1 Soustavy lineárních rovnic

1.1 Příklad.

V této první přednášce se chceme naučit postup, jak řešit soustavy lineárních rovnic. Metodu, kterou chceme používat, je dobře vidět na jednoduchém příkladě. Dejme tomu, ze chceme vyřešit jednoduchou soustavu dvou rovnic o dvou neznámých:

$$2x + 4y = 6, \qquad (1)$$

$$5x + 3y = 8 \qquad (2)$$

Obvykle se řeší takovéto jednoduché příklady tím, že jednu neznámou vypočítám z jedné rovnice pomocí druhé neznámé, dosadím do druhé rovnice a dostanu jednu rovnici o jedné neznámé. Tu vypočítám, dosadím do první rovnice výsledek a dopočítám zbývající proměnou. Tento způsob se ale těžko zobecňuje pro větší soustavy lineárních rovnic. Zkusme upravovat soustavu rovnic (aniž bychom změnili množinu jejich řešení) na jednodušší tvar tak, aby pak postupné vypočítávání jedné proměnné po druhé vedlo jednoduše k výsledku.

,

Upravíme nyní druhou rovnici tím, že k ní přičteme vhodný násobek první rovnice. Nejprve to uděláme pomalu a postupně.

První rovnici (tj. její levou i pravou stranu) vynásobíme číslem $-\frac{5}{2}$ a dostaneme novou rovnici $-5x - 10y = -15$. Nová soustava

$$-5x - 10y = -15, \qquad (1')$$

$$5x + 3y = 8 \qquad (2)$$

má zřejmě stejnou množinu řešení jako soustava původní.

Pak druhou rovnici nahradíme součtem první a druhé rovnice:

$$-5x - 10y = -15, \qquad (1')$$

$$-7y = -7, \qquad (2')$$

a můžeme si snadno rozmyslet, že výsledná soustava má také stejnou množinu řešení jako soustava původní (za chvíli si to odůvodníme pro obecný případ).

Rovnice $(2')$ tedy vznikla tak, že jsme k rovnici (2) přičetli rovnici (1) vynásobenou (nenulovým) číslem $-\frac{5}{2}$. Zároveň jsme se přesvědčili, že výsledná soustava $(1'), (2')$ má stejnou množinu řešení jako původní soustava $(1), (2')$.

Po této úpravě je již jednoduché vypočítat řešení soustavy. Z druhé rovnice plyne, že $y = 1$, po dosazení do první rovnice vyjde ihned $x = 1$.

Všimněte si, že jsme dělali zbytečnou práci, když jsme vypisovali pořád celé rovnice při příslušných úpravách. Každá rovnice soustavy je určena koeficienty u neznámých x a y a příslušnou pravou stranou. Rovnice (1) je určena trojicí $\{2, 4; 6\}$ a rovnice (2) je určena trojicí $\{5, 3; 8\}$. Při násobení rovnice číslem se násobí každé číslo v dané trojici, při sčítání (odčítání) rovnic sčítáme (odčítáme) prvky v trojicích složku po složce.

Pokud bychom měli 50 rovnic o 50 neznámých a podařilo se nám matici soustavy upravit na trojúhelníkovou matici, bylo by řešení soustavy opět stejně jednoduché (postupným výpočtem od nejjednodušší rovnice a dosazováním do rovnic předchozích).

Nyní zkusíme totéž udělat obecně, pro soustavu s libovolným počtem (m) rovnic o libovolném počtu (n) neznámých.

1.2 Obecná soustava lineárních rovnic.

Obecnou soustavou lineárních rovnic myslíme soustavu (S) rovnic tvaru

$$a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1,$$

$$a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2,$$

$$\vdots$$

$$a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m.$$

Koeficienty soustavy jsou dány množinou příslušných koeficientů

$$A = (a_{ij});\ i = 1, \ldots, m;\ j = 1, \ldots, n$$

a sloupcem pravých stran $b = (b_1, \ldots, b_m)$. Koeficienty soustavy budou standardně buď reálné, nebo komplexní čísla.

Řešením soustavy s reálnými koeficienty se nazývá libovolná n-tice reálných čísel $x = (x_1, \ldots, x_n)$ pro kterou jsou všechny rovnice soustavy splněny.

Jsou-li některé koeficienty soustavy komplexní čísla, hledáme řešení mezi n-ticemi komplexních čísel.

Hledání obecného řešení dané soustavy lineárních rovnic se provádí postupnou úpravou a transformací dané soustavy rovnic na jinou soustavu prováděnou tak, aby množina všech řešení původní soustavy byla totožná s množinou všech řešení nově utvořené soustavy lineárních rovnic a tak, aby výsledná soustava byla snadno řešitelná. Existuje algoritmus (postup), jak najít množinu všech řešení dané soustavy lineárních rovnic, založený na tzv. Gaussově eliminační metodě. Než si ho popíšeme, dohodneme se nejdříve na vhodném názvosloví.

1.3 Matice

Definice 1 (Matice, součin matic)
Maticí A typu $m \times n$ nazýváme obdélníkové schéma čísel

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

nebo stručněji: $A = (a_{ij});\ i = 1, \dots, m;\ j = 1, \dots, n$.

Pokud jsou všechna čísla v matici reálná, říkáme, že A je reálná matice. Obecně budeme uvažovat matice, jejíž prvky jsou komplexní čísla.

Index i je řádkový, index j je sloupcový. Matice typu $n \times n$ se nazývá čtvercová matice.

Matici můžeme rozdělit na jednotlivé řádky

$$r_i, i = 1, \dots, m;\ \ r_i = (a_{i1}, a_{i2}, \dots, a_{in}),$$

a jednotlivé sloupce

$$s_j, j = 1, \dots, n;\ \ s_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix},$$

Horní trojúhelníková matice je čtvercová matice $A = (a_{ij})$, která má pod diagonálou samé nuly, tj. $a_{ij} = 0$ pro $i > j$. Obdobně se definuje dolní trojúhelníková matice.

Definice 2 (Matice a rozšířená matice soustavy)
Je-li (S) obecná soustava lineárních rovnic, pak matici A danou tabulkou

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

nazveme maticí soustavy (S) a matici (A, b) danou tabulkou

$$(A, b) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix}$$

nazveme rozšířenou maticí soustavy (S).

Daná soustava rovnic je zřejmě jednoznačně určená odpovídající rozšířenou maticí soutavy. Místo upravování soutavy rovnic budeme tedy upravovat jen příslušnou rozšířenou matici soustavy.

1.4 Elementární transformace soustavy.

Definice 3 (Elementární úpravy matice)
Elementární úprava matice C je jedna z následujících úprav:

(i) vyměníme dva řádky matice;

(ii) vynásobíme řádek nenulovým číslem;

(iii) k danému řádku přičteme násobek jiného řádku;

(iv) přidáme k matici nebo ubereme z matice nulový řádek.

Lemma 1 *Elementární úpravy rozšířené matice soustavy lineárních rovnic nemění množinu řešení soustavy.*

Toto tvrzení si budeme chtít odůvodnit (dokázat). Uděláme to ale na příští přednášce. To je zároveň příležitost pro každého, aby si toto odůvodnění zkusil rozmyslet sám!

V dalším se budeme snažit elementárními úpravami převést danou soustavu (resp. rozšířenou matici této soustavy) na jednodušší tvar, ve kterém půjde snadno najít všechna řešení této nové (a tedu i původní) soustavy.

1.5 Gaussův algoritmus.

Poznámka.

Carl Friedrich Gauss, se narodil v roce 1777 v Braunschweigu a zemřel v roce 1855 v Göttingenu.

Základní pojednání o teorii čísel (Disquisitiones Arithmeticae) napsal již ve věku 21 let. I když jeho oficiální povolání bylo ředitel astronomické observatoře, patří mezi nejgeniálnější matematiky historie. Kromě zmíněné teorie čísel objevil neeukleidovskou geometrii (objev nikdy nepublikoval), vytvořil základy diferenciální geometrie (plochy v třírozměrném prostoru), má základní výsledky v komplexní analýze i algebře. Kromě toho se věnoval geodesii, magnetismu, astronomii a optice. Patří mezi nejvýraznější postavy v historii matematiky.

Definice 4 (Matice v odstupňovaném tvaru)
Nechť A je matice typu $m \times n$ a $r_k, k = 1, \ldots, m$ jsou její řádky. Řekneme, že matice A je v **odstupňovaném tvaru**, *pokud (nakreslete si!) platí:*

pro každý nenulový řádek $r_k, k = 2, \ldots, m$ je předchozí řádek r_{k-1} také nenulový a navíc první nenulový prvek zleva v řádku r_k má vyšší sloupcový index (je víc vpravo) než první nenulový prvek zleva v řádku r_{k-1}.

Příslušný první nenulový prvek zleva v takovémto řádku r_k se nazývá **pivot** *a sloupec, ve kterém se nachází se nazývá* **pivotní sloupec.**

Řekneme, že matice A je v **redukovaném odstupňovaném tvaru**, *pokud je navíc první nenulový prvek v každém nenulovém řádku roven jedné a zároveň je tento prvek jediným nenulovým prvkem ve svém sloupci.*

Všimněte si, že z definice matice v odstupňovaném tvaru plyne, že za každým nulovým řádkem už jsou všechny další nižší řádky všechny nulové. Takže takováto matice (pokud je nenulová) má buď všechny řádky nenulové, nebo má nejdříve určitý počet nenulových řádků a pak všechny další řadky jsou nulové. Navíc pro každé dva po sobě jdoucí nenulové řádky platí příslušná podmínka o postavení prvních nenulových prvků zleva.

Na cvičení si procvičíte níže uvedený Gaussův algoritmus, který ukazuje, že libovolnou matici lze převést elementárními úpravami na matici v odstupňovaném tvaru. Postupně s maticí A provádím níže popsané elementární úpravy, upravenou matici budu pro pohodlí znovu značit po každém kroku symbolem A.

Nechť A je matice typu $m \times n$.

[Krok 1.] Procházím sloupce matice A postupně od prvního dál a najdu první nenulový sloupec, jeho index označím ℓ.

[Krok 2.] Pokud je $a_{1\ell} \neq 0$, neudělám nic, v opačném případě vyměním první řádek matice za jiný řádek matice A, který má ℓ-tý prvek nenulový (takový řádek musí existovat, protože celý ℓ-tý sloupec není nulový). V upravené matici už platí $a_{1\ell} \neq 0$. Tomuto kroku se někdy říká **pivotace.**

[Krok 3.] První řádek matice vydělím číslem $a_{1\ell}$.

[Krok 4.] Postupně odečítám vhodné násobky prvního řádku od druhého, třetího, až posledního řádku tak, aby v upravené matici platilo

$$a_{2\ell} = \ldots = a_{m\ell} = 0.$$

Tím je dokončena první sada úprav, v dalších úpravách již nepoužívám první řádek a uvažuji jenom upravenou matici A bez prvního řádku. To je matice A' typu $(m-1) \times n$. Pro tuto matici A' provedu znovu kroky 1 - 4.

Po dokončení této druhé sady úprav přestanu uvažovat první dva řádky upravené matice a pro zbylou matici A'' typu $(m-2) \times n$ pokračuji opět analogickou třetí sadou úprav.

Je zřejmé, že po konečném počtu takovýchto úprav bude nakonec výsledkem matice, která je v odstupňovaném tvaru.

Existuje také další algoritmus, který převádí libovolnou matici v odstupňovaném tvaru na matici v redukovaném odstupňovaném tvaru. Nejdřív vynechám všechny nulové řádky. Pak přičítám vhodné násobky posledního řádku k předchozím řádkům tak dlouho, až všechny prvky v sloupci nad pivotem v posledním řádku jsou nulové.

Pak vynechám poslední řádek a se zmenšenou maticí opakuji tutéž úpravu. Po konečném počtu kroků zřejmě dostaneme matici v redukovaném odstupňovaném tvaru.

Příklad: Ukažme si nyní, jak je možné používat Gaussův algoritmus na řešení rovnic na jednoduchém příkladu.

Nechť je rozšířená matice (A, b) dána maticí

$$(A, b) = \begin{pmatrix} 0 & 1 & 2 & -1 & 0 & 5 \\ 0 & 0 & 0 & 1 & 2 & 7 \\ 0 & 0 & 0 & 1 & 4 & 8 \\ 0 & 0 & 0 & 0 & 4 & 2 \end{pmatrix}$$

Pak je snadné spočítat (rozmyslete si sami!), že elementárními úpravami lze tuto matici převést na matici schodovitého typu:

$$(C,d) = \begin{pmatrix} 0 & 1 & 2 & -1 & 0 & 5 \\ 0 & 0 & 0 & 1 & 2 & 7 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Poslední rovnice je triviální a je možné ji vynechat. Z třetí rovnice $2x_5 = 1$ vypočítáme $x_5 = 1/2$. Z druhé rovnice dostaneme $x_4 = 7 - 2x_5 = 7 - 1 = 6$. Z první rovnice pak vypočítáme

$$x_2 = 5 - 2x_3 + x_4 + 0 \cdot x_5 = 11 - 2x_3.$$

Celkem tedy má obecné řešení soustavy tvar $(x_1, 11 - 2x_3, x_3, 6, 1/2)$ a závisí na dvou libovolných parametrech x_1 a x_3.

Je instruktivní si rozepsat obecné řešení jako součet tří pětic (sčítání se dělá po složkách):

$$(x_1, 11-2x_3, x_3, 6, 1/2) = (0, 11, 0, 6, 1/2)+(x_1, 0, 0, 0, 0)+(0, -2x_3, x_3, 0, 0) =$$

$$= (0, 11, 0, 6, 1/2) + x_1(1, 0, 0, 0, 0) + x_3(0, -2, 1, 0, 0, 0).$$

Všimněte si, že pětice $(0, 11, 0, 6, 1/2)$ je (jedno speciální) řešení dané soustavy, zatímco pětice $(1, 0, 0, 0, 0)$ a $(0, -2, 1, 0, 0, 0)$ jsou řešení tzv. odpovídající homogenní soustavy, tj. soustavy, kde sloupec pravých stran nahradíme samými nulami. Obecné řešení soustavy závisí na dvou libovolných konstantách.

1.6 Operace s maticemi.

Ve výše uvedeném příkladu je vidět, že je pro popis obecného řešení výhodné napsat jej jako součet tří sčítanců. To je jeden speciální příklad toho, jak se obecně sčítají matice. Operace s maticemi (jejich sčítání, násobení číslem, resp. jejich násobení) jsou velmi šikovné operace pro přehledný zápis obecných soustav lineárních rovnic. Tyto operace si nyní podrobně popíšeme a pojmenujeme.

Jednotlivé prvky matic budou čísla. Budeme uvažovat jen dva případy - čísla reálná, nebo čísla komplexní. Je vhodné ale poznamenat, že se často uvažují matice s obecnějšími prvky - obzvlášť důležitý případ jsou matice, jejichž prvky patří do tzv. konečných těles.

Definice 5 Operace s maticemi
Symbolem $\mathbb{F}$ budeme označovat buď množinu reálných čísel $\mathbb{R}$, nebo množinu komplexních čísel $\mathbb{C}$. Prvky matic budou patřit do $\mathbb{F}$ a budeme jim říkat prostě čísla. Množinu všech matic typu $m \times n$ označíme symbolem $M_{mn}(\mathbb{F})$.

1. *Pokud $A = (a_{ij})$ a $B = (b_{ij})$ jsou dvě matice stejného typu $m \times n$, pak definujeme součet $C = A + B$ jako matici typu $m \times n$, jejíž prvky mají tvar $c_{ij} = a_{ij} + b_{ij},\ i = 1, \ldots, m;\ j = 1, \ldots, n.$*

2. *Pokud α je číslo a $A = (a_{ij})$ je matice typu $m \times n$, pak součin $\alpha \cdot A$ je matice stejného typu, definovaná předpisem*

$$\alpha\, A = (\alpha a_{ij}),\ i = 1, \ldots, m;\ j = 1, \ldots, n.$$

   tj. prvek matice $\alpha\, A$ v i-tém řádku a v j-tém sloupci se rovná číslu $\alpha\, a_{ij}$.

3. *Je-li A matice typu $m \times n$ a B matice typu $n \times p$, pak součin matic $C = A \cdot B$ je matice typu $m \times p$, definovaná předpisem*

$$c_{rs} = \sum_{k=1}^{n} a_{rk} b_{ks} = a_{r1} b_{1s} + \ldots a_{rn} b_{ns};\ r = 1, \ldots, m;\ s = 1, \ldots, p.$$

Operace s maticemi mají určité vlastnosti, které si postupně probereme.

Lemma 2 *Symbolem 0 označíme nulovou matici, tj. matici, která má všechny prvky nulové.*
Pro sčítání matic platí:

1. $\forall A, B, C \in M_{mn}(\mathbb{F}),\ A + (B + C) = (A + B) + C,$ *(*asociativita*)*

2. $\forall A \in M_{mn}(\mathbb{F}),\ A + 0 = 0 + A = A,$ *(*existence neutrálního prvku*)*

3. $\forall A \in M_{mn}(\mathbb{F}), \exists B \in M_{mn}(\mathbb{F}), A + B = 0,$ *(*existence opačného prvku*)*
   Matici B označíme symbolem $-A$, její prvky jsou čísla $(-a_{ij})$.

4. $\forall A, B \in M_{mn}(\mathbb{F}),\ A + B = B + A,$ *(*komutativita*)*

Toto jednoduché tvrzení nebudeme odůvodňovat (je to vhodné cvičení pro čtenáře, aby si zkusil odůvodnění uvědomit a napsat sám, je k tomu potřeba jen znalost definic a znalost vlastností reálných, resp. komplexních čísel).

Množina spolu s operací splňující výše uvedené 4 vlastnosti je příkladem tzv. (komutativní) grupy. O ní budeme mluvit podrobněji v další přednášce.

Násobení matic je o hodně složitější operace než je sčítání. Každé dvě matice stejného typu můžeme sečíst. Abychom mohli vynásobit dvě matice, je třeba, aby se jejich typy vhodně doplňovaly. Nemůžeme vynásobit libovolné dvě matice.

Lemma 3 *Předpokládejme, že $A \in M_{mn}, B, D \in M_{np}, C, F \in M_{pq}$. Pak platí*

1. $A\ (B\ C) = (A\ B)\ C$, *(asociativita násobení)*
2. $B\ (C + F) = B\ C + B\ F, (B + D)\ C = B\ C + D\ C$, *(distributivita)*
3. $\forall n \in \mathbb{N}$ *označíme symbolem $E_n \in M_{nn}$ takovou čtvercovou matici, která má na diagonále samé jedničky (tj. $e_{ii} = 1, i = 1, \ldots, n$) a všude jindy samé nuly.*

   Pak pro každou matici typu $m \times n$ platí

   $$E_m.A \ = \ A.E_n \ = \ A,$$

   (existence jednotkového prvku pro násobení matic)

Důkaz: Pro ověření první vlastnosti je podstatná následující úprava levé strany rovnosti

$$\sum_{k=1}^{n} a_{ik} \left(\sum_{l=1}^{p} b_{kl} c_{lj} \right) = \sum_{k=1}^{n} \sum_{l=1}^{p} a_{ik} b_{kl} c_{lj}.$$

Tatáž úprava platí i pravou stranu. Tedy obě strany se rovnají.

Stejně se ověří i druhá sada rovností (d.cv.).

Matice E_k v poslední rovnosti je jednotková matice, která má na diagonále samé jedničky a mimo diagonálu samé nuly. Příslušná rovnost se snadno ověří (udělejte sami!). Pokud nemůže dojít k nedorozumění, budeme označovat jednotkovou matici symbolem E. □

Násobení matic není (obecně) komutativní (najděte příklad!). Pro dobré pochopení násobení matic je vhodné si první činitel (v našem případě matici A) napsat pomocí jejích řádek $r_1, \ldots, r_m$ a druhý činitel (matici B) si napsat pomocí jejích sloupců $s_1, \ldots, s_n$. Potom prvek c_{ij} součinu je určen 'součinem' $r_i.s_j$, kde tento součin je podobný skalárnímu součinu vektorů v $\mathbb{R}^3$, t.j.

sečteme postupně součin prvních komponent, součin druhých komponent, atd. Podstatné je, že r_i i s_j musí mít stejný počet komponent, což je zaručeno podmínkou, že počet sloupců matice A je stejný jako počet řádků matice B. Jako důsledek např. zjistíme, že první řádek výsledné matice C je ovlivněn pouze prvním řádkem matice A (a celou maticí B). Podobně první sloupec výsledné matice C zavisí jen na prvním sloupci druhého činitele B (a na všech prvcích matice A).

1.7 Soustavy lineárních rovnic - diskuse

Vrátíme se nyní k diskusi o řešení soustav lineárních rovnic. Nejprve si odůvodníme tvrzení o tom, že elementární úpravy rozšířené matice soustavy nemění množinu řešení soustavy (Lemma 1).

Důkaz Lemmatu 1.

Jednotlivé řádky matice soustavy A si označíme $r_i,\ i = 1, \ldots, m$. Řádky r_i jsou matice typu $1 \times n$. Řešení soutavy označíme x a budeme je psát jako sloupec, tj. jako matici typu $n \times 1$. Pak má smysl jejich součin $r_i\ x$, výsledkem je číslo, tj. matice typu 1×1. Odpovídající j-tá rovnice soustavy pak má tvar

$$r_i\ x = b_i.$$

Celá soustava se dá napsat jednoduše ve tvaru

$$A\ x = b,$$

kde b je sloupec pravých stran. Zavedené označení nám usnadní zápis úprav, nutných pro odůvodnění lemmatu.

Je triviální, že elementární úpravy (i) nemění soustavu rovnic (jen jsme rovnice soustavy napsali v jiném pořadí). Také pro úpravu (ii) je úvaha jednoduchá, protože zřejmě (pro nenulové číslo α a pro libovolné $i, i = 1, \ldots, m$) platí

$$r_i\ x = b_i \iff (\alpha r_i)\ x = \alpha b_i$$

(rozmyslete si důkladně sami!).

Případ poslední elementární úpravy jsme podrobně rozebrali v jednoduchém případě v minulé přednášce. Postup v obecném případě je stejný. Úvahu budeme nyní formulovat již jen pomocí koeficientů příslušných vybraných rovnic. První řádek rozšířené matice (A, b) je matice tvaru (r_1, b_1).

Odpovídající první rovnice má pak tvar $r_1 \cdot x = b_1$. Stejně postupujeme pro ostatní řádky soustavy.

Nechť např. (pro ukázku, stejně se postupuje v ostatních případech) k prvnímu řádku rozšířené soustavy přičteme α násobek druhého řádku.

Po této úpravě dostaneme soustavu, jejíž první rovnice má změněné koeficienty

$$(r'_1, b'_1), \ldots, (r'_m, b'_m),$$

pro které

$$r'_1 = r_1 + \alpha r_2, r'_2 = r_2, \ldots, r'_m = r_m; b'_1 = b_1 + \alpha b_2, b'_2 = b_2, \ldots, b'_m = b_m.$$

Ověřme nyní, že se množina řešení touto úpravou nezmění.

Pokud x je řešení původní soustavy, tj. pokud

$$r_j \cdot x = b_j,\ j = 1, \ldots, m,$$

pak zřejmě

$$r'_j \cdot x = b'_j,\ j = 2, \ldots, m.$$

Pro první řádek dostaneme $r'_1 \cdot x = r_1 \cdot x + \alpha r_2 \cdot x = b_1 + \alpha b_2 = b'_1$, tedy x je také řešením nové soustavy.

