Podrobný minimální sylabus

přednášek Lineární algebra I a II pro informatiky

Jiří Matoušek
ve spolupráci
s Jiřím Rohnem a Jiřím Tůmou

Verze 20. IX. 2010

Předmluva

Lineární algebra je jedním ze základních kamenů pro jakékoli vážně míněné studium matematiky, informatiky, fyziky i inženýrských oborů.

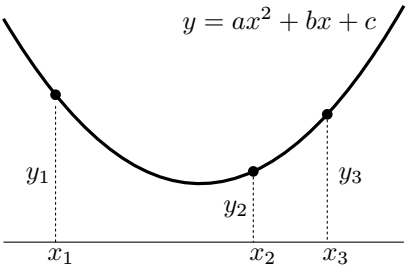
Kromě konkrétních poznatků byste se měli také přiučit logickému uvažování a vyjadřování obvyklému v matematice. Lineární algebra je nejspíš první axiomaticky budovaná teorie, s níž se setkáváte. Její základní objekt studia, tzv. vektorový prostor, je definován několika vlastnostmi (axiomy), z nichž se 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 můžete 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 spisek je na studium lineární algebry příliš stručný a nejsou v něm skoro žádné důkazy. Určitě sám o sobě **nestačí na přípravu ke zkoušce!** Může být ale užitečný pro zopakování látky a kontrolu, že jste nic důležitého nepřeskočili.

1 Soustavy lineárních rovnic

1. Příklad: proložení grafu kvadratické funkce (tvaru $y = ax^2+bx+c$) danými třemi body vede na soustavu 3 lineárních rovnic o 3 neznámých.

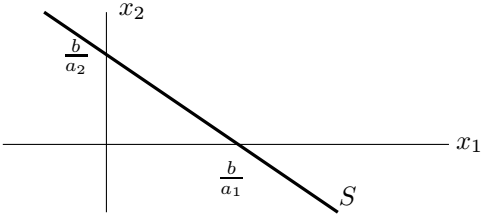


2. Rovnice $a_1x_1 + a_2x_2 = b$ (1 rovnice, 2 neznámé): množina řešení

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

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.)

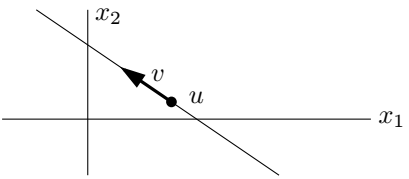
3. Geometricky odpovídá množina řešení přímce v rovině (pokud a_1 a a_2 nejsou obě rovna 0!):



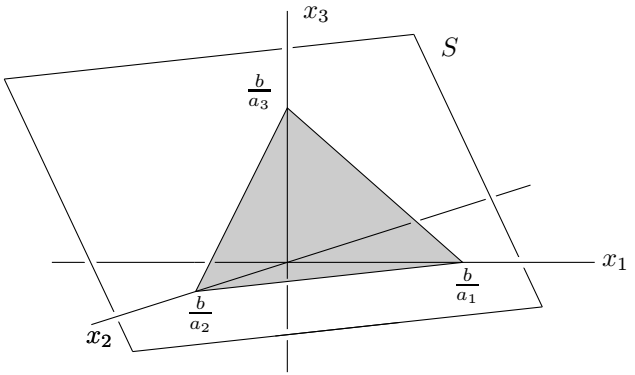
Jiný způsob vyjádření téže množiny (parametrický zápis):

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

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

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

(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, $i \neq j$.

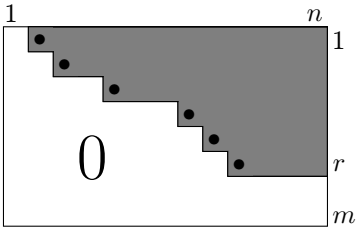
   Pomocí operací (a) a (b) lze simulovat i operace

   (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 $(A|\mathbf{b})$, t.j. matice A, k níž je zprava připsán sloupec $\mathbf{b}$. Tvrzení: elementární řádkové úpravy rozšířené matice nemění množinu řešení soustavy.

8. **Odstupňovaný tvar matice** A: 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 A 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 žádné řešení, jinak se všechna řešení dostanou tak, že neznámé x_j ve sloupcích neobsahujících pivot (těch je $n - r$) se 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 (2×2), geometrická interpretace (skoro rovnoběžné přímky).

3 Operace s maticemi, speciální typy matic

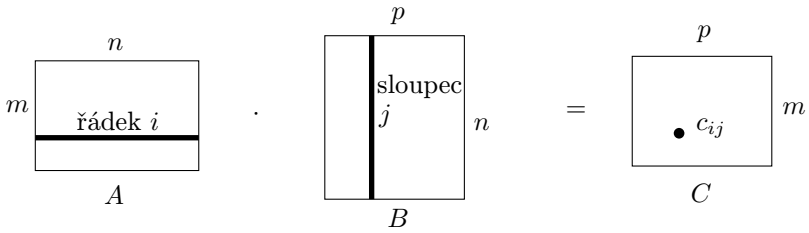
12. Součet matic (stejného typu!) po složkách, násobení reálným číslem po složkách.

