozorování: elementární řádkové úpravy matice nemění řádkový prostor ani jádro.

6 Lineární závislost, báze, dimenze

47. Soubor (konečná posloupnost) vektorů $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ je **lineárně nezávislý**, pokud z rovnosti $a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n = \mathbf{0}$ plyne $a_1 = a_2 = \cdots = a_n = 0$, tj. vektory lze nakombinovat na nulu jen jediným, triviálním způsobem.

    (V souboru, narozdíl od množiny, se mohou nějaké vektory opakovat, ale jakmile $\mathbf{v}_i = \mathbf{v}_j$, pak je soubor lineárně závislý.)

48. Alternativní, možná intuitivnější popis lineární nezávislosti: soubor $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ je lineárně nezávislý, pokud každé $\mathbf{v}_i$ „něco přidá" k lineárnímu obalu: $\mathbf{v}_i \notin \mathrm{span}(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n)$ pro každé $i = 1, 2, \ldots, n$.

49. Nekonečný soubor vektorů je lineárně nezávislý, pokud každý konečný podsoubor je lineárně nezávislý. (Co je nekonečný soubor? Jako množina, ale prvky se mohou opakovat, formálně zapisujeme nekonečný soubor $(\mathbf{v}_i)_{i\in I}$, kde I je nekonečná množina „indexů“.)

50. Příklady lineárně nezávislých souborů:

   - $(\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_n)$ řádky jednotkové matice I_n (čili tzv. **standardní báze** $\mathbb{R}^n$);
   - prvních r řádků matice v odstupňovaném tvaru;
   - $(x^i)_{i=0,1,\ldots}$ v $\mathbb{R}[x]$;
   - $(1, \sqrt{2})$ v $\mathbb{R}$ jako vektorovém prostoru nad $\mathbb{Q}$ (důkaz zahrnuje starořecký důkaz iracionality $\sqrt{2}$).

51. Soubor B vektorů ve vektorovém prostoru V se nazývá **systém generátorů** prostoru V, pokud $\mathrm{span}(B) = V$. Vektorový prostor se nazývá **konečně generovaný**, pokud má nějaký konečný systém generátorů.

> Lineárně nezávislý systém generátorů vektorového prostoru V se jmenuje **báze** prostoru V.

52. Příklady: prázdný systém je báze triviálního prostoru $\{\mathbf{0}\}$, systém $(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ je báze $\mathbb{K}^n$, $(1, x, x^2, \ldots)$ je báze $\mathbb{R}[x]$.

53. Tvrzení: Minimální systém generátorů (tj. žádný vlastní podsystém už negeneruje celý prostor) je báze. Tudíž z libovolného konečného systému generátorů lze vybrat bázi.

54. Tím jsme dokázali, že každý konečně generovaný prostor má bázi. Ve skutečnosti *každý vektorový prostor má bázi* (nedokazujeme, vyžaduje to axiom výběru).

55. Může jeden vektorový prostor mít různě velké báze? NE!! K důkazu potřebujeme **Steinitzovu větu o výměně**.

56. Nejdřív **lemma o výměně:** Je-li $G = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ systém generátorů prostoru V, $\mathbf{w} \in V$ je nějaký vektor, a $\mathbf{w} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + a_n\mathbf{v}_n$ je nějaké jeho vyjádření pomocí vektorů z G, potom kdykoli $a_i \neq 0$, je také $(\mathbf{v}_1, \ldots, \mathbf{v}_{i-1}, \mathbf{w}, \mathbf{v}_{i+1}, \ldots, \mathbf{v}_n)$ systém generátorů (tj. každý $\mathbf{v}_i$ s nenulovým koeficientem lze nahradit $\mathbf{w}$).

57. **Steinitzova věta o výměně:** Je-li $N = (\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m)$ lineárně nezávislý soubor vektorů ve V a $G = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ je systém generátorů V, pak $m \leq n$, a některých m vektorů z G lze nahradit vektory $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_m$ tak, že dostaneme opět systém generátorů. [Důkaz indukcí podle m; v indukčním kroku nejdřív dostat do G vektory $\mathbf{w}_1, \ldots, \mathbf{w}_{m-1}$, a pak použít lemma o výměně na výsledný systém generátorů a $\mathbf{w}_m$.]

58. Hlavní důsledek: Všechny báze konečně generovaného prostoru jsou konečné a mají stejný počet vektorů. (Ve skutečnosti v libovolném vektorovém prostoru mají všechny báze stejnou mohutnost, to nebudeme dokazovat.)

   Dimenze vektorového prostoru V je mohutnost nějaké (a tedy libovolné) báze V.

59. Další důsledek Steinitzovy věty: Libovolný lineárně nezávislý systém N v konečně generovaném prostoru V lze doplnit na bázi. [Důkaz: větu použít na N a libovolnou bázi prostoru V v roli G.]

60. Odtud: Je-li W podprostor konečně generovaného prostoru V, pak $\dim(W) \leq \dim(V)$ (speciálně je W konečně generovaný). Nastane-li rovnost, pak $W = V$.

61. Příklad: jaké jsou podprostory $\mathbb{R}^2$? Musejí mít dimenzi 0 (pak je to $\{\mathbf{0}\}$), 2 (pak je to $\mathbb{R}^2$), nebo 1, a jednodimenzionální vektorový prostor je tvořen všemi násobky nějakého nenulového vektoru, tedy je to přímka procházející $\mathbf{0}$. Podobně pro $\mathbb{R}^3$: přibudou roviny procházející $\mathbf{0}$.

62. Buď $B = (\mathbf{v}_1, \ldots, \mathbf{v}_n)$ báze vektorového prostoru V nad tělesem $\mathbb{K}$ a $\mathbf{v} \in V$ libovolný vektor. Pak $\mathbf{v}$ lze právě jedním způsobem vyjádřit jako $\mathbf{v} = a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$. Vektor $(a_1, a_2, \ldots, a_n) \in \mathbb{K}^n$ nazýváme **vektor souřadnic** vektoru $\mathbf{v}$ vzhledem k bázi B, označení $[\mathbf{v}]_B$.

7 Hledání báze, hodnost matice

63. Jak spočítat dimenzi (a najít bázi) prostoru $V = \mathrm{span}(\mathbf{a}_1, \ldots, \mathbf{a}_m)$, kde $\mathbf{a}_1, \ldots, \mathbf{a}_m$ jsou dané vektory z $\mathbb{K}^n$? Napíšeme $\mathbf{a}_1, \ldots, \mathbf{a}_m$ jako řádky matice A (pak V je řádkový prostor). *Gaussova eliminace* je algoritmus na hledání báze: nenulové řádky odstupňovaného tvaru tvoří bázi V.

   Hodnost matice A je definována jako dimenze jejího řádkového prostoru, a budeme ji značit $\mathrm{rank}\, A$.

   Hodnost je též rovna počtu nenulových řádků v odstupňovaném tvaru (a tudíž tento počet nezávisí na postupu Gaussovy eliminace, což z algoritmu samotného není zřejmé).

64. Elementární řádkové úpravy matice odpovídají jejímu násobení zleva vhodnými čtvercovými regulárními maticemi.

65. Co dělá násobení maticí A zleva s řádkovým a sloupcovým prostorem matice B:

   - Řádkový prostor $AB \subseteq$ řádkový prostor B.
   - Je-li $(\mathbf{v}_1, \ldots, \mathbf{v}_r)$ nějaká báze sloupcového prostoru B, pak $(A\mathbf{v}_1, \ldots, A\mathbf{v}_r)$ generuje sloupcový prostor AB.

66. Důsledky:

    (a) $\text{rank}(AB) \leq \text{rank}(B)$.

    (b) Násobení regulární maticí zleva, a speciálně elementární řádkové úpravy, nemění řádkový prostor (a tedy ani hodnost).

    (c) Násobení regulární maticí zleva, a speciálně elementární řádkové úpravy, nemění *dimenzi* sloupcového prostoru.