Naopak, pokud x řeší novou soustavu

$$r'_j \cdot x = b'_j,\ j = 1, \ldots,$$

pak víme, že $r_1 = r'_1 - \alpha r'_2,\ b_1 = b'_1 - \alpha b'_2$ a stejnou úvahou jako v předchozím případě ukážeme, že je to také řešení původní soustavy. Takže obě soustavy mají stejnou množinu řešení. □

Pomocí Gaussovy eliminace umíme soustavu obecně vyřešit. Následující věta popisuje, kolik řešení může soustava mít. Připomeňme si, že pro matici B ve schodovitém tvaru se každý první nenulový prvek na daném řádku nazývá pivot. Dohodněme se, že sloupec matice B nazveme pivotní, pokud obsahuje nějaký pivot.

Věta 1 *Předpokládejme, že (A, b) je rozšířená matice soustavy a že matice (A', b') je matice schodovitého tvaru, která vznikla z (A, b) konečnou posloupností elementárních úprav. Pak platí:*

1. *Řešení soustavy s rozšířenou maticí (A, b) existuje právě když sloupec b' není pivotní.*

   Pokud má soustava řešení, mohou nastat následující dva případy:

2. *Soustava má právě jedno řešení právě když každý sloupec matice A' je pivotní.*

3. *Soustava má nekonečně mnoho řešení v opačném případě.*

Důkaz:

1. Pokud sloupec b' je pivotní, pak příslušná řádka rozšířené matice má tvar $(0, \ldots, 0, b_p$ pro vhodné p, kde $b_p \neq 0$. Odpovídající rovnice má tvar
$$0.x_1 + \ldots + 0.x_n = b_p$$
a tato rovnice zřejmě nemá řešení.

   V opačném případě budeme postupně odspodu vypočítávat jednu proměnnou za druhou. Mohou nastat dva případy.

2. Pokud je každý sloupec matice A' pivotní, pak vypočítáme jednoznačně všechny proměnné.

3. Pokud existuje sloupec matice A', který není pivotní, tak při výpočtu řešení můžeme tuto proměnnou zvolit libovolně a počítat dál. V tomto případě zřejmě existuje nekonečně mnoho řešení.

□

Zajímavá (a důležitá) otázka je na kolika parametrech obecné řešení závisí v případě existence nekonečně mnoha řešení. Z výše uvedených úvah je zřejmé, že počet parametrů, na kterých obecné řešení závisí je roven počtu sloupců matice A', které nejsou pivotní. Nebo jinak (rozmyslete si!), počet parametrů je roven rozdílu počtu neznámých minus počet netriviálních řádek matice A'.

Na první pohled není vidět, jestli tento počet parametrů nezávisí na volbě posloupnosti elementárních úprav, které převádějí matici (A, b) na matici (A', b'). Ukáže se, že nezávisí, ale je již dost netriviální fakt a bude nám trvat nějakou dobu, než ho budeme schopni ověřit.

1.8 Elementární úpravy pomocí maticového součinu.

Elementární úpravy matice jsme definovali jako jisté operace s řádky matice. Je užitečné si uvědomit, že elementární úpravy matice A je možné popsat pomocí násobení matic.

Označme symbolem U_{ij} čtvercovou $m \times m$ matici, která má v i-tém řádku a v j-tém sloupci číslo 1 a všude jinde nulu. Připomeňme si, že $E_m = E$ označuje jednotkovou $m \times m$ matici. Jako drobné cvičení na násobení matic si rozmyslete (a příslušné matice U si nakreslete!), že:

1. Je-li A' matice vzniklá z matice A vynásobením i-tého řádku číslem α, pak $A' = U\,A$, kde $U = E + (\alpha - 1)\,U_{ii}$;

2. Je-li A' matice vzniklá z matice A výměnou i-tého a j-tého řádku, pak $A' = U\,A$, kde $U = E - U_{ii} - U_{jj} + U_{ij} + U_{ji}$;

3. Je-li A' matice vzniklá z matice A přičtením α násobku j-tého řádku k i-tému řádku, pak $A' = U\,A$, kde $U = E + \alpha\,U_{ij}$;

1.9 Inverzní matice

Definice 6 Inverzní matice
Označme symbolem E_n matici typu $n \times n$, která má na diagonále jedničky a jinde nuly (tuto matici nazveme jednotkovou maticí). Řekneme, že čtvercová matice A typu $n \times n$ je regulární, pokud existuje matice A^{-1}, pro kterou platí

$$A \cdot A^{-1} = A^{-1} \cdot A = E.$$

Matici A^{-1} nazýváme inverzní maticí k matici A.

Pokud matice A není regulární, nazveme ji singulární maticí.

Prostor všech čtvercových matic typu $n \times n$ má tedy bohatší strukturu. Pro dva libovolné jeho prvky je definován jejich součin, kterým je opět čtvercová matice stejného typu. Jednotková matice je zřejmě neutrální element vůči operaci násobení matic. Zajímavá otázka je, jestli pro každou nenulovou matici existuje inversní matice. V termínech předchozí definice to znamená, jestli je každá nenulová matice (tj. matice jejíž všechny prvky nejsou nulové) regulární. Snadná odpověď je, že to není pravda. Příkladem je libovolná $n \times n$ matice, která má celý jeden sloupec nulový (zkuste si sami rozmyslet, že je to snadný důsledek definice maticového násobení!).

Definice 7 *Množinu všech regulárních $n \times n$ reálných matic označíme $GL(n, \mathbb{R})$.*
Množinu všech regulárních $n \times n$ komplexních matic označíme $GL(n, \mathbb{C})$.

V následujícím lematu si shrneme vlastnosti operace násobení na $GL(n,\mathbb{R})$ (stejné vlastnosti má i operace násobení na $GL(n,\mathbb{C})$).

Lemma 4 *1.* $\forall A, B, \in GL(n,\mathbb{R}),\ \ A\,B \in GL(n,\mathbb{R})$;

2. $\forall A, B, C \in GL(n,\mathbb{R}), (A\,B)\,C = A\,(B\,C)$ *(asociativita)*

3. $\exists E \in GL(n,\mathbb{R}),\ \forall A \in GL(n,\mathbb{R}), E\,A = A\,E = A$; *(existence jednotkového prvku)*

4. $\forall A \in GL(n,\mathbb{R}), \exists A^{-1} \in GL(n,\mathbb{R});\ A\,A^{-1} = A^{-1}\,A = E$, *(existence inversního prvku)*

Všimněte si, že vlastnosti $GL(n,\mathbb{R})$ vzhledem k násobení jsou velmi podobné vlastnostem $M_{nn}(\mathbb{F})$ vzhledem ke sčítání (jen se příslušné prvky a odpovídající operace jinak nazývají). Později uvidíme, že to jsou dva základní příklady tzv. grupy, jen násobení (pro $n > 1$) není komutativní.

Důkaz:

(1) Jsou-li A a B regulární matice, pak platí rovnosti

$$A\,B\,B^{-1}\,A^{-1} = A\,A^{-1} = E;\ B^{-1}\,A^{-1}\,A\,B = B^{-1}\,B = E.$$

Z těchto vztahů ihned plyne, že AB je regulární a k ní inversní matice je rovna $B^{-1}\,A^{-1}$.

(2), (3) Tyto vlastnosti jsme si již ověřili dříve (v souvislosti s definicí násobení matic).

(4) Tady stačí ověřit, že matice inverzní k regulární matici je také regulární. To je okamžitý důsledek definice regulární matice (matice inverzní k matici A^{-1} je matice A). □

1.10 Maticové rovnice.

To, co jsme si právě rozmysleli, nám teď pomůže najít řešení tzv. maticových rovnic. Tím myslíme následující úlohu. Pokud $A \in M_{mn}(\mathbb{T})$, $B \in M_{mp}(\mathbb{T})$, pak hledáme matici $X \in M_{np}(\mathbb{T})$ takovou, že

$$AX = B.$$

V součinu matic AX závisí j-tý sloupec pouze na j-tém sloupci matice X. Proto jsou neznámé elementy $x_{1j}, x_{2j}, \ldots, x_{nj}$ tohoto sloupce řešením soustavy rovnic s rozšířenou maticí

$$\left(\begin{array}{ccccc|c} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} & b_{1j} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} & b_{2j} \\ \vdots & & \ddots & & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & \ldots & a_{mn} & b_{mj} \end{array}\right)$$

Úpravy, které budeme při řešení této soustavy rovnic provádět, abychom ji dostali do odstupňovaného tvaru, nezávisí na pravé straně, závisí pouze na matici A. Můžeme tak stejně dobře psát za svislou čáru všechny pravé strany, pro které nás řešení zajímá, tedy celou matici B. Existenci řešení a jejich počet pak odečteme po úpravě matice $(A|B)$ na odstupňovaný tvar. Je zřejmé, že ve výsledné matici X budou všechny sloupce záviset na stejném počtu parametrů, rovném počtu nepivotních sloupců v odstupňovaném tvaru matice A.

Zatím jsme si neuvedli příklady regulárních matic. Jednotková matice je jednoduchý příklad regulární matice. Další příklady jsme viděli, když jsme realizovali elementární úpravy matic pomocí násobení maticí U (zleva). Zkontrolujte, že všechny tři matice U (realizující elementární úpravy pomocí maticového násobení) jsou regulární (najděte příslušné inverzní matice!). V následujícím tvrzení is ukážeme, jak pro mnoho matic ukázat, že jsou regulární.

Lemma 5 *Nechť A je čtvercová matice, kterou lze upravit na jednotkovou matici. Pak A je regulární, existuje právě jedna matice C splňující $AC = E$, právě jedna matice D splňující $DA = E$ a $D = C = A^{-1}$.*

Důkaz: Uvažujme maticovou rovnici $AX = E$, která odpovídá soustavě rovnic s rozšířenou maticí $(A|E)$. Podle předpokladu existuje posloupnost elementárních úprav s maticemi $U_1, \ldots, U_q$ takových, že $U_q \ldots U_1 A = E$ a podle definice je A regulární, $A^{-1} = U_q \ldots U_1$. Po úpravě má rozšířená matice tvar $(E|U_q \ldots U_1 E)$, takže soustava rovnic má řešení $X = A^{-1}$. Tím jsme dokázali existenční část tvrzení. Pro libovolnou matici D splňující $E = DA$ musí platit $A^{-1} = DAA^{-1} = D$ a podobně pro libovolnou matici C splňující $E = AC$ platí $A^{-1} = A^{-1}AC = C$, čímž je dokázána i jednoznačnost. □

Příklad: Pro hledání inversní matice k dané čtvercové matici A je možný následující postup. Chci najít řešení maticové rovnice $A\,X = E$. Pokud taková matice X existuje, je to hledaná inversní matice A^{-1}. Víme již, že pokud

A je regulární (a existuje-li tedy inversní matice), lze ji převést elementárními úpravami na jednotkovou matici. Tedy existuje (regulární) matice U, pro kterou $U\,A = E$. Rozšířenou matici (A, E) rovnice $A\,X = E$ tedy násobením maticí U zleva převedeme na tvar $(U\,A\,,\,U\,E) = (E\,,\,U)$, která odpovídá rovnici $E\,X = U$. Tedy matice U je také řešením původní maticové rovnice $A\,X = E$. Je to tedy hledaná inversní matice. Na ukázku si spočítáme jednoduchý příklad.

Hledejme inverzní matici k matici

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$$

Upravujeme tedy rozšířenou matice odpovídající maticové rovnici $AX = E$:

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & -2 & -3 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array}\right)$$

Hledaná inverzní matice je

$$A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix},$$

jak snadno ověříme vynásobením s A.

2 Vektorové prostory

2.1 Definice vektorového prostoru.

Poznámka:

Symbolem $\mathbb{R}$, resp. $\mathbb{C}$ budeme označovat těleso reálných, resp. komplexních čísel. Pro množinu přirozených (resp. celých) čísel budeme používat označení $\mathbb{N}$ (resp. $\mathbb{Z}$) a množinu racionálních čísel označíme symbolem $\mathbb{Q}$. V přednášce budeme předpokládat, že standardní vlastnosti reálných, resp. komplexních čísel, jsou známy. Podrobnosti o jejich vlastnostech budou také připomenuty v přednášce z matematické analýzy.

Na začátku přednášky si budeme chtít zavést pojem vektoru a vektorového prostoru. Jako všechny pojmy v matematice, i v tomto případě jsou

vlastnosti vektorů odpozorovány ze známých příkladů (a pak explicitně formulovány). Nejdříve si tedy zopakujeme, které jsou základní příklady vektorů a vektorových prostorů. Nejznámější a intuitivně nejpochopitelnější příklad patří do geometrie, ale další podstatné příklady jsou vzaty z aritmetiky a analýzy.

Příklad:
1. Geometrie. Základní středoškolská představa o tom, co je vektor v rovině (či v prostoru), je orientovaná úsečka. Přesněji, dvě takové úsečky jsou považované za stejné, pokud jednu dostanu z druhé rovnoběžným přenosem. Základní operace, které mohu s vektory dělat, je jejich sčítání (definované geometricky pro dva vektory umístěné do stejného počátku pomocí příslušného rovnoběžníku). Vektor také můžeme vynásobit reálným číslem. Množina všech (geometrických) vektorů je základní příklad a inspirace pro níže uvedenou definici vektorového prostoru.

2a. Aritmetika. Množina $\mathbb{R}_n$ je množina všech n-tic $x = (x_1, \ldots, x_n)$ reálných čísel. Sčítání dvou prvků této množiny je definováno pomocí sčítání jejich odpovídajících komponent, násobení takovéto n-tice číslem se také definuje po složkách.

2b. Aritmetika. Množina $\mathbb{C}_n$ je množina všech n-tic $z = (z_1, \ldots, z_n)$ komplexních čísel. Sčítání dvou prvků této množiny je definováno pomocí sčítání jejich odpovídajících komponent, násobení takovéto n-tice komplexním číslem se také definuje po složkách. Toto je příklad, který motivuje definici vektorového prostoru nad tělesem $\mathbb{C}$ komplexních čísel.

3. Analýza. Označme symbolem V prostor všech polynomů jedné reálné proměnné, jejichž stupeň je menší nebo roven danému přirozenému číslu k. Budeme uvažovat polynomy s komplexními koeficienty. Obecný tvar takového polynomu je

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

kde a_i jsou komplexní čísla a x je reálná proměnná.

Pak opět můžeme definovat snadno součet dvou takovýchto polynomů a také součin libovolného komplexního čísla a daného polynomu předpisem:

$$(p_1 + p_2)(x) := p_1(x) + p_2(x); p_1, p_2 \in V,$$

$$(\alpha p_1)(x) := \alpha(p_1(x)).$$

Pokud tedy

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0,$$

$$q(x) = b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0,$$

pak

$$[p+q](x) = (a_n + b_n)x^n + (a_{n-1} + b_{n-1})x^{n-1} + \ldots + (a_1 + b_1)x + (a_0 + b_0).$$

Všimněte si, že tedy existuje vzájemně jednoznačné zobrazení mezi prostorem $\mathbb{C}_{n+1}$ a prostorem V všech polynomů stupně nejvýše n, které zachovává (respektuje) obě operace. Všechny popsané případy mají něco společného. Daný prostor je množina a pro její prvky je definována operace sčítání a operace násobení číslem (reálným, resp. komplexním).

Než si napíšeme dofinici, která všechny tyto případy zahrnuje a zobecňuje, uvedeme si nejprve příklady a definici jednodušší struktury, která se skládá jen z množiny s jednou operací. Příklad množiny všech matic daného typu s operací sčítání a množiny $GL(n, \mathbb{R})$ s operací násobení matic mají hodně společného. Přesto, že v jednom případě jde o operaci sčítání a v druhém případě o operaci násobení, vlastnosti těchto operací jsou velmi podobné. To vede k následující definici. Při formulaci příslušných vlastností budeme používat (pro přehlednost a pro úsporu místa) symbol $\forall$, který znamená 'pro všechny' a symbol $\exists$, který znamená 'existuje (existují)'.

Definice 8 (Grupa)
Grupa G je množina G spolu s operací

$$\circ : G \times G \mapsto G,$$

která má následující vlastnosti:

(i) $(a \circ b) \circ c = a \circ (b \circ c)$ *pro všechny* $a, b, c \in G$ *(asociativita),*

(ii) *existuje prvek* $e \in G$ *(neutrální element) s vlastností, že pro všechny* $a \in G$ *platí* $e \cdot a = a \cdot e = a$,

(iii) *pro každé* $a \in G$ *existuje prvek* $b \in G$ *s vlastností* $a \cdot b = b \cdot a = e$ *(existence inversního prvku); prvek b označíme symbolem* a^{-1} *a nazveme inversním elementem k a.*

Pokud navíc platí, že

(iv) $a \circ b = b \circ a$ *pro všechny* $a, b \in G$ *(komutativita),*

pak nazveme grupu G *komutativní grupa.*

Příklad:

Dva motivující příklady příklady jsme uvedli před definicí. Jejich speciálním případem jsou $(\mathbb{R}, +)$ a $(\mathbb{R} - \{0\}, \cdot)$. To jsou tedy příklady grup. Další příklady je možné hledat například mezi podmnožinami těchto dvou grup. Dvojice $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ a $(\mathbb{Q} - \{0\}, \cdot)$ jsou příklady grup, zatímco dvojice $(\mathbb{N}, +)$, $(\mathbb{N} \cup \{0\}, +)$ a $(\mathbb{Z}, \cdot)$ nejsou grupy (proč?). Další příklady budete probírat na cvičení.

Označení. V definici vektorového prostoru hraje podstatnou roli těleso skalárů (čísel). Pojem těleso se definuje v algebře, ale my si tuto definici nebudeme nyní uvádět. Budeme uvažovat jen dva případy, těleso reálných čísel $\mathbb{R}$ a těleso komplexních čísel $\mathbb{C}$ a pro jednoduchost označení budeme používat symbol $\mathbb{T}$ pro to z nich, které právě uvažujeme. Tedy buď $\mathbb{T} = \mathbb{R}$, nebo $\mathbb{T} = \mathbb{C}$.

Definice 9 Vektorový prostor
Vektorový prostor V *nad tělesem* $\mathbb{T}$ *je množina* V *spolu s dvěma operacemi (zobrazeními)*

(i) $+ : V \times V \to V \ \ \{v_1, v_2\} \mapsto v_1 + v_2$ *(sčítání vektorů);*

(ii) $\cdot : \mathbb{T} \times V \to V$ *(násobení vektoru číslem),*

pro které platí následující vlastnosti (které budou splňovat následující axiomy):

I. Dvojice $(V, +)$ *je komutativní grupa.*

II.a) pro všechny $v \in V$ *platí* $1 \cdot v = v$,

II.b) pro všechny $\alpha, \beta \in \mathbb{R}(\mathbb{C}), v \in V$ *platí* $\alpha \cdot (\beta \cdot v) = (\alpha\beta) \cdot v$,

III.a) pro všechny $\alpha, \beta \in \mathbb{R}(\mathbb{C}), v \in V$ *platí* $(\alpha + \beta) \cdot v = \alpha \cdot x + \beta \cdot v$,

III.b) pro všechny $\alpha \in \mathbb{R}(\mathbb{C}), u, v \in V$ *platí* $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$.

Prvky množiny V *se nazývají vektory (budeme je typicky označovat malými písmeny latinské abecedy). Prvky tělesa* $\mathbb{T}$, *se nazývají čísla (budeme je typicky označovat malými písmeny řecké abecedy).*

Všimněte si, že prázdná množina nemůže být vektorovým prostorem, protože každý vektorový prostor musí obsahovat alespoň jeden prvek - neutrální prvek vzhledem ke sčítání, který budeme označovat symbolem o. Nejmenší

vektorový prostor (říká se mu triviální vektorový prostor) je jednoprvková množina, její jediný prvek je nulový vektor o a výsledek jakékoliv operace je vždy vektor o.

Ze základních vlastností sčítání a násobení formulovaných v definici je možné odvodit řadu dalších vlastností (důsledků). Dvě z nich jsou formulovány v následujícím jednoduchém tvrzení.

Lemma 6 *Je-li V vektorový prostor, pak platí:*

(1) $\forall u \in V : 0 \cdot u = o$,

(2) $\forall u \in V : (-1) \cdot u = -u$.

Odůvodnění (důkaz).

(1) Z vlastností formulovaných v definici vektorového prostoru plyne ihned, že $(1+0)\cdot u = u \ \forall u \in V$. Tedy platí také $u+0\cdot u = u \ \forall u \in V$. Přičteme-li k oboum stranám této rovnosti vektor $(-u)$, vyjde požadovaný vztah $0 \cdot u = o$.

(2) Pro všechny $u \in V$ platí $[1 + (-1)] \cdot u = 0 \cdot u = o$. Tedy platí také $u + (-1) \cdot u = o$. Po přičtení vektoru $(-u)$ na obě strany rovnosti dostaneme požadovaný vztah.

2.2 Vektorové podprostory,

Definice 1 *Nechť V je vektorový prostor nad $\mathbb{T}$ a W je neprázdná podmnožina V uzavřená vzhledem ke sčítání a násobení číslem, tj. taková, že $\forall v, w \in W$, $\forall r \in \mathbb{T}$ platí $v + w \in W$ a $rv \in W$. Pak nazýváme W **podprostorem** vektorového prostoru V, značíme $W \leq V$.*

Lemma 1 *Nechť V je vektorový prostor nad $\mathbb{T}$ a W jeho podprostor. Pak W je vektorový prostor nad $\mathbb{T}$.*

Důkaz: Podmínky v definici podprostoru zaručují, že součet i násobení jsou uzavřené na W a tedy jsou na něm jakožto operace dobře definovány. Postupně ověříme axiomy:

1. Asociativita plyne ihned z definice: $\forall u, v, w \in W$ platí $u + (v + w) = (u + v) + w$, neboť $u, v, w \in V$ a tam to platí. Podobně se postupuje při ověřování komutativity, obou distributivních zákonů, a při ověření asociativity násobení a vlastnosti $1 \cdot v = v$.

2. Pro libovolný $v \in W$ díky uzavřenosti na násobení platí $0.v = o \in W$, kde o je nulový vektor ve V. Tedy ve W existuje neutrální prvek vzhledem ke sčítání.

3. Pro všechna $v \in W$ patří i opačný prvek $-v = (-1).v$ znovu do W díky uzavřenosti na násobení. Pro v a $-v$ platí z axiomů na V rovnost $v + (-v) = 0$, takže opačný prvek ve V je opačným prvkem i ve W.

□

Následující lemma nám umožní sloučit dvě podmínky charakterizující podprostor do jedné, což učiní následující důkazy o něco elegantnějšími.

Lemma 2 *Nechť V je vektorový prostor nad $\mathbb{T}$ a W jeho podmnožina. Pak $W \leq V$, právě když $\forall u, v \in W$ a $\forall r, s \in \mathbb{T}$ je $ru + sv \in W$.*

Důkaz: Tvrzení říká, že nějaké dvě podmínky jsou ekvivalentní ("právě když"). Je tedy potřeba ověřit, že podmnožina splňující podmínky v definici podprostoru splňuje i podmínku v tvrzení, a naopak, podmnožina splňující podmínku v tvrzení vyhovuje definici. Pokud W je podprostor, $u, v \in W$, $r, s \in \mathbb{T}$, pak rv i su patří do W z druhé podmínky v definici a $rv + su \in W$ z první podmínky. Naopak, pokud všechny $u, v \in W$ splňují $ru + sv \in W$ pro všechny skaláry r, s, pak stačí zvolit $r = 1, s = 1$ a získáváme první podmínku v definici, a volbou $s = 0$ získáváme druhou. □

Příklad:

Nechť vektorový prostor V je rovina, jak vypadají všechny podprostory v prostoru V? Nakreslete si je! Jsou to všechny přímky procházející počátkem, pak podprostor $\{0\}$, skládající se z jednoho bodu, a to počátku (triviální podprostor) a celý prostor V.

Rozmyslte si obdobně, jak vypadají všechny vektorové podprostory v trojrozměrném prostoru - jsou to opět všechny přímky procházející počátkem, všechny roviny procházející počátkem, triviální prostor a celý prostor.