13. **Transponovaná matice** A^T: prvek a_{ij} přijde na pozici (j, i). **Symetrická matice:** čtvercová (tj. $n \times n$), $A^T = A$.

14. **Jednotková matice** I_n (čtvercová, jedničky v pozicích (i, i), $i = 1, 2, \ldots$, nuly všude jinde).

15. Matice A je **diagonální**, pokud má nenulové prvky pouze na hlavní diagonále, tj. $a_{ij} = 0$ pro všechna $i \neq j$.

16. **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 $m \times n$.

17. 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.)

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

19. Násobení matic je asociativní.

20. 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}.

21. Které matice mají inverzní matici? V odpovědi se potřebuje následující pojem: Čtvercová matice A se nazývá **regulární**, pokud soustava $A\mathbf{x} = \mathbf{0}$ má jediné řešení (tj. $\mathbf{x} = \mathbf{0}$).

22. 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.

23. V důkazu i na jiné věci se hodí tvrzení: Matice je regulární $\Leftrightarrow$ v (nějakém) odstupňovaném tvaru platí $r = n \Leftrightarrow$ soustava $A\mathbf{x} = \mathbf{b}$ má právě jedno řešení pro každé $\mathbf{b}$.

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

25. 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.

26. Elementární řádkové úpravy matice odpovídají jejímu násobení zleva vhodnými čtvercovými regulárními maticemi. Součin regulárních matic je regulární, takže posloupnost elementárních řádkových úprav matice odpovídá jejímu násobení zleva vhodnou regulární maticí.

4 Grupy a permutace

27. Teď odbočíme od hlavního tématu lineární algebry a probereme dvě důležité matematické struktury – grupy a tělesa. Poprvé zde narazíme na *abstraktní přístup* v matematice, kde se objekty definují pomocí axiomů („pravidel hry“).

28. 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.

29. Na binární operace se můžeme dívat jako na zobecnění „čtyř základních početních úkonů“ – sčítání, odčítání, násobení, dělení. Sčítání, odčítání a násobení jsou vskutku příklady binárních operací na množině $\mathbb{R}$ všech reálných čísel. (Ale zajímavých příkladů binárních operací je mnohem více, a zdaleka se nemusejí týkat jen čísel.)

30. *Pozor*, dělení není binární operace na na množině $\mathbb{R}$ (ale je to binární operace na množině $\mathbb{R}\setminus\{0\}$). Odčítání není binární operace na množině všech přirozených čísel.

31. Binární operace se zpravidla označují symboly $\circ$, $*$, $+$ a podobně. Zapisujeme je podobně jako základní početní úkony, tj. $a \circ b$ znamená výsledek binární operace $\circ$ provedené na a a b.

32. Dvě důležité vlastnosti:

> Binární operace $\circ$ na množině X se nazývá **komutativní**, pokud platí $a \circ b = b \circ a$ pro všechna $a, b \in X$, a nazývá se **asociativní**, pokud $a \circ (b \circ c) = (a \circ b) \circ c$ pro všechna $a, b, c \in X$.

33. Příklady: Sčítání $+$ na $\mathbb{R}$ je jak asociativní, tak komutativní. Odčítání $-$ na $\mathbb{R}$ není ani asociativní, ani komutativní (ověřit!).

34. Jedním z nejdůležitějších objektů v celé matematice je **grupa**. Je definována **axiomy**, tj. vlastnostmi, které musí splňovat.

> **Grupa** je dvojice $(G, \circ)$ kde G je množina a $\circ$ je binární operace na G, splňující následující axiomy:
>
> (A) Operace $\circ$ je asociativní.
>
> (E) Existuje prvek $e \in G$ takový, že $a \circ e = e \circ a = e$ pro všechna $a \in G$. (Takové e se nazývá **jednotkový prvek** uvažované grupy, někdy též **neutrální prvek**.)
>
> (I) Pro každé $a \in G$ existuje $b \in G$ takové, že $a \circ b = b \circ a = e$, kde e je jednotkový prvek. (Takové b se označuje zápisem a^{-1} a nazývá se **inverzní prvek** k prvku a.)

35. Poznámky:

- *Pozor*, definice grupy zahrnuje též požadavek, že kdykoli $a, b \in G$, pak také $a \circ b \in G$ (ten je obsažn v definici binární operace).