67. Věta (jeden z „divů“ lineární algebry): hodnost matice je též rovna dimenzi sloupcového prostoru. Důkaz: pro redukovaný odstupňovaný tvar je vidět a obecně se použije Gaussova eliminace plus (b) a (c) z předchozího bodu.

68. Z odstupňovaného tvaru můžeme též najít bázi $\text{Ker}(A)$, a zjistit, že

$$\dim(\text{Ker}\, A) + \text{rank}(A) = n$$

pro každou matici A s n sloupci.

8 Lineární zobrazení

69. Zobrazení $f: U \to V$, kde U a V jsou vektorové prostory (nad týmž tělesem!), je **lineární** pokud $f(\mathbf{u}+\mathbf{v}) = f(\mathbf{u}) + f(\mathbf{v})$ a $f(a\mathbf{u}) = af(\mathbf{u})$, pro každé $\mathbf{u}, \mathbf{v} \in U$ a $a \in \mathbb{K}$.

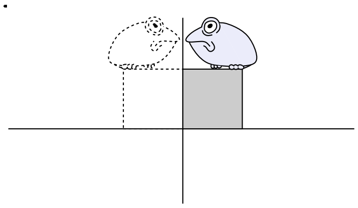
70. Složení lineárních zobrazení je zase lineární zobrazení (pokud je ovšem lze skládat!).

71. Příklad (jednoduchý): lineární zobrazení $\mathbb{R}^1 \to \mathbb{R}^1$ je nutně tvaru $x \mapsto ax$, $a \in \mathbb{R}$.

72. Lineární zobrazení $\mathbb{R}^2 \to \mathbb{R}^2$ jsou už dost zajímavá. Příklady:

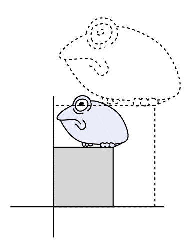
    - projekce na osu x,
    - projekce na danou přímku procházející $\mathbf{0}$,
    - **zrcadlení**, např.:

      $(x, y) \mapsto (-x, y)$



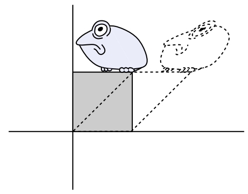
    - **zvětšení** (homotetie), např.:

      $(x, y) \mapsto (1.7x, 1.7y)$



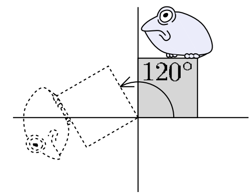
- **zkosení**, např.:

  $(x, y) \mapsto (x + y, y)$

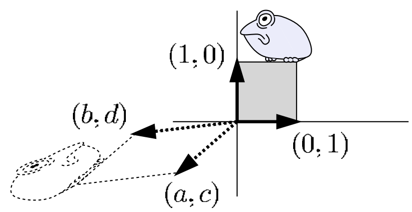


- **rotace** kolem $\mathbf{0}$, např.:

  $(x, y) \mapsto (-\frac{1}{2}x - \frac{\sqrt{3}}{2}y, \frac{\sqrt{3}}{2}x - \frac{1}{2}y)$



73. Obecný tvar: $f(x, y) = (ax + by, cx + dy)$, jiná nejsou. Maticový tvar: $f(\mathbf{v}) = A\mathbf{v}$, kde $\mathbf{v} \in \mathbb{R}^2$ je sloupcový vektor (x, y) a A je matice s řádky (a, b), (c, d).



$(x, y) \mapsto (ax + by, cx + dy)$

74. Tvrzení: Buďte U, V vektorové prostory a B nějaká báze U. Pro každé zobrazení $f: B \to V$ existuje právě jedno lineární zobrazení $\bar{f}: U \to V$ splňující $\bar{f}(b) = f(b)$ pro všechna $b \in B$. Jinými slovy: každá volba hodnot na bázi jednoznačně určuje lineární zobrazení.

75. Z toho: víme-li už (geometricky), že např. otočení kolem $\mathbf{0}$ o úhel τ je lineární zobrazení, můžeme jej snadno vyjádřit; vyjde, že to je $(x, y) \mapsto (x \cos\tau - y \sin\tau, x \sin\tau + y \cos\tau)$.

76. Věta: Libovolné lineární zobrazení $f: \mathbb{R}^n \to \mathbb{R}^m$ má tvar $f(\mathbf{x}) = A\mathbf{x}$, kde $\mathbf{x}$ je sloupcový vektor z $\mathbb{R}^n$ a A je matice $m \times n$; její *sloupce* jsou obrazy bázových vektorů $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Matice obvyklých geometrických transformací, např. otočení kolem počátku, se objevují např. v počítačové grafice.

77. Matice lineárního zobrazení obecně: V prostoru U máme zvolenou jeho bázi B, v prostoru V bázi C, a $f: U \to V$ je lineární zobrazení. **Matice f vzhledem k bázím B a C**, označení $[f]_{B,C}$, je matice typu $\dim(V) \times \dim(U)$, jejíž j-tý sloupec je $[f(\mathbf{u}_j)]_C$, tj. souřadnice obrazu j-tého vektoru z B vzhledem k bázi C. Pro každé $\mathbf{u} \in U$ platí

$$[f(\mathbf{u})]_C = [f]_{B,C}[\mathbf{u}]_B.$$

Pozor, je potřeba rozlišovat mezi $\mathbf{u}$ (to je vektor z obecného vektorového prostoru, a jeho násobení maticí obecně není definováno) a vektorem $[\mathbf{u}]_B$ (to je vektor z $\mathbb{K}^n$)!

78. *Skládání lineárních zobrazení a násobení matic:* Jsou-li V_1, V_2, V_3 vektorové prostory a B_i je nějaká báze V_i, $f\colon V_2 \to V_1$ je lineární zobrazení s maticí A vzhledem k bázím B_2 a B_1, a $g\colon V_3 \to V_2$ je lineární zobrazení s maticí B vzhledem k bázím B_3 a B_2, pak $f \circ g\colon V_3 \to V_1$ má matici AB vzhledem k bázím B_3 a B_1. V symbolech:

$$[f \circ g]_{B_3,B_1} = [f]_{B_2,B_1}[g]_{B_3,B_2}.$$

Důkaz z asociativity násobení matic.

79. Příklad: násobení matic rotací kolem počátku v $\mathbb{R}^2$ dává součtové vzorce pro sinus a kosinus.

80. Jsou-li B a C dvě báze prostoru V, potom matice identického zobrazení $\mathrm{id}\colon V \to V$ vzhledem k bázím B a C, neboli $[\mathrm{id}]_{B,C}$, se nazývá **matice přechodu** od B k C. Slouží k přepočítávání souřadnic: $[\mathbf{v}]_C = [\mathrm{id}]_{B,C}[\mathbf{v}]_B$.

81. Co to znamená že vektorové prostory V a W jsou „stejné“? Existuje mezi nimi **isomorfismus** $f\colon V \to W$, což je lineární zobrazení, k němuž existuje inverzní zobrazení a to je též lineární (což je právě když f je lineární, prosté a na). Isomorfismus je něco jako přejmenování vektorů: vektory v isomorfních prostorech mohou „vypadat“ jinak, ale „chovají se“ naprosto stejně.

82. Tvrzení: Isomorfismus zobrazuje bázi na bázi, a tudíž zachovává dimenzi.

83. Tvrzení (n-dimenzionální vektorový prostor nad $\mathbb{K}$ je „jen jeden“): každý n-dimenzionální vektorový prostor V nad $\mathbb{K}$ je isomorfní $\mathbb{K}^n$.

Důkaz: zvol bázi B prostoru V, isomorfismus $f\colon V \to \mathbb{K}^n$ se definuje předpisem $f(\mathbf{v}) = [\mathbf{v}]_B$ (vektoru se přiřadí jeho vektor souřadnic). Poznámka: mnoho isomorfismů = mnoho „možných pohledů“ na daný vektorový prostor!