Intuitivně cítíme rozdíl mezi velikostí těchto různých podprostorů. Přímka je jednodimenzionální objekt, zatímco rovina je dvoudimenzionální a celý prostor trojdimenzionální. V dalším si budeme chtít pojem dimenze vektorového prostoru zavést formálně.

Příklad 1 *Pojem podprostoru umožňuje zkonstruovat mnoho dalších příkladů vektorových prostorů:*

1. *Nechť V je vektorový prostor nad $\mathbb{T}$ a v vektor v něm. Pak množina $\langle v\rangle := \{rv | r \in \mathbb{T}\}$ je vektorový podprostor V, který se nazývá **lineární obal** v. Ve vektorových prostorech, které mají geometrickou interpretaci (třeba $\mathbb{R}^n$), je to vlastně přímka o směru v procházející počátkem.*

2. *Nechť $a_j \in \mathbb{T}$ pro $j \in \{1, \ldots, n\}$, pak množina W_a všech vektorů $x \equiv (x_1, \ldots, x_n) \in \mathbb{T}^n$, které splňují lineární rovnici $\sum_{j=1}^n a_j x_j = 0$, je podprostorem $\mathbb{T}^n$. Stačí použít ekvivalentní podmínku z lemmatu, neboť pokud $x, y \in W_a$ a $r, s \in \mathbb{T}$, pak*

$$\sum_{j=1}^{n} a_j(rx_j + sy_j) = r\sum_{j=1}^{n} a_j x_j + s\sum_{j=1}^{n} a_j y_j = r.0 + s.0 = 0,$$

   *tedy $rx + sy \in W_a$. Všimněte si, že pokud by v rovnici byla pravá strana nenulová, pak by podmínka splněna nebyla a množina řešení by nebyla vektorovým prostorem. Rovnice s nulou na pravé straně se nazývá **homogenní**, s nenulovou pravou stranou **nehomogenní**.*

3. *Množina všech matic v odstupňovaném tvaru je podprostor množiny všech matic daného typu (ověřte sami).*

4. *Množina všech omezených posloupností je podprostor množiny všech posloupností. Stačí si uvědomit, že součet dvou omezených posloupností je omezená a násobek omezené posloupnosti je také omezená posloupnost. Podobně i množina všech konvergentních posloupností (při ověření využijete větu o algebře limit z matematické analýzy) nebo množina všech posloupností, jejichž k-tý člen je nulový.*

5. *Množina $P(x, \mathbb{T})$ všech polynomů v proměnné x s koeficienty v $\mathbb{T}$ je vektorový prostor. Jednak je možné chápat jej jako podprostor prostoru všech funkcí na $\mathbb{T}$. Druhá interpretace vychází z toho, že při sčítání polynomů se sčítají příslušné koeficienty u mocnin x a při násobení polynomu číslem se také násobí posloupnost koeficientů člen po členu. Polynom je tedy možné chápat jako posloupnost čísel z $\mathbb{T}$, která má pouze konečný počet nenulových členů. Množina takových posloupností je podprostorem v množině všech posloupností.*

6. *Množina $P_k(x, \mathbb{T})$ všech polynomů stupně nejvýše k. Pokud bychom vynechali slovo nejvýše, chyběl by například nulový vektor.*

7. *Množina všech omezených funkcí, množina všech spojitých funkcí na $\mathbb{R}$, množina všech násobků funkce $\cos x$,... Pokud $p \in M$, pak množina všech funkcí, pro něž $f(p) = 0$, je vektorový prostor, zatímco množina všech funkcí, pro něž $f(p) = 17$, není. Množiny funkcí zadané podmínkou na existenci a nulovost limity či derivace v nějakém bodě jsou vektorové prostory, opět z vlastností limity a derivace funkce.*

8. *Podprostor má strukturu vektorového prostoru vždy nad celou číselnou množinou $\mathbb{T}$. Tedy $\mathbb{C}^n$ nad $\mathbb{R}$ není podprostorem $\mathbb{C}^n$ nad $\mathbb{C}$, ani naopak.*

Další příklady podporstorů přidáme použitím množinových operací. Z názorné geometrické představy je dobře vidět, že průnik dvou podprostorů je opět podprostor. Je také snadné si najít názorný příklad toho, že sjednocení dvou podprostorů nemusí být (a zpravidla není) podprostor. Stačí si představit sjednocení dvou různých přímek (procházejících počátkem) v rovině. Proto se zavádí pojem 'spojení dvou (nebo více) podprostorů'.

Definice 2 *Nechť I je indexová množina a $\{W_i | i \in I\}$ je systém podprostorů vektorového prostoru V. Definujme **spojení** $\bigvee_{i\in I} W_i$ těchto podprostorů jako množinu všech vektorů tvaru $\sum_{j\in J} w_j$, kde $J \subset I$ je nějaká konečná podmnožina, $w_j \in W_j$.*

Spojení dvou podprostorů se značí $W_1 \vee W_2$. Rozmyslete si na příkladech, jaký je rozdíl mezi spojením a sjednocením. Kdy je sjednocení dvou vektorových podprostorů také vektorový podprostor?

Věta 2 *Nechť V je vektorový prostor, I je indexová množina a $\{W_i, i \in I\}$ je systém podprostorů prostoru V indexovaných I. Pak platí:*

1. *Průnik těchto podprostorů $\bigcap_{i\in I} W_i$ je podprostorem V. Navíc pro každý podprostor $U \leq V$, pro nějž $\forall i \in I$, $U \leq W_i$, platí také $U \leq \bigcap_{i\in I} W_i$.*

2. *Spojení těchto podprostorů $\bigvee_{i\in I} W_i$ je podprostorem V. Navíc pro každý podprostor $U \leq V$, pro nějž $\forall i \in I$, $W_i \leq U$, platí také $\bigvee_{i\in I} W_i \leq U$.*

Důkaz: Nechť $r, s \in \mathbb{R}$.

1. Pokud $u, v \in \bigcap_{i\in I} W_i$, pak $\forall i \in I$, $u, v \in W_i$. Všechny W_i jsou podprostory, tedy $\forall i \in I$, $ru + sv \in W_i$, čili $ru + sv \in \bigcap_{i\in I} W_i$. Druhá část je zřejmá, protože každý podprostor U všech W_i je jejich podmnožinou, tudíž také podmnožinou jejich průniku. Protože je U uzavřen na operace, je také podprostorem $\bigcap_{i\in I} W_i$.

2. Nechť $u, v \in \bigvee_{i\in I} W_i$, tedy existují konečné množiny J, K a vektory $u_j \in W_j, j \in J$, a $v_k \in W_k, k \in K$ takové, že platí $u = \sum_{j\in J} u_j$ a $v = \sum_{k\in K} v_k$. Pak tedy $ru + sv = \sum_{j\in J} ru_j + \sum_{k\in K} sv_k$ je součet konečně mnoha prvků z jednotlivých podprostorů $W_\ell, \ell \in J \cup K$, a tedy patří do $\bigvee_{i\in I} W_i$. Tím je dokázána první část druhého tvrzení.

   Pokud U je podprostor V takový, že $W_i \leq U$ pro všechna $i \in I$ a $w \in \bigvee_{i\in I} W_i$, pak pro nějakou konečnou množinu $J \subset I$ a pro všechna $j \in J$ existují vektory $w_j \in W_j$ takové, že $w = \sum_{j\in J} w_j$. Protože $\forall j \in J, W_j \leq U$, je pro tato j také $w_j \in U$. Z uzavřenosti U na součty vektorů $w \equiv \sum_{j\in J} w_j \in U$, což jsme měli dokázat.

□

Druhé části obou tvrzení vlastně říkají, že průnik je největší (vzhledem k inkluzi) podprostor obsažený ve všech podprostorech v systému a spojení je nejmenší (vzhledem k inkluzi) podprostor, který obsahuje všechny podprostory v systému (což je možné vzít za ekvivalentní a názornější definici spojení podprostorů). Je důležité mít na paměti, že v definici spojení figurují pouze konečné součty, protože nekonečné součty nemáme (bez prostředků matematické analýzy) definovány.

2.3 Generátory, lineární nezávislost, baze, dimenze

Jak víme, (netriviální) podprostory v $\mathbb{R}^3$ jsou přímky nebo roviny obsahující počátek. Přímka i rovina se skládají z nekonečné množiny bodů, ale intuitivně je zřejmé, že rovina má 'víc bodů' než přímka. Říkáme často, že přímka je jednodimenzionální (její body závisí na jednom reálném parametru) a rovina je dvoudimenzionální (její body závisí na dvou libovolných reálných parametrech). Cílem této části je zavést si pojem dimenze vektorového prostoru, který bude klasifikovat, jak jsou vektorové prostory velké.

Definice 10 *Nechť V je vektorový prostor. Jsou-li dány konečná množina vektorů $M = \{v_1, \ldots, v_n\} \subset V$, pak každý vektor $w \in V$ tvaru*

$$w = \alpha_1.v_1 + \ldots + \alpha_n.v_n,\ \alpha_1, \ldots, \alpha_n \in \mathbb{T}$$

nazveme lineární kombinací vektorů z množiny M. Řekneme, že lineární kombinace je triviální, pokud všechny koeficienty $\alpha_i, i = 1, \ldots, n$ jsou rovny nule. V opačném případě nazveme lineární kombinaci netriviální.

Nechť M je libovolná podmnožina V. Lineární obal $\langle M \rangle$ množiny M je množina všech lineárních kombinací vektorů ze všech konečných podmnožin $x_1, \ldots, x_n$ množiny M.

Pokud pro množinu $M \subset V$ platí, že $\langle M \rangle = V$, pak řekneme, že množina M generuje V. Prvky množiny M se nazývají generátory V.

Řekneme, že vektorový prostor V je konečně generovaný, pokud existuje konečná množina $M \subset V$, která ho generuje.

Stejně jako v případě spojení vektorových podprostorů, i tady si můžeme formulovat ekvivalentní definici lineárního obalu množiny M. Vektorový podprostor W je lineárním obalem množiny M, pokud W je nejmenší podprostor ve V obsahující M. (Odůvodnění si rozmyslete sami, lze to udělat stejně jako pro případ spojení vektorových podprostorů.) Pokud $M = \emptyset$, pak $\langle M \rangle$ je definován jako triviální vektorový prostor $\{o\}$. Pro M neprázdnou definice znamená, že každý vektor z $w \in W$ lze zapsat jako lineární kombinaci konečného počtu vektorů z M, $w = \sum_{i=1}^{k} r_i v_i$, $v_i \in M$.

Množina generátorů je způsob, jak při popisu podprostoru nevypisovat všechny vektory v něm, ale vystačit si jen s některými. Pokud dále některé z nich jdou vyjádřit pomocí jiných, lze je vynechat a dosáhnout tak popisu efektivnějšího. K tomu slouží pojem lineární závislosti.

Definice 3 *Nechť M je neprázdná množina vektorů z vektorového prostoru V. Řekneme, že M je **lineárně závislá**, pokud existuje netriviální lineární kombinace prvků M, jejímž výsledkem je nulový vektor. V opačném případě je M **lineárně nezávislá**.*

Triviální kombinace samozřejmě dává nulový vektor vždy, jde tedy o to, zda existuje ještě nějaká jiná. Pokud například skupina vektorů $v_1, v_2, \ldots, v_k$ obsahuje nulový vektor, dejme tomu na pozici j, pak stačí vzít $r_j = 1$ a ostatní $r_i = 0$ a pak máme $\sum_{i=1}^{k} r_i v_i = 0$, tedy množina $M = \{v_1, v_2, \ldots, v_k\}$ je lineárně závislá. Podobně pokud množina obsahuje s vektorem v také nějaký jeho další násobek rv, je lineárně závislá, protože stačí brát koeficienty $-r$ a 1 u těchto dvou vektorů a vynulovat koeficienty ostatní.

Je užitečné si uvědomit následující jednoduché tvrzení.

Množina je lineárně závislá právě tehdy, když lze nějaký její vektor vyjádřit jako lineární kombinaci ostatních. Vskutku, rovnost $v = \sum_{i=1}^{k} r_i v_i$ snadno přepíšeme na $0 = v - \sum_{i=1}^{k} r_i v_i$ a naopak z netriviální lineární kombinace $\sum_{i=1}^{j} s_i u_i$ můžeme vyjádřit kterýkoli vektor u_i s nenulovým koeficientem s_i pomocí ostatních.

Platí také několik následujících snadných tvrzení, které jsou jednoduchým důsledkem výše uvedených definic.

1. Pokud je množina M lineárně závislá, pak je lineárně závislá i každá její nadmnožina (protože každá netriviální lineární kombinace prvků z M je totiž zároveň lineární kombinací prvků z každé nadmnožiny).

2. Pokud je množina M lineárně nezávislá, pak je lineárně nezávislá i každá její podmnožina.

3. Pokud je množina M lineárně nezávislá a $v \in V$, pak $M' = M \cup \{v\}$ je také lineárně nezávislá právě když $v \notin \langle M \rangle$.

4. Pokud M generuje vektorový prostor V, pak jej generuje i každá $N \subset V$, která je nadmnožinou M.

Definice 4 *Lineárně nezávislá množina, která generuje vektorový prostor $V \neq 0$, se nazývá **baze** V. Pokud $V = \{o\}$, je jeho bazí prázdná množina. **Dimenze** konečně generovaného vektorového prostoru V je počet prvků (libovolné) baze V.*

Vektorový prostor V dimenze n budeme značit symbolem V_n. Baze je klíčový pojem lineární algebry, protože nám umožňuje definovat pojem dimenze jakožto počet prvků libovolné baze. V tomto kurzu se soustředíme na prostory, které mají dimenzi konečnou. Baze tak, jak ji budeme definovat, stejně není v prostorech nekonečné dimenze příliš užitečným pojmem - sice vždy existuje (za předpokladu platnosti axiomu výběru), ale v mnoha běžných případech nelze žádnou konkrétní zkonstruovat.

V definici baze jsou dvě podezřelé věci. Ta podstatná je otázka, jestli všechny baze (konečně generovaného) vektorového prostoru mají stejný počet prvků, aby pojem dimenze byl dobře definován. Další věc, kterou je třeba vyjasnit je to, jestli mají baze konečně generovaných vektorových prostorů opravdu jen konečně mnoho prvků.

Lemma 3 *Pokud V je konečně generovaný vektorový prostor, pak z každé jeho množiny generátorů lze vybrat konečnou bazi.*

Důkaz: Můžeme předpokládat, že V je netriviální. Nejprve ukážeme, že z každé nekonečné množiny generátorů M prostoru $V \neq 0$ lze vybrat konečnou podmnožinu, která také generuje V. Protože V je konečně generovaný, existuje množina $N = \{v_1, \ldots, v_k\}$, která generuje V. Protože M generuje V, lze každý vektor z N zapsat jako lineární kombinaci prvků z M, $v_i = \sum_{j=1}^{k_i} r_{ij} u_{ij}$. Označme $M_i = \{u_{i1}, \ldots, u_{ik_i}\}$. Libovolný vektor $v \in V$ lze zapsat jako lineární kombinaci prvků z N a tedy

$$v = \sum_{i=1}^{k} s_i v_i = \sum_{i=1}^{k} \sum_{j=1}^{k_i} (s_i r_{ij}) u_{ij}$$

také jako lineární kombinaci prvků z $M' := \bigcup_{i=1}^{k} M_i$. Tedy M' je hledaná konečná podmnožina.

Lze tedy předpokládat, že množina generátorů M je konečná. Pokud je množina M lineárně nezávislá, pak je to hledaná baze. Pokud je lineárně závislá, pak je existuje netriviální lineární kombinace $\sum_{i=1}^{n} r_i v_i = 0$, a je tedy možné některý z vektorů v_j vyjádřit pomocí ostatních jako $v_j = -\frac{1}{r_j} \sum_{i \neq j} r_i v_i$. Libovolný vektor $v \in V$ pak lze napsat jako

$$v = \sum_{i=1}^{n} s_i v_i = \sum_{i \neq j} s_i v_i - \frac{s_j}{r_j} \sum_{i \neq j} r_i v_i = \sum_{i \neq j} \left(s_i - \frac{s_j}{r_j} r_i \right) v_i,$$

tedy jako lineární kombinaci prvků $M_1 = M \setminus \{v_j\}$.

Nyní můžeme úvahu opakovat. Pokud je množina M_1 lineárně nezávislá, je to hledaná baze. Pokud je lineárně závislá, je možno stejným postupem ukázat, že i po vynechání vhodného prvku z M_1 generuje zbylá množina M_2 celé V. Je zřejmé, že po konečném počtu kroků (nejpozději až zbyde jen jeden nenulový vektor) dojdeme k množině $M_j \subset M$, která je bazí V.

□

Následující tvrzení vešlo pod známost pod názvem Steinitzova věta nebo Steinitzovo lemma o výměně. Říká, že v množině generátorů můžeme vyměnit vhodné prvky "kus za kus" s prvky nějaké lineárně nezávislé množiny tak, abychom po výměně měli stále množinu generátorů. Důsledkem bude mimojiné skutečnost, že všechny báze mají stejný počet prvků, a tedy že dimenze je dobře definována.

Věta 3 *(Steinitz)*

Buď $M = \{u_1, \ldots, u_n\}, n \geq 1$ množina generátorů vektorového prostoru V a $N = \{v_1, \ldots, v_k\}, k \geq 1$ lineárně nezávislá množina ve V. Pak $k \leq n$ a při vhodném očíslování vektorů $u_1, \ldots, u_n$ množina $\{v_1, \ldots, v_k, u_{k+1}, \ldots u_n\}$ generuje V.

Důkaz: Budeme postupovat indukcí podle počtu k prvků množiny N. Pokud $k = 1$, pak jistě platí $1 \leq n$. Protože M generuje V, existují čísla r_i taková, že $v_1 = \sum_{i=1}^{n} r_i u_i$, a protože $v_1 \neq 0$, musí pro některý index j být $r_j \neq 0$. Pokud $j \neq 1$, pak přečíslujeme vektory u_i, aby $r_1 \neq 0$. Lze tedy psát $u_1 = \frac{1}{r_1} v_1 - \sum_{i=2}^{n} \frac{r_i}{r_1} u_i$. Každý vektor, který je lineární kombinací $u_1, \ldots, u_n$, je tudíž také lineární kombinací $v_1, u_2, \ldots, u_n$, čili $\langle v_1, u_2, \ldots, u_n \rangle = V$.

Předpokládejme proto platnost tvrzení pro $k - 1$, ukážeme, že pak musí platit i pro k. Pokud $\{v_1, \ldots, v_k\}$ jsou lineárně nezávislé, pak $\{v_1, \ldots, v_{k-1}\}$ jsou lineárně nezávislé a podle indukčního předpokladu množina

$$\{v_1, \ldots, v_{k-1}, u_k, \ldots, u_n\}$$

generuje V a $n \geq k - 1$.

Nejdříve ukážeme, že $n \geq k$. Kdyby totiž platilo $n = k - 1$, pak by byl vektor v_k lineární kombinací vektorů $v_1, \ldots, v_{k-1}$, což je ve sporu s lineární nezávislostí množiny $\{v_1, \ldots, v_k\}$.

Tedy v_k lze vyjádřit jako $\sum_{i=1}^{k-1} r_i v_i + \sum_{i=k}^{n} r_i u_i$, kde pro nějaké $j \geq k$ musí být $r_j \neq 0$, jinak bychom opět dostali spor s lineární nezávislostí množiny $\{v_1, \ldots, v_k\}$. Přečíslujme zbylé vektory $u_k, \ldots, u_n$ tak, aby $j = k$, pak je možné podobně jako v případě $k = 1$ vyjádřit u_k jako lineární kombinaci množiny $\{v_1, \ldots, v_k, u_{k+1}, \ldots, u_n\}$, a tedy i libovolný vektor jako lineární kombinaci vektorů z této množiny. □

Jako přímé důsledky Stenitzovy věty dostaneme následující tvrzení (odůvodnění si rozmyslete sami!):

1. Nechť V je konečně generovaný vektorový prostor. Pak všechny baze V mají stejný (konečný) počet prvků. Dimenze vektorového prostoru je tedy dobře definovaný pojem.

2. Je-li V konečně generovaný vektorový prostor a W podprostor V, pak také W je konečně generovaný.

3. Je-li W podprostor V, pak lze libovolnou bazi W doplnit na bazi V.

4. Nechť je $\dim V = n$. Je-li množina $N = \{v_1, \ldots, v_k\}$ lineárně nezávislá, pak $k \leq n$, a pokud $k = n$, pak je N baze V.

5. Nechť je $\dim V = n$. Pokud pro množinu $M = \{u_1, \ldots, u_k\}$ platí $\langle M \rangle = V$, pak $k \geq n$, a pokud $k = n$, pak M je baze V.

Poslední dvě tvrzení říkají (v nepřesném, ale intuitivně srozumitelném vyjádření), že baze jsou největší lineárně nezávislé množiny a nejmenší množiny generátorů.

Uveďme si nyní několik příkladů bazí a dimenzí podprostorů, jimiž jsme se dosud zabývali.

1. Množina vektorů $\{e_1, \ldots, e_n\}$ aritmetického vektorového prostoru $\mathbb{T}^n$, kde

$$\begin{aligned} e_1 &= (1, 0, 0, \ldots, 0, 0), \\ e_2 &= (0, 1, 0, \ldots, 0, 0), \\ &\vdots \\ e_n &= (0, 0, 0, \ldots, 0, 1), \end{aligned}$$

   se nazývá **kanonická baze**. Tedy $\dim \mathbb{T}^n = n$.

2. Množina matic $\{E_{ij}, i \in \{1, \ldots, n\}, j \in \{1, \ldots, m\}\}$, kde E_{ij} je matice, jejíž ij-tý element je 1 a ostatní 0, je baze prostoru $M_{mn}(\mathbb{T})$ nad $\mathbb{T}$ dimenze mn.

3. Množina $\{1, x, x^2, \ldots\}$ je baze prostoru všech polynomů $P(x, \mathbb{T})$ nad $\mathbb{T}$. Není to tedy prostor konečné dimenze.

4. Množina $\{(1, 0), (i, 0), (0, 1), (0, i)\}$ je baze prostoru $\mathbb{C}^2$ nad $\mathbb{R}$. Tento prostor má tedy dimenzi 4, zatímco $\mathbb{C}^2$ nad $\mathbb{C}$ má dimenzi 2.

Další důležité příklady uvidíme v následující přednášce, v níž se budeme zabývat vztahem dimenze a řešení soustavy lineárních rovnic.

Věta 4 (o dimenzi spojení a průniku) *Nechť V je vektorový prostor a U, W jsou dva jeho podprostory konečné dimenze. Pak*

$$\dim U + \dim W = \dim U \cap W + \dim U \vee W$$

Důkaz: Prostor $U \cap W$ je podprostorem prostoru W a je tedy také konečné dimenze. Zvolme v něm libovolnou bázi $\{v_1, \ldots, v_k\}$, tuto bázi lze doplnit vektory $u_1, \ldots, u_p$ na bázi U a vektory $w_1, \ldots, w_q$ na bázi W. Ukážeme, že množina $M = \{u_1, \ldots, u_p, v_1, \ldots, v_k, w_1, \ldots, w_q\}$ je bází $U \vee W$.