- Místo „grupa $(G, \circ)$“ se často říká jen „grupa G“, pokud je jasné, jaká operace se myslí.
- Místo $a \circ b$ se často píše jen ab (podobně jako u násobení), opět pokud je operace zřejmá z kontextu.

36. Z axiomů se dá odvodit řada dalších vlastností grupy. Příklady větiček: V každé grupě existuje právě jeden jednotkový prvek. Pro každý prvek a v libovolné grupě existuje právě jeden inverzní prvek. V grupě je možné „krátit“, tj. z $a \circ c = b \circ c$ plyne $a = b$.

37. *Všechny* vlastnosti grup je nutné odvodit z axiomů. Například to, že něco platí pro jednu určitou grupu, nebo i pro spoustu různých grup, vůbec neznamená, že by to muselo platit pro všechny grupy.

38. I když axiomy grupy vypadají jednoduše, je svět grup velice složitý a i po více než stu letech zkoumání skrývá před matematiky spoustu tajemství. Koncem minulého století se podařilo dokázat takzvanou „obří větu“ o grupách (která, zhruba řečeno, popisuje všechny možné konečné „stavební kameny“ grup). Její důkaz má několik *tisíc* stran a jedna z konkrétních grup, které se v obří větě objevují, takzvané *monstrum*, má přibližně 8×10^{53} prvků. (Nelekejte se, lineární algebra je snazší než teorie grup, a o grupách probereme jen věci velmi jednoduché.)

39. K čemu jsou grupy? V matematice se objevují v důkazu neřešitelnosti rovnic pátého stupně algebraickými operacemi, v teorii čísel, v kombinatorickém počítání a v řadě jiných odvětví. Ve fyzikálních teoriích hrají většinou klíčovou roli předpoklady určitých symetrií přírodních zákonů, a tyto symetrie jsou popsány vhodnými grupami. S grupami se pracuje i v krystalografii, kryptografii, analýze obrazu a v dalších oborech. Některá použití uvidíme i v lineární algebře.

40. Ještě jeden pojem: **Podgrupa** grupy $(G, \circ)$ je podmnožina $H \subseteq G$ taková, že $e \in H$ (kde e je jednotkový prvek G), $a^{-1} \in H$ pro každé $a \in H$, a $a \circ b \in H$ pro každé $a, b \in H$. Tj. H tvoří grupu vzhledem k operaci „zděděné“ z G.

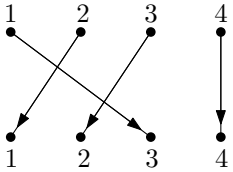
41. Příklady grup (a podgrup):

    - $(\mathbb{R}, +)$; $(\mathbb{Z}, +)$ (kde $\mathbb{Z}$ značí množinu všech celých čísel); množina všech kladných racionálních čísel s násobením; množina $\{-1, 1\}$ s násobením. Ve všech těchto případech je operace komutativní a mluvíme o **komutativních**, neboli **abelovských**, grupách.

- $(\mathbb{Z}, +)$ je podgrupou $(\mathbb{R}, +)$; $(\mathbb{N}, +)$ *není* podgrupou $(\mathbb{Z}, +)$ (protože to není grupa).
- Pro každé n tvoří množina všech *regulárních* matic typu $n \times n$ s operací násobení grupu. Pro $n \geq 2$ tato grupa *není* komutativní. (Naopak množina vůbec všech matic typu $n \times n$ grupu netvoří.)
- Množina všech otočení kolem počátku v třírozměrném prostoru s operací skládání tvoří grupu, která také není komutativní (otočíme-li třeba hrnek kolem osy x o $90°$ a pak kolem osy z také o $90°$, není to totéž, jako otočení o $90°$ kolem osy z následované otočením o $90°$ kolem osy x – vyzkoušejte).

42. Dalším bohatým zdrojem příkladů jsou permutace. Připomeňme: **Permutace** množiny X je vzájemně jednoznačné zobrazení (bijekce) $X \to X$. Označíme S_n = množina všech permutací množiny $\{1, 2, \ldots, n\}$.

43. Pro permutace se používá dvouřádkový zápis, např. $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$, nebo obrázek se šipkami (bipartitní graf):



44. Permutace skládáme jako zobrazení; pro $p, q \in S_n$ je složení $p \circ q$ definováno předpisem $p \circ q(i) = p(q(i))$, $i = 1, 2, \ldots, n$. Množina S_n s operací $\circ$ tvoří grupu, zvanou **symetrická grupa**.

45. Pro $n \geq 3$ je grupa S_n nekomutativní.

46. Podgrupy symetrických grup se nazývají **permutační grupy**.

47. Časem budeme potřebovat *znaménko permutace*. Definujeme napřed množinu **inverzí** permutace p:

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

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

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

49. **Transpozice** je permutace zaměňující dva prvky. Tvrzení: Transpozice má znaménko -1. Každá permutace je složením transpozic.