84. Tvrzení: Je-li $\dim(U) = \dim(V) = n$, $f\colon U \to V$ je lineární, a A je matice f vzhledem k nějakým bázím, potom f je isomorfismus, právě když A je regulární. (Odtud jiný důkaz věty o inverzní matici z bodu 23).

85. *Afinní podprostory:* Podmnožina F vektorového prostoru V, která je buď prázdná, nebo tvaru $F = \mathbf{x} + U = \{\mathbf{x} + \mathbf{u} : \mathbf{u} \in U\}$, kde U je (vektorový) podprostor V, se nazývá **afinní podprostor** (též *lineární množina* nebo *lineál*) ve V.

86. Platí $U = \{\mathbf{u} - \mathbf{v} : \mathbf{u}, \mathbf{v} \in F\}$, a tedy F určuje U. **Dimenzi** F definujeme jako $\dim(U)$. Např. obecné přímky a roviny v $\mathbb{R}^3$ jsou afinní podprostory. Terminologie: 1-dimenzionální afinní podprostor se nazývá **přímka**, 2-dimenzionální **rovina**, $(n-1)$-dimenzionální afinní podprostor n-dimenzionálního prostoru se jmenuje **nadrovina**.

87. Je-li $f\colon U \to V$ lineární zobrazení a $\mathbf{b} \in V$ daný vektor, potom $f^{-1}(\mathbf{b})$ je afinní podprostor U; je-li neprázdný, má tvar $\mathbf{x} + \mathrm{Ker}(f)$, kde $\mathbf{x}$ je nějaký (libovolný) vektor splňující $f(\mathbf{x}) = \mathbf{b}$.

88. Totéž v řeči matic: množina všech řešení soustavy $A\mathbf{x} = \mathbf{b}$, kde A je $m \times n$ matice a $\mathbf{b}$ je m-složkový vektor, je buď prázdná, anebo má tvar $\mathbf{x}_0 + L$, kde $\mathbf{x}_0$ je nějaké libovolné řešení soustavy $A\mathbf{x} = \mathbf{b}$ a L je množina všech řešení **homogenní** soustavy $A\mathbf{x} = \mathbf{0}$. Hledání všech řešení soustavy $A\mathbf{x} = \mathbf{b}$: najdeme jedno řešení $\mathbf{x}_0$ (pokud existuje) a nějakou bázi pro prostor řešení homogenní soustavy $A\mathbf{x} = \mathbf{0}$, tj. $\mathrm{Ker}(A)$.

89. Shrnutí toho, co zatím víme o řešení soustavy lineárních rovnic $A\mathbf{x} = \mathbf{b}$, a různé pohledy na to:

   - Pohled vektorověprostorový: je $\mathbf{b}$ v podprostoru generovaném sloupci A?
   - Pohled geometrický: průnik nadrovin v $\mathbb{K}^n$.
   - Pohled lineárnězobrazeňový: vzor vektoru $\mathbf{b}$ při lineárním zobrazení $\mathbf{x} \mapsto A\mathbf{x}$, řešení je afinní podprostor $\mathbb{K}^n$.

9 Prostory se skalárním součinem

90. V „čistém“ vektorovém prostoru nemáme pojmy jako „délka“ a „úhel“. Přidáním skalárního součinu je tam můžeme elegantně zavést. *Pozor*, zde budeme uvažovat jen vektorové prostory nad reálnými nebo komplexními čísly!!

91. **Prostor se skalárním součinem** je vektorový prostor V nad $\mathbb{R}$ nebo nad $\mathbb{C}$ plus zobrazení $V \times V \to \mathbb{R}$ (nebo $\to \mathbb{C}$), zvané **skalární součin**, označení $\langle \mathbf{u} \,|\, \mathbf{v} \rangle$ (není v literatuře jednotné, též $\langle \mathbf{u}, \mathbf{v} \rangle$, $\mathbf{u} \cdot \mathbf{v}$ a pod.). Axiomy:

(PD)	$\langle \mathbf{v} \,|\, \mathbf{v} \rangle \geq 0$, rovnost pouze pro $\mathbf{v} = \mathbf{0}$,
(L1)	$\langle a\mathbf{u} \,|\, \mathbf{v} \rangle = a \langle \mathbf{u} \,|\, \mathbf{v} \rangle$ (pro a reálné či komplexní číslo),
(L2)	$\langle \mathbf{u} + \mathbf{v} \,|\, \mathbf{w} \rangle = \langle \mathbf{u} \,|\, \mathbf{w} \rangle + \langle \mathbf{v} \,|\, \mathbf{w} \rangle$,
(k)	$\langle \mathbf{v} \,|\, \mathbf{u} \rangle = \overline{\langle \mathbf{u} \,|\, \mathbf{v} \rangle}$ (tedy v reálném případě $\langle \mathbf{v} \,|\, \mathbf{u} \rangle = \langle \mathbf{u} \,|\, \mathbf{v} \rangle$).

92. Základní příklad je **standardní skalární součin** na $\mathbb{R}^n$: $\langle \mathbf{x} \,|\, \mathbf{y} \rangle = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$.

93. Standardní skalární součin v $\mathbb{R}^n$ je nejobvyklejší, ale není to jediná možnost pro skalární součin na $\mathbb{R}^n$. Třeba v rovině můžeme taky definovat $\langle \mathbf{x} \,|\, \mathbf{y} \rangle = x_1 y_1 + \frac{1}{3} x_1 y_2 + \frac{1}{3} x_2 y_1 + x_2 y_2$ (to souvisí s pozitivně definitními maticemi, které probereme později).

94. Na prostoru V se skalárním součinem definujeme **normu** vektoru $\mathbf{v} \in V$ předpisem $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v} \,|\, \mathbf{v} \rangle}$. Význam: $\|\mathbf{v}\|$ je „délka" vektoru $\mathbf{v}$. **Vzdálenost** dvou vektorů $\mathbf{u}, \mathbf{v} \in V$ definujeme jako číslo $\|\mathbf{u} - \mathbf{v}\|$.

95. Pro standardní skalární součin na $\mathbb{R}^n$ tak dostaneme takzvanou **euklidovskou normu**:

$$\|\mathbf{x}\| = \sqrt{\langle \mathbf{x} \,|\, \mathbf{x} \rangle} = \sqrt{x_1^2 + x_2^2 + \cdots + x_n^2}$$

a obvyklý způsob počítání vzdálenosti bodů v euklidovském prostoru (podle Pythagorovy věty).

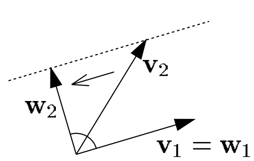
96. Poznámka: Normy se uvažují i bez návaznosti na skalární součin. Obecně **norma** na vektorovém prostoru V (nad $\mathbb{R}$ nebo nad $\mathbb{C}$) je zobrazení $p\colon V \to \mathbb{R}$, splňující následující axiomy: $p(\mathbf{v}) \geq 0$, rovnost pouze pro $\mathbf{v} = \mathbf{0}$, $p(a\mathbf{v}) = |a| \cdot p(\mathbf{v})$ (a je reálné nebo komplexní číslo) a trojúhelníková nerovnost $p(\mathbf{u}) + p(\mathbf{v}) \geq p(\mathbf{u} + \mathbf{v})$. Ze skalárních součinů se dostanou příklady norem, ale zdaleka ne každá norma pochází ze skalárního součinu. Důležité příklady norem na $\mathbb{R}^n$, které se nedostanou z žádného skalárního součinu, jsou třeba $\|\mathbf{x}\|_1 = |x_1| + |x_2| + \cdots + |x_n|$ (takzvaná ℓ_1 norma nebo též manhattanská norma) nebo $\|\mathbf{x}\|_\infty = \max(|x_1|, |x_2|, \ldots, |x_n|)$ (ℓ_∞ norma nebo též maximová norma).