Je zřejmé, že M generuje $U \vee W$. Každý vektor $v \in U \vee W$ je součtem nějakého vektoru $u \in U$ a nějakého vektoru $w \in W$. Každý z nich je lineární kombinací prvků M a tedy i v je lineární kombinací prvků M. Předpokládejme nyní, že

$$0 = \sum_{i=1}^{p} r_i u_i + \sum_{i=1}^{k} s_i v_i + \sum_{i=1}^{q} t_i w_i$$

Tedy vektor

$$u = -\sum_{i=1}^{p} r_i u_i = \sum_{i=1}^{k} s_i v_i + \sum_{i=1}^{q} t_i w_i$$

je zároveň prvkem U a W, tedy prvkem jejich průniku. Je proto možné jej vyjádřit jako $u = \sum_{i=1}^{k} x_i v_i$. Pak ale

$$\sum_{i=1}^{k} x_i v_i + \sum_{i=1}^{p} r_i u_i = 0$$
$$\sum_{i=1}^{k} (s_i - x_i) v_i + \sum_{i=1}^{q} t_i w_i = 0$$

Jelikož množiny $\{u_1, \ldots, u_p, v_1, \ldots, v_k\}$ a $\{v_1, \ldots, v_k, w_1, \ldots, w_q\}$ jsou lineárně nezávislé, musí být v obou rovnostech všechny koeficienty nulové. To ale znamaná, že i množina M je lineárně nezávislá.

Zkonstruovali jsme tedy z báze prostoru $U \cap W$ báze prostorů U, W a $U \vee W$. Dokazovaná rovnost plyne prostým dosazením počtů prvků těchto bází: $(p + k) + (k + q) = k + (p + k + q)$. □

Speciální případ věty o dimenzi spojení a průniku nastává, pokud platí $U \cap W = \{o\}$. Pak mluvíme místo o spojení o **direktním součtu** $U \oplus W$ podprostorů. Stejně jako spojení, i direktní součet má smysl definovat i pro více prostorů:

Definice 5 *Nechť V je vektorový prostor, I indexová množina a $\{W_i | i \in I\}$ systém podprostorů V indexovaný touto množinou. Řekneme, že V je přímý*

(direktní) součet podprostorů $W_i, i \in I$ a označíme to symbolem

$$V = \bigoplus_{i \in I} W_i,$$

pokud:

(i) $V = \bigvee_{i \in I} W_i$

(ii) pro každé $j \in I$ *platí* $W_j \cap \left(\bigvee_{i \neq j} W_i \right) = \{o\}$.

Věta 5 *Nechť V je vektorový prostor, I indexová množina, $\{W_i | i \in I\}$ systém podprostorů V a $\bigvee_{i \in I} W_i = V$. Pak platí $V = \bigoplus_{i \in I} W_i$ právě když pro každý vektor $v \in V$ existuje právě jedno vyjádření ve tvaru*

$$v = \sum_{j \in J} w_j,$$

kde J je konečná množina I a kde $w_j \in W_j, j \in J$ jsou nenulové vektory.

Důkaz: Pro důkaz ekvivalence musíme dokázat obě implikace.

(i) $\Rightarrow$: Existence požadovaného zápisu $v = \sum_{j \in J} w_j$ plyne z definice $\bigvee_{i \in I} W_i$, přičemž jistě můžeme vzít takový zápis, v němž jsou všechny vektory w_j nenulové. Pokud by existoval druhý takový zápis $v = \sum_{k \in K} w'_k$, pak $0 = \sum_{i \in J \cup K} (w_i - w'_i)$, kde jsme dodefinovali $w_i = 0$ pro $i \in K \setminus J$ a $w'_i = 0$ pro $i \in J \setminus K$. Pro každé $j \in J \cup K$ je

$$w_j - w'_j = - \sum_{\substack{i \in (J \cup K) \\ i \neq j}} (w_i - w'_i) \in W_j \cap \left(\bigvee_{\substack{i \in I \\ i \neq j}} W_i \right),$$

což je podle předpokladu nulový podprostor, tudíž oba zápisy jsou totožné.

(i) $\Leftarrow$: Naopak, předpokládejme, že rozklad $v = \sum_{j \in J} W_j$ je jednoznačný, chceme ukázat, že $V = \bigoplus_{j \in J} W_j$, tj. (podle definice), že pro každé $j \in I$ platí $W_j \cap \left(\bigvee_{i \neq j} W_i \right) = \{o\}$.

Zvolme $j \in I$ pevně. Pokud by existoval nenulový vektor $v \in W_j \cap \left(\bigvee_{i \neq j} W_i \right)$, pak tedy existuje konečná podmonžina $K \subset (J \setminus \{j\})$ a vektory $w_k \in W_k, k \in K$ takové, že

$$v = \sum_{k \in K} w_k.$$

Pak ale $o = \sum_{k \in K} w_k - v$ a nulový vektor je vyjádřen pomocí dvou různých součtů (vždy je možné napsat o jako triviální součet!), což je spor s předpokládanou jednoznačností rozkladu. □

Věta 6 *Nechť $W_1, \ldots, W_k$ jsou podprostory V_n takové, že $\bigoplus_{i=1}^{k} W_i$ existuje. Pak*

$$\sum_{i=1}^{k} \dim W_i = \dim \bigoplus_{i=1}^{k} W_i$$

Důkaz: Budeme postupovat matematickou indukcí. Pro $k = 2$ tvrzení plyne z věty o dimenzi spojení a průniku. Předpokládejme tedy, že platí pro $k - 1$. Uvažujme podprostory $W_1, \ldots, W_k$ takové, že $\bigoplus_{i=1}^{k} W_i$ existuje. Pak

$$\forall j \in \{1, \ldots, k\}, \quad W_j \cap \bigvee_{\substack{i=1 \\ i \neq j}}^{k} W_i = 0$$

a tím pádem také

$$\forall j \in \{1, \ldots, k-1\}, \quad W_j \cap \bigvee_{\substack{i=1 \\ i \neq j}}^{k-1} W_i = 0$$

Tedy $\bigoplus_{i=1}^{k-1} W_i$ existuje a podle indukčního předpokladu $\sum_{i=1}^{k-1} \dim W_i = \dim \bigoplus_{i=1}^{k-1} W_i$. Protože $W_k \cap \bigoplus_{i=1}^{k-1} W_i = 0$, plyne z věty o dimenzi spojení a průniku

$$\dim \bigoplus_{i=1}^{k} W_i = \dim W_k + \dim \bigoplus_{i=1}^{k-1} W_i = \sum_{i=1}^{k} \dim W_i.$$

□

3 Hodnost matice

V předchozí části přednášky jsem si definovali zakladní pojmy týkající se skupiny vektorů M ve vektorovém prostoru V - lineární obal $\langle M \rangle$, lineární závislost a lineární nezávislost, pojem baze a dimenze vektorového podprostoru. Nyní bychom se chtěli naučit, jak v konkrétních případech zjistit, zda je skupina vektorů lineárně závislá či nezávislá; jak spočítat dimenzi lineárního obalu dané množiny. K tomu se nám bude hodit následující informace.

Lemma 4 *Nechť $M_0 = (v_1, \ldots, v_p)$ je skupina vektorů ve vektorovém prostoru V nad $\mathbb{T}$, $j, k \in \{1, \ldots, p\}$, $j \neq k$, $r, s \in \mathbb{T}$, $r \neq 0$. Označme*

$$M_1 = (v_1, \ldots, v_{k-1}, rv_k, v_{k+1}, \ldots, v_p)$$
$$M_2 = (v_1, \ldots, v_{k-1}, v_k + sv_j, v_{k+1}, \ldots, v_p)$$

Pak platí, že $\langle M_0 \rangle = \langle M_1 \rangle = \langle M_2 \rangle$. Dále platí, že M_0 je lineárně nezávislá, právě když je lineárně nezávislá M_1 a právě když je lineárně nezávislá M_2.

Důkaz: Dokážeme tvrzení pouze pro M_2, případ M_1 je zcela analogický a vlastně jednodušší. Pokud $v \in \langle M_0 \rangle$, pak existují $r_i \in \mathbb{T}$, že $v = \sum_{i=1}^{p} r_i v_i$. Pro pohodlí předpokládejme $k < j$. Pak lze v zapsat také jako

$$v = \sum_{i=1}^{k-1} r_i v_i + r_k(v_k + sv_j) + \sum_{i=k+1}^{j-1} r_i v_i + (r_j - sr_k)v_j + \sum_{i=j+1}^{p} r_i v_i,$$

tedy $v \in \langle M_2 \rangle$. Naopak pokud $v \in \langle M_2 \rangle$, pak existují $s_i \in \mathbb{T}$ taková, že

$$v = \sum_{i=1}^{k-1} s_i v_i + s_k(v_k + sv_j) + \sum_{i=k+1}^{p} s_i v_i,$$

můžeme přepisem získat

$$v = \sum_{i=1}^{j-1} s_i v_i + (s_k s + s_j)v_j + \sum_{i=j+1}^{p} s_i v_i,$$

čili $v \in \langle M_0 \rangle$. Tím jsme dokázali obě inkluze $\langle M_0 \rangle \subset \langle M_2 \rangle$ i $\langle M_2 \rangle \subset \langle M_0 \rangle$ a tím pádem rovnost obou množin.

Podobně ověříme, že se zachovává lineární (ne)závislost. Pokud M_2 je lineárně nezávislá a $\sum_{i=1}^{p} r_i v_i = 0$, pak musí být v lineární kombinaci

$$\sum_{i=1}^{k-1} r_i v_i + r_k(v_k + sv_j) + \sum_{i=k+1}^{j-1} r_i v_i + (r_j - sr_k)v_j + \sum_{i=j+1}^{p} r_i v_i,$$

prvků M_2 všechny koeficienty nulové. To ale znamená $r_i = 0$, pokud i není k ani j, dále $r_k = 0$, a díky tomu $r_j = r_j - sr_k = 0$. Tedy lineární kombinace $\sum_{i=1}^{p} r_i v_i$ musí být triviální, a tedy M_0 je lineárně nezávislá. Stejným způsobem lze ověřit opačnou implikaci. □

Z lemmatu ihned plyne, že se také při elementárních transformacích zachovává dimenze lineárního obalu a vlastnosti "býti bází lineárního obalu".

Podstatnou informací pro podobné výpočty je následující jednoduché tvrzení:

Lemma 5 *Je-li matice A v odstupňovaném tvaru a je-li $M = \{r_1, \ldots, r_\ell\}$ množina všech netriviálních řádků matice A, pak je množina M lineárně nezávislá a tvoří bazi lineárního obalu $\langle M \rangle$. Dimenze $\langle M \rangle$ je tedy rovna ℓ, tj. počtu netriviálních řádků matice A.*

Odůvodnění je prosté. Předpokládejme, že $\sum_{j=1}^{\ell} \alpha_i r_i = o$, chceme dokázat, že pak všechny koeficienty $\alpha_i, i = 1, \ldots \ell$ jsou nulové. Podíváme se nejdřív na první pivotní sloupec. Pro něj $a_{1,i_1} \neq 0$ a $a_{2,i_1} = \ldots a_{\ell,i_1} = 0$. Tedy $a_{1,i_1}\alpha_1 + 0 \cdot \alpha_2 + \ldots + 0 \cdot \alpha_\ell = 0$, tedy $\alpha_1 = 0$. Pak vynecháme první řádek r_1 matice A a stejnou úvahu opakujeme.

Chceme-li zjistit lineární nezávislost (nebo dimenzi lineárního obalu) pro skupinu vektorů z aritmetického vektorového prostoru, sestavíme matici, která bude mít tyto vektory jako řádky, a pomocí Gaussova algoritmu převedeme matici do odstupňovaného tvaru, ve kterém je příslušná vlastnost vidět na první pohled.

Příklad 2 *Určeme dimenzi lineárního obalu množiny $\{(3, -6, 1, -1), (1, -2, 3, 1), (-2, 4, 0, 1), (0, 0, 2, 1)\}$ v $\mathbb{R}^4$. Úpravou vhodné matice*

$$\begin{pmatrix} 1 & -2 & 3 & 1 \\ 3 & -6 & 1 & -1 \\ -2 & 4 & 0 & 1 \\ 0 & 0 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 3 & 1 \\ 0 & 0 & -8 & -4 \\ 0 & 0 & 6 & 3 \\ 0 & 0 & 2 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -2 & 3 & 1 \\ 0 & 0 & -8 & -4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

zjišťujeme, že dimenze je 2. Při úpravě můžeme vynechat nulové řádky, tím se lineární obal ani dimenze nezmění.

Dimenze lineárního obalu řádků dané matice je podstatná informace o příslušné matici, která má svůj vlastní název, který si zavedeme v následující definici.

Definice 6 *Nechť $A \in M_{mn}(\mathbb{T})$ je matice. Jejím **řádkovým podprostorem** R_A rozumíme lineární obal skupiny všech m řádků matice A, chápaných jako vektory ve vektorovém prostoru $\mathbb{T}^n$. **Hodnost** $h(A)$ **matice** A definujeme jako dimenzi prostoru R_A.*

Sloupcový podprostor *S_A matice A je lineární obal skupiny všech n sloupců matice A, chápaných jako prvky $\mathbb{T}^m$.*

Předchozí lemma tedy říká, že elementárními úpravami matice se zachovává řádkový prostor a tedy i hodnost matice. Tím pádem také víme, jak hodnost matice spočítat. Stačí matici převést do odstupňovaného tvaru, v něm už je skupina všech nenulových řádků lineárně nezávislá (rozmyslete si proč). Hodnost (původní i upravené) matice je potom rovna počtu nenulových řádků v matici v odstupňovaném tvaru.

Pokud jsme si zavedli zvlaštní název hodnost matice pro dimenzi řádkového prostoru R_A matice A, neměli bychom si také nějak nazvat dimenzi sloupcového prostoru S_A? Pro hodnost matice platí jedno docela záhadné a nečekané tvrzení - dimenze S_A je vždy stejná jako dimenze R_A. Totéž se dá vyjádřit pomocí následujících pojmů pro reálné, resp. komplexní, matice.

Definice 7 *Nechť $A \in M_{mn}(\mathbb{T})$ je matice. Pak matici $A^T \in M_{nm}(\mathbb{T})$, jejíž ij-tý element je definován vztahem $a^T_{ij} := a_{ji}$, nazveme* ***maticí transponovanou*** *k A.*

Pokud $\mathbb{T} = \mathbb{C}$ a $\bar{r}$ označuje komplexně sdružené číslo k $r \in \mathbb{C}$, pak matice $A^\dagger \in M_{nm}(\mathbb{T})$, kde ij-tý element je $a^\dagger_{ij} := \bar{a}_{ji}$, nazveme ***maticí hermitovsky sdruženou*** *k A.*

Matici transponovanou tedy získáme prostým překlopením podle diagonály, takže z i-tého řádku v A se stane i-tý sloupec v A^T. Hermitovské sdružení je transpozice následovaná komplexním sdružením.

Věta 7 *Nechť $A \in M_{mn}(\mathbb{R})$, pak $h(A) = h(A^T)$. Nechť $B \in M_{mn}(\mathbb{C})$, pak $h(B) = h(B^\dagger)$.*

Tvrzení $h(A) = h(A^T)$ vlastně říká, že dimenze řádkového a sloupcového prostoru A je stejná. To je opravdu záhadné a neočekávané, protože jsou to podprostory ve dvou obecně různých aritmetických vektorových prostorech, $\mathbb{R}^n$ a $\mathbb{R}^m$! Větu bychom mohli dokázat (dosti složitým) ověřením , že ačkoli se při řádkových úpravách matice mění její sloupcový prostor, jeho dimenze se zachovává. Podobným postupem bychom dokázali i $h(B) = h(B^\dagger)$. My ale důkaz odložíme až na dobu, kdy budeme mít definovány pojmy lineárního zobrazení a skalárního součinu, které dodají novou interpretaci hodnosti matice a transponované matici. Důkaz využívající tuto interpretaci je přehlednější a jistým způsobem v sobě lépe nese smysl dokazovaného tvrzení.

Tato klíčová věta má několik důsledků.

Věta 8 *Nechť $A \in M_{mn}(\mathbb{T})$, $B \in M_{np}(\mathbb{T})$ jsou matice. Pak*

$$h(AB) \leq h(A), \;\; h(AB) \leq h(B)$$

Důkaz: Sloupce matice AB jsou lineární kombinací sloupců matice A, tedy $S_{AB} \leq S_A$ a tedy $h(AB) \leq h(A)$. Řádky AB jsou zase lineární kombinací řádků B, takže i $h(AB) \leq h(B)$. □

Věta 9 *Nechť $A \in M_{nn}(\mathbb{T})$ je čtvercová matice. Pak A je regulární právě když $h(A) = n$.*

Důkaz:

Pokud A je regulární, pak má inverzní matici A^{-1}, $A^{-1}A = E_n$. Podle předchozí věty tedy $n = h(E_n) = h(A^{-1}A) \leq h(A)$. Řádkové prostory matic A a A^{-1} jsou podprostory $\mathbb{T}^n$, tedy také $h(A) \leq n$. Musí být tedy $h(A) = n$.

Pokud naopak $h(A) = n$, pak po převedení matice A elementárními úpravami do redukovaného odstupňovaného tvaru bude výsledkem zřejmě jednotková matice. Pak stačí použít již dokázané Lemma 5. □

Věta 10 *Nechť $A \in M_{mn}(\mathbb{T})$ je libovolná matice, $B \in M_{mm}(\mathbb{T})$, $C \in M_{nn}(\mathbb{T})$ jsou regulární matice. Pak $h(BAC) = h(A)$.*

Důkaz: Platí $h(BAC) \leq h(BA) \leq h(A)$ a také $h(A) = h(B^{-1}BACC^{-1}) \leq h(A) = h(BACC^{-1}) \leq h(BAC)$. □

3.1 Frobeniova věta

Kritérium řešitelnosti soustavy rovnic je možné elegantně vyjádřit pomocí hodnosti matice. Nejdříve popíšeme pomocí hodnosti matic množinu všech řešení homogenní soustavy. Následující tvrzení je zásadně důležité pro popis množiny všech řešení lineárních rovnic z následujícího důvodu. Víme již, že velmi často je množina všech řešení nekonečná. Popsat množinu řešení, která má nekonečně mnoho prvků je problém, který je například prakticky neřešitelný pro množiny řešení soustav nelineárních (např. polynomiálních) rovnic. Speciální vlastností soustav lineárních rovnic, je že množina řešení homogenní soustavy má strukturu vektorového prostoru! Stačí tedy najít nějakou (konečnou) bazi tohoto prostoru a všechny jeho prvky jsou (libovolné) lineární kombinace této baze. Navíc dimenze tohoto prostoru měří velikost prostoru řešení a říká, na kolika parametrech množina všech řešení závisí.

Věta 11 *Nechť $A \in M_{mn}(\mathbb{T})$ je matice. Množina řešení homogenní soustavy rovnic $Ax = 0$ s maticí A tvoří vektorový podprostor v $\mathbb{T}^n$. Jeho dimenze $n - h(A)$.*

Důkaz: Už jsme zmiňovali, že množina řešení homogenní soustavy rovnic je podprostor $\mathbb{T}^n$. Upravme matici A na redukovaný odstupňovaný tvar, z nějž vynecháme všechny nulové řádky. Počet nenulových řádků se rovná $p = h(A)$, tedy existuje právě $q := n - h(A)$ nepivotních sloupců. Pro přehlednost můžeme přeuspořádat neznámé tak, aby pivotními sloupci byly sloupce $1, \ldots, p$. Upravená matice pak má tvar

$$\begin{pmatrix} 1 & 0 & \ldots & 0 & c_{11} & c_{12} & \ldots & c_{1q} \\ 0 & 1 & \ldots & 0 & c_{21} & c_{22} & \ldots & c_{2q} \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \ldots & 1 & c_{p1} & c_{p2} & \ldots & c_{pq} \end{pmatrix},$$

čímž jsme definovali matici $C \in M_{pq}(\mathbb{T})$. Množina vektorů

$$\begin{aligned} M = \{&(-c_{11}, -c_{21}, \ldots, -c_{p1}, 1, 0, \ldots, 0) \\ &(-c_{12}, -c_{22}, \ldots, -c_{p2}, 0, 1, \ldots, 0) \\ &\vdots \\ &(-c_{1q}, -c_{2q}, \ldots, -c_{pq}, 0, 0, \ldots, 1)\} \end{aligned}$$

je lineárně nezávislá a každý její vektor je řešením soustavy rovnic. Nechť $(x_1, \ldots, x_n)$ je libovolné řešení soustavy, označme jeho posledních q složek $r_1, \ldots, r_q$. Dosazením do všech rovnic soustavy zjistíme, že pro všechna $i \in \{1, \ldots, p\}$ už musí být $x_i = -\sum_{j=1}^{q} c_{ij} r_j$. Vzniklý vektor řešení

$$\left(-\sum_{j=1}^{q} c_{1j} r_j, -\sum_{j=1}^{q} c_{2j} r_j, \ldots, -\sum_{j=1}^{q} c_{pj} r_j, r_1, \ldots, r_q \right),$$

je lineární kombinací vektorů z M s koeficienty $r_1, \ldots, r_q$. Každé řešení soustavy $Ax = 0$ je tedy v lineárním obalu množiny M, proto je M bází prostoru řešení a $q = n - h(A)$ je dimenze tohoto prostoru. □

Napříště tedy budeme řešení homogenní soustavy rovnic vyjadřovat pomocí báze prostoru řešení. Ve skutečnosti je to jen drobná modifikace zápisu pomocí parametrů. Když se podíváme na příklad soustavy rovnic z první

přednášky a odmyslíme si pravou stranu (pokud je nulová, zůstane nulová i po všech řádkových úpravách), dostaneme matici v redukovaném odstupňovaném tvaru

$$\begin{pmatrix} 1 & 0 & -2 & -2 & 0 & -3 \\ 0 & 1 & 3 & -1 & 0 & -3 \\ 0 & 0 & 0 & 0 & 1 & -2 \end{pmatrix}$$

Musíme se přenést přes drobnou kosmetickou vadu, že pivotní sloupce nejsou na prvních třech místech, přesto ale snadno identifikujeme matici C z důkazu

$$\begin{pmatrix} -2 & -2 & -3 \\ 3 & -1 & -3 \\ 0 & 0 & -2 \end{pmatrix}$$

a napíšeme bázové vektory prostoru řešení:

$$\begin{aligned} u &= (2, -3, 1, 0, 0, 0), \\ v &= (2, \quad 1, 0, 1, 0, 0), \\ w &= (3, \quad 3, 0, 0, 2, 1) \end{aligned}$$

Libovolné řešení má tedy tvar lineární kombinace $ru+sv+tw$, kde $r, s, t \in \mathbb{R}$. Když tuto lineární kombinaci zapíšeme jako jeden vektor závislý na r, s, t, vidíme, že

$$(2s + 2r + 3t, -3s + r + 3t, r, s, 2t, t)$$

je právě tvar řešení, který bychom dostali původní metodou s parametry.

Zbývá nám popsat řešení soustav nehomogenních.