50. V jazyce teorie grup bychom posledně zmíněné tvrzení formulovali takto: Množina $T \subseteq S_n$ všech transpozic generuje grupu S_n. Obecná definice: Buď G grupa a $M \subseteq G$ libovolná podmnožina G. Řekneme, že M **generuje** grupu G (nebo že M je *množina generátorů* G), pokud jediná podgrupa G obsahující M je samotná G.

51. Ekvivalentně, každé $a \in G$ lze vyjádřit z konečně mnoha prvků z M pomocí grupové operace a operace inverze. (Jemnůstka: $M = \emptyset$ generuje grupu $\{e\}$ tvořenou jen z jednotkovým prvkem.)

52. Některé populární hlavolamy jsou vlastně permutační grupy v přestrojení. *Hra v patnáct* je krabička se 4×4 políčky, v níž jsou kostičky číslované 1 až 15 a jedno volné políčko, pomocí něhož lze kostičky přesouvat (vodorovně nebo svisle).

Kolem roku 1880 se statisíce lidí snažily vyřešit hlavolam, přerovnat pozici na obrázku do pozice lišící se pouze prohozením čísel 14 a 15. To nemá řešení, jak se dá ukázat pomocí znaménka permutace.

53. Modernější grupový hlavolam je známá *Rubikova kostka*. Tam chceme vyjádřit daný prvek jisté permutační grupy (zamíchanou polohu kostky) pomocí generátorů (otočení jednotlivých stěn). (Nedávno se podařilo rozsáhlými výpočty ukázat, že každou pozici lze vyřešit nejvýš 20 tahy, a pro jisté pozice je 20 tahů nutných.)

5 Tělesa (v algebře)

54. S racionálními, reálnými, komplexními čísly můžeme dělat „čtyři základní početní úkony“; máme operace sčítání a násobení a odvozené (inverzní) operace odčítání a dělení.

55. Těleso je algebraická struktura, v níž jsou definovány operace s podobnými vlastnostmi (a s jejímiž prvky tudíž můžeme „počítat“ podobně jako s reálnými čísly). Opět ho definujeme axiomy.

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

(SG) Množina $\mathbb{K}$ s operací $+$ tvoří *komutativní grupu*. Jednotkový prvek této grupy značíme 0 a prvek inverzní k a značíme $-a$.

(NG) Množina $\mathbb{K} \setminus \{0\}$ s operací $\cdot$ tvoří *komutativní grupu*. Jednotkový prvek této grupy značíme 1 a prvek inverzní k a značíme 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) $0 \neq 1$.

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, pro něž násobení nemusí být komutativní (sčítání ano). Zde budeme tělesem rozumět jen komutativní těleso.

56. 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!!!).

57. 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.

58. Značení $\mathbb{Z}_n$ (zbytkové třídy modulo n, reprezentované čísly $0, 1, \ldots, n-1$, s operacemi sčítání a násobení modulo n). $\mathbb{Z}_3$ je těleso, $\mathbb{Z}_4$ NENÍ!!!

59. 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 je 0 v $\mathbb{Z}_n$. 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 (prostost).

60. Označení: GF(q) konečné těleso s q prvky (Galois Field). Existuje, právě když q je mocnina prvočísla, a pak existuje právě jedno (bez

důkazu). Konečná tělesa jsou velmi významná pro informatiku (např. pro kódy, třeba na CD nebo DVD).

61. **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.

6 Vektorové prostory

62. 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.

63. 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.

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:

(SG) Množina V s operací $+$ tvoří *komutativní grupu*. Její neutrální prvek značíme $\mathbf{0}$, a vektor inverzní k vektoru $\mathbf{v}$ značíme $-\mathbf{v}$. [Pozor, máme teď dvě (různé) 0 — jednu v $\mathbb{K}$ a jednu (tučnou) ve V!!!]

(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 $\mathbf{v} \in V$ (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 $\mathbf{u}, \mathbf{v} \in V$.

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

64. 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 $\mathrm{GF}(2)$ (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 $\mathbb{Q}$ (rac. čísly).

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

66. **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 $\mathbf{v} \in W$.

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

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

69. 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 systému vektorů. Tvrzení (explicitní popis podprostoru generovaného X): $\operatorname{span}(X)$ je množina všech lineárních kombinací vektorů z X.

70. 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: $\operatorname{Ker} A$ (kernel).

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

7 Lineární závislost, báze, dimenze

71. Soubor (konečná posloupnost) vektorů $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ je **lineárně nezávislý**, pokud z rovnosti $a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v} = \mathbf{0}$ 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.)

72. 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“.)

73. 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 $\mathbb{Q}$.

