Podrobný minimální sylabus

přednášky Lineární algebra I pro informatiky

Jiří Matoušek
ve spolupráci
s Jiřím Rohnem a Jiřím Tůmou

Verze 3. IX. 2004

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.

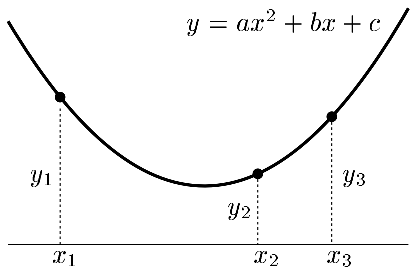
Takto jsou vystavěna i jiná odvětví matematiky, ale lineární algebra je poměrně jednoduchá a rozvíjení matematické teorie se na ní dá zvlášť dobře ilustrovat. Časem můžete ocenit i sílu této teorie: otázky o lineárních rovnicích, které jsou na první pohled zapeklité a bez přípravy těžko řešitelné i pro 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.

Nedávno byla na MFF UK přednáška Lineární algebra pro první ročník rozšířena o téma lineární programování. Tuto část sylabus záměrně nezahrnuje, protože koncepce její výuky zatím není ustálena.

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.

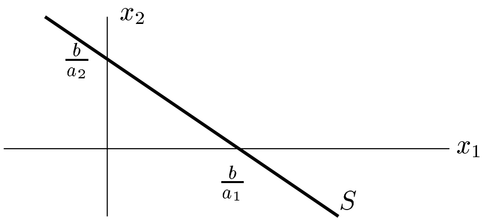


2. Rovnice $a_1x_1 + a_2x_2 = b$ (1 rovnice, 2 neznámé): množina řešení

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

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.)

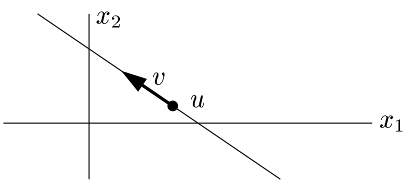
3. Geometricky odpovídá množina řešení přímce v rovině (pokud a_1 a a_2 nejsou obě rovna 0!):



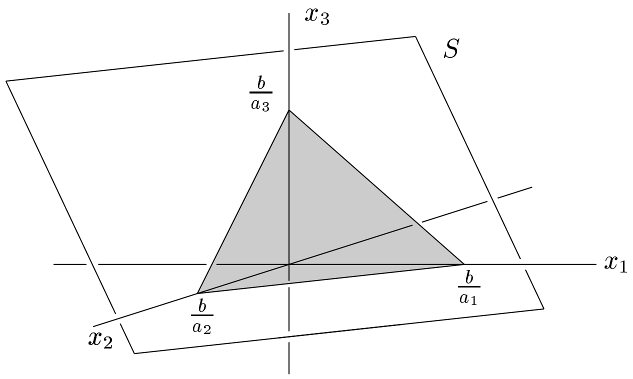
Jiný způsob vyjádření téže množiny (parametrický zápis):

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

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

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

(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.

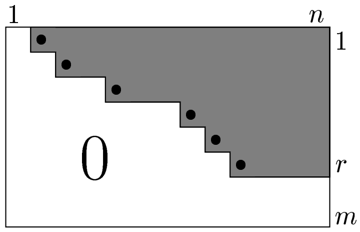
2 Řešení soustav: Gaussova eliminační metoda

6. **Elementární řádkové úpravy matice:**

(a) vynásobení i-tého řádku nenulovým číslem t,
(b) přičtení t-násobku j-tého řádku k i-tému řádku, $i \neq j$,
(c) záměna dvou řádků (toto lze simulovat pomocí operací (a) a (b)).

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, $0 \le r \le m$, 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

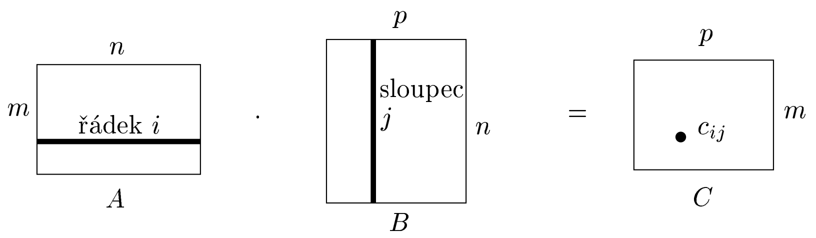
12. Součet matic (stejného typu!) po složkách, násobení reálným číslem po složkách.

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 (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: $AI_n = I_mA = A$, pro libovolnou A typu $m \times n$.

17. Násobení a transpozice: $(AB)^T = B^TA^T$ (přesněji: součin AB je definován, právě když je definován součin B^TA^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 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.