Věta 12 *Nechť $A \in M_{mn}(\mathbb{T})$ je matice, $b \in \mathbb{T}^m$ vektor pravých stran. Soustava rovnic $Ax = b$ má řešení, právě když $h(A) = h(A|b)$.*

Důkaz: Přepišme soustavu rovnic následovně:

$$\begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} x_1 + \begin{pmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{pmatrix} x_2 + \ldots + \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} x_n = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix},$$

Splnit tuto rovnost nějakými hodnotami $x_1, \ldots, x_n$ je totéž jako najít lineární kombinaci sloupců matice A, která se rovná vektoru $b \in \mathbb{T}^m$. To je možné právě tehdy, když vektor b náleží do sloupcového prostoru matice A, tedy

když jeho přidání ke sloupcům A nezvýši dimenzi jimi generovaného prostoru. Dimenze sloupcového prostoru je podle předchozí věty rovna dimenzi prostoru řádkového. Jinými slovy, hodnost matice soustavy a rozšířené matice soustavy musejí být stejné. □

Věta 13 *Nechť $Ax = b$ je soustava rovnic s maticí $A \in M_{mn}(\mathbb{T})$ a vektorem pravých stran $b \in \mathbb{T}^m$. Nechť $x^P \equiv (x_1^P, \ldots, x_n^P)$ je libovolné řešení této soustavy. Pak pro libovolné řešení $x \equiv (x_1, \ldots, x_n)$ soustavy $Ax = b$ existuje řešení $x^H \equiv (x_1^H, \ldots, x_n^H)$ homogenní soustavy se stejnou maticí $Ax = 0$ takové, že $x = x^P + x^H$.*

Důkaz: Pokud $Ax^P = b$ a $Ax = b$, potom $A(x - x^P) = 0$, tedy $x^H := x - x^P$ je řešením homogenní rovnice. □

Znamená to tedy, že stačí najít jediné libovolné řešení nehomogenní soustavy rovnic (tzv. **partikulární řešení**) a to nám spolu s obecným řešením homogenní soustavy dá všechna řešení soustavy nehomogenní. Výslednou množinu řešení soustavy $Ax = b$ pak budeme obvykle zapisovat ve tvaru $x^P + \langle v_1, \ldots, v_q \rangle$, kde $\{v_1, \ldots, v_q\}$ je báze prostoru řešení $Ax = 0$. Partikulární řešení nejpohodlněji najdeme tak, že dosadíme za všechny neznámé na nepivotních sloupcích nuly. Konkrétně pokud soustava rovnic vede na odstupňovaný tvar

$$\left(\begin{array}{cccccccc|c} 1 & 0 & \ldots & 0 & c_{11} & c_{12} & \ldots & c_{1q} & b'_1 \\ 0 & 1 & \ldots & 0 & c_{21} & c_{22} & \ldots & c_{2q} & b'_2 \\ \vdots & & \ddots & \vdots & \vdots & & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & c_{p1} & c_{p2} & \ldots & c_{pq} & b'_p \end{array}\right),$$

pak její partikulární řešení je $(b'_1, \ldots, b'_p, 0 \ldots, 0)$. Pro soustavu z první přednášky to znamená, že obecné řešení je

$$(9, 2, 0, 0, 4, 0) + \langle (2, -3, 1, 0, 0, 0), (2, 1, 0, 1, 0, 0), (3, 3, 0, 0, 2, 1) \rangle,$$

což opět můžeme srovnat se zápisem pomocí parametrů.

Shrneme teď do jedné věty to, co jsme si právě rozmysleli.

Věta 14 (Frobeniova)

1. *Nechť A je $m \times n$ matice. Prostor řešení homogenní soustavy m rovnic o n neznámých $A\,x = 0$ je vektorový podprostor prostoru $\mathbb{R}^n$. Je-li hodnost $h(A)$ matice A rovna k, pak dimenze prostoru řešení je rovna $n-k$. Obecné řešení homogenní lineární soustavy rovnic se tedy napíše jako lineární kombinace zvolené baze prostoru řešení a závisí na $n-k$ libovolných parametrech.*

2. *Předpokládejme, že je nehomogenní soustava lineárních rovnic zadaná rozšířenou maticí (A, b), kde A je typu $m \times n$. Je to tedy soustava m rovnic o n neznámých. Pak nastane právě jedna z následujících možností.*

   1. $h(A) < h(A, b)$; pak soustava nemá řešení;

   2. $h(A) = h(A, b) = n$; pak má soustava právě jedno řešení;

   3. $h(A) = h(A, b) = k < n$; pak má soustava nekonečně mnoho řešení. Obecné řešení soustavy je rovno součtu jednoho (partikulárního) řešení a obecného řešení odpovídající homogenní soustavy. Obecné řešení tedy závisí na $n-k$ libovolných parametrech.

4 Lineární zobrazení

4.1 Definice lineárního zobrazení a jeho vlastnosti.

Definice 11 *Nechť V a V' jsou dva vektorové prostory nad $\mathbb{T}$. Řekneme, že zobrazení f z V do W je **lineární,** pokud platí:*

(i) $\forall u, v \in V : f(u+v) = f(u) + f(v)$,

(ii) $\forall r \in \mathbb{T}, u \in V : f(r\,u) = r\,f(u)$.

*Alternativní název pro lineární zobrazení je **homomorfismus** V do W. Množinu*

$$\mathrm{Ker}(f) := \{v \in V | f(v) = 0\}$$

*nazveme **jádrem** zobrazení f. Obor hodnot zobrazení f označíme* $\mathrm{Im}(f)$. *Tedy*

$$\mathrm{Im}(f) = \{w \in W | \exists\, v \in V, f(v) = w\}.$$

Lemma 6 *Nechť V a W jsou dva vektorové prostory nad $\mathbb{T}$. Zobrazení $f : V \to W$ je homomorfizmus, právě když $\forall u, v \in V$ a $\forall r, s \in \mathbb{T}$ platí*

$$f(ru + sv) = rf(u) + sf(v).$$

Důkaz: Podobné sloučení dvou podmínek do jedné jsme viděli už v případě definice podprostoru a důkaz zde je zcela analogický. □

Příklad:

1. Je-li $V = \mathbb{R}^n$, $W = \mathbb{R}^m$ a A matice typu $m \times n$, pak můžeme definovat zobrazení f_A z V do W předpisem

   $$f_A(x) := A \cdot x,$$

   kde $\cdot$ znamená maticové násobení a $x \in V = \mathbb{R}^n$ a $y \in W = \mathbb{R}^m$ chápeme jako sloupcové vektory. Použitím definice maticového násobení se lze snadno přesvědčit, že zobrazení f_A je lineární.

2. Předpokládejme, že W, W' jsou dva ortogonální podprostory vektorového prostoru V konečné dimenze, pro které platí $W \oplus W' = V$. Pak lze definovat zobrazení $\pi : V \to W$ takto: Pro každý vektor $v \in V$ existuje jednoznačný rozklad $v = w + w'$, $w \in W$, $w' \in W'$. Pak definujeme $\pi(v) := w$. Ukažte, že zobrazení π je lineární zobrazení. Toto zobrazení π se obvykle nazývá projekce V na podprostor W. Všimněte si, že tato projekce není určena jen výběrem podprostoru W, ale závisí také na volbě doplňkového podprostoru W'.

3. Je-li V prostor všech polynomů v jedné proměnné, pak zobrazení 'derivace'

   $$f : V \mapsto V;\ [f(p)](x) = p'(x)$$

   je lineární zobrazení.

   Obecněji, jsou-li $a_i \in V$, $i = 1, \ldots, n$ dané polynomy, pak zobrazení

   $$f : V \mapsto V;\ [f(p)](x) = a_n(x)p^{(n)}(x) + \ldots + a_1(x)p'(x) + a_0(x)p(x)$$

   nazýváme lineární diferenciální operátor, a je to také příklad lineárního zobrazení. Rovnice tvaru $f(p) = q$, $p, q \in V$ se nazývá (lineární) obyčejná diferenciální rovnice.

4. Je-li V prostor všech polynomů v několika proměnných $x_1, \ldots, x_n$, a jsou-li $a_i \in V$, $i = 0, \ldots, n$ dané polynomy ve V, pak zobrazení

$$f : V \mapsto V;\ [f(p)](x) = a_1(x)\frac{\partial p}{\partial x_1} + \ldots + a_n(x)\frac{\partial p}{\partial x_n} + a_0(x)p(x)$$

nazýváme lineární parciální diferenciální operátor (prvního řádu), a je to také příklad lineárního zobrazení. Rovnice tvaru $f(p) = q$, $p, q \in V$ se nazývá (lineární) parciální diferenciální rovnice (1. řádu).

Nejznámější příklad paricálního diferenciálního operátoru druhého řádu je **Laplaceův operátor** Δ, definovaný předpisem

$$[\Delta(p)](x) := \sum_{i=1}^{n} \frac{\partial^2 p}{\partial x_i^2}(x).$$

5. Dalším příkladem lineárního operátoru je tzv. integrální operátor. Je-li $V = \mathbb{C}(\langle a, b\rangle)$ vektorový prostor všech spojitých funkcí na intervalu $\langle a, b\rangle \subset \mathbb{R}$, $V' = \mathbb{C}(\langle c, d\rangle)$ vektorový prostor všech spojitých funkcí na intervalu $\langle c, d\rangle \subset \mathbb{R}$, a je-li dána spojtá funkce $K = K(x, y)$ dvou proměnných na součinu $\langle a, b\rangle \times \langle c, d\rangle$, pak definujeme zobrazení $\phi : V \mapsto V'$ předpisem

$$[\phi(f)](y) := \int_a^b K(x, y)f(x)dx, f \in V.$$

Ověřte, že toto zobrazení ϕ je lineární.

Věta 15 *Nechť f je lineární zobrazení vektorového prostoru V do vektorového prostoru W. Pak:*

(1) $\mathrm{Ker}(f)$ *a* $\mathrm{Im}(f)$ *jsou vektorové podprostory V, resp. W.*

(2) $\dim \mathrm{Ker}(f) + \dim \mathrm{Im}(f) = \dim V$.

Důkaz:

(1) Jsou-li $u, v \in \mathrm{Ker}(f)$, pak $f(u) = f(v) = 0$ a tedy i $f(u + v) = f(u) + f(v) = 0$.

Podobně, je-li $f(u) = 0, r \in \mathbb{T}$, pak $f(r\,x) = r\,f(u) = 0$.

Obdobně se ukáže, že i obraz $\mathrm{Im}(f)$ je vektorový prostor.

(2) Zvolme si basi $v_1, \ldots, v_k$ prostoru $\mathrm{Ker}(f)$ libovolně. Tedy $\dim \mathrm{Ker}(f) = k$. Tuto bazi je možno doplnit na basi $v_1, \ldots, v_k, v_{k+1}, \ldots, v_m$ prostoru V, tedy $\dim V = m$. Stačí nyní dokázat, že množina $f(v_{k+1}), \ldots, f(v_m)$ je bazí prostoru $\mathrm{Im}(f)$. Chceme si tedy rozmyslet, že tato množina generuje celý prostor $\mathrm{Im}(f)$ a že jsou tyto vektory lineárně nezávislé.

(i) Vezměme si libovolný vektor $y \in \mathrm{Im}(f)$. Tedy existuje vektor $x \in V$ takový, že $f(x) = y$. Vektor x rozložíme do base $x = \sum_{i=1}^{m} \xi_i v_i$. Pak ale

$$y = f(x) = f(\sum_{i=1}^{m} \xi_i v_i) = \sum_{i=1}^{m} \xi_i f(v_i) = \sum_{i=k+1}^{m} \xi_i f(v_i),$$

protože $f(v_1) = \ldots = f(v_k) = 0$.

(ii) Ověřme nyní, že množina vektorů $f(v_{k+1}), \ldots, f(v_m)$ je lineárně nezávislá. Předpokládejme, že existují čísla $\beta_{k+1}, \ldots, \beta_m$ taková, že

$$\sum_{i=k+1}^{m} \beta_i f(v_i) = f\left(\sum_{i=k+1}^{m} \beta_i v_i\right) = 0.$$

Pak ale $\sum_{i=k+1}^{m} \beta_i v_i \in \mathrm{Ker}(f)$ a existují tedy čísla $\gamma_1, \ldots, \gamma_k$ taková, že

$$\sum_{i=k+1}^{m} \beta_i v_i - \sum_{i=1}^{k} \gamma_i v_i = 0.$$

Protože vektory $v_1, \ldots, v_m$ jsou lineárně nezávislé, jsou všechny koeficienty v této lineární kombinaci rovny nule.

Věta 16 *[Frobenius] Nechť $f : V \to W$ je lineární zobrazení. Pak:*

(1) Množina všech řešení homogenní lineární rovnice $f(v) = 0$ (tj. $\mathrm{Ker}(f)$) je lineární podprostor V; je-li $\{v_1, \ldots, v_k\}$ jeho base, pak množina všech řešení homogenní rovnice je právě množina všech vektorů tvaru

$$v = \sum_{i=1}^{k} \alpha_i v_i; \alpha_i \in \mathbb{T}.$$

Dimenze prostoru řešení je dána vztahem

$$\dim V - \dim \mathrm{Im}(f).$$

(2) Je-li v_0 pevné řešení nehomogenní rovnice $f(v) = w$ (tzv. partikulární řešení rovnice s pravou stranou), pak množina všech řešení rovnice $f(u) = w$ s pravou stranou má tvar

$$\{v \in V | v = v_1 + v_0, f(v_1) = 0\}.$$

Důkaz: První část tvrzení je okamžitým důsledkem Věty 15. Druhá část plyne z toho, že pro každé další řešení v rovnice $f(v) = w$ platí $f(v - v_0) = 0$. □

Poznámka: Věta 16 je opravdu velmi jednoduchá, ale má zásadní význam. Setkáme se s ní ihned v paragrafu o řešení soustav lineárních rovnic, později v analýze (nebo už teď ve fyzice) pro řešení lineárních diferenciálních rovnic a v mnoha dalších variantách v budoucnosti.

Definice 8 *Homomorfizmus, který je prostý, nazýváme **monomorfizmem**, pro homomorfizmus, který je "na"udeme užívat pojem **epimorfizmus**. Vzájemně jednoznačný homomorfizmus, tedy lineární zobrazení, které je zároveň mono- a epimorfizmem, se nazývá **izomorfizmus**.*

Že je zobrazení $f : V \to V'$ "na" (nebo též **surjektivní**) znamená, že $\mathrm{Im}(f) = V'$, což nám dává charakterizaci epimorfizmů pomocí obrazu. Monomorfizmy je zase možné charakterizovat podmínkou na jádro $\mathrm{Ker}(f) = \{o\}$. Pokud totiž f je prosté, pak nulový vektor z V' může mít pouze jeden vzor, a tím je nulový vektor z V, čili $\mathrm{Ker}(f) = \{o\}$. Naopak, pokud $\mathrm{Ker}\, f = \{o\}$, a pro dva vektory $u, v \in V$ platí $f(u) = f(v)$, pak $f(u - v) = o$ a tedy $u - v \in \mathrm{Ker}(f)$, čili $u - v = 0$. Ověřili jsme tedy, že kdykoli $f(u) = f(v)$, musí už být $u = v$, což není nic jiného, než že f je prosté.

Z věty o dimenzi jádra a obrazu pak plynou další skutečnosti, platné v případě zobrazení na prostorech konečné dimenze. Pokud $f : V_n \to V'$ je monomorfizmus, pak $n = \dim \mathrm{Im}(f) + \dim \mathrm{Ker}(f) = \dim \mathrm{Im}(f)$. Odtud získáme následující vlastnost izomorfizmů:

Věta 17 *Nechť $f : V_n \to V'$ je izomorfizmus. Pak $\dim V_n = \dim V'$.*

Důkaz: Protože f je monomorfizmus na V_n, máme $\dim \mathrm{Im}(f) = n$. Je to také epimorfizmus, tedy $\mathrm{Im}(f) = V'$. Tedy $\dim V' = n$. □

Pokud mezi dvěma prostory existuje izomorfizmus, říkáme, že jsou **izomorfní**. Věta říká, že jsou-li dva prostory, z nichž jeden je konečné dimenze,

izomorfní, pak mají stejnou dimenzi. Platí i opačná implikace, k jejímu důkazu ale budeme potřebovat zkonstruovat pro libovolné dva vektorové prostory stejné dimenze izomorfizmus mezi nimi. K tomu je nutné zavést pojem souřadnic, což učiníme ještě v této kapitole.

Zobrazení, jehož zdrojový i cílový prostor jsou stejné, $f : V \to V$, se nazývá **endomorfizmus**. Pokud je endomorfizmus zároveň izomorfizmem, říkáme mu **automorfizmus**. Všimněte si, že z věty o dimenzi jádra a obrazu plyne, že pokud je V konečné dimenze, pak stačí, aby byl endomorfizmus jedním z dvojice monomorfizmus, epimorfizmus, a automaticky už musí být i tím druhým z dvojice, a tedy také automorfizmem. Prostory nekonečné dimenze tuto vlastnost ale nemají, zkuste najít protipříklad!

Uveďme si několik dalších příkladů homomorfizmů vektorových prostorů a jejich vlastností:

1. Pro $A \in M_{mn}(\mathbb{T})$ je f_A monomorfizmus, právě když A má lineárně nezávislé sloupce, tedy $h(A) = n$. Je to epimorfizmus, právě když sloupce generují celé $\mathbb{T}^m$, tedy $h(A) = m$. Tedy f_A je izomorfizmem, právě když A je čtvercová matice hodnosti $n = m$, čili regulární matice.

2. Je-li $V = W_1 \oplus W_2$ přímý součet a $P : V \mapsto W_1$ je odpovídající projekce, pak pro P platí $P^2 = P$, což je vlastnost charakterizující **projekce**. Je to epimorfizmus, není to monomorfizmus.

3. Inkluze $\mathbb{T}^n \subset \mathbb{T}^m$, $n < m$ definuje monomorfizmus $i : (x_1, \ldots, x_n) \to (x_1, \ldots, x_n, 0 \ldots, 0)$, který není epimorfizmem.

4. $V = \mathbb{R}$ se standardními operacemi a $V' = \mathbb{R}^+$ s operacemi $\oplus$ a $\odot$, kde $u \oplus v = uv$ a $r \odot u = u^r$ jsou vektorové prostory nad $\mathbb{R}$. Pak $\exp : u \to e^u$ je jejich izomorfizmus.

5. $V = C(-\infty, \infty)$, $V' = \mathbb{R}$. $E_a : f \to f(a)$ je epimorfizmus.

Následující věta říká, že libovolné zobrazení báze vektorového prostoru do jiného prostoru lze jednoznačně rozšířit na lineární, jinými slovy, že homomorfizmus je jednoznačně určen svými hodnotami na nějaké bázi.

Věta 18 *Nechť V a V' jsou dva vektorové prostory nad $\mathbb{T}$, nechť $M = \{v_1, \ldots, v_n\}$ je báze V. Pak pro libovolnou n-tici vektorů $v'_1, \ldots, v'_n \in V'$ existuje právě jedno lineární zobrazení $f : V \to V'$ takové, že*

$$f(v_i) = v'_i, \ i = 1, \ldots, n.$$

Důkaz: Libovolný vektor $v \in V$ lze zapsat jako $v = \sum_{i=1}^{n} r_i v_i$. Definujeme pak $f(v) = \sum_{i=1}^{n} r_i v'_i$. Je zřejmé, že takto definované f je lineární zobrazení a platí $f(v_i) = v'_i,\ i = 1, \ldots, n$. Tím je dokázána existence, zbývá jednoznačnost. Pokud by existovalo lineární zobrazení g takové, že $g(v_i) = v'_i$, $i = 1, \ldots, n$, pak pro libovolný vektor $v = \sum_{i=1}^{n} r_i v_i$ máme

$$g(v) = g\left(\sum_{i=1}^{n} r_i v_i\right) = \sum_{i=1}^{n} r_i g(v_i) = \sum_{i=1}^{n} r_i v'_i = f(v),$$

tedy $g = f$. □

Jako cvičení si můžete zkusit zjistit a dokázat, co plyne pro homomorfizmus f z toho, že skupina vektorů $F(M)$ je lineárně nezávislá, případně generuje V', případně je bází V'. Také si rozmyslete, co se stane, když M bude lineárně nezávislá, ale nebude bází V, případně když M bude lineárně závislá. Jako jednoduché cvičení ponecháváme i důkaz následujícího lemmatu:

Lemma 7 *Nechť V, W jsou dva vektorové prostory nad $\mathbb{T}$, $f : V \to W$ je izomorfizmus a M skupina vektorů ve V. Pak M je lineárně nezávislá, právě když $f(M)$ je lineárně nezávislá, a M generuje V, právě když $f(M)$ generuje W.*

5 Operace s homomorfizmy

Nechť V, W jsou dva vektorové prostory nad $\mathbb{T}$. Označme $\mathrm{Hom}(V, W)$ množinu všech homomorfizmů z V do W a $\mathrm{End}(V)$ množinu všech endomorfizmů prostoru V, tedy $\mathrm{End}(V) \equiv \mathrm{Hom}(V, V)$. Na množině $\mathrm{Hom}(V, W)$ máme definováno sčítání homomorfizmů a násobení homomorfizmu číslem: pro libovolný vektor $v \in V$ a libovolné $r \in \mathbb{T}$

$$(f + g)(v) := f(v) + g(v)$$
$$(rf)(v) := rf(v)$$

Rozmyslete si, co tato definice znamená: na prvním řádku definujeme nové zobrazení $f+g$ tím, na co zobrazuje libovolný vektor, říkáme, že to má být na součet vektorů $f(v)$ a $g(v)$. Podobně na druhém řádku říkáme, že zobrazení rf má vektor v zobrazit na r-násobek vektoru $f(v)$. Sami ověřte, že definice je korektní, tedy že součet dvou homomorfizmů je homomorfizmus a násobek homomorfizmu je homomorfizmus. Také si rozmyslete, že $f_A + f_B$ je vlastně f_{A+B} a $rf_A = f_{rA}$.

Věta 19 *Nechť V, W jsou dva vektorové prostory nad $\mathbb{T}$. Množina* $\mathrm{Hom}(V,W)$ *s operacemi sčítání homomorfizmů a násobení homomorfizmu číslem je vektorový prostor. Pokud* $\dim V = n$ *a* $\dim W = m$*, pak*

$$\dim \mathrm{Hom}(V,W) = mn.$$

Důkaz: Ověření, že $\mathrm{Hom}(V,W)$ s danými operacemi splňuje axiomy vektorového prostoru, ponecháváme čtenáři za cvičení. Abychom určili dimenzi tohoto prostoru, použijeme předchozí větu, která říká, že každé lineární zobrazení je jednoznačně určeno svými hodnotami na předem zvolené bazi a že tyto hodnoty mohou být zvoleny libovolně. Existuje tedy podle této věty vzájemně jednoznačné zobrazení mezi $\mathrm{Hom}(v,W)$ a množinou

$$\underbrace{W \times \ldots \times W}_{n} = \{(w_1, \ldots, w_n) | w_i \in W,\, i = 1, \ldots, n\}.$$

Je snadné ověřit, že toto zobrazení je lineární, tedy je to izomorfismus. Stačí tedy zjistit dimenzi prostoru $W \times \ldots \times W$ (n činitelů). To stačí ověřit pro $W \times W$ (obecný případ se snadno dokáže indukcí). Ale je-li $\{v_1, \ldots, v_m\}$ baze W, pak zřejmě (ověřte!)

$$\{(v_1, o), \ldots, (v_m, o), (o, v_1), \ldots, (o, v_m)\}$$

je baze $W \times W$ a $\dim W \times W = \dim W + \dim W$. Tedy dimenze $\underbrace{W \times \ldots \times W}_{n}$ je rovna $n \dim W = \dim V \dim W$. □

Speciální situace nastává, když $W = \mathbb{T}$. Prostor $V^* := \mathrm{Hom}(V, \mathbb{T})$ má stejnou dimenzi jako prostor V a říká se mu **duální prostor** k V. Blíže se duálním prostorem budeme zabývat v letním semestru.

Označme $1_V \in \mathrm{End}(V)$ identický endomorfizmus prostoru V, definovaný vztahem $\forall v \in V$, $1_V(v) = v$. Je zřejmé, že je to lineární zobrazení, prosté a na, tedy izomorfizmus. Pokud $V = \mathbb{T}^n$, pak $1_V \equiv f_E$, kde E je jednotková matice.

Věta 20 *Nechť V, V', V'' jsou vektorové prostory nad $\mathbb{T}$, $f : V \to V'$, $g : V' \to V''$ jsou dva homomorfizmy. Pak*

1. *Složené zobrazení $gf : V \to V''$ je homomorfizmus.*
2. *Pokud g a f jsou monomorfizmy, pak gf je monomorfizmus.*

3. *Pokud g a f jsou epimorfizmy, pak gf je epimorfizums.*

4. *Pokud g a f jsou izomorfizmy, pak gf je izomorfizums.*

5. *Pokud gf je monomorfizmus, pak f je monomorfizums.*

6. *Pokud gf je epimorfizmus, pak g je epimorfizums.*

7. *Zobrazení f je izomorfizmus, právě když existuje homomorfizmus $f^{-1} : V' \to V$, pro který $ff^{-1} = 1_{V'}$ a $f^{-1}f = 1_V$. Homomorfizmus f^{-1} je těmito podmínkami určen jednoznačně a je to izomorfizmus.*

Důkaz: Nechť $r, s \in \mathbb{T}$, $u, v \in V$.