97. Geometrická interpretace standardního skalárního součinu na $\mathbb{R}^n$: $\langle \mathbf{x} \,|\, \mathbf{y} \rangle = \|\mathbf{x}\| \cdot \|\mathbf{y}\| \cdot \cos\varphi$, kde φ je úhel mezi vektory $\mathbf{x}$ a $\mathbf{y}$. Tímto vzorcem se definuje „úhel vektorů" i v obecném prostoru se skalárním součinem.

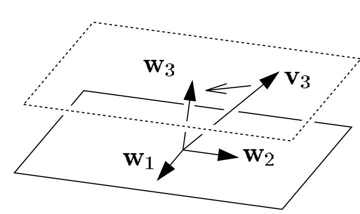
98. **Cauchyho-Schwarzova nerovnost** $\langle \mathbf{u} \,|\, \mathbf{v} \rangle \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|$. Důkaz: uvážit kvadratický mnohočlen $p(t) = \langle \mathbf{u} + t\mathbf{v} \,|\, \mathbf{u} + t\mathbf{v} \rangle$, ten musí mít nekladný diskriminant. Geometrický význam, souvislost s kosinovou a Pythagorovou větou. Definice **kolmosti** vektorů $\mathbf{u}$ a $\mathbf{v}$: $\langle \mathbf{u} \,|\, \mathbf{v} \rangle = 0$.

99. **Ortogonální systém** (nenulové navzájem kolmé vektory), **ortonormální systém** (navíc jednotkové), jejich lineární nezávislost. Vyjádření vektoru $\mathbf{v}$ v ortonormální bázi $B = (\mathbf{b}_1, \ldots, \mathbf{b}_n)$: i-tá souřadnice je $\langle \mathbf{v} \,|\, \mathbf{b}_i \rangle$. Souřadnice se někdy nazývají **Fourierovy koeficienty** vektoru $\mathbf{v}$ vzhledem k bázi B.

100. **Gramova-Schmidtova ortogonalizace:** algoritmus, který z dané báze $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ udělá ortogonální bázi $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n$. Postup: pro $k = 1, 2, \ldots, n$ polož $\mathbf{w}_k = \mathbf{v}_k - \sum_{i=1}^{k-1} \frac{\langle \mathbf{v}_k \,|\, \mathbf{w}_i \rangle}{\|\mathbf{w}_i\|^2} \mathbf{w}_i$. (Koeficienty u $\mathbf{w}_i$ jsou zvoleny tak, aby $\langle \mathbf{w}_k \,|\, \mathbf{w}_i \rangle = 0$.) Geometrická ilustrace:



2. krok (výpočet $\mathbf{w}_2$)



3. krok (výpočet $\mathbf{w}_3$)

Tvrzení: lineární obal prvních k vektorů zůstává zachován pro všechna k. Poznámka: G.-S. ortogonalizace je numericky nestabilní, ale jsou známy stabilní varianty.

101. Teoretický důsledek G.-S. ortogonalizace: Libovolný ortogonální systém v konečnědimenzionálním prostoru se dá rozšířit na ortogonální bázi.

102. **Ortogonální doplněk** množiny M:

$$M^{\perp} = \{\mathbf{v} \in V : \langle \mathbf{v} \,|\, \mathbf{x} \rangle = 0 \text{ pro všechna } \mathbf{x} \in M\}.$$

103. Ještě jeden pohled na homogenní soustavu lineárních rovnic $A\mathbf{x} = \mathbf{0}$: množina řešení = ortogonální doplněk množiny řádků matice A.

104. Vlastnosti ortogonálního doplňku (vše v konečné dimenzi):

    (i) Je to podprostor.
    (ii) Je-li $M_1 \subseteq M_2$, pak $M_2^{\perp} \subseteq M_1^{\perp}$.
    (iii) $M^{\perp} = (\operatorname{span} M)^{\perp}$.
    (iv) Je-li U podprostor, pak $(U^{\perp})^{\perp} = U$.
    (v) Platí $\dim(U^{\perp}) = \dim(V) - \dim(U)$.

    (i)–(iii) jsou snadné a (iv),(v) plynou z rozšiřitelnosti ortogonální báze.

105. Pojem **ortogonální matice** (hloupá, ale tradiční terminologie): čtvercová, $AA^T = I_n$. Pozorování: čtvercová matice má ortonormální sloupce, právě když $A^{-1} = A^T$. Tudíž: má-li čtvercová matice ortonormální řádky, pak má i ortonormální sloupce.

106. **Ortogonální projekce** na podprostor W; projekce bodu $\mathbf{x}$ je bod, který je z celého W k $\mathbf{x}$ nejblíže. Jednoznačnost, vyjádření formulí.

10 Determinant

107. **Permutace** je vzájemně jednoznačné zobrazení (bijekce) $X \to X$. Označení S_n = množina všech permutací množiny $\{1, 2, \ldots, n\}$. Množina **inverzí** permutace p:

$$I(p) = \{(i,j) : i < j \text{ a } p(i) > p(j)\}.$$

Interpretace: křížení v dvouřádkovém znázornění p šipkami. **Znaménko permutace** $\operatorname{sgn}(p) = (-1)^{|I(p)|}$.

108. Tvrzení (skládání permutací a znaménko): $\operatorname{sgn}(p \circ q) = \operatorname{sgn}(p)\operatorname{sgn}(q)$. Důkaz: obrázek se šipkami.

109. **Transpozice** = permutace zaměňující dva prvky. Transpozice má znaménko -1, a každá permutace je složením transpozic.

110. Každé čtvercové matici A teď přiřadíme podivuhodné číslo, zvané **determinant**, takto:

$$\det(A) = \sum_{p \in S_n} \operatorname{sgn}(p) \prod_{i=1}^{n} a_{i,p(i)}$$

(vzoreček s $n!$ členy).

111. Příklad: pro matici 2×2 máme $\det(A) = a_{11}a_{22} - a_{12}a_{21}$.

112. Tvrzení: Determinant trojúhelníkové matice je součinem diagonálních prvků.

113. Tvrzení: $\det(A^T) = \det(A)$ (důkaz přerovnáním součinu a sumy v definici determinantu).

114. Tvrzení: Přerovnáním sloupců podle permutace q se determinant násobí $\operatorname{sgn}(q)$ (důkaz podobný předchozímu).

    - Důsledek: Záměna dvou řádků mění znaménko determinantu.
    - Důsledek důsledku: Jestliže matice A má dva shodné řádky, pak $\det(A) = 0$.

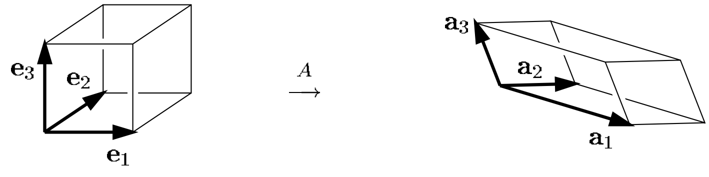
115. Tvrzení: Determinant je lineární funkcí každého řádku.

116. Důsledek: Co dělají elementární řádkové operace (násobení řádku číslem t násobí determinant číslem t, přičtení j-tého řádku k i-tému řádku nemění determinant). Totéž pro sloupce.

117. Determinant se téměř nikdy nepočítá podle definice (to by bylo neefektivní). Výpočet $\det(A)$ Gaussovou eliminací.

    - Důsledek: čtvercová matice A je regulární, právě když $\det(A) \neq 0$.
    - Důsledek: Hodnost matice se nezmění přechodem k většímu tělesu; např. jsou-li nějaké vektory s racionálními složkami lineárně nezávislé nad $\mathbb{Q}$, pak jsou lineárně nezávislé i nad $\mathbb{R}$.

118. Geometrický význam determinantu: Lineární zobrazení $\mathbb{R}^n \to \mathbb{R}^n$ odpovídající matici A převádí jednotkovou krychli na rovnoběžnostěn objemu $|\det(A)|$:



(a plochu či objem obecné množiny mění v poměru $1 : |\det(A)|$). Neformální zdůvodnění.