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

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

31. **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 **neutrální** (nulový) prvek 0 vzhledem ke sčítání, pro nějž platí $a + 0 = a$ pro každé $a \in \mathbb{K}$.
(SI)	Pro každé $a \in \mathbb{K}$ existuje **opačný** prvek b, 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 vzhledem k násobení, pro nějž platí $1 \cdot a = a$ 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.

32. 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).

33. 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.

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

35. 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“: $\mathbb{Z}_n \setminus \{0\} \to \mathbb{Z}_n \setminus \{0\}$ surjektivní (na). Trik: ověřit injektivitu (prostost).

36. 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).

37. **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

38. Zatím pro nás vektory byly uspořádané n-tice reálných čísel, tvaru $\mathbf{v} = (v_1, \dots, v_n)$, 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.

39. 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.

40. **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 **neutrální** (nulový) prvek$\mathbf{0} \in V$ vzhledem ke sčítání vektorů, pro nějž platí $\mathbf{v} + \mathbf{0} = \mathbf{v}$ 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 $-\mathbf{v}$, 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 $a\mathbf{v} \in V$.

41. 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 $\mathbb{Q}$ (rac. čísly).

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

43. **Podprostor** vektorového prostoru V je podmnožina $W \subseteq V$, která je vektorovým prostorem vzhledem k $\mathbf{0}$, „+" a „·" 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 $\mathbf{v} \in W$.

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

45. 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 podprostorů W, které X obsahují. Označení: $\mathrm{span}(X)$ (v literatuře též $\langle X \rangle$, $\mathcal{L}(X)$, $[X]$, název též **lineární obal $\boldsymbol{X}$**).

46. 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): $\mathrm{span}(X)$ je množina všech lineárních kombinací vektorů z X.

47. 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

48. 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.)

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 $\mathbb{Q}$.

51. 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 $i = 1, 2, \ldots, n$.

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

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

53. 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 $\mathbb{R}[x]$.

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

55. 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**).

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

57. 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 $\mathbf{w}$).

58. **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.

59. 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.

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

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

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

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

62. 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 $\mathbf{0}$.

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

7 Hledání báze, hodnost matice

64. Jak spočítat dimenzi (a najít bázi) prostoru $V = \mathrm{span}(\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m)$, 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 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).

65. Věta (jeden z „divů" lineární algebry): hodnost matice je též rovna dimenzi sloupcového prostoru. Důkaz: Pro redukovaný odstupňovaný tvar je vidět, a stačí ověřit, že elementární řádkové operace (nebo obecněji násobení regulární maticí zleva) nemění *dimenzi* sloupcového prostoru (i když mění sloupcový prostor).

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

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

pro každou matici A s n sloupci.

67. Platí $\mathrm{rank}(AB) \leq \min(\mathrm{rank}(A), \mathrm{rank}(B))$ (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.

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

8 Lineární zobrazení

69. Zobrazení $f\colon V \to W$, kde V a W 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 $\mathbf{u}, \mathbf{v} \in V$ a $a \in \mathbb{K}$.

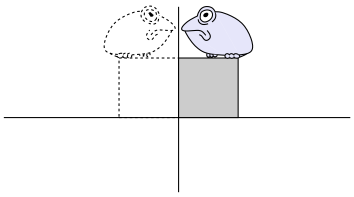
70. Složení lineárních zobrazení je zase lineární zobrazení (pokud je ovšem lze skládat!).

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:

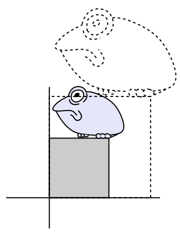
- projekce na osu x,
- projekce na danou přímku procházející $\mathbf{0}$,
- **zrcadlení**, např.:

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

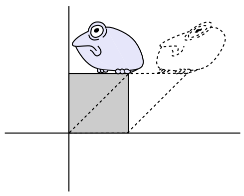
- **zvětšení** (homotetie), např.

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

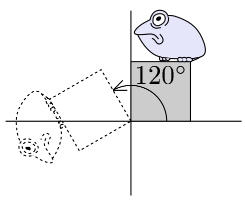
- **zkosení**, např.:

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

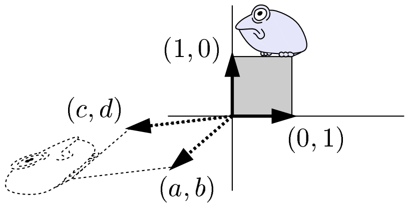
  

- **rotace** kolem $\mathbf{0}$, např.:

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

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

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

77. 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.

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

79. *Skládání lineárních zobrazení a násobení matic:* Jsou-li $f : \mathbb{K}^n \to \mathbb{K}^m$ a $g : \mathbb{K}^p \to \mathbb{K}^n$ lineární, a A, B jsou jejich matice vzhledem ke standardním bázím, pak $f \circ g$ je též lineární a má matici AB (zase vzhledem ke standardním bázím); tím je vysvětleno pravidlo násobení matic. Důkaz: $f(g(\mathbf{x})) = A(B\mathbf{x}) = (AB)\mathbf{x}$.