1. $gf(ru + sv) = g(rf(u) + sf(v)) = rgf(u) + rgf(v)$

2. Pokud g, f jsou prostá a $u \neq v$, pak $f(u) \neq f(v)$ a $g(f(u)) \neq g(f(v))$, tedy gf je prosté.

3. Pokud g, f jsou surjektivní a $u'' \in V''$, pak existuje $u' \in V'$ takové, že $g(u') = u''$ a $u \in V$, že $f(u) = u'$. Tedy $gf(u) = u''$, gf je na.

4. Plyne z předchozích dvou bodů.

5. Pokud $u \in \operatorname{Ker} f$, pak $gf(u) = g(0) = 0$. Protože gf je monomorfizmus, musí být $u = 0$. Tedy $\operatorname{Ker} f = 0$, čili f je monomorfizmus.

6. Pokud g není na, pak ani $g \circ f$ nemůže být na.

7. Pokud existuje f^{-1} splňující $ff^{-1} = 1_{V'}$, což je epimorfizmus, pak podle předchozího bodu musí být f také epimorfizmus. Podobně z $f^{-1}f = 1_V$ plyne, že f je monomorfizmus, celkově je tedy f izomorfizmus. Naopak, pokud f je izomorfizmus, pak je na, tedy pro každé $u' \in V'$ existuje $u \in V$, že $f(u) = u'$, a je prosté, tedy toto u existuje právě jedno. Definujme $f^{-1}(u') := u$. Snadno se ověří, že f^{-1} je lineární zobrazení, vlastnosti $ff^{-1} = 1_{V'}$ a $f^{-1}f = 1_V$ jsou zřejmé. Zbývá ověřit jednoznačnost: pokud by existovalo $g : V' \to V$, $fg = 1_{V'}$ a $gf = 1_V$, pak $g = gff^{-1} = f^{-1}$.

□

Zobrazení f^{-1} budeme samozřejmě nazývat **inverzní** homomorfizmus. Opět si rozmyslete, že $(f_A)^{-1} = f_{A^{-1}}$. Z věty jsme se dozvěděli, že všechny prvky

množiny všech automorfizmů $\mathrm{Aut}(V)$ prostoru V mají inverzní prvek vzhledem k operaci skládání zobrazení. Spolu s asociativitou skládání a faktem, že identita je automorfizmus, dostáváme, že množina $\mathrm{Aut}(V)$ s operací skládání je grupa.

Zatím jsme vždy ilustrovali všechny pojmy týkající se homomorfizmů pomocí zobrazení typu f_A pro nějakou matici A. Nyní si ukážeme, že se všemi zobrazeními mezi prostory konečné dimenze se dá počítat jako se zobrazeními tohoto typu.

Definice 9 *Nechť V_n je vektorový prostor nad $\mathbb{T}$, $M = \{u_1, \ldots, u_n\}$ jeho báze a $u \in V$. **Souřadnicemi** vektoru u vzhledem k bázi M budeme rozumět sloupcový vektor $(u)_M := (x_1, \ldots, x_n)^T$, kde x_i jsou koeficienty lineární kombinace $u = \sum_{i=1}^{n} x_i u_i$.*

Koeficienty lineární kombinace vzhledem k bázi jsou určeny jednoznačně, definice je tedy korektní a navíc zadává bijekci mezi množinami V_n a $\mathbb{T}^n$. Ověřte sami, že je tato bijekce lineárním zobrazením, tedy izomorfizmem. Podle lemmatu 7 je skupina vektorů $v_1, \ldots, v_k$ lineárně nezávislá, resp. generuje V_n právě tehdy, když je množina vektorů jejich souřadnic $(v_1)_M, \ldots, (v_k)_M$ lineárně nezávislá, resp. generuje T^n.

Pomocí souřadnic můžeme dokázat zesílení věty 17 na ekvivalenci:

Věta 21 *Nechť V a W jsou dva vektorové prostory konečné dimenze nad $\mathbb{T}$. Pak V a W jsou izomorfní právě když* $\dim V = \dim W$.

Důkaz: Zbývá sestrojit izomorfizmus mezi prostory V a W stejné dimenze. Zvolme M bázi V a N bázi W, existují izomorfizmy $f : V \to \mathbb{T}^n$, $g : W \to \mathbb{T}^n$ určené přiřazením vektoru jeho souřadnic vzhledem k dané bázi: $f(v) := (v)_M$, $g(w) = (w)_N$. Pak $g^{-1}f$ je izomorfizmus V a W. □

Definice 10 *Nechť V_n je vektorový prostor nad $\mathbb{T}$, $M = \{u_1, \ldots, u_n\}$, $M' = \{u'_1, \ldots, u'_n\}$ dvě báze v něm. Matici $R \in M_{nn}(\mathbb{T})$, jejíž i-tý sloupec pro všechna $i \in \{1, \ldots, n\}$ je vektorem souřadnic vektoru u'_i vzhledem k bázi M, nazýváme **maticí přechodu** od M k M'.*

Podle definice tedy $\sum_{i=1}^{n} r_{ij} u_i = u'_j$ pro všechna $j \in \{1, \ldots, n\}$. Označme souřadnice libovolného vektoru $u \in V$ vzhledem k M' jako $(u)_{M'} \equiv x' \equiv (x'_1, \ldots, x'_n)^T$. Pak

$$u = \sum_{j=1}^{n} x'_j u'_j = \sum_{j=1}^{n} \sum_{i=1}^{n} x'_j r_{ij} u_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} r_{ij} x'_j \right) u_i$$

Když označíme souřadnice u vzhledem k M jako $(u)_M \equiv x \equiv (x_1, \ldots, x_n)^T$, pak $u = \sum_{i=1}^n x_i u_i$ a protože souřadnice vzhledem k dané bázi jsou určeny jednoznačně, musí být $x_i = \sum_{j=1}^n r_{ij} x'_j$ pro všechna $i \in \{1, \ldots, n\}$. Tedy matice přechodu umožňuje vypočítat "nečárkované" souřadnice x jako součin Rx' matice přechodu od M k M' a "čárkovaných" souřadnic.

Praktický výpočet matice přechodu se nejlíp provede přímo z definice. Pokud $M = \{(1,1),(2,3)\}$ a $M' = \{(1,2),(3,4)\}$ v $\mathbb{R}^2$ pak soustava rovnic s maticí

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 3 \\ 1 & 3 & 2 & 4 \end{array}\right)$$

právě řeší úlohu vyjádřit vektory z M' (pravé strany) pomocí vektorů báze M (sloupce matice soustavy). Tedy po úpravě na jednotkovou matici vlevo přečteme vpravo přímo matici R.

Definice 11 *Nechť $f : V_n \to V_m$ je homomorfizmus vektorových prostorů nad $\mathbb{T}$. **Maticí homomorfizmu** f vzhledem k bázím $M = \{u_1, \ldots, u_n\} \subset V_n$ a $N = \{v_1, \ldots, v_m\} \subset V_m$ rozumíme matici $(f)_{NM} \in M_{mn}(\mathbb{T})$, jejíž i-tý sloupec je pro všechna $i \in \{1, \ldots, n\}$ roven $(f(u_i))_N$, tedy souřadnicím f-obrazu i-tého bázového vektoru báze M vzhledem k bázi N.*

Označme opět souřadnice vektoru $u \in V$ vzhledem k M jako $(u)_M \equiv (x_1, \ldots, x_n)^T$ a matici $(f)_{NM}$ jako A. Pak

$$f(u) = \sum_{j=1}^n x_j f(u_j) = \sum_{j=1}^n x_j \sum_{i=1}^m a_{ij} v_i = \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} x_j \right) v_i$$

Tedy souřadnice $f(u)$ vzhledem k N se dostanou jako součin matice homomorfizmu A a souřadnic u vzhledem k M:

$$(f(u))_N = (f)_{NM} (u)_M$$

Naopak, pro libovolnou matici $A \in M_{mn}(\mathbb{T})$ má zobrazení f, definované na bázi M předpisem $f(u_i) = \sum_{j=1}^m a_{ji} v_j$, matici $(f)_{NM}$ rovnou A. Libovolnému homomorfizmu $f \in \mathrm{Hom}(V_n, V_m)$ je tedy přiřazena matice $(f)_{NM} \in M_{mn}(\mathbb{T})$, a to bijektivně. Nedá příliš práce ověřit, že toto zobrazení $F : \mathrm{Hom}(V_n, V_m) \to M_{mn}(\mathbb{T})$ je homomorfizmus vektorových prostorů. Tedy prostory $\mathrm{Hom}(V_n, V_m)$ a $M_{mn}(\mathbb{T}) \simeq \mathbb{T}^{mn}$ jsou izomorfní a mají tudíž stejnou

dimenzi, čímž jsme znovu ověřili, že $\dim \mathrm{Hom}(V_n, V_m) = mn$. Zároveň vidíme, že pojem matice homomorfizmu můžeme chápat jako způsob, jak zavést souřadnice na prostoru $\mathrm{Hom}(V_n, V_m)$, které budou v nějakém smyslu kompatibilní s již zavedenými souřadnicemi na prostorech V_n a V_m.

Vrátíme-li se k našemu příkladu zobrazení typu $f_A : \mathbb{R}^n \to \mathbb{R}^m$, definovanému předpisem $f_A(x) = Ax$, vidíme, že matice A je rovna matici $(f_A)_{K'K}$ homomorfizmu f_A vzhledem ke kanonickým bázím v $K \subset \mathbb{R}^n$ a $K' \subset \mathbb{R}^m$. Proto se dají všechna lineární zobrazení mezi dvěma aritmetickými vektorovými prostoru zapsat jako f_A pro nějakou matici A.

Lemma 8 *Nechť U, V, W jsou tři vektorové prostory nad $\mathbb{T}$ a M, N, P po řadě báze v nich, $f : U \to V$, $g : V \to W$ homomorfizmy. Pak*

1. $(1_U)_{MM} = E$
2. $(gf)_{PM} = (g)_{PN}(f)_{NM}$
3. *Pokud f je izomorfizmus, pak $(f^{-1})_{MN} = (f)^{-1}_{NM}$.*

Důkaz: První tvrzení je zřejmé z definice. Pro druhé stačí vzít libovolný vektor $u \in U$ a rozepsat

$$(g)_{PN}(f)_{NM}(u)_M = (g)_{PN}(f(u))_N = (g(f(u)))_P = (gf)_{PM}(u)_M.$$

To musí platit pro libovolný vektor $(u)_M$. Vezmeme-li $(u)_M = e_i$, i-tý prvek kanonické báze, pak rovnost říká, že i-tý sloupec matice $(g)_{PN}(f)_{NM}$ a matice $(gf)_{PN}$ se rovnají. Protože i je libovolné, rovnají se matice jako celek.

Třetí tvrzení je důsledkem prvních dvou a vztahu $f^{-1}f = 1_U$. □

Třetí tvrzení říká, že pokud je f izomorfizmus, pak je jeho matice vzhledem k libovolným bázím regulární. Naopak, pro regulární matici A a dané dvě báze M a N lze sestrojit homomorfizmy $f : U \to V$ a $g : V \to U$ takové, že $(f)_{NM} = A$ a $(g)_{MN} = A^{-1}$. Pak ale podle druhého bodu lemmatu $(gf)_{MM} = E$ a $(fg)_{NN} = E$, tedy $gf = 1_U$ a $fg = 1_V$ a tedy $g = f^{-1}$, protože inverzní izomorfizmus je určen jednoznačně.

Věta 22 *Nechť V, W jsou dva vektorové prostory konečné dimenze nad $\mathbb{T}$, $M \subset V$, $N \subset W$ báze v nich, $f : V \to W$ homomorfizmus. Pak $h(f) = h\left((f)_{NM}\right)$.*

Důkaz: Označme $M = \{u_1, \ldots, u_n\}$. Pak

$$h(f) = \dim \mathrm{Im}\, gf = \dim\langle f(u_1), \ldots f(u_n)\rangle = \dim\langle f(u_1)_N, \ldots, f(u_n)_N\rangle = h\left((f)_{NM}\right)$$

□

Lemma 9 *Nechť V je vektorový prostor nad $\mathbb{T}$ konečné dimenze a M, M' jsou dvě báze v něm. Pak matice $(1_V)_{MM'}$ je rovna matici přechodu od báze M k bázi M'.*

Důkaz: Pokud aplikujeme homomorfizmus 1_V na libovolný vektor $u \in V$, dostaneme z definice matice homomorfizmu

$$(u)_M = (1_V(u))_M = (1_V)_{MM'}\,(u)_{M'}$$

To znamená, že pokud vynásobíme maticí přechodu od M k M' "čárkované" souřadnice vektoru u, získáme jeho nečárkované souřadnice, což je přesně způsob, jak transformuje souřadnice matice přechodu od M k M'. □

Věta 23 *Nechť V, W jsou dva vektorové prostory konečné dimenze nad $\mathbb{T}$, M, M' báze V, N, N' báze W a $f : V \to W$ homomorfizmus. Pak*

$$(f)_{N'M'} = (1_W)_{N'N}\,(f)_{NM}\,(1_V)_{MM'}$$

Důkaz: Jde jen o přímočaré užití druhého bodu lemmatu 8 na f zapsané jako složení $1_W \circ f \circ 1_V$. □

Protože matici homomorfizmu můžeme chápat jako zavedení souřadnic na prostoru $\mathrm{Hom}(V, W)$, které jsou v nějakém smyslu kompatibilní se zvolenými souřadnicemi na V a W, popisuje tato věta vlastně pravidlo, jak se tyto souřadnice transformují. V druhém semestru podobným způsobem odvodíme pravidla transformace libovolných tenzorů.

Věta se nejčastěji používá v případě $V = W$, $M = N$, $M' = N'$. Pak s využitím $(1_V)^{-1}_{M'M} = (1_V)_{MM'}$ dostáváme

$$(f)_{M'M'} = (1_V)_{M'M}\,(f)_{MM}\,(1_V)^{-1}_{M'M}$$

Operaci, kdy se matici A přiřadí matice RAR^{-1} nazýváme **konjugováním** matice A maticí R. Víme již, že konjugování zachovává hodnost a podle poslední věty vlastně odpovídá vyjadřování endomorfizmu v různých bázích. O maticích A a B, pro něž existuje regulární matice Q taková, že $B = RAR^{-1}$, řekneme, že jsou **podobné**, značíme $A \sim B$.

Příklad 3 *Spočtěme matici lineárního zobrazení $f : \mathbb{R}^3 \to \mathbb{R}^2$, které je definováno předpisem $f(x, y, z) = (x + z, x - 2y)$ vzhledem ke kanonickým bázím, k bázím $M = \{(2, 3, 0), (3, 4, 0), (0, 0, 1)\}$, $N = \{(1, 2), (1, 3)\}$ a k bázím*

$M' = \{(1,0,1),(1,1,2),(0,1,0)\}$, $N' = \{(1,1),(2,1)\}$. *Určeme jádro zobrazení* gf, *kde* $g : \mathbb{R}^2 \to \mathbb{R}^4$ *je lineární zobrazení přiřazující vektoru* $(3,1)$ *vektor* $(1,-1,0,1)$ *a vektoru* $(2,1)$ *vektor* $(-1,1,0,-1)$.

Nejjednodušší je určit matici

$$(f)_{KK} = \begin{pmatrix} 1 & 0 & 1 \\ 1 & -2 & 0 \end{pmatrix}$$

Sloupce matice $(f)_{NM}$ *jsou souřadnice obrazů báze* M *vzhledem k bázi* N. *Stačí tedy řešit soustavu*

$$\left(\begin{array}{cc|ccc} 1 & 1 & 2 & 3 & 1 \\ 2 & 3 & -4 & -5 & 0 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 0 & 10 & 14 & 3 \\ 0 & 1 & -8 & -11 & -2 \end{array}\right),$$

čili

$$(f)_{NM} = \begin{pmatrix} 10 & 14 & 3 \\ -8 & -11 & -2 \end{pmatrix}$$

Matici $(f)_{N'M'}$ *můžeme spočítat podobně, ale pojďme si vyzkoušet použít matice přechodu* $(1)_{N'N}$ *a* $(1)_{MM'}$. *Ty se dostanou vyjádřením vektorů báze* N *vůči* N'

$$\left(\begin{array}{cc|cc} 1 & 2 & 1 & 1 \\ 1 & 1 & 2 & 3 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 3 & 5 \\ 0 & 1 & -1 & -2 \end{array}\right)$$

a vektorů báze M' *vzhledem k* M

$$\left(\begin{array}{ccc|ccc} 2 & 3 & 0 & 1 & 1 & 0 \\ 3 & 4 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{array}\right) \sim \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -4 & -1 & 3 \\ 0 & 1 & 0 & 3 & 1 & -2 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{array}\right).$$

Tedy

$$(f)_{N'M'} = \begin{pmatrix} 3 & 5 \\ -1 & -2 \end{pmatrix} \begin{pmatrix} 10 & 14 & 3 \\ -8 & -11 & -2 \end{pmatrix} \begin{pmatrix} -4 & -1 & 3 \\ 3 & 1 & -2 \\ 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -5 & -4 \\ 1 & 4 & 2 \end{pmatrix}$$

Snadno ověříme, že přímý výpočet dává stejný výsledek:

$$\left(\begin{array}{cc|ccc} 1 & 2 & 2 & 3 & 0 \\ 1 & 1 & 1 & -1 & -2 \end{array}\right) \sim \left(\begin{array}{cc|ccc} 1 & 0 & 0 & -5 & -4 \\ 0 & 1 & 1 & 4 & 2 \end{array}\right).$$

Zobrazení g jsme dostali definované hodnotami na bázi $P = \{(3,1),(2,1)\}$. Tedy matice g vzhledem k bázi P a kanonické bázi v $\mathbb{R}^4$ je

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

Matice složeného homomorfizmu je součin matic jednotlivých homomorfizmů, pokud je báze v prostředním prostoru pro oba homomorfizmy stejná:

$$(gf)_{KM'} = (g)_{KN'}(f)_{N'M'} = \begin{pmatrix} 1 & -1 \\ -1 & 1 \\ 0 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & -5 & -4 \\ 1 & 4 & 2 \end{pmatrix} = \begin{pmatrix} -1 & -9 & -6 \\ 1 & 9 & 6 \\ 0 & 0 & 0 \\ -1 & -9 & -6 \end{pmatrix}$$

Jádrem homomorfizmu gf jsou všechny vektory, pro něž $gf(u) = 0$, čili pro jejichž souřadnice $(u)_{M'} \equiv (x,y,z)$ vzhledem k M' platí $(gf)_{KM'}(u)_{M'} = 0$. Tedy $(u)_{M'} \in \langle(-6,0,1),(-9,1,0)\rangle$. Ze souřadnic vypočteme samotné bázové vektory jádra $(-6)(1,0,1)+(0,1,0)$ a $(-9)(1,0,1)+(1,1,2)$ a máme

$$\operatorname{Ker} gf = \langle(-6,1,-6),(-8,1,-7)\rangle.$$

Bylo by samozřejmě možné postupovat i jinými způsoby, například vypočítat

$$(gf)_{KK} = (g)_{KK}(f)_{KK} = (g)_{KM'}(1)_{M'K}(f)_{KK}$$

, k čemuž nám ještě chybí matice přechodu od M' ke K, a řešit soustavu rovnic s maticí $(gf)_{KK}$. Pak bychom ušetřili poslední krok, protože výsledek by vyšel v souřadnicích vzhledem ke kanonické bázi.

6 Skalární součin

V této kapitole se podíváme na příklad dodatečné struktury, kterou je možné definovat na vektorovém prostou, na skalární součin. Zavedením skalárního součinu získává čistě algebraický objekt geometrické vlastnosti - umíme říct, kdy jsou vektory kolmé, změřit jejich velikost, definovat úhel mezi nimi. Některé báze se stanou význačnými - ortogonální a ortonormální báze. Mezi lineárními zobrazeními, která byla definována jako podmnožina všech zobrazení, která se chovají hezky k algebraické struktuře vektorového prostoru,

budeme moci vybrat menší podmnožinu lineárních zobrazení, která se chovají hezky i k dodatečné struktuře geometrické, kterou s sebou přináší skalární součin.

Definice 12 *Nechť V je vektorový prostor nad $\mathbb{T}$, přičemž $\mathbb{T}$ je $\mathbb{R}$ nebo $\mathbb{C}$. Zobrazení $g : V \times V \to \mathbb{T}$, které splňuje $\forall u, v, w \in V$, $\forall \lambda \in \mathbb{T}$*

1. $g(\lambda u, v) = \lambda g(u, v) = g(u, \overline{\lambda} v)$
2. $g(u + v, w) = g(u, w) + g(v, w)$, $g(u, v + w) = g(u, v) + g(u, w)$
3. $g(u, v) = \overline{g(v, u)}$
4. $g(u, u) \geq 0$, *přičemž* $g(u, u) = 0$ *nastává pouze pro* $u = 0$,

nazýváme ***skalární součin*** *na V.*

Jsou to vlastně dvě definice v jedné. V reálném případě je $\overline{\lambda} = \lambda$, tedy první dvě podmínky vlastně říkají, že pokud do prvního nebo druhého argumentu zobrazení $g(\cdot, \cdot)$ dosadíme libovolný vektor, pak vzniklé zobrazení z V do $\mathbb{R}$ je lineární. Takové zobrazení z $V \times V$ do $\mathbb{R}$ se nazývá **bilineární forma**. Podobně lze definovat pojem trilineární, kvadrilineární nebo obecně **multilineární formy**. V komplexním případě je situace jiná, při vytknutí konstanty z druhého argumentu přibere tato konstanta komplexní sdružení. Taková vlastnost se nazývá **antilinearitou**, dobrým příkladem antilineárního zobrazení je $f : \mathbb{C} \to \mathbb{C}$, $f(z) := \bar{z}$. Pro zobrazení z $V \times V$ do $\mathbb{C}$, které je v jedné složce lineární a v druhé antilineární, se používá pojem **seskvilineární forma**.

Třetí podmínka opět říká něco trochu jiného na reálném a na komplexním vektorovém prostoru. Mluvíme o **symetrické** bilineární, resp. **hermitovské** seskvilineární formě. Poslední podmínka má smysl v reálném i komplexním případě, protože z předchozí podmínky plyne, že $g(u, u)$ je vždy reálné číslo a má tedy smysl ho porovnávat s nulou. O bilineární formě, splňující čtvrtou podmínku říkáme, že je **pozitivně definitní**. Funkce $\|u\|_g := \sqrt{g(u, u)}$ se nazývá **norma** příslušná skalárnímu součinu g. Pozitivní definitnost zaručuje, že norma je dobře definovaná a že nulovou normu má pouze nulový vektor.

Pokud bude jasné, s jakým skalárním součinem na prostoru pracujeme, budeme jej značit místo $g(u, v)$ jen (u, v) a jeho normu $\|u\|$. Naopak, pokud budeme chtít explicitně vyznačit, že na prostoru V používáme skalární součin g, budeme jej psát jako dvojici (V, g).

6.1 Geometrie definovaná skalárním součinem

Skalární součin umožňuje definovat na vektorovém prostoru pojem vzdálenosti. Abstraktně se vzdálenost na nějaké množině zavádí pomocí pojmu **metriky**:

Definice 13 *Nechť M je množina. Funkci $\rho : M \times M \to \mathbb{R}$ nazýváme metrikou na M, pakliže splňuje pro všechny body $x, y, z \in M$ následující axiomy:*

1. $\rho(x, y) \geq 0$ *a* $\rho(x, y) = 0$ *právě když* $x = y$
2. $\rho(x, y) = \rho(y, x)$
3. $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$

Dvojici (M, ρ) pak nazýváme ***metrický prostor****.*

První axiom říká, že vzdálenost je vždy nezáporná a žádné dva různé body nemohou mít nulovou vzdálenost. Druhý axiom vyjadřuje symetrii pojmu vzdálenosti a třetímu se říká **trojúhelníková nerovnost**.