119. Poznámka: Znaménko determinantu je dáno orientací obrazu standardní báze. Pro regulární $n \times n$ matice A, B platí $\mathrm{sgn}(\det(A)) = \mathrm{sgn}(\det(B))$, právě když se dají propojit „spojitou cestou“ z regulárních matic.

120. Věta (o násobení determinantů): $\det(AB) = \det(A)\det(B)$. Důkaz: pro singulární A snadné, regulární A můžeme pomocí Gaussovy eliminace vyjádřit jako součin elementárních matic (odpovídajících řádkovým úpravám), a tedy násobení A odpovídá posloupnosti elementárních řádkových úprav matice B. Důsledek věty: $\det(A^{-1}) = \det(A)^{-1}$.

121. Rozvoj determinantu podle i-tého řádku:

$$\det(A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}),$$

kde A_{ij} označuje matici vzniklou z A vynecháním i-tého řádku a j-tého sloupce. Důkaz: Podle linearity determinantu jako funkce řádku stačí ověřit pro případ, kdy i-tý řádek je vektor $\mathbf{e}_j$ standardní báze.

122. Vzorec pro inverzní matici k dané regulární matici A: na místě (i, j) je $(-1)^{i+j} \det(A_{ji}) / \det(A)$ (znovu dokazuje existenci inverzní matice).

123. **Cramerovo pravidlo:** Je-li A čtvercová regulární matice, pak (jediné) řešení soustavy $A\mathbf{x} = \mathbf{b}$ má i-tou složku $\det(A_{i \to \mathbf{b}}) / \det(A)$, kde čtvercová matice $A_{i \to \mathbf{b}}$ vznikne z A nahrazením i-tého sloupce vektorem $\mathbf{b}$. Zcela nepraktické pro výpočet, ale užitečné pro odvození vlastností řešení (a též ukazuje, že determinant vzniká přirozeně při řešení soustavy lineárních rovnic).

11 Vlastní čísla

124. Vlastní čísla souvisejí s mnoha otázkami v geometrii (např. jak vypadají isometrie euklidovského prostoru), ve fyzice (jak zní zvon, rezonance, všemožná spektra…), v teorii grafů (jak dobrý je daný graf jako schéma telefonního propojení).

125. My se teď k vlastním číslům dostaneme přes vyšetřování struktury *endomorfismů*, tj. lineárních zobrazení vektorového prostoru V do sebe. Všimněme si, že pro zobrazení $X \to X$ vzniká řada otázek, které pro obecné zobrazení $X \to Y$ nemají smysl, například o pevných bodech a iteracích. Pro lineární zobrazení se takové otázky řeší právě pomocí vlastních čísel.

126. Uvažujeme lineární zobrazení $f\colon V \to V$, V konečnědimenzionalní, chceme najít bázi $(\mathbf{v}_1, \dots, \mathbf{v}_n)$ tak, aby matice f vzhledem k ní byla „jednoduchá“. Zde je podstatné, že máme jen jednu bázi ve V!

127. Připomenutí: matice přechodu $T = [\mathrm{id}]_{B,B'}$ od báze B k bázi B'. Tvrzení: Matice přechodu od B' k B je T^{-1}. Důkaz: přímým výpočtem, nebo pomocí isomorfismů s $\mathbb{K}^n$.

128. Tudíž, je-li A matice zobrazení $f: V \to V$ vzhledem k bázi B, pak matice f vzhledem k bázi B' je TAT^{-1}, kde T je matice přechodu od B k B'. Čtvercové matice A a A' se nazývají **podobné**, pokud $A' = TAT^{-1}$ pro nějakou regulární matici T.

129. Náš cíl v řeči matic: k dané čtvercové matici A najít podobnou matici A' v „jednoduchém" tvaru (uvidíme, že často se poštěstí A' diagonální, i když ne vždycky). Kdo nemá rád lineární zobrazení, může toto vzít jako výchozí bod.

130. Diagonální tvar je dobrý například k rychlému výpočtu mocnin matice (tj. iterací lineárního zobrazení), a je z něj též vidět, jak se iterace budou chovat. Protože: je-li $A = TDT^{-1}$ pro D diagonální, pak $A^k = TD^kT^{-1}$, a D^k má na diagonále k-té mocniny prvků diagonály D.

131. Varování: Elementární řádkové úpravy *nezachovávají* podobnost matic! Teď musíme matice upravovat mnohem opatrněji!!

132. Co dělá lineární zobrazení $\mathbb{R}^n \to \mathbb{R}^n$ s diagonální maticí? Natahuje či zkracuje, a případně zrcadlí, ve směru každé souřadnicové osy. Pro diagonalizaci matice obecného zobrazení potřebujeme „správné osy", v jejichž směrech ono zobrazení natahuje či zkracuje, ale zachovává směr. To vede k definici vlastních čísel a vektorů.

Je-li $f: V \to V$ lineární zobrazení, kde V je vektorový prostor nad tělesem $\mathbb{K}$, pak číslo $\lambda \in \mathbb{K}$ se nazývá **vlastní číslo** zobrazení f, právě když existuje *nenulový* vektor $\mathbf{v} \in V$ takový, že $f(\mathbf{v}) = \lambda\mathbf{v}$. **Vlastní vektor** příslušný k λ je každé $\mathbf{v} \neq \mathbf{0}$ splňující $f(\mathbf{v}) = \lambda\mathbf{v}$.

Poznámky.

- Tedy $\mathbf{v}$ je ten „dobrý směr", v němž f účinkuje jako násobení číslem λ.
- Je-li $\mathbf{v}$ vlastní vektor a $t \in \mathbb{K}$ je nenulové, pak též $t\mathbf{v}$ je vlastní vektor.
- Pozor: $\mathbf{v}$ nesmí být $\mathbf{0}$, ale λ může být 0!
- Vlastní vektor $\mathbf{v}$ generuje 1-dimenzionální **invariantní podprostor**. Obecně, podprostor W prostoru V se nazývá invariantní podprostor zobrazení f, pokud $f(W) \subseteq W$.

133. Pro čtvercovou matici A jsou vlastní čísla a vlastní vektory definovány stejně jako pro lineární zobrazení určené A. Explicitně:

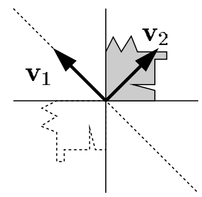
Je-li A čtvercová matice nad tělesem $\mathbb{K}$, potom se číslo $\lambda \in \mathbb{K}$ nazývá **vlastní číslo** matice A, pokud existuje vektor $\mathbf{v} \neq \mathbf{0}$ splňující rovnici

$$A\mathbf{v} = \lambda\mathbf{v}.$$

Opět, zapřisáhlí odpůrci lineárních zobrazení se mohou spokojit s touto maticovou definicí vlastních čísel.

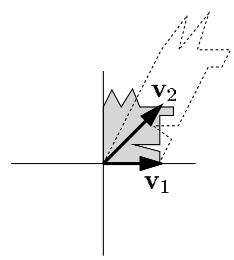
134. Příklady, co se může dít v rovině:

- Matice $\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$, zrcadlení podle přímky $y = -x$:



Vlastní čísla 1 (vlastní vektor $\mathbf{v}_1 = (-1, 1)$) a -1 ($\mathbf{v}_2 = (1, 1)$), $(\mathbf{v}_1, \mathbf{v}_2)$ tvoří bázi, a zobrazení má vzhledem k ní diagonální matici $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

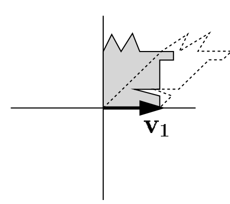
- Matice $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$, zkosení a roztažení:



Vlastní čísla 1 ($\mathbf{v}_1 = (1, 0)$) a 2 ($\mathbf{v}_2 = (1, 1)$), $(\mathbf{v}_1, \mathbf{v}_2)$ zase tvoří bázi, a zobrazení má vzhledem k ní diagonální matici $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$.