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

81. Obecněji: Jsou-li V_1, V_2, V_3 vektorové prostory a B_i je nějaká báze V_i, $f : V_2 \to V_1$ je lineární zobrazení s maticí A vzhledem k bázím B_2 a B_1, a $g : V_3 \to V_2$ je lineární zobrazení s maticí B vzhledem k bázím B_3 a B_2, pak $f \circ g : V_3 \to V_1$ má matici AB vzhledem k bázím B_3 a B_1.

82. Speciálně: jsou-li B a C dvě báze prostoru V, potom matice identického zobrazení $\mathrm{id} : V \to V$ 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 $A\mathbf{x}$.

83. Co to znamená že vektorové prostory V a W jsou „stejné“? Existuje mezi nimi **isomorfismus** $f: V \to W$, 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.

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

   (Poznámka: mnoho isomorfismů = mnoho „možných pohledů“ na daný vektorový prostor!)

84. Pojmy pro lineární zobrazení $f: U \to V$: vzor $\mathbf{0}$ je **jádro** f, označované $\operatorname{Ker} f$ (to je podprostor U), **obraz** $f(U) = \operatorname{Im} f$ je podprostor V.

85. Definice: **hodnost** lineárního zobrazení f je číslo $\dim(\operatorname{Im} f)$. Pozorování: je-li A matice zobrazení f (vzhledem k nějakým bázím, nejjednodušší případ je $f: \mathbb{R}^n \to \mathbb{R}^m$ a standardní báze), potom $\operatorname{Im} f$ je isomorfní sloupcovému prostoru matice A, a tedy hodnost f je rovna (sloupcové) hodnosti matice A.

86. Platí (pro konečnědimenzionální V)

$$\dim(\operatorname{Ker} f) + \dim(\operatorname{Im} f) = \dim(U).$$

   (Jako pro matice.) Odtud například plyne, že f je prosté právě když $\operatorname{Ker} f = \{\mathbf{0}\}$; potom f je isomorfismus prostoru U s prostorem $\operatorname{Im} f$ a zobrazuje bázi na bázi. Vždycky $\dim(\operatorname{Im} f) \leq \dim(U)$, tedy lineární zobrazení nemůže zvýšit dimenzi.

87. Lineární zobrazení $f: \mathbb{K}^n \to \mathbb{K}^n$ má hodnost n právě když je isomorfismus. V tom případě pak má i inverzní zobrazení f^{-1}, pro nějž $f^{-1} \circ f = f \circ f^{-1} = \mathrm{id}$. Pomocí lineárních zobrazení jsou snadno vidět tvrzení, která jsme měli o inverzních maticích.

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

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

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

91. 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

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

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

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

94. 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 $\mathbf{y}$.

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

96. **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).

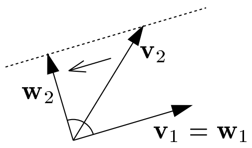
97. Standardní skalární součin v $\mathbb{R}^n$ je nejobvyklejší, ale není to jediná možnost pro skalární součin na $\mathbb{R}^n$. Třeba v rovině můžeme taky definovat $\langle \mathbf{x} \,|\, \mathbf{y} \rangle = x_1y_1 + \frac{1}{3}x_1y_2 + \frac{1}{3}x_2y_1 + x_2y_2$ (to souvisí s pozitivně definitními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

98. 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 $\|\mathbf{u} - \mathbf{v}\|$).

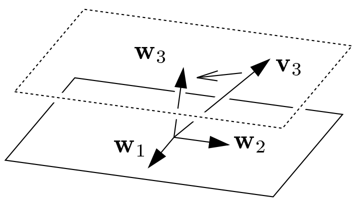
99. **Cauchyho-Schwarzova nerovnost** $\langle \mathbf{u}|\mathbf{v}\rangle \leq \|\mathbf{u}\| \cdot \|\mathbf{v}\|$. Důkaz: uvážit kvadratický mnohočlen $p(t) = \langle \mathbf{u} + t\mathbf{v}, \mathbf{u} + t\mathbf{v}\rangle$, ten musí mít nekladný diskriminant. Geometrický význam, souvislost s kosinovou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

100. **Ortogonální systém** (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.

101. **Gramova-Schmidtova ortogonalizace:** algoritmus, který z dané báze $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ udělá ortonormální 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.

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):

- Je to podprostor.
- Je-li $U_1 \subseteq U_2$, pak $U_2^{\perp} \subseteq U_1^{\perp}$.

- Je-li U podprostor, pak $(U^\perp)^\perp = U$ (z rozšiřitelnosti ortogonální báze).
- Platí $\dim(U^\perp) = \dim(V) - \dim(U)$.

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.