Příklad 4 *Na prostoru $\mathbb{R}^n$ lze zavést metriku různými způsoby. Tradiční je metrika euklidovská, $\rho_2(x, y) := \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2}$. Jsou ale i jiné způsoby, například metrika manhattanská, $\rho_1(x, y) := \sum_{i=1}^{n} |x_i - y_i|$, nebo metrika maximová, $\rho_\infty(x, y) := \max_{1 \leq i \leq n} |x_i - y_i|$. Zkuste si u každé z nich ověřit platnost axiomů.*

Věta 24 *Nechť V je vektorový prostor se skalárním součinem. Pak pro libovolné vektory $u, v \in V$ platí*

1. $|(u, v)| \leq \|u\|\|v\|$
2. $\|u - v\| \leq \|u\| + \|v\|$
3. *Dvojice (V, ρ), kde $\rho : V \times V \to \mathbb{R}$ je definována $\rho(u, v) := \|u - v\|$, tvoří metrický prostor.*

Důkaz: Pro $v = 0$ je první tvrzení zřejmé. Pokud $v \neq 0$, pak

$$0 \leq \left\| u - \frac{(u,v)}{\|v\|^2} v \right\|^2 = \|u\|^2 - \frac{(u,v)}{\|v\|^2}(v,u) - \frac{\overline{(u,v)}}{\|v\|^2}(u,v) + \frac{|(u,v)|^2}{\|v\|^4}\|v\|^2 =$$
$$= \|u\|^2 - 2\frac{|(u,v)|^2}{\|v\|^2} + \|u\|^2 - \frac{|(u,v)|^2}{\|v\|^2} = \|u\|^2 - \frac{|(u,v)|^2}{\|v\|^2},$$

což vede po úpravě na dokazovanou nerovnost. Tu pak využijeme na dokázání druhého tvrzení:

$$\|u-v\|^2 = \|u\|^2-(u,v)-(v,u)+\|v\|^2 \leq \|u\|^2+2\|u\|\|v\|+\|v\|^2 = (\|u\| + \|v\|)^2$$

Třetí tvrzení je zřejmé: první axiom metriky je důsledkem čtvrté vlastnosti skalárního součinu, druhý axiom plyne z první vlastnosti a trojúhelníková nerovnost je důsledkem druhého tvrzení této věty. □

Prvnímu tvrzení se říká Cauchyova nerovnost (někdy též Schwarzova nebo Buňakovského). Věta vlastně ověřuje korektnost následující definice, která zavádí na vektorovém prostoru se skalárním součinem nejdůležitější geometrické pojmy:

Definice 14 *Nechť V je vektorový prostor se skalárním součinem g, $u, v \in V$. Pak číslo $\|u - v\|$ nazýváme **vzdáleností vektorů** u a v. Řekneme, že $u, v \in V$ jsou **kolmé**, pokud $g(u, v) = 0$, značíme $u \perp v$. Pokud V je reálný vektorový prostor, pak číslo $\varphi \in \langle 0, \pi \rangle$, pro které platí $\cos\varphi = \frac{(u,v)}{\|u\|\|v\|}$, nazýváme **úhlem mezi vektory** u a v.*

Metrice $\rho(u, v) := \|u - v\|$ se říká metrika indukovaná skalárním součinem. Pokud V je reálný vektorový prostor, splňuje tato metrika vztah

$$(u, v) = \frac{1}{4}\left(\rho(u, -v)^2 - \rho(u, v)^2\right),$$

kterému se někdy říká **polarizační identita** a který se dá snadno dokázat z definic (zkuste si a pokuste se také napsat verzi pro komplexní vektorový prostor). Je to vlastně rekonstrukce skalárního součinu z jím indukované metriky. Metriky, které polarizační identitu nesplňují, nemohou být indukovány skalárním součinem. Ověřte sami, že to je případ maximové i manhattanské metriky a zkuste také dokázat, že pokud ρ splňuje vlastnosti metriky a definujeme $\forall u, v \in V$ číslo (u, v) pomocí polarizační identity, pak toto zobrazení splňuje vlastnosti skalárního součinu.

Pokud (M, ρ) a (N, σ) jsou dva metrické prostory a $f : M \to N$ je zobrazení, které $\forall x, y \in M$ splňuje $\rho(x, y) = \sigma(f(x), f(y))$, pak se toto f nazývá **izometrie**. Z polarizační identity plyne, že homomorfizmus $f : (V, g) \to (W, h)$ dvou vektorových prostorů se skalárním součinem je izometrie, právě tehdy když $\forall u, v \in V$ platí $g(u, v) = h(f(u), f(v))$. Lineární zobrazení s touto vlastností se nazývají v reálném, resp. komplexním případě **ortogonální**, resp. **unitární**. Ze čtvrté vlastnosti skalárního součinu plyne, že takové zobrazení musí být monomorfizmus. Pokud je $(V, g) = (W, h)$ a jde tedy

o endomorfizmus, musí být f izomorfizmem. Je jednoduché ověřit, že množina všech ortogonálních endomorfizmů prostoru (V, g) tvoří grupu, a stejně tak i množina všech unitárních endomorfizmů.

7 Skalární součin v souřadnicích

Je-li V vektorový prostor konečné dimenze se skalárním součinem, $M = \{u_1, \ldots, u_n\}$ jeho báze, u, v dva vektory z V a $x \equiv (x_1, \ldots, x_n)^T = (u)_M$, $y \equiv (y_1, \ldots, y_n)^T = (v)_M$ jejich souřadnice, potom

$$(u, v) = \left(\sum_{i=1}^{n} x_i u_i, \sum_{i=1}^{n} y_i u_i \right) = \sum_{i,j=1}^{n} x_i \overline{y}_j (u_i, u_j) = x^T Q \overline{y},$$

kde jsme číslo (u_i, u_j) identifikovali jako ij-tý element matice Q. Ta se nazývá **maticí skalárního součinu** vzhledem k bázi M. Je to symetrická, resp. hermitovská matice, neboť $(u_i, u_j) = \overline{(u_j, u_i)}$, tedy $Q = Q^+$. Jak se na matici Q projeví podmínka pozitivní definitnosti, to je trochu složitější a více o tom budeme moci říct až v příštím semestru, kdy budeme studovat bilineární formy podrobněji. Zde se omezíme jen na pozorování, že pro $Q = E$ je

$$(u, v) = \sum_{i=1}^{n} x_i \overline{y}_i$$
$$\|u\| = \sqrt{|x_1|^2 + |x_2|^2 + \ldots + |x_n|^2}$$

a pozitivní definitnost je zjevně zaručena. Skalárnímu součinu na $\mathbb{R}^n$, resp. $\mathbb{C}^n$, jehož matice vzhledem ke kanonické bázi je E, se říká **standardní skalární součin**. Vidíme, že standardní skalární součin je právě ten, který indukuje na $\mathbb{R}^n$ euklidovskou metriku.

Co se stane s maticí Q při změně báze? Pokud M' je další báze ve V a R je matice přechodu od M k M', tedy pro souřadnice platí $x = Rx'$, pak také $x^T = x'^T R^T$ a tudíž

$$(u, v) = x^T Q \overline{y} = x'^T R^T Q \overline{R} \overline{y}', \tag{1}$$

čili maticí skalárního součinu vzhledem k M' je $R^T Q \overline{R}$. Pokud chceme, aby matice skalárního součinu vzhledem k bázi M' byla stejná jako k M, dostáváme podmínku $Q = R^T Q \overline{R}$. Všechny matice R, které pro dané pevné Q

tuto podmínku splňují, tvoří grupu vzhledem k násobení (ověřte sami!). Speciálně pokud $Q = E$, zjednoduší se podmínka na $R^+R = E$ v komplexním případě, resp. na $R^TR = E$ v reálném případě. Takovým maticím R se pak říká **unitární**, resp. **ortogonální**, a příslušná grupa matic stupně n se značí $U(n)$, resp. $O(n)$.

Jaký je vztah mezi unitárními maticemi a unitárními endomorfizmy? Pokud V_n je prostor se skalárním součinem, $f \in \mathrm{End}(V)$ je unitární endomorfizmus, M je báze V_n, vůči níž mají vektory $u, v \in V$ souřadnice $(u)_M = x$, $(v)_M = y$, f matici A a skalární součin matici Q, pak

$$x^TQ\overline{y} = (u, v) = (f(u), f(v)) = x^TA^TQ\overline{A}\overline{y}$$

Pokud $Q = E$, dostáváme $A^+A = E$. Tedy vzhledem k bázi, vůči níž je matice skalárního součinu jednotková, má unitární endomorfizmus unitární matici a podobně ortogonální endomorfizmus má vůči takové bázi ortogonální matici. Existuje taková báze vždy a pokud ano, jak ji najít?

8 Ortonormální báze

Definice 15 *Nechť V je prostor se skalárním součinem g. Bázi prostoru V, v níž je každý vektor kolmý na všechny ostatní, nazýváme **ortogonální báze**, pokud navíc je norma všech vektorů rovna jedné, mluvíme o **ortonormální bázi**.*

Pokud V_n je vektorový prostor konečné dimenze, pak matice skalárního součinu vzhledem k ortogonální bázi je diagonální s kladnými hodnotami na diagonále a vzhledem k ortonormální bázi je to jednotková matice E. Vidíme tedy, že je-li M ortonormální báze, pak M' je také ortonormální právě když matice přechodu od M k M' je ortogonální, resp. unitární matice. Pokud najdeme jednu ortonormální bázi, pak už se dokážeme alespoň teoreticky dostat ke všem ostatním prostřednictvím elementů $O(n)$ resp. $U(n)$. Postup, jak ortonormální bázi získat postupnými úpravami libovolné báze, nese název **Grammova-Schmidtova ortogonalizace**. Uvažujme $M = \{u_1, \ldots, u_n\}$ bázi V_n a definujme $v_1 := u_1$. Vektor

$$v_2 := u_2 - \frac{(u_2, v_1)}{\|v_1\|^2} v_1,$$

je kolmý na v_1, stačí dosadit. Dále definujme

$$v_3 := u_3 - \frac{(u_3, v_1)}{\|v_1\|^2} v_1 - \frac{(u_3, v_2)}{\|v_2\|^2} v_2,$$

opět vidíme, že v_3 je kolmé na v_1 i na v_2. Pokračováním tohoto postupu získáme ortogonální bázi a vydělením každého vektoru jeho normou bázi ortonormální. Přesně to formuluje následující věta:

Věta 25 *Nechť V_n je vektorový prostor se skalárním součinem g a $M = \{u_1, \ldots, u_n\}$ jeho báze. Pak existuje ortonormální báze $M' = \{u'_1, \ldots, u'_n\}$ prostoru V_n taková, že $\forall k \in \{1, \ldots, n\}$, $\langle u_1, \ldots, u_k \rangle = \langle u'_1, \ldots, u'_k \rangle$.*

Důkaz: Budeme postupovat indukcí podle n. Pokud $n = 1$, pak definujme $v_1 := u_1$, $u'_1 := \frac{v_1}{\|v_1\|}$, tvrzení věty platí. Nechť nyní $n > 1$ a předpokládejme platnost tvrzení pro všechny prostory dimenze menší nebo rovné n. Takovým prostorem je i $\langle u_1, \ldots, u_n \rangle$, takže podle indukčního předpokladu v něm máme ortonormální bázi $\{u'_1, \ldots, u'_n\}$, pro kterou $\forall k \in \{1, \ldots, n\}$, $\langle u_1, \ldots, u_k \rangle = \langle u'_1, \ldots, u'_k \rangle$. Definujme nyní

$$v_{n+1} = u_{n+1} - \sum_{i=1}^{n} (u_{n+1}, u'_i) u'_i.$$

Tento vektor je kolmý na u'_i, $\forall i \in \{1, \ldots, n\}$. Dále po úpravě vidíme, že $u_{n+1} \in \langle v_{n+1} \rangle \vee \langle u'_1, \ldots, u'_n \rangle = \langle v_{n+1} \rangle \vee \langle u_1, \ldots, u_n \rangle$, tedy v_{n+1} nemůže být nulový vektor. Proto má smysl definovat $u'_{n+1} := \frac{v_{n+1}}{\|v_{n+1}\|}$. Je pak zjevné, že $\|u'_{n+1}\| = 1$, $u'_{n+1} \in \{u'_1, \ldots, u'_n\}^\perp$ a $\langle u'_1, \ldots, u'_{n+1} \rangle = \langle u_1, \ldots, u_{n+1} \rangle$. Tím je věta dokázána. □

Triviálním důsledkem věty je, že v každém vektorovém prostoru (V_n, g) nad $\mathbb{T}$ existuje ortonormální báze. Je zřejmé, že lineární zobrazení, které i-tému bázovému vektoru této báze přiřadí i-tý prvek kanonické báze $\mathbb{T}^n$, je izometrie (V_n, g) a $\mathbb{T}^n$ se standardním skalárním součinem. Dostáváme tedy zesílení dříve dokázaného tvrzení, že každý vektorový prostor konečné dimenze je izomorfní nějakému $\mathbb{T}^n$, nyní již víme, že je mu dokonce izometrický (ať už je skalární součin na V jakýkoli).

Zastavme se ještě u klíčového kroku v důkazu věty. Máme ortonormální množinu $M = \{u'_1, \ldots, u'_n\}$, jejímž lineárním obalem je $W := \langle M \rangle$. Zobrazení $P_W : V \to V$, které vektoru u přiřazuje vektor $\sum_{i=1}^{n} (u, u'_i) u'_i$ je zjevně homomorfizmus, jehož obrazem je právě W. Navíc platí, že $P_W P_W = P_W$ (ověřte

sami) a všechny vektory kolmé na W zobrazuje P_W na nulu. Je to tedy **ortogonální projekce** na podprostor W. V důkazu věty tedy konstruujeme v_{n+1} tak, že odečítáme od u_{n+1} jeho ortogonální průmět na W, vzniklý rozdíl je kolmý na W a tedy i na všechny vektory z M.

Mezi ortogonálními maticemi a ortonormálními bázemi je ještě jeden zajímavý vztah. Podmínka ortogonality matice R se dá přepsat jako $R^T R = E$. Prvek na pozici ij součinu matic na levé straně je vlastně euklidovským skalárním součinem i-tého a j-tého řádku matice R, takže podmínka ortogonality znamená, že řádky matice R tvoří ortonormální bázi $\mathbb{R}^n$. Podobně řádky unitární matice tvoří ortonormální bázi $\mathbb{C}^n$. Vynásobením rovnosti $R^T R = E$, resp. $R^+ R = E$ zleva R a zprava R^{-1} dostáváme $RR^T = E$, resp. $RR^+ = E$, tedy že ortonormální bázi tvoří i sloupce.

Příklad 5 *Nalezněme ortonormální bázi podprostoru* $\langle (1,2,2,-1), (1,1,-5,3), (3,2,8,-7)\rangle$ *v* $\mathbb{R}^4$ *se standardním skalárním součinem. Označme vektory po řadě* u_1, u_2, u_3 *a vezměme* $v_1 := u_1$. *Platí* $\|v_1\|^2 = 10$ *a* $(u_2, v_1) = 1+2-10-3 = -10$. *Tedy*

$$v_2 = u_2 - \frac{(u_2, v_1)}{\|v_1\|^2} v_1 = (1,1,-5,3) - \frac{-10}{10}(1,2,2,-1) = (2,3,-3,2)$$

Vidíme, že skutečně $v_2 \perp v_1$. *Spočteme* $\|v_2\|^2 = 26$, $(u_3, v_1) = 30$ *a* $(u_3, v_2) = -26$, *takže*

$$v_3 = (3,2,8,-7) - \frac{30}{10}(1,2,2,-1) - \frac{-26}{26}(2,3,-3,2) = (2,-1,-1,-2),$$

což je opět vektor kolmý na v_2 *i* v_1, $\|v_3\|^2 = 10$. *Nakonec vydělíme každý vektor jeho normou a získáváme ortonormální bázi*

$$\left\{ \frac{1}{\sqrt{10}}(1,2,2,-1), \frac{1}{\sqrt{26}}(2,3,-3,2), \frac{1}{\sqrt{10}}(2,-1,-1,-2) \right\}$$

9 Ortogonální doplněk a dualita

Množinu všech vektorů kolmých na všechny prvky množiny $M \subset V$ nazýváme **ortogonální doplněk** M, značíme $M^\perp$. Jak souvisí tento pojem s doplňkem podprostoru definovaným v kapitole o vektorových prostorech?

Věta 26 *Nechť* V *je vektorový prostor se skalárním součinem* g, W *jeho podprostor konečné dimenze. Pak ortogonální doplněk* $W^\perp$ *podprostoru* W *je doplňkem podprostoru* W *ve* V_n, *tedy* $W \oplus W^\perp = V_n$.

Důkaz: Dokazujeme vlastně dvě tvrzení: $W \cap W^\perp = 0$ a $W \vee W^\perp = V$. Pokud $u \in W \cap W^\perp$, pak $u \perp u$, čili $(u,u) = 0$ a tudíž $u = 0$. Pro druhé tvrzení předpokládejme, že existuje $u \in V_n$, $u \notin W \oplus W^\perp$. Zvolme ve W ortonormální bázi $\{u_1, \ldots, u_k\}$ a položme $v := u - \sum_{i=1}^k (u, u_i)u_i$. Pak také $v \notin W \oplus W^\perp$ a tedy i $v \notin W^\perp$. Na druhou stranu pro libovolný vektor $w = \sum_{j=1}^k r_j u_j$ z W platí

$$(v,w) = \left(u - \sum_{i=1}^k (u,u_i)u_i, \sum_{j=1}^k r_j u_j\right) = \\ = \sum_{j=1}^k \overline{r}_j (u,u_j) - \sum_{j=1}^k \sum_{i=1}^k \overline{r}_j (u,u_i)(u_i,u_j) = 0,$$

tedy $v \in W^\perp$, což je spor. □

Ortogonální doplněk podmnožiny ve V je podprostorem V. Stačí ověřit, že $u^\perp \equiv \{u\}^\perp$ je podprostor pak již musí být $M^\perp = \bigcap_{u \in M} u^\perp$ jakožto průnik podprostorů také. Platí též, že $M^\perp = \langle M \rangle^\perp$, neboť pokud je vektor kolmý na všechny prvky z M, je kolmý i na každou jejich lineární kombinaci a naopak, pokud je kolmý na všechny lineární kombinace, pak je speciálně kolmý i na ty z nich, které jsou rovny přímo vektorům z M. Operace ortogonálního doplňku tedy přiřazuje podprostorům ve V jiné podprostory. Pokud navíc V je prostorem konečné dimenze n a W jeho podprostor, pak z předchozí věty plyne $\dim W^\perp = n - \dim W$. Použijeme-li operaci ortogonálního doplňku dvakrát, vidíme jednak, že $\forall w \in W$ je w kolmé na všechny prvky z $W^\perp$, tedy $W \leq (W^\perp)^\perp$. Zároveň $\dim (W^\perp)^\perp = n - \dim W^\perp = \dim W$, tudíž musí být $(W^\perp)^\perp = W$. Operacím, které jsou stejně jako vzetí ortogonálního doplňku k podprostoru samy sobě inverzní, se obecně říká **involuce** nebo **duality**, dalšími příklady jsou třeba komplexní sdružení nebo středová či osová souměrnost v prostoru. Dualita zprostředkovaná skalárním součinem páruje podprostory do dvojic, jejichž členové jsou si navzájem ortogonálním doplňkem. Podobně jsou párována do dvojic i lineární zobrazení:

Definice 16 *Nechť $(V,g), (W,h)$ jsou dva prostory nad $\mathbb{T}$ se skalárním součinem a $f \in \mathrm{Hom}(V,W)$. Pak homomorfizmus $f^* \in \mathrm{Hom}(W,V)$, který $\forall v \in V$, $\forall w \in W$ splňuje*

$$h(w, f(v)) = g(f^*(w), v),$$

*nazýváme **duálním** nebo též **adjungovaným homomorfizmem** k f.*

Nechť M je ortonormální báze (V_m, g), N je ortonormální báze (W_n, h), $f \in \mathrm{Hom}(V_m, W_n)$, $(v)_M \equiv x \equiv (x_1, \ldots, x_m)^T$, $(w)_N \equiv y \equiv (y_1, \ldots, y_n)^T$ a $A := (f)_{NM}$, $B := (f^*)_{MN}$. Matice skalárního součinu g i h je vzhledem k libovolné ortogonální bázi jednotková. Pak

$$\sum_{i=1}^{n} y_i \overline{\left(\sum_{j=1}^{m} a_{ij} x_j \right)} = (w, f(v)) = (f^*(w), v) = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \sum b_{ji} y_i \right) \overline{x}_j$$

Porovnáme-li obě strany, vidíme, že rovnost pro libovolná v a w vyžaduje, aby $\overline{a}_{ij} = b_{ji}$ pro libovolné indexy i, j, čili $B = A^+$ nebo v reálném případě $B = A^T$. Pokud tedy A je matice zobrazení f, pak matice transponovaná, resp. hermitovsky sdružená, je maticí zobrazení adjungovaného. Odtud je konečně vidět, čím je zavedení operace transponování a hermitovského sdružení matice motivováno. Protože jsou tyto operace definovány pro libovolnou matici, je zřejmé, že na prostoru konečné dimenze má každý homomorfizmus k sobě homomorfizmus adjungovaný. Z $(A^T)^T = A$ a $(A^+)^+ = A$ plyne, že $(f^*)^* = f$, jedná se tedy skutečně o dualitu.

Konečně se dostáváme do bodu, kdy je můžeme nově interpretovat a elegantněji dokázat tvrzení $h(A) = h(A^T)$ a $h(B) = h(B^+)$ z kapitoly o hodnosti matice.

Věta 27 *Nechť $A \in M_{mn}(\mathbb{R})$, pak $h(A) = h(A^T)$. Nechť $B \in M_{mn}(\mathbb{C})$, pak $h(B) = h(B^\dagger)$.*

Tvrzení vlastně říká, že obraz homomorfizmu z $\mathbb{T}^m$ do $\mathbb{T}^n$ má stejnou dimenzi jako obraz jeho duálu. Vektor $w \in \mathbb{T}^n$ je prvkem $(\mathrm{Im}\, f)^\perp$, právě když $\forall v \in \mathbb{T}^m$ platí

$$0 = h(w, f(v)) = g(f^*(w), v),$$

tedy $f^*(w) \in (\mathbb{T}^m)^\perp = 0$ neboli $w \in \mathrm{Ker}\, f^*$. Tedy $(\mathrm{Im}\, f)^\perp = \mathrm{Ker}\, f^* \subset \mathbb{T}^n$, čili

$$\dim \mathrm{Im}\, f + \dim \mathrm{Ker}\, f^* = n$$

Podle věty o dimenzi jádra a obrazu ale také

$$\dim \mathrm{Im}\, f^* + \dim \mathrm{Ker}\, f^* = n$$

Tedy $\dim \mathrm{Im}\, f = \dim \mathrm{Im}\, f^*$.