- Otočení kolem počátku o úhel α: Pokud α není násobkem π, nemá žádná (reálná) vlastní čísla a matice není podobná žádné diagonální matici. *Ale* pokud povolíme komplexní čísla, diagonalizovat lze!

- Matice $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, zkosení:



Jediné vlastní číslo 1 a jediný vlastní vektor $(1, 0)$ (až na skalární násobek), nelze diagonalizovat, ani komplexní čísla nepomůžou.

135. Dva exotičtější příklady:

- V = prostor všech reálných funkcí na $[0,1]$ majících spojité derivace všech řádů; operátor derivace $D\colon V \to V$, $f \mapsto f'$, je lineární zobrazení. Každé $\lambda \in \mathbb{R}$ je vlastním číslem, příslušný vlastní vektor je funkce $x \mapsto e^{\lambda x}$. Důležité při řešení lineárních diferenciálních rovnic s konstantními koeficienty.
- V = prostor všech nekonečných reálných posloupností $(y_0, y_1, y_2, \ldots)$ splňujících $y_{n+2} = y_{n+1} + y_n$ pro všechna $n = 0, 1, \ldots$ (jako rekurence pro Fibonacciho čísla). $P\colon V \to V$ je operátor posunutí doleva, $(y_0, y_1, y_2, \ldots) \mapsto (y_1, y_2, y_3, \ldots)$. Vlastní vektory zobrazení P jsou zjevně násobky posloupnosti tvaru $(\lambda^0, \lambda^1, \lambda^2, \ldots)$, ptáme se, pro jaká λ je taková posloupnost ve V. Z toho vyjdou 2 vlastní čísla $\lambda_{1,2} = (1 \pm \sqrt{5})/2$.

136. Pozorování: Buď $f\colon V \to V$ lineární. Báze, vzhledem k níž má f diagonální matici, existuje, právě když existuje báze složená z vlastních vektorů. Příslušná diagonální matice má na diagonále právě vlastní čísla f.

137. Tvrzení: Jsou-li $\lambda_1, \ldots, \lambda_k$ *navzájem různá* vlastní čísla zobrazení f (či matice A), a $\mathbf{v}_i$ je nějaký vlastní vektor příslušný λ_i, potom $\mathbf{v}_1, \ldots, \mathbf{v}_k$ jsou lineárně nezávislé. Důkaz indukcí podle k.

138. Důsledek: Je-li A matice typu $n \times n$ a má-li n navzájem různých vlastních čísel, pak je diagonalizovatelná. (Obrácená implikace neplatí!)

139. To je jednoduchá postačující podmínka pro diagonalizovatelnost. Jiná, kterou dokážeme časem, praví, že každá *symetrická* čtvercová matice je diagonalizovatelná.

140. Nyní vyjádříme vlastní čísla matice jako kořeny mnohočlenu. Všimneme si, že pro pevné λ je $A\mathbf{v} = \lambda\mathbf{v}$ homogenní soustavou n rovnic pro n neznámých složek vektoru $\mathbf{v}$. Matice této soustavy je $A - \lambda I_n$, a proto λ je vlastní číslo, právě když je $A - \lambda I_n$ singulární, neboli právě když $\det(A - \lambda I_n) = 0$.

    Charakteristický mnohočlen čtvercové matice A definujeme jako $p_A(t) = \det(A - tI_n)$, kde t je proměnná.

    Podle definice determinantu je to skutečně mnohočlen, a má stupeň přesně n. Vlastní čísla A jsou právě jeho kořeny.

141. Jsou-li A a B podobné matice, pak $p_A(t) = p_B(t)$, a tudíž A a B mají tatáž vlastní čísla. Můžeme tedy mluvit i o charakteristickém mnohočlenu $p_f(t)$ lineárního zobrazení $f\colon V \to V$ na prostoru konečné dimenze.

142. Jak hledat vlastní čísla dané matice, a jak charakteristický mnohočlen:

    - „Ručně“: můžeme počítat $\det(A - tI_n)$ eliminací, s t ovšem musíme zacházet jako s neznámou, takže pracujeme s maticemi, jejichž prvky jsou mnohočleny v proměnné t (a ne jen čísla jako obvykle). Gaussovu eliminaci je třeba pozměnit tak, aby nepoužívala dělení! V jednodušších případech můžeme tak najít $p_A(t)$.

- $p_A(t)$ lze též hledat vhodnými úpravami matice A zachovávajícími podobnost. Matice se převede na tvar, v němž je $p_A(t)$ „vidět". Viz např. učebnice numerické matematiky. Kořeny $p_A(t)$ se hledají obecně numerickými metodami.
- Ve „skutečných" aplikacích, kdy je třeba najít vlastní čísla např. matic 1000×1000, se vlastní čísla zjišťují jinými (hlavně iterativními) postupy, které vůbec nepočítají charakteristický mnohočlen (například tzv. *QR algoritmem*).
- Důležitá poznámka: Stanovení vlastních čísel je výpočetně „dobře zvládnutelná" úloha (existují polynomiální a prakticky rozumně efektivní, i když komplikované, algoritmy), narozdíl od těžkých problémů (jako třeba obarvení grafu a jiných NP-úplných úloh). Vlastní čísla se používají v algoritmech pro přibližné řešení některých takových těžkých úloh.

143. *Důležité koeficienty charakteristického mnohočlenu.* Pišme

$$p_A(t) = (-1)^n t^n + c_{n-1} t^{n-1} + \cdots + c_1 t + c_0.$$

Potom, jak se dá vidět z definice determinantu, $c_0 = \det(A)$ a $c_{n-1} = (-1)^{n-1}.\operatorname{trace}(A)$, kde číslu $\operatorname{trace}(A) = a_{11} + a_{22} + \cdots + a_{nn}$ se říká **stopa** matice A. Tedy determinanty i stopy podobných matic se rovnají (což se dá snadno vidět i jinak), a můžeme mluvit o determinantu či stopě lineárního zobrazení $f \colon V \to V$.

144. *Připomenutí o mnohočlenech.* **Základní věta algebry:** Každý mnohočlen stupně aspoň 1 s reálnými či komplexními koeficienty má aspoň jeden komplexní kořen (poměrně těžké, zde bez důkazu). Má-li $p(x)$ kořen α, pak $p(x) = (x - \alpha)q(x)$ pro nějaký mnohočlen $q(x)$ (tohle je pravda nad každým tělesem a je to snadné). Důsledek (indukcí): Mnohočlen $p(x)$ stupně n s reálnými či komplexními koeficienty lze napsat ve tvaru $p(x) = a_n(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, kde $\alpha_1, \ldots, \alpha_n$ jsou komplexní čísla. Jiný způsob zápisu: $p(x) = a_n(x-\beta_1)^{r_1}(x-\beta_2)^{r_2}\cdots(x-\beta_k)^{r_k}$, kde $\beta_1, \ldots, \beta_k$ jsou navzájem různá komplexní čísla a $r_1 + r_2 + .. + r_k = n$. Zde r_i se nazývá **násobnost** kořene β_i.

145. Poznámka: Je-li číslo λ kořenem mnohočlenu $p_A(t)$ násobnosti r, říkáme, že λ je vlastním číslem matice A **algebraické násobnosti** r (speciálně, není-li λ vůbec vlastní číslo, má algebraickou násobnost 0). Jestliže A lze diagonalizovat, pak algebraická násobnost λ udává, kolikrát se λ opakuje na diagonále v diagonálním tvaru.

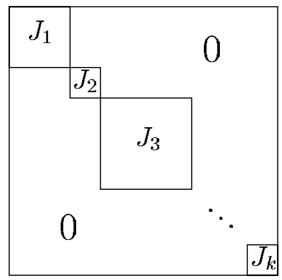
146. Nad komplexními čísly můžeme charakteristický mnohočlen rozložit na součin lineárních činitelů:

$$p_A(t) = (-1)^n (t - \lambda_1)(t - \lambda_2) \cdots (t - \lambda_n).$$

Potom máme $\det(A) = \lambda_1 \lambda_2 \cdots \lambda_n$ a $\operatorname{trace}(A) = \lambda_1 + \lambda_2 + \cdots + \lambda_n$ (každé vlastní číslo bereme s jeho algebraickou násobností). Pro diagonální (či diagonalizovatelné) matice je to vidět přímo.