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

75. Definice: Nechť B je soubor vektorů ve vektorovém prostoru V; nazývá se **systém generátorů** V pokud $\mathrm{span}(B) = V$.

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

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

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

78. Věta: *každý vektorový prostor má bázi.* Důkaz vyžaduje axiom výběru. Dokázali jsme (jen) pro prostory, mající nějaký konečný systém generátorů (říká se jim **konečně generované**).

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

80. 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 $\mathbf{w} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \cdots + \cdots a_n\mathbf{v}_n$ 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. vektor $\mathbf{v}_i$ s nenulovým koeficientem lze nahradit $\mathbf{w}$).

81. **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.

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

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

83. Další důsledek Steinitzovy věty: Libovolný lineárně nezávislý systém v konečně generovaném prostoru lze doplnit na bázi.

84. Odtud: Je-li W podprostor konečně generovaného prostoru V, pak

$$\dim(W) \leq \dim(V)$$

(speciálně je W konečně generovaný). Nastane-li rovnost, pak $W = V$.

85. 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 $\mathbb{R}^3$: přibydou roviny procházející $\mathbf{0}$.

86. Pojem: **souřadnice vektoru vzhledem k dané bázi**.

8 Hledání báze, hodnost matice

87. Jak spočítat dimenzi (a najít bázi) prostoru $V = \operatorname{span}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m)$, kde $\mathbf{a}_1$,...,$\mathbf{a}_m$ jsou dané vektory z $\mathbb{K}^n$? Napíšeme $\mathbf{a}_1$,...,$\mathbf{a}_m$ 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 $\operatorname{rank} A$.

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).

88. Věta (jeden z „divů“ lineární algebry): hodnost matice je též rovna dimenzi sloupcového prostoru. Důkaz:

– Pro redukovaný odstupňovaný tvar je vidět.

– Elementární řádkové operace, a obecněji násobení regulární maticí R zleva, nemění *dimenzi* sloupcového prostoru (i když mění sloupcový prostor). To se dostane z tvrzení: Je-li $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ báze sloupcového prostoru A, potom $\{R\mathbf{v}_1, \ldots, R\mathbf{v}_n\}$ generuje sloupcový prostor RA.

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

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

pro každou matici A s n sloupci.

90. Platí $\operatorname{rank}(AB) \leq \min(\operatorname{rank}(A), \operatorname{rank}(B))$ (A, B matice takové, ze součin AB je definován). Protože: řádkový prostor $AB \subseteq$ řádkový prostor B, a sloupcový prostor $AB \subseteq$ sloupcový prostor A.

91. Odtud: $\operatorname{rank}(RA) = \operatorname{rank}(A)$ pro (čtvercovou) regulární R.

9 Lineární zobrazení

92. Zobrazení $f\colon U \to V$, 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 $a \in \mathbb{K}$.

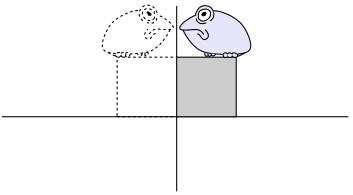
93. Složení lineárních zobrazení je zase lineární zobrazení (pokud je ovšem lze skládat!).

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

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

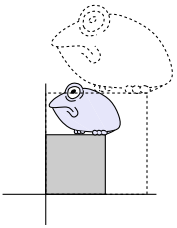
- projekce na osu x,
- projekce na danou přímku procházející $\mathbf{0}$,
- **zrcadlení**, např.:

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



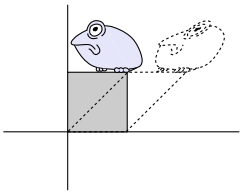
- **zvětšení** (homotetie), např.

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



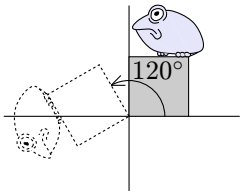
- **zkosení**, např.:

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

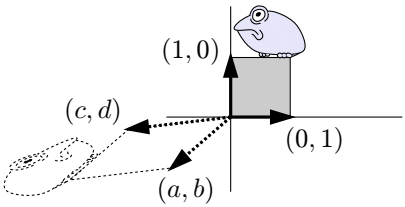


- **rotace** kolem **0**, např.:

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



96. 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).



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

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

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

99. Příklad: Nechť $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ jsou vrcholy pravidelného n-úhelníka se středem v **0**, ukažte $\mathbf{s} = \sum_{i=1}^{n} \mathbf{v}_i = \mathbf{0}$. Elegantní řešení: buď τ otočení kolem **0** o úhel $\frac{2\pi}{n}$, potom $\tau(\mathbf{s}) = \mathbf{s}$, a tedy $\mathbf{s} = \mathbf{0}$.

100. Libovolné lineární zobrazení $f\colon \mathbb{R}^n \to \mathbb{R}^m$ 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.