10 Determinanty

V kapitole o maticích jsme definovali pojem stopy čtvercové matice A stupně n, $\operatorname{Tr} A = \sum_{i=1}^{n} a_{ii}$. Jednou z jejích vlastností je, že pro tři matice $A, B, C \in M_{nn}(\mathbb{T})$ je $\operatorname{Tr} ABC = \operatorname{Tr} CAB$. Speciálně pro R regulární platí $\operatorname{Tr} R^{-1}AR = \operatorname{Tr} RR^{-1}A = \operatorname{Tr} A$. Pokud tedy A je matice endomorfizmu $f \in \operatorname{End} V_n$ vzhledem k bázi M, pak matice tohoto endomorfizmu vzhledem k jakékoli jiné bázi M' má tvar $R^{-1}AR$, kde R je matice přechodu od M k M', a tedy má i stejnou stopu. Lze tedy definovat $\operatorname{Tr} f$ stopu endomorfizmu f. Je to číslo, které je třeba spočítat z vyjádření f vzhledem k nějaké bázi, ale výsledek na volbě této báze nezávisí. Takovému číslu se v matematice říká **invariant**. V této kapitole se budeme zabývat jiným invariantem, kterému se říká **determinant matice**. Determinant má oproti stopě názornější geometrický význam, jeho definice je ale komplikovanější, a než ji budeme moci napsat, musíme se nějaký čas zabývat něčím, co samo o sobě s lineární algebrou nemá příliš společného.

11 Permutace

Permutace je bijektivní zobrazení konečné množiny na sebe. Množina může být jakákoliv, ale obvykle se bere prostě $\{1, \ldots, n\}$. Množinu všech permutací této množiny značíme S_n. Složení dvou permutací je permutace, identické zobrazení je permutace a inverzní zobrazení k permutaci je také permutace. Tedy S_n s operací skládání tvoří grupu, tzv. **symetrickou grupu** na n prvcích. Místo skládání někdy mluvíme o součinu permutací. Obvyklý zápis permutace π je pomocí dvou řádků

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix},$$

a pokud nehrozí nedorozumění, můžeme psát jenom řádek obrazů $(\pi(1), \pi(2), \ldots, \pi(n))$. Je snadné dokázat indukcí, že na n prvcích existuje právě $n!$ permutací.

Příklad 6 *Grupa S_3 sestává právě z šesti prvků:* $(1,2,3)$, $(1,3,2)$, $(2,1,3)$, $(2,3,1)$, $(3,1,2)$ *a* $(3,2,1)$. *Inverzní prvek k $\pi = (2,3,1)$ je $\pi^{-1} = (3,1,2)$, protože $\pi(1) = 2$, takže musí být $\pi^{-1}(2) = 1$, atd. Příklad složení dvou permutací zapíšeme pro přehlednost ve dvouřádkovém zápise:*

$$\pi \circ \rho \equiv \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

Levá strana je složení dvou permutací, takže nejprve je třeba zobrazit každý prvek permutací ρ a poté permutací π, např.

$$(\pi \circ \rho)(1) = \pi(\rho(1)) = \pi(3) = 1$$

Definice 17 *Nechť $\pi \in S_n$ a (i,j), $i < j$ je dvojice indexů z $\{1,\ldots,n\}$ Řekneme, že $(\pi(i), \pi(j))$* ***tvoří inverzi*** *v π, pakliže $\pi(i) > \pi(j)$. Počet všech takových dvojic nazveme $I(\pi)$,* ***počet inverzí*** *permutace π.*

Pozor, pojmy tvořit inverzi a počet inverzí nemají žádnou souvislost s inverzní permutací, jsou to prostě ty dvojice čísel, které se na druhém řádku zápisu permutace vyskytují v opačném pořadí než na prvním. Například pro permutaci $(4,2,1,3)$ tvoří inverzi dvojice $(4,2)$, $(4,1)$, $(4,3)$ a $(2,1)$.

Lemma 10 *Nechť $\pi, \rho \in S_n$. Pak existuje celé číslo k takové, že $I(\pi \circ \rho) = I(\pi) + I(\rho) + 2k$.*

Důkaz: Nechť $i < j$, pak nastává právě jedna z následujících možností:

$$\begin{aligned}
(--): &\quad \rho(i) < \rho(j), \pi(\rho(i)) < \pi(\rho(j)) \\
(-+): &\quad \rho(i) < \rho(j), \pi(\rho(i)) > \pi(\rho(j)) \\
(+-): &\quad \rho(i) > \rho(j), \pi(\rho(i)) > \pi(\rho(j)) \\
(++): &\quad \rho(i) > \rho(j), \pi(\rho(i)) < \pi(\rho(j))
\end{aligned}$$

Označme počty dvojic odpovídající těmto variantám jako I_{--}, I_{-+}, I_{+-} a I_{++}. Varianty $(+-)$ a $(++)$ dávají inverzi permutace ρ, varianty $(-+)$ a $(++)$ inverzi permutace π a varianty $(-+)$ a $(+-)$ inverzi permutace $\pi \circ \rho$. Tedy

$$I(\pi \circ \rho) = I_{-+} + I_{+-} = (I_{-+} + I_{++}) + (I_{+-} + I_{++}) - 2I_{++} = I(\pi) + I(\rho) + 2k,$$

kde $k = -I_{++}$. □

Definice 18 *Nechť $\pi \in S_n$.* ***Znaménkem permutace*** *budeme rozumět číslo* $\operatorname{sgn}(\pi) := (-1)^{I(\pi)}$.

Identická permutace id neobsahuje žádnou inverzi, tedy její znaménko je $\operatorname{sgn}(\mathrm{id}) = 1$. Z lemmatu plyne, že $\operatorname{sgn}(\pi \circ \rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$, a z těchto dvou vlastností dohromady, že $\operatorname{sgn}(\pi^{-1} \circ \pi) = 1$, tedy $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$.

Označíme-li $\mathbb{Z}_2$ grupu tvořenou množinou $\{1, -1\}$ s operací násobení, znamenají tyto vlastnosti, že zobrazení $\operatorname{sgn} : S_n \to \mathbb{Z}_2$ je **grupový homomorfizmus**. Podobně jako u vektorových prostorů, i zde pojem homomorfizmus vyjadřuje, že se zobrazení chová hezky k dané struktuře, v tomto případě struktuře grupy. Můžeme definovat **jádro grupového homomorfizmu** $\operatorname{Ker} \operatorname{sgn}$ jako množinu všech $\pi \in S_n$, pro něž $\operatorname{sgn} \pi = 1$. To je také grupa (ověřte sami), kterou označujeme A_n, grupa všech **sudých permutací**, nebo též **alternující grupa**. Permutace, pro které $\operatorname{sgn} \pi = -1$ se nazývají **liché** a zjevně grupu netvoří.

Označme $\operatorname{Supp} \pi$ **nosič permutace**, tedy množinu všech indexů $i \in \{1, \ldots, n\}$ takových, že $\pi(i) \neq i$. Permutace s dvouprvkovým nosičem se nazývají **transpozice**, vlastně pouze vyměňují nějaký prvek i s jiným prvkem j, budeme je značit $[i, j]$. Například $(1, 4, 3, 2)$ je transpozice $[2, 4] \equiv [4, 2]$.

Transpozice $[1, 2]$ obsahuje právě jednu inverzi a je to tedy lichá permutace. Transpozici $[i, j]$, $i < j$ lze zapsat jako $\rho^{-1} \circ [1, 2] \circ \rho$, kde ρ je libovolná permutace, pro kterou $\rho(i) = 1$, $\rho(j) = 2$. Pak ale

$$\operatorname{sgn}([i, j]) = \operatorname{sgn}(\rho^{-1}) \operatorname{sgn}([1, 2]) \operatorname{sgn}(\rho) = \operatorname{sgn}([1, 2]),$$

tedy každá transpozice je lichá permutace.

Transpozice je speciální případ **cyklu**, což je permutace s k-prvkovým nosičem $\{i_1, i_2, \ldots i_k\}$ taková, že $\pi(i_j) = i_{j+1}$ pro všechna $j \in \{1, \ldots, k-1\}$ a $\pi(i_k) = i_1$. Cyklus označíme $[i_1, i_2, \ldots, i_k]$, číslo k se nazývá **délkou cyklu**. Dva cykly nazveme nezávislými, pokud jsou jejich nosiče disjunktní.

Věta 28 *Každou permutaci lze zapsat jako součin nezávislých cyklů. Každou permutaci lze zapsat jako součin transpozic.*

Důkaz: Stačí vzít libovolný prvek $i_{1,1} \in \operatorname{Supp} \pi$. Jeho obraz označíme $i_{1,2} := \pi(i_{1,1})$, dále $i_{1,3} := \pi(i_{1,2})$ atd. Množina je konečná, takže pro nějaké $k_1 \in N$ musí nastat $i_{1,k_1+1} = i_{1,1}$. Definujme π_1 permutaci, jejíž nosič je $\{i_{1,1}, \ldots, i_{1,k_1}\}$ a na této množině má stejné hodnoty jako π, je to zjevně cyklus délky k_1. Zvolme $i_{2,1} \in \operatorname{Supp} \pi \setminus \operatorname{Supp} \pi_1$ a opakujme postup, získáme takto N cyklů π_j o délce k_j, které jsou nezávislé a platí $\pi = \pi_1 \circ \ldots \circ \pi_N$.

Cyklus $[i_1, \ldots, i_k]$ je roven například součinu transpozic $[i_1, i_2][i_2, i_3] \ldots [i_{k-1} i_k]$ (rozmyslete si podrobně). Pokud tento rozklad použijeme pro každý cyklus $\pi_1, \ldots, \pi_N$, dostáváme zápis permutace jako součinu transpozic. □

Z důkazu je zřejmé, že rozklad na nezávislé cykly je až na pořadí jednoznačný. Rozklad na transpozice jednoznačný zdaleka není, už cyklus lze

rozložit na transpozice mnoha jinými způsoby (najděte nějaký) a také lze do kteréhokoli místa vložit součin typu $[i,j][j,i]$. Protože ale víme, že transpozice je lichá permutace a že sgn je grupový homomorfizmus, vidíme, že znaménko permutace lze také spočítat jako $(-1)^N$, kde N je počet transpozic v libovolném rozkladu na transpozice, nebo také $(-1)^C$, kde C je počet cyklů sudé délky v rozkladu na nezávislé cykly. To bývá obvykle rychlejší metoda výpočtu znaménka permutace než vypisování seznamu všech inverzí.

Věta 29 *Nechť $n > 1$. Grupa A_n má $\frac{n!}{2}$ prvků.*

Důkaz: Zvolme pevnou transpozici, například $[1,2]$. Zobrazení $T : S_n \to S_n$ definované jako $T(\pi) = [1,2] \circ \pi$ je bijekce na konečné množině, přičemž obrazem liché permutace je sudá a naopak. Pak ale množina lichých a sudých permutací musí být stejně velká, tedy sudých permutací je právě $\frac{n!}{2}$. □

11.1 Determinant

Definice 19 *Nechť $A \in M_{nn}(\mathbb{T})$. Determinantem matice A nazveme číslo*

$$\det A := \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} a_{2\pi(2)} \dots a_{n\pi(n)}$$

Vidíme tedy, že determinant je součet $n!$ členů, z nichž každý je součinem n elementů matice vynásobeným znaménkem permutace. V každém takovém součinu se vyskytuje právě jeden element z každého řádku a právě jeden element z každého sloupce. Definice je tedy nejen znebespadlá, ale také prakticky nepříliš použitelná, protože s rostoucím n roste počet operací velmi rychle.

Místo $\det A$ budeme také používat označení $|A|$ nebo u konkrétní matice nahradíme závorky svislicemi. Pokud A je matice 2×2, pak

$$\det A \equiv \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \operatorname{sgn}(12) a_{11} a_{22} + \operatorname{sgn}(21) a_{12} a_{21} = a_{11} a_{22} - a_{12} a_{21}$$

Podobně

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} a_{22} a_{33} + a_{12} a_{23} a_{31} + a_{13} a_{21} a_{32}$$
$$- a_{11} a_{23} a_{32} + a_{13} a_{22} a_{31} - a_{12} a_{21} a_{33} +$$

Označme řádky matice A jako $a_1, a_2, \ldots, a_n$, determinant matice A bude výhodné občas značit také jako $|a_1, \ldots, a_n|$.

Věta 30 *Nechť $A \in M_{nn}(\mathbb{T})$.*

1. $|A| = |A^T|$
2. *Pokud $r \in \mathbb{T}$, pak* $|a_1, \ldots, ra_i, \ldots, a_n| = r|a_1, \ldots, a_i, \ldots, a_n|$.
3. *Pokud* $|a_1, \ldots, a_i + a_i', \ldots, a_n| = |a_1, \ldots, a_i, \ldots, a_n| + |a_1, \ldots, ra_i', \ldots, a_n|$
4. *Pokud* $1 \leq i < j \leq n$, *pak* $|a_1, \ldots, a_i, \ldots, a_j, \ldots, a_n| = -|a_1, \ldots, a_j, \ldots, a_i, \ldots, a_n|$

Důkaz: Podle definice

$$\begin{aligned}|A| &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} a_{2\pi(2)} \ldots a_{n\pi(n)} = \sum_{\rho \in S_n} \operatorname{sgn}(\rho^{-1}) a_{1\rho^{-1}(1)} a_{2\rho^{-1}(2)} \ldots a_{n\rho^{-1}(n)} \\ &= \sum_{\rho \in S_n} \operatorname{sgn}(\rho) a_{\rho(1)1} a_{\rho(2)2} \ldots a_{\rho(n)n} = \sum_{\rho \in S_n} \operatorname{sgn}(\rho) a^T_{1\rho(1)} a^T_{2\rho(2)} \ldots a^T_{n\rho(n)} = |A^T|\end{aligned}$$

Nejprve jsme využili toho, že pokud ρ běží přes celou S_n, pak ρ^{-1} také, pak jsme přeuspořádali činitele v součinu a použili $\operatorname{sgn}(\rho) = \operatorname{sgn}(\rho^{-1})$.

Druhé tvrzení plyne z

$$\sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} \ldots (ra_{i\pi(i)}) \ldots a_{n\pi(n)} = r \sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} \ldots a_{i\pi(i)} \ldots a_{n\pi(n)}$$

a podobně zřejmé je i tvrzení třetí.

Zobrazení, které π přiřazuje $\pi' = \pi \circ [i, j]$, je bijekce S_n na S_n, takže

$$\begin{aligned}|A| &= \sum_{\pi' \in S_n} \operatorname{sgn}(\pi') a_{1\pi'(1)} \ldots a_{i\pi'(i)} \ldots a_{j\pi'(j)} \ldots a_{n\pi'(n)} \\ &= \sum_{\pi \in S_n} \operatorname{sgn}(\pi \circ [i, j]) a_{1\pi(1)} \ldots a_{i\pi(j)} \ldots a_{j\pi(i)} \ldots a_{n\pi(n)} \\ &= -\sum_{\pi \in S_n} \operatorname{sgn}(\pi) a_{1\pi(1)} \ldots a_{j\pi(i)} \ldots a_{i\pi(j)} \ldots a_{n\pi(n)},\end{aligned}$$

čímž je dokázáno čtvrté tvrzení.

□

Tato věta má řadu důsledků. Z prvního tvrzení plyne, že druhé a třetí tvrzení platí i pro sloupce. Z druhého je jasné, že determinant matice, která

obsahuje nulový řádek (nebo sloupec), je nulový. Čtvrté tvrzení vlastně říká, že při transpozici na řádky se determinant vynásobí znaménkem transpozice, a protože libovolnou permutaci lze získat jako součin transpozic, permutace řádků způsobí vynásobení determinantu znaménkem permutace. Ze čtvrtého tvrzení také plyne, že pokud má matice dva stejné řádky, pak je její determinant nulový. Pokud tedy do i-tého řádku matice přičteme r-násobek j-tého řádku pro $i \neq j$, pak je ve druhém tvrzení s $a'_i = ra_j$ poslední člen nulový a tedy se determinant nezmění. Přičítáním násobků ostatních řádků, přehazováním pořadí řádků a násobením řádku číslem je možné matici převést na horní trojúhelníkovou. Determinant horní trojúhelníkové matice je ale roven součinu diagonálních elementů, protože v definici determinantu všechny členy kromě členu příslušejícího $\pi = \mathrm{id}$ obsahují alespoň jeden prvek pod diagonálou, a ten je roven 0. Determinant matice lze tedy počítat Gaussovou eliminací, jen si musíme dát pozor, že změny pořadí řádků a násobení číslem determinant změní. Na druhou stranu ale můžeme využívat i sloupcové úpravy, pokud je to výhodné.

Věta 31 *Matice $A \in M_{nn}(\mathbb{T})$ je regulární, právě když $|A| \neq 0$.*

Důkaz: Matice A je regulární právě když $h(A) = n$. Pokud matici převedeme Gaussovou eliminací na horní troúhelníkovou, pak se hodnost zachová a nulovost či nenulovost determinantu také. Ale determinant horní trojúhelníkové matice je nenulový, právě když jsou nenulové všechny prvky na diagonále a právě tehdy je i hodnost matice rovna n. □

Věta 32

$$\det A \cdot B = \det A . \det B.$$

Důkaz: Označme $C = A \cdot B$. Jsou-li c_i, resp. a_i sloupce matice C, resp. A, pak zřejmě pro každé k platí $c_{ki} = \sum_j a_{kj} b_{ji}$, tedy $c_i = \sum_j a_j b_{ji}$. Víme tedy, že

$$\det C = \det(c_1, \ldots, c_n) = \det(\sum_j a_j b_{j1}, c_2, \ldots, c_n) = \sum_j b_{j1} \det(a_j, c_2, \ldots, c_n).$$

Postupným dosazovaním za $c_2, \ldots, c_n$ a využitím linearity v jednotlivých sloupcích dostaneme

$$\det C = \sum_{j_1} \ldots \sum_{j_n} b_{j_1 1} \ldots b_{j_n n} \det(a_{j_1}, \ldots, a_{j_n}).$$

Ale $\det(a_{j_1}, \ldots, a_{j_n})$ je nula, pokud zobrazení $\pi : i \to j_i$ není prosté (opakují se sloupce matice). Tedy se vlastně sčítá přes všechny permutace $\pi \in P_n$. Navíc

$$\det(a_{\pi(1)}, \ldots, a_{\pi(n)}) = \operatorname{sign}(\pi) \det(a_1, \ldots, a_n).$$

Tedy výsledek má tvar

$$\det C = [\sum_{\pi \in P_n} \operatorname{sign}(\pi) b_{\pi(1)1} \ldots b_{\pi(n)n}] \det(a_1, \ldots, a_n)] = \det B . \det A.$$

□

Poznámka:

Věta o determinantu součinu má jako okamžitý důsledek dvě tvrzení:

(i) $\det A^{-1} \det A = 1$.

(ii) $\det C^{-1} A C = \det A$.

Tedy podobné matice mají stejný determinant a je tedy pravda, že determinant je (po stopě) další invariant pro relaci podobnosti matic.

11.2 Aplikace determinantu.

Definice 12 *Nechť A je $n \times n$ matice. Nechť A_{IJ} je podmatice vzniklá z matice A vynecháním řádku s indexy z množiny $I \subset \{1, \ldots, n\}$ a vynecháním sloupců s indexy z množiny $J \subset \{1, \ldots, n\}$. Pokud mají množiny I a J stejný počet prvků, budeme determinant $|A_{IJ}|$ nazývat IJ-tým* **minorem matice** *A. Pokud $I = J$, nazýváme tento determinant* **hlavním minorem.**

Je-li $I = \{i\}$ a $J = \{j\}$, pak se tento minor nazývá **prvním minorem** *a značí se $|A_{ij}|$. Číslo*

$$\hat{A}_{ij} := (-1)^{i+j} |A_{ij}|$$

se nazývá ij-tým **kofaktorem**, *nebo* **algebraickým doplňkem** *matice A.*

Lemma 7 (Rozvoj determinantu podle sloupce)
Nechť j je pevně vybrané číslo sloupce, pak

$$\det A = \sum_{i=1}^{n} a_{ij} \hat{A}_{ij},$$

kde $\hat{A}_{ij}$ je ij-tý algebraický doplněk matice A.

Totéž tvrzení analogicky platí i pro rozvoj determinantu podle zvoleného řádku.

Důkaz: Předpokládejme nejdříve, že $j = 1$. Vyjádřeme nyní determinant matice A, která má vlastnost, že jediný nenulový prvek v prvním sloupci je prvek a_{1i}, kde i je daný index. Pokud navíc $i = 1$, pak přímo z definice plyne $\det A = a_{11} \det A_{11}$. Pro $i \neq 1$ stačí posunout i-tý řádek na první místo a pořadí ostatních ponechat. Determinant se při takovéto operaci vynásobí znaménkem příslušné permutace, které je (indukcí) rovno $(-1)^{i+1}$. Věta tedy platí pro takovéto matice.

První sloupec si mohu napsat jako lineární kombinace kanonické baze, tj. $s_1 = a_{11}e_1 + \ldots a_{1n}e_n$. Pak už stačí jen použít linearitu determinantu vůči prvnímu sloupci a výše dokázaná tvrzení.

Pokud j je různé od jedné, pak uděláme permutaci slouců pomocí cyklu, který převede j na 1, 1 na 2, atd. až $j - 1$ na j. Pokud tuto permutaci použijeme na sloupce, přehodíme j-tý sloupec na první a ostatní se posunou doprava. Tím dostaneme novou matici $\tilde{A}$. Znaménko této permutace je $(-1)^{j-1}$. Tím dostaneme novou matici $\tilde{A}$, a tedy, $|\tilde{A}| = (-1)^{-1}j|A|$. Pak použijeme tvrzení pro $j = 1$ s tím, že příslušné algebraické doplňky jsou stejné. □

Lemma 8 (Výpočet inverzní matice)
Označme A_{ij} matici, která vznikne z matice A vynecháním i-tého řádku a j-tého sloupce.

Pak inverzní matice $B = A^{-1}$ má tvar

$$b_{ij} = (-1)^{i+j}(\det A)^{-1} \det A_{ji}$$

(všimněte si přehození pořadí indexů!).

Důkaz: Jednotková matice $1_{n\times n}$ má prvky δ_{ik}, kde δ je tzv. Kronekerovo delta. Je definováno tak, že $\delta_{ik} = 1$ pro $i = k$ a $\delta_{ik} = 0$ pro $i \neq k$. Označme symbolem e_j jednotkový vektor (sloupec) s 1 na j-tém místě. Definujme si matici C předpisem

$$c_{ij} = (-1)^{i+j} \det A_{ji} = \det(a_1, \ldots, a_{i-1}, e_j, a_{i+1}, \ldots, a_n).$$

Pak stačí ověřit rovnost $C \cdot A = \det A.1_{n\times n}$.

Ale

$$(C \cdot A)_{ik} = \sum_j c_{ij}a_{jk} = \sum_j \det(a_1, \ldots, a_{i-1}, e_j, a_{i+1}, \ldots, a_n)a_{jk} =$$

$$= \det(a_1, \ldots, a_{i-1}, a_k, a_{i+1}, \ldots, a_n).$$

Nyní stačí si uvědomit, poslední determinant se rovná číslu $\det A$ pro $i = k$ a nule pro $i \neq k$ (v příslušné matici se opakují sloupce). □

Věta 33 (Cramer)
Předpokládejme, že matice A je regulární, označme a_i její sloupce. Pak soustava lineárních rovnic $A \cdot x = f$ s pravou stranou f má právě jedno řešení dané vzorcem

$$x_j = (\det A)^{-1} \det(a_1, \ldots, a_{j-1}, f, a_{j+1}, \ldots, a_n).$$

Důkaz: Víme už, že řešení existuje jediné a je dáno vztahem $x = A^{-1} \cdot f$. Stačí tedy použít předchozí vzorec pro inverzní matici a dostaneme (s použitím označení předchozího lemmatu)

$$x_j = \sum_k b_{jk} f_k = \sum_k (\det A)^{-1} \det(a_1, \ldots, a_{j-1}, e_k, a_{j+1}, \ldots, a_n) f_k =$$

$$= (\det A)^{-1} \det(a_1, \ldots, a_{j-1}, f, a_{j+1}, \ldots, a_n).$$

□