147. Matice, které nelze diagonalizovat: nemají bázi z vlastních vektorů, musí mít nutně nějaké násobné vlastní číslo λ a dimenze řešení soustavy $(A - \lambda I_n)\mathbf{x} = 0$ je menší než algebraická násobnost λ.

148. Věta (**Jordanův normální tvar**): Buď A komplexní matice typu $n \times n$. Pak existuje matice J podobná A, tzv. Jordanův normální tvar A, následujícího tvaru:



kde $J_1, J_2, \ldots, J_k$ jsou tzv. **Jordanovy buňky**, J_i je typu $n_i \times n_i$ $(n_1 + n_2 + \cdots + n_k = n)$ a vypadá takhle:

$$J_i = \begin{pmatrix} \lambda_i & 1 & 0 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_i & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \lambda_i & 1 & 0 & \ldots & 0 \\ & & & \vdots & & & \\ 0 & 0 & 0 & 0 & \ldots & \lambda_i & 1 \\ 0 & 0 & 0 & 0 & \ldots & 0 & \lambda_i \end{pmatrix}.$$

Ta λ_i nemusí být navzájem různá; celkově se na diagonále matice J objeví každé vlastní číslo matice A tolikrát, kolik je jeho algebraická násobnost. Speciálně, pro diagonalizovatelnou matici A jsou všechna $n_i = 1$. Dále, J je určena jednoznačně až na přerovnání těch J_i, takže soubor $(\lambda_1, n_1), \ldots, (\lambda_k, n_k)$ jednoznačně reprezentuje třídu ekvivalence podobných matic. (Počet opakování čísla λ mezi $\lambda_1, \ldots, \lambda_k$ je jeho *geometrická násobnost*.) Zdůrazněme, že podobnost matic se zde bere nad tělesem komplexních čísel, i kdyby všechny prvky výchozí matice A byly reálné. Větu nebudeme dokazovat (důkaz pracný).

149. Jordanovy buňky velikosti větší než 1×1 jsou to, co „zabraňuje diagonalizaci“. Z jistého hlediska jsou „vzácné“, např. pro náhodně generovanou matici A se vyskytnou s malou pravděpodobností, ale je řada přirozených příkladů. Třeba: V vektorový prostor mnohočlenů stupně nejvýš 3, $D: V \to V$ zobrazení derivace. Matice je podobná Jordanově buňce 4×4 s vlastním číslem 0 na diagonále.

150. Definice: Buď V reálný vektorový prostor se skalárním součinem. Lineární zobrazení $f: V \to V$ se nazývá **ortogonální**, pokud zachovává skalární součin, tj. pokud $\langle f(\mathbf{u}) \,|\, f(\mathbf{v}) \rangle = \langle \mathbf{u} \,|\, \mathbf{v} \rangle$ pro každé $\mathbf{u}, \mathbf{v} \in V$.

151. Tvrzení (ortogonální zobrazení a ortogonální matice): Lineární zobrazení $f\colon V \to V$, kde V je konečnědimenzionální reálný vektorový prostor se skalárním součinem, je ortogonální, právě když jeho matice vzhledem k nějaké ortonormální bázi je ortogonální (tj. $AA^T = I_n$). V důkazu se použije lemátko: Jsou-li A a B matice typu $n\times n$ a platí-li $\mathbf{x}^T A\mathbf{y} = \mathbf{x}^T B\mathbf{y}$ pro každé dva vektory $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, pak $A = B$.

152. Poznámka: Analogické pojmy a výsledky existují i pro komplexní případ, mluví se o *unitárních* zobrazeních a maticích.

153. Poznámka fyzikálně mechanická: Ortogonální zobrazení zjevně zachovává též délky, $\|f(\mathbf{v})\| = \|\mathbf{v}\|$, a pro případ prostoru $\mathbb{R}^n$ se standardním skalárním součinem je to tedy **isometrie** fixující počátek souřadnic. Dá se dokonce ukázat, a není to příliš těžké, že každá isometrie $f\colon \mathbb{R}^n \to \mathbb{R}^n$ (tj. zobrazení splňující $\|f(\mathbf{u}) - f(\mathbf{v})\| = \|\mathbf{u} - \mathbf{v}\|$ pro každé $\mathbf{u}, \mathbf{v} \in \mathbb{R}^n$), pro niž $f(\mathbf{0}) = \mathbf{0}$, musí být lineární, a tedy je to ortogonální zobrazení. Proto se pohyb tuhých těles například v $\mathbb{R}^3$ popisuje pomocí ortogonálních matic.

154. Teď s pomocí ortogonálních matic ukážeme dříve slíbené tvrzení, že symetrické matice jsou diagonalizovatelné, a ještě trochu víc. Věta: Každá symetrická reálná matice A typu $n\times n$ má všechna vlastní čísla reálná, a existuje (reálná) ortogonální matice T taková, že TAT^{-1} je diagonální.

155. Hlavní kroky důkazu:

- Každé vlastní číslo je reálné: počítat dvěma způsoby $\overline{\mathbf{v}}^T A\mathbf{v}$, kde $\mathbf{v}$ je nějaký (možná komplexní) vlastní vektor.
- Zbytek indukcí podle n, v indukčním kroku vzít nějaký jednotkový vlastní vektor $\mathbf{v}$ jako první sloupec, doplnit na ortogonální matici S a uvážit, jak vypadá $SAS^{-1} = SAS^T$.

12 Pozitivně definitní matice

156. *Symetrická* reálná matice A typu $n\times n$ se nazývá

- **pozitivně definitní**, pokud pro všechna nenulová $\mathbf{x} \in \mathbb{R}^n$ platí $\mathbf{x}^T A\mathbf{x} > 0$, a
- **pozitivně semidefinitní**, pokud pro všechna $\mathbf{x} \in \mathbb{R}^n$ platí $\mathbf{x}^T A\mathbf{x} \geq 0$.

Pozitivně definitní matice jsou jistá analogie kladných čísel (asi nejlepší analogie, jaká se dá pro matice definovat).

157. Tvrzení: Pro čtvercovou reálnou symetrickou matici A je ekvivalentní:

(i) A je pozitivně semidefinitní.

(ii) Všechna vlastní čísla A jsou nezáporná.

(iii) Existuje matice U taková, že $U^T U = A$.

Analogie pro pozitivně definitní: vlastní čísla ostře kladná, matice U má hodnost n.

158. Poznámky: Ekvivalence (i)$\Leftrightarrow$(iii) intuitivně říká, že matice je pozitivně semidefinitní, právě když má „odmocninu“. Matice U v (iii) se dá dokonce vzít horní trojúhelníková, pak dostaneme tzv. *Choleského rozklad* matice A (tento pojem se používá většinou pro pozitivně definitní matice).

159. Poznámka (další ekvivalentní podmínka pro pozitivní semidefinitnost – Jacobiho, bez důkazu): Pro $k = 1, 2, \ldots, n$ platí $\det(A_k) \geq 0$, kde A_k značí matici vzniklou z A vymazáním posledních $n-k$ řádků a $n-k$ sloupců.

160. Pozitivní definitnost v analýze: vystupuje v kritériu pro lokální extrém funkce více proměnných.

161. Souvislost s prostory se skalárním součinem: Je-li A pozitivně definitní matice typu $n \times n$, pak předpis $\langle \mathbf{x} \,|\, \mathbf{y} \rangle = \mathbf{x}^T A \mathbf{y}$ definuje skalární součin na $\mathbb{R}^n$ (a dokonce všechny možné skalární součiny na $\mathbb{R}^n$ mají tento tvar).