101. Pojem: **matice (lineárního) zobrazení** $f\colon U \to V$ **vzhledem k daným bázím** prostorů U a V; j-tý sloupec té matice jsou souřadnice obrazu j-tého vektoru z báze prostoru U vzhledem k bázi prostoru V.

102. *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. Důkaz z asociativity násobení matic: Buď $\mathbf{v} \in V_3$, $\mathbf{x}$ vektor jeho souřadnic, pak $g(\mathbf{v})$ má souřadnice $B\mathbf{x}$ a $f(g(\mathbf{x}))$ souřadnice $A(B\mathbf{x}) = (AB)\mathbf{x}$.

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

104. 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 se nazývá **matice přechodu** od B k C. Je-li $\mathbf{x}$ vektor souřadnic nějakého $\mathbf{v} \in V$ vzhledem k bázi B, potom souřadnice $\mathbf{v}$ v bázi C jsou dány vektorem $A\mathbf{x}$, kde A je matice přechodu od B k C.

105. 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.

106. Isomorfismus zobrazuje bázi na bázi, a tudíž zachovává dimenzi.

107. 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 V, isomorfismus přiřazuje vektoru $\mathbf{v} \in V$ jeho souřadnice v té bázi. (Poznámka: mnoho isomorfismů = mnoho „možných pohledů“ na daný vektorový prostor!)

108. 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 3).

109. *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.

110. 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**.

111. 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 $f(\mathbf{x}) = \mathbf{b}$.

112. 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. $\mathrm{Ker}(A)$.

113. 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 $\mathbb{K}^n$.

10 Prostory se skalárním součinem

114. (Standardní) operace **skalárního součinu** na $\mathbb{R}^n$: dvojici vektorů $\mathbf{x}, \mathbf{y}$ přiřazuje číslo $\langle \mathbf{x}|\mathbf{y}\rangle = x_1y_1 + x_2y_2 + \cdots + x_ny_n$.

115. (Euklidovská) délka vektoru $\mathbf{x}$ (též zvaná **norma**):

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

116. Geometrická interpretace: $\langle \mathbf{x}|\mathbf{y}\rangle = \|\mathbf{x}\| \cdot \|\mathbf{y}\| \cdot \cos\varphi$, kde φ je úhel mezi vektory $\mathbf{x}$ a $\mathbf{y}$.

117. V „čistém“ vektorovém prostoru nemáme pojmy jako „délka“ a „úhel“. Přidáním skalárního součinu je tam můžeme elegantně zavést.

118. **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 $\langle \mathbf{v}|\mathbf{u}\rangle = \langle \mathbf{u}|\mathbf{v}\rangle$ v reálném případě).

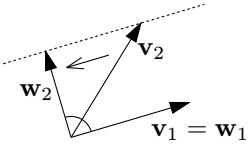
119. Standardní skalární součin v $\mathbb{R}^n$ je nejobvyklejší, ale není to jediná možnost pro skalární součin na $\mathbb{R}^n$. Třeba v rovině můžeme taky definovat $\langle \mathbf{x}\,|\,\mathbf{y}\rangle = x_1y_1 + \frac{1}{3}x_1y_2 + \frac{1}{3}x_2y_1 + x_2y_2$ (to souvisí s pozitivně definitními maticemi, které probereme později).

120. Pojem **normy:** norma na vektorovém prostoru V (nad $\mathbb{R}$ nebo nad $\mathbb{C}$) je zobrazení $V \to \mathbb{R}$, značení $\|\mathbf{v}\|$ a pod.; axiomy: $\|\mathbf{v}\| \geq 0$, rovnost pouze pro $\mathbf{v} = \mathbf{0}$, $\|a\mathbf{v}\| = |a| \cdot \|\mathbf{v}\|$ (a je reálné nebo komplexní číslo), trojúhelníková nerovnost $\|\mathbf{u}\| + \|\mathbf{v}\| \geq \|\mathbf{u}+\mathbf{v}\|$. Norma $\|\mathbf{v}\|$ má význam „délky“ vektoru $\mathbf{v}$. Skalární součin určuje normu $\|\mathbf{v}\| = \sqrt{\langle \mathbf{v}|\mathbf{v}\rangle}$, ale zdaleka ne každá norma pochází ze skalárního součinu. Ze standardního skalárního součinu na $\mathbb{R}^n$ zmíněného výše dostaneme euklidovskou normu ($\|\mathbf{v}\|$ je právě délka vektoru podle Pythagorovy věty) a euklidovskou vzdálenost (vzdálenost bodů $\mathbf{u}$ a $\mathbf{v}$ je $\|\mathbf{u} - \mathbf{v}\|$).

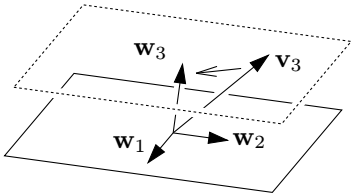
121. **Cauchyho-Schwarzova nerovnost** $\langle \mathbf{u}|\mathbf{v}\rangle \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|$. Důkaz: uvážit kvadratický mnohočlen $p(t) = \langle \mathbf{u} + t\mathbf{v}|\mathbf{u} + t\mathbf{v}\rangle$, ten musí mít nekladný diskriminant. Geometrický význam, souvislost s kosinovou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

122. **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.

123. **Gramova-Schmidtova ortogonalizace:** algoritmus, který z dané báze $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ udělá ortogonální bázi $\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_n$; lineární obal prvních k vektorů zůstává zachován pro všechna k. Geometrická ilustrace:



2. krok (výpočet $\mathbf{w}_2$)



3. krok (výpočet $\mathbf{w}_3$)

Věta: Rozšiřitelnost libovolného ortonormálního systému na ortonormální bázi (v konečnědimenzionálním prostoru!). Poznámka: G.-S. ortogonalizace je numericky nestabilní, ale jsou známy stabilní varianty.

124. **Ortogonální doplněk** množiny M:

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

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

126. 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 $\left(U^\perp\right)^\perp = U$.

(v) Platí $\dim(U^\perp) = \dim(V) - \dim(U)$.

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

127. 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.

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

11 Determinant

129. Každé čtvercové maticí A 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).

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

131. Determinant trojúhelníkové matice je součinem diagonálních prvků.

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

133. 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 $\det(A) = 0$.

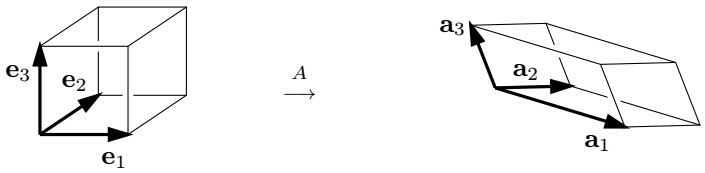
134. Determinant je lineární funkcí každého svého řádku.

135. 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.

136. 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 $\mathbb{R}$.

137. 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.

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

139. Věta (o násobení determinantů): $\det(AB) = \det(A)\det(B)$. Důkaz: pro signulární A snadné, regulární A můžeme pomocí Gaussovy eliminace vyjádřit jako součin elemenátních matic (odpovídajících řádkovým úpravám), a tedy násobení A odpovídá posloupnosti elementárních řádkových úprav matice B.

140. 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.

141. 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).

142. **Cramerovo pravidlo:** Je-li A čtvercová regulární matice, pak (jediné) řešení soustavy $A\mathbf{x} = \mathbf{b}$ má i-tou složku rovnou $\det(A_{i\to\mathbf{b}})/\det(A)$, 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).

12 Vlastní čísla

143. Vlastní čísla souvisejí s mnoha otázkami v geometrii (např. jak vypadají isometrie euklidovského prostoru), ve fyzice (jak zní zvon), v teorii grafů (jak dobrý je daný graf jako schéma telefoního propojení), atd.

144. My se k vlastním číslům teď 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. Takové otázky pro lineární zobrazení se řeší právě pomocí vlastních čísel.

145. Uvažujeme lineární zobrazení $f\colon V \to V$, V konečnědimenzionalní, chceme najít bázi $(\mathbf{v}_1, \ldots, \mathbf{v}_n)$ tak, aby matice f vzhledem k ní byla „jednoduchá“. Zde je podstatné, že máme jen jednu bázi ve V! (Doporučeno k rozmyšlení: Je-li $f\colon V \to V$ lineární zobrazení hodnosti r, pak lze zvolit dvě báze V tak, že matice f vzhledem k nim je matice I_r doplněná dole a zprava nulami.)

146. Připomenutí: **matice přechodu** od báze $B = (\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n)$ k bázi $B' = (\mathbf{v}'_1, \mathbf{v}'_2, \ldots, \mathbf{v}'_n)$ má v j-tém sloupci souřadnice $\mathbf{v}_j$ v bázi B'. Tvrzení: Matice přechodu od B' k B je T^{-1}. Důkaz: přímým výpočtem, nebo pomocí isomorfismů s $\mathbb{K}^n$.

147. Tudíž, je-li A matice zobrazení $f\colon V \to V$ 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.

148. 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.

149. Diagonální tvar je například dobrý 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.

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

151. 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 $f\colon V \to V$ 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 $\mathbf{v}$ splňující $f(\mathbf{v}) = \lambda\mathbf{v}$, tedy i $\mathbf{0}$.

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 $f(W) \subseteq W$.