162. Důležitá metoda v optimalizaci a jiných algoritmech: **semidefinitní programování** = hledání maxima lineární funkce přes množinu všech pozitivně semidefinitních matic, jejichž prvky splňují dané lineární rovnice a nerovnosti. Je znám efektivní algoritmus.

163. Geometrický příklad (konstrukce z tyčí v euklidovském prostoru): M je daná symetrická reálná matice typu $(n+1)\times(n+1)$ (jejíž řádky i sloupce jsou výjimečně, pro pohodlné značení, indexovány od 0). Kdy existují body $\mathbf{x}_0, \mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbb{R}^d$ tak, že $\|\mathbf{x}_i - \mathbf{x}_j\| = m_{ij}$, pro všechna i, j? Odpověď: Definujme pomocnou $n\times n$ matici G, $g_{ij} = \frac{1}{2}(m_{0i}^2 + m_{j0}^2 - m_{ij}^2)$. Pokud ta $\mathbf{x}_i$ existují a $\mathbf{x}_0 = \mathbf{0}$, pak $g_{ij} = \langle \mathbf{x}_i \,|\, \mathbf{x}_j \rangle$. Existují, právě když $G = U^T U$ pro nějakou $d\times n$ matici U. Speciálně, pro $d = n$, ta $\mathbf{x}_i$ existují, právě když G je pozitivně semidefinitní.

13 Kvadratické formy

164. **Kvadratická forma** na $\mathbb{R}^n$ je každá funkce $f\colon \mathbb{R}^n \to \mathbb{R}$ tvaru

$$f(x_1, x_2, \ldots, x_n) = \sum_{i=1}^{n} \sum_{j=i}^{n} a_{ij} x_i x_j$$

(pozor, druhá suma je od i, ne od 1!) pro nějaká čísla $a_{ij} \in \mathbb{R}$. Je to tedy kvadratický mnohočlen, kde každý jednočlen má stupeň 2. Dá se psát v maticovém tvaru $f(\mathbf{x}) = \mathbf{x}^T B \mathbf{x}$, kde B je symetrická **matice kvadratické formy** daná předpisem

$$b_{ij} = \begin{cases} a_{ii} & \text{pro } i = j \\ a_{ij}/2 & \text{pro } i < j \\ a_{ji}/2 & \text{pro } i > j. \end{cases}$$

165. Poznámka: Kvadratická forma f je **pozitivně definitní**, pokud $f(\mathbf{x}) > 0$ pro všechna $\mathbf{x} \in \mathbb{R}^n \setminus \{\mathbf{0}\}$, to je jako pro matice. Podobně pozitivně semidefinitní.

166. Obecněji, pro vektorový prostor V nad tělesem $\mathbb{K}$ definujeme:

   - **Bilineární formu** jako každé zobrazení $b: V \times V \to \mathbb{K}$ takové, že $b(a_1\mathbf{u}_1 + a_2\mathbf{u}_2, \mathbf{v}) = a_1 b(\mathbf{u}_1, \mathbf{v}) + a_2 b(\mathbf{u}_2, \mathbf{v})$ (tj. b je lineární v první složce) a $b(\mathbf{u}, a_1\mathbf{v}_1 + a_2\mathbf{v}_2) = a_1 b(\mathbf{u}, \mathbf{v}_1) + a_2 b(\mathbf{u}, \mathbf{v}_2)$ (b je lineární ve druhé složce).
   - **Kvadratickou formu** jako každé zobrazení $f: V \to \mathbb{K}$ dané předpisem $f(\mathbf{v}) = b(\mathbf{v}, \mathbf{v})$ pro nějakou bilineární formu b.

   Potom pro danou bázi $(\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ prostoru V definujeme **matici $\boldsymbol{B}$ kvadratické formy** f předpisem $b_{ij} = \frac{1}{2}(f(\mathbf{v}_i + \mathbf{v}_j) - f(\mathbf{v}_i) - f(\mathbf{v}_j))$. Pro $\mathbb{R}^n$ a standardní bázi to souhlasí s předchozí definicí.

167. Co když se změní báze? Buď $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ stará báze, $(\mathbf{v}'_1, \ldots, \mathbf{v}'_n)$ nová báze a T matice přechodu (tj. $\mathbf{v}_j = t_{1j}\mathbf{v}'_1 + t_{2j}\mathbf{v}'_2 + \cdots + t_{nj}\mathbf{v}'_n$). Pak vyjde $B' = S^T B S$, kde $S = T^{-1}$ je matice přechodu obráceně, B je matice kvadratické formy vzhledem ke staré bázi a B' její matice vzhledem k nové bázi. (Pozor, pro lineární zobrazení $V \to V$ to bylo $A' = TAT^{-1}$, tady je to jinak!)

168. Změnou báze chceme přivést matici kvadratické formy na „pěkný“ tvar, podobně jako jsme to dělali pro endomorfismy. Vyjde to mnohem jednodušeji:

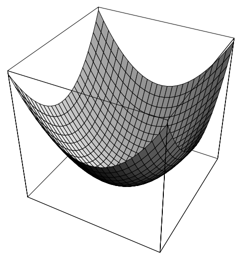
   Věta **(Sylvesterův zákon setrvačnosti kvadratických forem)**: Pro každou kvadratickou formu f na konečnědimenzionálním reálném vektorovém prostoru existuje báze, vzhledem k níž má f diagonální matici, která má na diagonále pouze jedničky, minus jedničky a nuly. Navíc počet jedniček a počet minus jedniček vyjdou stejně pro každou takovou bázi (odtud „setrvačnost“).

169. Víceméně totéž v řeči matic: Pro každou symetrickou reálnou matici B existuje regulární matice S (jejíž sloupce jsou navíc navzájem ortogonální), pro niž je matice $S^T B S$ diagonální a na diagonále má pouze $+1$, -1 a 0. Přitom počet těch $+1$ a -1 nezávisí na volbě takové S.

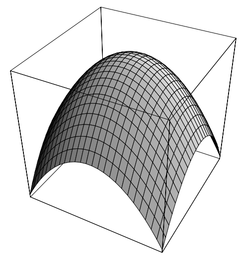
170. Snadná část důkazu je existence S: Z části o vlastních číslech víme, že existuje ortonormální T taková, že $D = T^T B T$ je diagonální a má na diagonále vlastní čísla B (protože B je reálná symetrická). Zbývá rozložit $D = U^T D_0 U$, kde U je diagonální s odmocninami absolutních hodnot vlastních čísel na diagonále a D_0 je diagonální jako ve větě. Setrvačnost je pracnější.

171. Poznámka: Pro pozitivně definitní formy se dostanou na diagonále pouze jedničky, pro pozitivně semidefinitní jen jedničky a nuly.

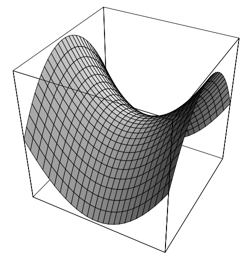
172. Pro $n = 2$ věta říká, že každá kvadratická forma $f\colon \mathbb{R}^2 \to \mathbb{R}$ se dá lineární transformací roviny převést na právě jeden z následujících typů (na obrázcích jsou jejich grafy):



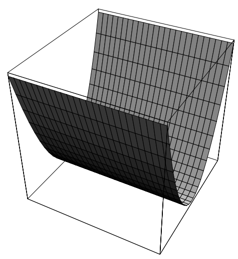
$x_1^2 + x_2^2$



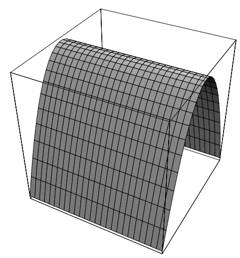
$-x_1^2 - x_2^2$



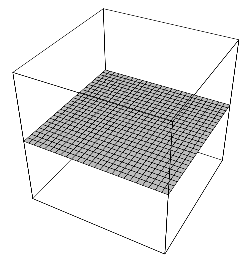
$x_1^2 - x_2^2$



x_1^2



$-x_1^2$



0