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

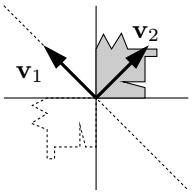
Je-li A čtvercová matice nad tělesem $\mathbb{K}$, potom číslo $\lambda \in \mathbb{K}$ se nazývá **vlastní číslo** matice A, pokud existuje vektor $\mathbf{v} \neq \mathbf{0}$ splňující rovnici

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

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

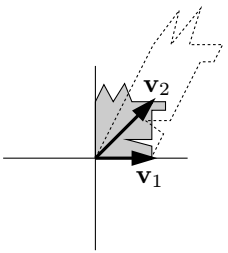
153. Příklady, co se může dít v rovině:

- 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 $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

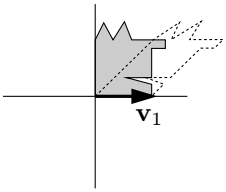
- Matice $\begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$, zkosení a roztažení:



  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.

154. 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 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 $\lambda_{1,2} = (1 \pm \sqrt{5})/2$.

155. 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.

156. 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 příslusný λ_i, potom $\mathbf{v}_1, \ldots, \mathbf{v}_k$ jsou lineárně nezavislé. Důkaz indukcí podle k.

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

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

159. 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 o 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.

160. 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.

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

- „Ručně:“ můžeme počítat $\det(A - tI_n)$ eliminací, s t ovšem musíme záchazet 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 jednoduchých 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). Vlastních čísel se někdy používá v algoritmech pro přibližné řešení některých takových těžkých úloh.

162. *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 $f\colon V \to V$ na prostoru konečné dimenze.

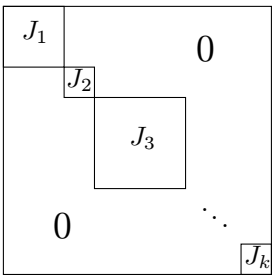
163. *Připomenutí o mnohočlenech.* **Základní věta algebry:** Každý mnohočlen stupně aspoň 1 s reálnými či komplexními koeficienty má aspoň jeden komplexní kořen (poměrně těžké, zde bez důkazu). Má-li $p(x)$ kořen α, pak $p(x) = (x-\alpha)q(x)$ pro nějaký mnohočlen $q(x)$ (tohle je pravda nad každým 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.

164. 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.

165. 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.

166. 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.

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

168. 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, $D\colon V \to V$ zobrazení derivace. Matice je podobná Jordanově buňce 4×4 s vlastním číslem 0 na diagonále.

169. Definice: Buď V reálný vektorový prostor se skalárním součinem. Lineární zobrazení $f\colon V \to V$ 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 $\mathbf{u}, \mathbf{v} \in V$.

170. 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 $A = B$.

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

172. 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 pohyb tuhých těles například v $\mathbb{R}^3$ se popisuje pomocí ortogonálních matic.

173. 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.

174. 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 a doplnit na ortogonální matici S, uvážit, jak vypadá $SAS^{-1} = SAS^T$.

13 Pozitivně definitní matice

175. *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).

176. 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.

177. Poznámky: Ekvivalence (i)⇔(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).

178. Poznámka: Další ekvivalentní podmínka pro pozitivní semidefinitnost:

    (iv) 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.

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

180. 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).

181. 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.

182. Geometrický příklad (konstrukce z tyčí v euklidovském prostoru): M je daná symetrická reálná matice typu $(n+1)\times(n+1)$. 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 $g_{ij} = \langle \mathbf{x}_i \,|\, \mathbf{x}_j \rangle$. Ona 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.

14 Kvadratické formy

183. **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 a

někdy se nazývá **analytické vyjádření kvadratické formy**. Kvadratickou formu lze zapsat i v maticovém tvaru $f(\mathbf{x}) = \mathbf{x}^T B\mathbf{x}$, kde B je symetrická **matice kvadratické formy** daná předpisem

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

184. 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.

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

- **Bilineární formu** jako každé zobrazení $b\colon V \times V \to \mathbb{K}$ 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 $f\colon V \to \mathbb{K}$ 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 konečné dimenze definujeme **matici B kvadratické formy** b předpisem $b_{ij} = \frac{1}{2}(f(\mathbf{v}_i + \mathbf{v}_j) - f(\mathbf{v}_i) - f(\mathbf{v}_j))$.

186. 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 bilineární/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!)

187. Změnou báze bychom chtěli 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“).

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

189. Snadná část důkazu je existence S: Z části o vlastních číslech víme, že existuje ortonormální T taková, že $D = T^T BT$ 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.

190. Poznámka: Pro pozitivně definitní formy se dostanou na diagonále pouze jedničky (a formu lze pak počítat standardním skalárním součinem), pro pozitivně semidefinitní jen jedničky a nuly.

191. 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):